LAMPS Working Group
Internet-Draft
Updates: 8551 (if approved)
Intended status: Standards Track
Expires: 10 July 2025

D. K. Gillmor
American Civil Liberties Union
B. Hoeneisen
pEp Project
A. Melnikov
Isode Ltd

6 January 2025

Header Protection for Cryptographically Protected E-mail
draft-ietf-lamps-header-protection-25

Abstract

S/MIME version 3.1 introduced a mechanism to provide end-to-end cryptographic protection of e-mail message headers. However, few implementations generate messages using this mechanism, and several legacy implementations have revealed rendering or security issues when handling such a message.

This document updates the S/MIME specification (RFC8551) to offer a different mechanism that provides the same cryptographic protections but with fewer downsides when handled by legacy clients. Furthermore, it offers more explicit usability, privacy, and security guidance for clients when generating or handling e-mail messages with cryptographic protection of message headers.

The Header Protection scheme defined here is also applicable to messages with PGP/MIME cryptographic protections.

About This Document

This note is to be removed before publishing as an RFC.

The latest revision of this draft can be found at https://dkg.gitlab.io/lamps-header-protection/. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-lamps-header-protection/.

Discussion of this document takes place on the LAMPS Working Group mailing list (mailto:spasm@ietf.org), which is archived at https://mailarchive.ietf.org/arch/browse/spasm/. Subscribe at https://www.ietf.org/mailman/listinfo/spasm/.

Source for this draft and an issue tracker can be found at https://gitlab.com/dkg/lamps-header-protection.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Privacy and security issues regarding e-mail Header Protection in S/MIME and PGP/MIME have been identified for some time. Most current implementations of cryptographically protected electronic mail protect only the body of the message, which leaves significant room for attacks against otherwise-protected messages. For example, lack of Header Protection allows an attacker to substitute the message subject and/or author.

This document describes how to cryptographically protect message headers, and provides guidance for the implementer of a Mail User Agent (MUA) that generates, interprets, and replies to such a message. It uses the term "Legacy MUA" to refer to an MUA that does not implement this specification. This document takes particular care to ensure that messages interact reasonably well with Legacy MUAs.

1.1. Update to RFC 8551

An older scheme for Header Protection was specified in S/MIME 3.1 ([RFC8551]), which involves wrapping a message/rfc822 MIME object with a Cryptographic Envelope around the message to protect. This document refers to that scheme as RFC 8551 Header Protection, or "RFC8551HP". Substantial testing has shown that RFC8551HP does not interact well with some Legacy MUAs (see Section 1.1.1).

This specification supersedes RFC8551HP, effectively replacing the final two paragraphs of Section 3.1 of [RFC8551].

In this specification, all Header Fields gain end-to-end cryptographic integrity and authenticity by being copied directly into the Cryptographic Payload without using an intervening message/rfc822 MIME object. In an encrypted message, some Header Fields can also be made confidential by removing or obscuring them from the outer Header Section.

This specification also offers substantial security, privacy, and usability guidance for sending and receiving MUAs that was not considered in RFC 8551.

1.1.1. Problems with RFC 8551 Header Protection

Several Legacy MUAs have difficulty rendering a message that uses RFC8551HP. These problems can appear on signed-only messages, as well as signed-and-encrypted messages.

In some cases, some mail user agents cannot render message/rfc822 message subparts at all, in violation of baseline MIME requirements as defined on page 5 of [RFC2049]. A message using RFC8551HP is unreadable by any recipient using such an MUA.

In other cases, the user sees an attachment suggesting a forwarded e-mail message, which -- in fact -- contains the protected e-mail message that should be rendered directly. In most of these cases, the user can click on the attachment to view the protected message.

However, viewing the protected message as an attachment in isolation may strip it of any security indications, leaving the user unable to assess the cryptographic properties of the message. Worse, for encrypted messages, interacting with the protected message in isolation may leak contents of the cleartext, for example, if the reply is not also encrypted.

Furthermore, RFC8551HP lacks any discussion of the following points, all of which are provided in this specification:

* Which Header Fields should be given end-to-end cryptographic integrity and authenticity protections (this specification mandates protection of all Header Fields that the sending MUA knows about).

* How to securely indicate the sender’s intent to offer Header Protection and encryption, which lets a receiving MUA detect messages whose cryptographic properties may have been modified in transit (see Section 2.1.1).

* Which Header Fields should be given end-to-end cryptographic confidentiality protections in an encrypted message, and how (see Section 3).

* How to securely indicate the sender’s choices about which Header Fields were made confidential, which lets a receiving MUA reply or forward an encrypted message safely without accidentally leaking confidential material (see Section 2.2).

These stumbling blocks with Legacy MUAs, missing mechanisms, and missing guidance create a strong disincentive for existing MUAs to generate messages using RFC8551HP. Because few messages have been produced, there has been little incentive for those MUAs capable of upgrading to bother interpreting them better.

In contrast, the mechanisms defined here are safe to adopt and produce messages with very few problems for Legacy MUAs. And, Section 4.10 provides useful guidance for rendering and replying to RFC8551HP messages.

1.2. Risks of Header Protection for Legacy MUA Recipients

Producing a signed-only message using this specification is risk-free. Such a message will render in the same way on any Legacy MUA as a Legacy Signed Message (that is, a signed message without Header Protection). An MUA conformant to this specification that encounters such a message will be able to gain the benefits of end-to-end cryptographic integrity and authenticity for all Header Fields.

An encrypted message produced according to this specification that has some user-facing Header Fields removed or obscured may not render as desired in a Legacy MUA. In particular, those Header Fields that were made confidential will not be visible to the user of a Legacy MUA. For example, if the Subject Header Field outside the Cryptographic Envelope is replaced with [...], a Legacy MUA will render the [...] anywhere the Subject is normally seen. This is the only risk of producing an encrypted message according to this specification.

A workaround "Legacy Display" mechanism is provided in this specification (see Section 2.1.2). Legacy MUAs will render "Legacy Display Elements" to the user, albeit not in the same location that the Header Fields would normally be rendered.

Alternately, if the sender of an encrypted message is particularly concerned about the experience of a recipient using a Legacy MUA, and they are willing to accept leaking the user-facing Header Fields, they can simply adopt the No Header Confidentiality Policy (see

Section 3.2.3). A signed and encrypted message composed using the No Header Confidentiality Policy offers no usability risk for a reader using a Legacy MUA, and retains end-to-end cryptographic integrity and authenticity properties for all Header Fields for any reader using a conformant MUA. Of course, such a message has the same (non-existent) confidentiality properties for all Header Fields as a Legacy Encrypted Message (that is, an encrypted message made without Header Protection).

1.3. Motivation

Users generally do not understand the distinction between message body and message header. When an e-mail message has cryptographic protections that cover the message body, but not the Header Fields, several attacks become possible.

For example, a Legacy Signed Message has a signature that covers the body but not the Header Fields. An attacker can therefore modify the Header Fields (including the Subject header) without invalidating the signature. Since most readers consider a message body in the context of the message’s Subject header, the meaning of the message itself could change drastically (under the attacker’s control) while still retaining the same cryptographic indicators of integrity and authenticity.

In another example, a Legacy Encrypted Message has its body effectively hidden from an adversary that snoops on the message. But if the Header Fields are not also encrypted, significant information about the message (such as the message Subject) will leak to the inspecting adversary.

However, if the sending and receiving MUAs ensure that cryptographic protections cover the message Header Section as well as the message body, these attacks are defeated.

1.3.1. Backward Compatibility

If the sending MUA is unwilling to generate such a fully protected message due to the potential for rendering, usability, deliverability, or security issues, these defenses cannot be realized.

The sender cannot know what MUA (or MUAs) the recipient will use to handle the message. Thus, an outbound message format that is backward compatible with as many legacy implementations as possible is a more effective vehicle for providing the whole-message cryptographic protections described above.

This document aims for backward compatibility with Legacy MUAs to the extent possible. In some cases, like when a user-visible header like the Subject is cryptographically hidden, a Legacy MUA will not be able to render or reply to the message exactly the same way as a conformant MUA would. But accommodations are described here that ensure a rough semantic equivalence for Legacy MUA even in these cases.

1.3.2. Deliverability

A message with perfect cryptographic protections that cannot be delivered is less useful than a message with imperfect cryptographic protections that can be delivered. Senders want their messages to reach the intended recipients.

Given the current state of the Internet mail ecosystem, encrypted messages in particular cannot shield all of their Header Fields from visibility and still be guaranteed delivery to their intended recipient.

This document accounts for this concern by providing a mechanism (Section 3) that prioritizes initial deliverability (at the cost of some header leakage) while facilitating future message variants that shield more header metadata from casual inspection.

1.4. Other Protocols to Protect E-Mail Header Fields

A separate pair of protocols also provides some cryptographic protection for the e-mail message header integrity: DomainKeys Identified Mail (DKIM) [RFC6376], as used in combination with Domain-based Message Authentication, Reporting, and Conformance (DMARC) [RFC7489]. This pair of protocols provides a domain-based reputation mechanism that can be used to mitigate some forms of unsolicited e-mail (spam).

However, the DKIM+DMARC suite provides cryptographic protection at a different scope, as it is usually applied by and evaluated by a mail transport agent (MTA). DKIM+DMARC typically provide MTA-to-MTA protection, whereas this specification provides MUA-to-MUA protection. This is because DKIM+DMARC are typically applied to messages by (and interpreted by) MTAs, whereas the mechanisms in this document are typically applied and interpreted by MUAs.

A receiving MUA that relies on DKIM+DMARC for sender authenticity should note Section 10.1.

Furthermore, the DKIM+DMARC suite only provides cryptographic integrity and authentication, not encryption. So cryptographic confidentiality is not available from that suite.

The DKIM+DMARC suite can be used on any message, including messages formed as defined in this document. There should be no conflict between DKIM+DMARC and the specification here.

Though not strictly e-mail, similar protections have been in use on Usenet for signing and verification of message headers for years. See [PGPCONTROL] and [PGPVERIFY-FORMAT] for more details. Like DKIM, these Usenet control protections offer only integrity and authentication, not confidentiality.

1.5. Applicability to PGP/MIME

This document specifies end-to-end cryptographic protections for e-mail messages in reference to S/MIME ([RFC8551]).

Comparable end-to-end cryptographic protections can also be provided by PGP/MIME ([RFC3156]).

The mechanisms in this document should be applicable in the PGP/MIME protections as well as S/MIME protections, but analysis and implementation in this document focuses on S/MIME.

To the extent that any divergence from the mechanism defined here is necessary for PGP/MIME, that divergence is out of scope for this document.

1.6. Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

The key words "SPECIFICATION REQUIRED" and "IETF REVIEW" that appear in this document when used to describe namespace allocation are to be interpreted as described in [RFC8126].

1.7. Terms

The following terms are defined for the scope of this document:

* S/MIME: Secure/Multipurpose Internet Mail Extensions (see [RFC8551])

* PGP/MIME: MIME Security with OpenPGP (see [RFC3156])

* Message: An E-Mail Message consisting of Header Fields (collectively called "the Header Section of the message") followed, optionally, by a Body; see [RFC5322].

  Note: To avoid ambiguity, this document avoids using the terms "Header" or "Headers" in isolation, but instead always uses "Header Field" to refer to the individual field and "Header Section" to refer to the entire collection.

* Header Field: A Header Field includes a field name, followed by a colon (":"), followed by a field body (value), and terminated by CRLF; see Section 2.2 of [RFC5322] for more details.

* Header Section: The Header Section is a sequence of lines of characters with special syntax as defined in [RFC5322]. The Header Section of a Message contains the Header Fields associated with the Message itself. The Header Section of a MIME part (that is, a subpart of a message) typically contains Header Fields associated with that particular MIME part.

* Body: The Body is the part of a Message that follows the Header Section and is separated from the Header Section by an empty line (that is, a line with nothing preceding the CRLF); see [RFC5322]. It is the (bottom) section of a Message containing the payload of a Message. Typically, the Body consists of a (possibly multipart) MIME [RFC2045] construct.

* Header Protection (HP): cryptographic protection of e-mail Header Sections (or parts of it) by means of signatures and/or encryption.

* Cryptographic Layer, Cryptographic Payload, Cryptographic Envelope, Cryptographic Summary, Structural Header Fields, Main Body Part, User-Facing Header Fields, and MUA are all used as defined in [I-D.ietf-lamps-e2e-mail-guidance]

* Legacy MUA: an MUA that does not understand Header Protection as defined in this document. A Legacy Non-Crypto MUA is incapable of doing any end-to-end cryptographic operations. A Legacy Crypto MUA is capable of doing cryptographic operations, but does not understand or generate messages with Header Protection.

* Legacy Signed Message: an e-mail message that was signed by a Legacy MUA, and therefore has no cryptographic authenticity or integrity protections on its Header Fields.

* Legacy Encrypted Message: an e-mail message that was signed and encrypted by a Legacy MUA, and therefore has no cryptographic authenticity, integrity, or confidentiality protections on any of its Header Fields.

* Header Confidentiality Policy (HCP): a functional specification of which Header Fields should be removed or obscured when composing an encrypted message with Header Protection. An HCP is considered more "conservative" when it removes or obscures fewer Header Fields. When it removes or obscures more Header fields, it is more "ambitious". See Section 3.

* Ordinary User: a user of an MUA who follows a simple and minimal experience, focused on sending and receiving e-mails. A user who opts into advanced configuration, expert mode, or the like is not an "Ordinary User".

1.8. Document Scope

This document describes sensible, simple behavior for a program that generates an e-mail message with standard end-to-end cryptographic protections, following the guidance in [I-D.ietf-lamps-e2e-mail-guidance]. An implementation conformant to this document will produce messages that have cryptographic protection that covers the message’s Header Fields as well as its body.

1.8.1. In Scope

This document also describes sensible, simple behavior for a program that interprets such a message, in a way that can take advantage of these protections covering the Header Fields as well as the body.

The message generation guidance aims to minimize negative interactions with any Legacy receiving MUA while providing actionable cryptographic properties for modern receiving clients.

In particular, this document focuses on two standard types of cryptographic protection that cover the entire message:

* A cleartext message with a single signature, and

* An encrypted message that contains a single cryptographic signature.

1.8.2. Out of Scope

The message composition guidance in this document (in Section 5.2) aims to provide minimal disruption for any Legacy MUA that receives such a message. However, a Legacy MUA by definition does not implement any of the guidance here. Therefore, the document does not attempt to provide guidance for Legacy MUAs directly.

Furthermore, this document does not explicitly contemplate other variants of cryptographic message protections, including any of these:

* Encrypted-only message (Without a cryptographic signature. See Section 5.3 of [I-D.ietf-lamps-e2e-mail-guidance].)

* Triple-wrapped message

* Signed message with multiple signatures

* Encrypted message with a cryptographic signature outside the encryption.

All such messages are out of scope of this document.

1.9. Example

This section gives an overview by providing an example of how MIME messages with Header Protection look like.

Consider the following MIME message:

```
A 笏披棋笊エapplication/pkcs7-mime; smime-type="enveloped-data"
   竊ァ (decrypts to)
B  笏披棋笊エapplication/pkcs7-mime; smime-type="signed-data"
    廾ゥ (unwraps to)
C   笏披溌笊エmultipart/alternative; hp="cipher"
D    笏懌棋笊エtext/plain; hp-legacy-display="1"
E    笏披棋笊エtext/html; hp-legacy-display="1"
```

Observe that:

* Node A and B are collectively called the Cryptographic Envelope. Node C (including its sub-nodes D and E) is called the Cryptographic Payload ([I-D.ietf-lamps-e2e-mail-guidance]).

* Node A contains the traditional unprotected ("outer") Header Fields. Node C contains the protected ("inner") Header Fields.

* The presence of the hp attribute (see Section 2.1.1) on the Content-Type of node C allows the receiver to know that the sender applied Header Protection. Its value allows the receiver to distinguish whether the sender intended for the message to be confidential (hp="cipher") or not (hp="clear"), since encryption may have been added in transit (see Section 10.2).

The "outer" Header Section on node A looks as follows:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: [...]
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: application/pkcs7-mime; smime-type="enveloped-data"
MIME-Version: 1.0
```

The "inner" Header Section on node C looks as follows:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Keywords: Contract, Urgent
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: multipart/alternative; hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:08:43 -0500
HP-Outer: From: Bob <bob@example.net>
HP-Outer: To: Alice <alice@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <20230111T210843Z.1234@lhp.example>
```

Observe that:

* Between node C and node A, some Header Fields are copied as-is (Date, From, To, Message-ID), some are obscured (Subject), and some are removed (Keywords).

* The HP-Outer Header Fields (see Section 2.2) of node C contain a protected copy of the Header Fields in node A. The copy allows the receiver to recompute for which Header Fields the sender provided confidentiality by removing or obscuring them.

* The copying/removing/obscuring and the HP-Outer only apply to Non-Structural Header Fields, not to Structural Header Fields like Content-Type or MIME-Version (see Section 1.1 of [I-D.ietf-lamps-e2e-mail-guidance]).

* If the sender intends no confidentiality and doesn't encrypt the message, it doesn't remove or obscure Header Fields. All Non-Structural Header Fields are copied as-is. No HP-Outer Header Fields are present.

Node D looks as follows:

```
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";

Subject: Handling the Jones contract
Keywords: Contract, Urgent

Please review and approve or decline by Thursday, it's critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

Observe that:

* The sender adds the removed and obscured User-Facing Header Fields (see Section 1.1.2 of [I-D.ietf-lamps-e2e-mail-guidance]) to the main body (note the empty line after the Content-Type). This is called the Legacy Display Element. It allows a user with a Legacy MUA which doesn't implement this document to understand the message, since the Header Fields will be shown as part of the main body.

* The hp-legacy-display="1" attribute (see Section 2.1.2) indicates that the sender added a Legacy Display Element. This allows receivers that implement this document to recognise the Legacy Display Element and distinguish it from user-added content. The receiver then hides the Legacy Display Element and doesn't display it to the user.

* The hp-legacy-display is added to the node to which it applies, not on any outer nodes (e.g., not to node C).

For more examples, see Appendix D and Appendix E.

2. Internet Message Format Extensions

This section describes relevant, backward-compatible extensions to the Internet Message Format ([RFC5322]). Subsequent sections offer concrete guidance for an MUA to make use of these mechanisms, including policy decisions and recommended pseudocode.

2.1. Content-Type parameters

This document introduces two parameters for the Content-Type Header Field, which have distinct semantics and use cases.

2.1.1. Content-Type parameter: hp

This specification defines a parameter for the Content-Type Header Field named hp (for Header Protection). This parameter is only relevant on the Content-Type Header Field at the root of the Cryptographic Payload. The presence of this parameter at the root of the Cryptographic Payload indicates that the sender intends for this message to have end-to-end cryptographic protections for the Header Fields.

The parameter's defined values describe the sender's cryptographic intent when producing the message:

hp Value	Authenticity	Integrity	Confidentiality	Description
"clear"	yes	yes	no	This message has been signed by the sender with Header Protection
"cipher"	yes	yes	yes	This message has been signed by the sender, with Header Protection, and is encrypted to the recipients

Table 1: hp parameter for Content-Type Header Field

A sending implementation MUST NOT produce a Cryptographic Payload with parameter hp="cipher" for a non-encrypted message (that is, where none of the Cryptographic Layers in the Cryptographic Envelope of the message provide encryption). Likewise, if a sending implementation is sending an encrypted message with Header Protection, it MUST emit an hp="cipher" parameter, regardless of which Header Fields were made confidential.

Note that hp="cipher" indicates that the message itself has been encrypted by the sender to the recipients, but makes no assertions about which Header Fields have been removed or obscured. This can be derived from the Cryptographic Payload itself (see Section 4.2).

A receiving implementation MUST NOT mistake the presence of an hp="cipher" parameter in the Cryptographic Payload for the actual presence of a Cryptographic Layer that provides encryption.

2.1.2. Content-Type parameter: hp-legacy-display

This specification also defines an hp-legacy-display parameter for the Content-Type Header Field. The only defined value for this parameter is 1.

This parameter is only relevant on a leaf MIME node of Content-Type text/html or text/plain within a well-formed message with end-to-end cryptographic protections. Its presence indicates that the MIME node it is attached to contains a decorative "Legacy Display Element". The Legacy Display Element itself is used for backward-compatible visibility of any removed or obscured User-Facing Header Field in a Legacy MUA.

Such a Legacy Display Element need not be rendered to the user of an MUA that implements this specification, because the MUA already knows the correct Header Field information, and can render it to the user in the appropriate part of the MUA’s user interface rather than in the body of the message.

See Section 5.2.2 for how to insert a Legacy Display Element into a text/plain Main Body Part. See Section 5.2.3 for how to insert a Legacy Display Element into a text/html Main Body Part. See Section 4.5.3 for how to avoid rendering a Legacy Display Element.

2.2. The HP-Outer Header Field

This document also specifies a new Header Field: HP-Outer.

This Header Field is used only in the Header Section of the Cryptographic Payload of an encrypted message. It is not relevant for signed-only messages. It documents, with the same cryptographic guarantees shared by the rest of the message, the sender's choices about Header Field confidentiality. It does so by embedding a copy within the Cryptographic Envelope of every non-structural Header Field that the sender put outside the Cryptographic Envelope. This Header Field enables the MUA receiving the encrypted message to reliably identify whether the sending MUA intended to make a Header Field confidential (see Section 11.3).

The HP-Outer Header Fields in a message's Cryptographic Payload are useful for ensuring that any confidential Header Field will not be automatically leaked in the clear if the user replies to or forwards the message. They may also be useful for an MUA that indicates the confidentiality status of any given Header Field to the user.

An implementation that composes encrypted e-mail MUST include a copy of all non-structural Header Fields deliberately exposed to the outside of the Cryptographic Envelope using a series of HP-Outer Header Fields within the Cryptographic Payload. These HP-Outer MIME Header Fields should only ever appear directly within the Header Section of the Cryptographic Payload of a Cryptographic Envelope offering confidentiality. They MUST be ignored for the purposes of evaluating the message's Header Protection if they appear in other places.

Each instance of HP-Outer contains a non-structural Header Field name and the value that this Header Field was set in the outer (unprotected) Header Section. The HP-Outer Header Field can appear multiple times in the Header Section of a Cryptographic Payload.

If a non-structural Header Field name Z is present in Header Section of the Cryptographic Payload, but doesn't appear in an HP-Outer Header Field value at all, then the sender is effectively asserting that every instance of Z was made confidential by removal from the Outer Header Section. Specifically, it means that no Header Field Z was included on the outside of the message's Cryptographic Envelope by the sender at the time the message was injected into the mail system.

See Section 5.2 for how to insert HP-Outer Header Fields into an encrypted message. See Section 4.3 for how to determine the end-to-end confidentiality of a given Header Field from an encrypted message with Header Protection using HP-Outer. See Section 6.1 for how an MUA can safely reply to (or forward) an encrypted message without leaking confidential Header Fields by default.

2.2.1. HP-Outer Header Field Definition

The syntax of this Header Field is defined using the following ABNF [RFC5234], where field-name, WSP, VCHAR, and FWS are defined in [RFC5322]:

```
hp-outer     =   "HP-Outer:" [FWS] field-name ": "
                    hp-outer-value CRLF

hp-outer-value  =   (*([FWS] VCHAR) *WSP)
```

Note that hp-outer-value is the same as unstructured from Section 3.2.5 of [RFC5322], but without the obsolete obs-unstruct option.

3. Header Confidentiality Policy

An MUA composing an encrypted message according to this specification may make any given Header Field confidential by removing it from Header Section outside the Cryptographic Envelope, or by obscuring it by rewriting it to a different value in that outer Header Section. The composing MUA faces a choice for any new message: which Header Fields should be made confidential, and how?

This section defines the "Header Confidentiality Policy" (or HCP) as a well-defined abstraction to encourage MUA developers to consider, document, and share reasonable policies across the community. It establishes a registry of known HCPs, defines a small number of simple HCPs in that registry, and makes a recommendation for a reasonable default.

Note that such a policy is only needed when the end-to-end protections include encryption (confidentiality). No comparable policy is needed for other end-to-end cryptographic protections (integrity and authenticity), as they are simply uniformly applied so that all Header Fields known by the sender have these protections.

This asymmetry is a consequence of complexities in existing message delivery systems, some of which may reject, drop, or delay messages where all Header Fields are removed from the top-level MIME object.

Note that no representation of the HCP itself ever appears "on the wire". However, the consumer of the encrypted message can see the decisions that were made by the sender’s HCP via the HP-Outer Header Fields (see Section 2.2).

3.1. HCP Definition

In this document, we represent that Header Confidentiality Policy as a function hcp:

* hcp(name, val_in) 竊val_out: this function takes a non-structural Header Field identified by name with initial value val_in as arguments, and returns a replacement header value val_out. If val_out is the special value null, it means that the Header Field in question should be removed from the set of Header Fields visible outside the Cryptographic Envelope.

In the pseudocode descriptions of various choices of HCP in this document, any comparison with the name input is done case-insensitively. This is appropriate for Header Field names, as described in [RFC5322].

Note that hcp is only applied to non-structural Header Fields. When composing a message, Structural Header Fields are dealt with separately, as described in Section 5.2.

As an example, an MUA that obscures the Subject Header Field by replacing it with the literal string "[...]", hides all Cc'ed recipients, and does not offer confidentiality to any other Header Fields would be represented as (in pseudocode):

```
hcp_example_hide_cc(name, val_in) → val_out:
    if lower(name) is 'subject':
        return '[...]'
    else if lower(name) is 'cc':
        return null
    else:
        return val_in
```

For alignment with common practice as well as the ABNF in Section 2.2.1 for HP-Outer, val_out MUST be one of the following:

* identical to val_in, or

* the special value null (meaning that the Header Field will be removed from the outside of the message), or

* a sequence of printable and whitespace (that is, space or tab) 7-bit clean ASCII characters (of course, non-ASCII text can be encoded as ASCII using the encoded-word construct from [RFC2047])

The HCP can compute val_out using any technique describable in pseudocode, such as copying a fixed string or invocations of other pseudocode functions. If it alters the value, it MUST NOT include control or NUL characters in val_out. val_out SHOULD match the expected ABNF for the Header Field identified by name.

3.1.1. HCP Avoids Changing From addr-spec

The From Header Field should also be treated specially by the HCP, to enable defense against possible e-mail address spoofing (see Section 10.1). In particular, for hcp("From", val_in), the addr-spec of val_in and the addr-spec of val_out SHOULD match according to Section 4.4.5, unless the sending MUA has additional knowledge coordinated with the receiving MUA about more subtle addr-spec equivalence or certificate validity.

3.2. Initial Registered HCPs

This document formally defines three Header Confidentiality Policies with known and reasonably well-understood characteristics as a way to compare and contrast different possible behavioral choices for a composing MUA. These definitions are not meant to preclude the creation of other HCPs.

The purpose of the registry of HCPs is to facilitate HCP evolution and interoperability discussion among MUA developers and MTA operators.

(The example hypothetical HCP described in Section 3.1 above, hcp_example_hide_cc, is deliberately not formally registered, as it has not been evaluated in practice.)

3.2.1. Baseline Header Confidentiality Policy

The most conservative recommended Header Confidentiality Policy only provides confidentiality for Informational Fields, as defined in Section 3.6.5 of [RFC5322]. These fields are "only human-readable content" and thus their content should not be relevant to transport agents. Since most Internet messages today do have a Subject Header Field, and some filtering engines might object to a message without a Subject, this policy is conservative and merely obscures that Header Field by replacing it with a fixed string [...]. By contrast, Comments and Keywords are comparatively rare, so these fields are removed entirely from the Outer Header Section.

```
hcp_baseline(name, val_in) → val_out:
    if lower(name) is 'subject':
        return '[...]'
    else if lower(name) is in ['comments', 'keywords']:
        return null
    else:
        return val_in
```

hcp_baseline is the recommended default HCP for a new implementation, as it provides meaningful confidentiality protections and is unlikely to cause deliverability or usability problems.

3.2.2. Shy Header Confidentiality Policy

Alternately, a slightly more ambitious (and therefore more privacy-preserving) Header Confidentiality Policy might avoid leaking human-interpretable data that MTAs generally don't care about. The additional protected data isn't related to message routing or transport, but but might reveal sensitive information about the sender or their relationship to the recipients. This "shy" HCP builds on hcp_baseline, but also:

* avoids revealing the display-name of each identified e-mail address, and

* avoids leaking the sender's locally-configured time zone in the Date Header Field.

```
hcp_shy(name, val_in) → val_out:
   if lower(name) is 'from':
      if val_in is an RFC 5322 mailbox:
         return the RFC 5322 addr-spec part of val_in
   if lower(name) in ['to', 'cc']:
      if val_in is an RFC 5322 mailbox-list:
         let val_out be an empty mailbox-list
         for each mailbox in val_in:
            append the RFC 5322 addr-spec part of mailbox to val_out
         return val_out
   if lower(name) is 'date':
      if val_in is an RFC 5322 date-time:
          return the UTC form of val_in
   else if lower(name) is 'subject':
      return '[...]'
   else if lower(name) is in ['comments', 'keywords']:
      return null
   return val_in
```

hcp_shy requires more sophisticated parsing and Header Field manipulation, and is not recommended as a default HCP for new implementations.

3.2.3. No Header Confidentiality Policy

Legacy MUAs can be conceptualized as offering a "No Header Confidentiality" Policy, which offers no confidentiality protection to any Header Field:

```
hcp_no_confidentiality(name, val_in) → val_out:
    return val_in
```

A conformant MUA that is not modified by local policy or configuration MUST NOT use hcp_no_confidentiality by default.

3.3. Default Header Confidentiality Policy

An MUA MUST have a default Header Confidentiality Policy that offers confidentiality for the Subject Header Field at least. Local policy and configuration may alter this default, but the MUA SHOULD NOT require the user to select an HCP.

hcp_baseline provides confidentiality for the Subject Header Field by replacing it with the literal string "[...]". It also provides confidentiality for the other less common Informational Header Fields (Comments and Keywords) by removing them entirely from the outer Header Section. This is a sensible default because most users treat the Informational Fields of a message (particularly the Subject) the same way that they treat the body, and they are surprised to find that the Subject of an encrypted message is visible.

3.4. HCP Evolution

This document does not mandate any particular Header Confidentiality Policy, though it offers guidance for MUA implementers in selecting one in Section 3.3. Future documents may recommend or mandate such a policy for an MUA with specific needs. Such a recommendation might be motivated by descriptions of metadata-derived attacks, or stem from research about message deliverability, or describe new signalling mechanisms, but these topics are out of scope for this document.

3.4.1. Offering More Ambitious Header Confidentiality

An MUA MAY offer even more ambitious confidentiality for Header Fields of an encrypted message than defined in Section 3.2.2. For example, it might implement an HCP that removes the To and Cc Header Fields entirely, relying on the SMTP envelope to ensure proper routing. Or it might remove References and In-Reply-To so that message threading is not visible to any MTA. Any more ambitious choice might result in deliverability, rendering, or usability issues for the relevant messages, so testing and documentation will be valuable to get this right.

The authors of this document hope that implementers with deployment experience will document their chosen Header Confidentiality Policy and the rationale behind their choice.

3.4.2. Expert Guidance for Registering Header Confidentiality Policies

There is no formal syntax specified for the Header Confidentiality Policy, but any attempt to specify an HCP for inclusion in the registry needs to provide:

* a stable reference document clearly indicating the distinct name for the proposed HCP

* pseudocode that other implementers can clearly and unambiguously interpret

* a clear explanation of why this HCP is different from all other registered HCPs

* any relevant considerations related to deployment of the HCP (for example, known or expected deliverability, rendering, or privacy challenges and possible mitigations)

When the proposed HCP produces any non-null output for a given Header Field name, val_out SHOULD match the expected ABNF for that Header Field. If the proposed HCP does not match the expected ABNF for that Header Field, the documentation should explicitly identify the relevant circumstances and provide a justification for the deviation.

An entry should not be marked as "Recommended" unless it has been shown to offer confidentiality or privacy improvements over the status quo and have minimal or mitigatable negative impact on messages to which it is applied, considering factors such as message deliverability and security. Only one entry in the table (hcp_baseline) is initially marked as "Recommended". In the future, more than one entry may be marked as "Recommended".

4. Receiving Guidance

An MUA that receives a cryptographically protected e-mail will render it for the user.

The receiving MUA will render the message body, a selected subset of Header Fields, and (as described in Section 3 of [I-D.ietf-lamps-e2e-mail-guidance]) provide a summary of the cryptographic properties of the message.

Most MUAs only render a subset of Header Fields by default. For example, most MUAs render From, To, Cc, Date, and Subject Header Fields to the user, but few render Message-Id or Received.

An MUA that knows how to handle a message with Header Protection makes the following four changes to its behavior when rendering a message:

* If the MUA detects that an incoming message has protected Header Fields:

  - For a Header Field that is present in the protected Header Section, the MUA SHOULD render the protected value, and ignore any unprotected counterparts that may be present (with a special exception for the From Header Field (see Section 4.4).

  - For a Header Field that is present only in the unprotected Header Section, the MUA SHOULD NOT render that value. If it does render the value, the MUA SHOULD indicate that the rendered value is unprotected. For an exception to this, see Section 7 for a discussion of some specific Header Fields that are known to be added in transit, and therefore are not expected to have end-to-end cryptographic protections.

* The MUA SHOULD include information in the message's Cryptographic Summary to indicate the types of protection that applied to each rendered Header Field (if any).

* If any Legacy Display Elements are present in the body of the message, it does not render them.

* When replying to a message with confidential Header Fields, the replying MUA avoids leaking into the cleartext of the reply any Header Fields which were confidential in the original. It does this even if its own Header Confidentiality Policy would not have treated those Header Fields as confidential. See Section 6 for more details.

Note that an MUA that handles a message with Header Protection does _not_ need to render any new Header Fields that it did not render before.

4.1. Identifying that a Message has Header Protection

An incoming message can be identified as having Header Protection using the following test:

* The Cryptographic Payload has parameter hp set to "clear" or "cipher". See Section 4.5 for rendering guidance.

When consuming a message, an MUA MUST ignore the hp parameter to Content-Type when it encounters it anywhere other than the root of the message's Cryptographic Payload.

4.2. Extracting Protected and Unprotected ("Outer") Header Fields

When a message is encrypted and it uses Header Protection, an MUA extracts a list of protected Header Fields (names and values), as well as a list of Header Fields that were added by the original message sender in unprotected form to the outside of the message's Cryptographic Envelope.

The following algorithm takes a reference message refmsg as input, which is encrypted with Header Protection as described in this document (that is, the Cryptographic Envelope includes a Cryptographic Layer that provides encryption, and the hp parameter for the Content-Type Header Field of the Cryptographic Payload is cipher). It produces as output a pair of lists of (h,v) Header Fields.

4.2.1. HeaderSetsFromMessage

Method Signature:

HeaderSetsFromMessage(refmsg) → (refouter, refprotected)

Procedure:

1. Let refheaders be the list of (h,v) protected Header Fields found in the root of the Cryptographic Payload

2. Let refouter be an empty list of Header Field names and values

3. Let refprotected be an empty list of Header Field names and values

4. For each (h,v) in refheaders:

    i. If h is HP-Outer:

        a. Split v into (h1,v1) on the first colon (:) followed by any amount of whitespace.

        b. Append (h1,v1) to refouter

    ii. Else:

        a. Append (h,v) to refprotected

5. Return refouter, refprotected

Note that this algorithm is independent of the unprotected Header Fields. It derives its output only from the normal Header Fields and the HP-Outer Header Fields, both contained inside the Cryptographic Payload.

4.3. Updating the Cryptographic Summary

Regardless of whether a cryptographically protected message has protected Header Fields, the Cryptographic Summary of the message should be modified to indicate what protections the Header Fields have. This field-by-field status is complex and isn't necessarily intended to be presented in full to the user. Rather, it represents the state of the message internally within the MUA, and may be used to influence behavior like replying to the message (see Section 6.1).

Each Header Field individually has exactly one of the following protection states:

* unprotected (has no Header Protection)

* signed-only (bound into the same validated signature as the enclosing message, but also visible in transit)

* encrypted-only (only appears within the Cryptographic Payload; the corresponding external Header Field was either removed or obscured)

* signed-and-encrypted (same as encrypted-only, but additionally is under a validated signature)

If the message does not have Header Protection (as determined by Section 4.1), then all of the Header Fields are by definition unprotected.

If the message has Header Protection, an MUA SHOULD use the following algorithm to compute the protection state of a protected Header Field (h,v) (that is, an element of refprotected from Section 4.2):

4.3.1. HeaderFieldProtection

Method signature:

HeaderFieldProtection(msg, h, v) → protection_state

Procedure:

1. Let ct be the Content-Type of the root of the Cryptographic Payload of msg.

2. Compute (refouter, refprotected) from HeaderSetsFromMessage(msg).

3. If (h, v) is not in refprotected):

    i. Abort, v is not a valid value for header h

4. Let is_sig_valid be false

5. If the message is signed:

    i. Let is_sig_valid be the result of validating the signature

6. If the message is encrypted, and if ct has a parameter hp="cipher", and if (h,v) is not in refouter:

    i. Return signed-and-encrypted if is_sig_valid otherwise encrypted-only

7. Return signed-only if is_sig_valid otherwise unprotected

Note that:

* This algorithm is independent of the unprotected Header Fields. It derives the protection state only from (h,v) and the set of HP-Outer Header Fields, both of which are inside the Cryptographic Envelope.

* If the signature fails validation, the MUA lowers the affected state to unprotected or encrypted-only without any additional warning to the user, as specified by Section 3.1 of [I-D.ietf-lamps-e2e-mail-guidance].

* Data from signed-and-encrypted and encrypted-only Header Fields may still not be fully private (see Section 11.2).

* Encryption may have been added in transit to an originally signed-only message. Thus only consider Header Fields to be confidential if the sender indicates it with the hp="cipher" parameter.

* The protection state of a Header Field may be weaker than that of the message body. For example, a message body can be signed-and-encrypted, but a Header Field that is copied unmodified to the unprotected Header Section is signed-only.

If the message has Header Protection, Header Fields that are not in refprotected (e.g., because they were added in transit), are unprotected.

Rendering the cryptographic status of each Header Field is likely to be complex and messy --- users may not understand it. It is beyond the scope of this document to suggest any specific graphical affordances or user experience. Future work should include examples of successful rendering of this information.

4.4. Handling Mismatch of From Header Fields

End-to-end (MUA-to-MUA) Header Protection is good for authenticity, integrity, and confidentiality, but it potentially introduces new issues when an MUA depends on its MTA to authenticate parts of the Header Section. The latter is typically the case in modern e-mail systems.

In particular, when an MUA depends on its MTA to ensure that the e-mail address in the (unprotected) From Header Field is authentic, but the MUA renders the e-mail address of the protected From Header Field that differs from the address visible to the MTA, this could create a risk of sender address spoofing (see Section 10.1). This potential risk applies to signed-only messages as well as signed-and-encrypted messages.

4.4.1. Definitions

4.4.1.1. From Header Field Mismatch

"From Header Field Mismatch" is defined as follows:

The addr-spec of the inner From Header Field doesn’t match the addr-spec of the outer From Header Field (see Section 4.4.5).

Note: The unprotected From Header Field used in this comparison is the actual outer Header Field (as seen by the MTA), not the value indicated by any potential inner HP-Outer.

4.4.1.2. No Valid and Correctly Bound Signature

"No Valid and Correctly Bound Signature" is defined as follows:

There is no valid signature made by a certificate for which the MUA has a valid binding to the protected From address. This includes:

* the message has no signature, or

* the message has a broken signature, or

* the message has a valid signature, but the receiving MUA does not see any valid binding between the signing certificate and the addr-spec of the inner From Header Field.

Note: There are many possible ways that an MUA could choose to validate a certificate-to-address binding. For example, the MUA could ensure the certificate is issued by one of a set of trusted certification authorities, it could rely on the user to do a manual out-of-band comparison, it could rely on a DNSSEC signal ([RFC7929] or [RFC8162]), and so on. It is beyond the scope of this document to describe all possible ways an MUA might validate the certificate-to-address binding, or to choose among them.

4.4.2. Warning for From Header Field Mismatch

To mitigate the above described risk of sender address spoofing, an MUA SHOULD warn the user whenever both of the following conditions are met:

* From Header Field Mismatch (as defined in Section 4.4.1.1), and

* No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

This warning should be comparable to the MUA’s warning about messages that are likely spam or phishing, and it SHOULD show both of the non-matching From Header Fields.

4.4.3. From Header Field Rendering

Furthermore, a receiving MUA that depends on its MTA to authenticate the unprotected (outer) From Header Field SHOULD render the outer From Header Field (as an exception to the guidance in the beginning of Section 4), if both of the following conditions are met:

* From Header Field Mismatch (as defined in Section 4.4.1.1), and

* No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

An MUA MAY apply a local preference to render a different display name (e.g., from an address book).

See Section 10.1.1 for an detailed explanation of this rendering guidance.

4.4.4. Handling Protected From Header Field when Responding

When responding to a message, an MUA has different ways to populate the recipients of the new message. Depending on whether it is a Reply, a Reply-All, or a Forward, an MUA may populate the composer view using a combination of the referenced message’s From, To, Cc, Reply-To, Mail-Followup-To Header Fields, or any other signals.

When responding to a message with Header Protection, an MUA MUST only use the protected Header Fields when populating the recipients of the new message.

This avoids compromise of message confidentiality when a MITM attacker modifies the unprotected From address of an encrypted message, attempting to learn the contents through a misdirected reply. Note that with the rendering guidance above, a MITM attacker can cause the unprotected From Header Field to be displayed. Thus when responding, the populated To address may differ from the rendered From address. However, this change in addresses should not cause more user confusion than the address change caused by a Reply-To in a Legacy Message does.

4.4.5. Matching addr-specs

When generating (Section 3.1.1) or consuming (Section 4.4) a protected From Header Field, the MUA considers the equivalence of two different addr-spec values.

First, the MUA MUST check whether the domain part of an addr-spec being compared contains any U-label [RFC5890]. If it does, it MUST be converted to the A-label form is described in [RFC5891]. We call a domain converted in this way (or the original domain, if it didn't contain any U-label) "the ASCII version of the domain part". Second, the MUA MUST compare the ASCII version of the domain part of the two addr-specs by standard DNS comparison: assume ASCII text, and compare alphabetic characters case-insensitively, as described in Section 3.1 of [RFC1035]. If the domain parts match, then the two local-parts are matched against each other. The simplest and most common comparison for the local-part is also an ASCII-based, case-insensitive match. If the MUA has special knowledge about the domain and, when composing, it can reasonably expect the receiving MUAs to have the same information, it MAY match the local-part using a more sophisticated and inclusive matching algorithm.

It is beyond the scope of this document to recommend a more sophisticated and inclusive matching algorithm.

4.5. Rendering a Message with Header Protection

When the Cryptographic Payload's Content-Type has the parameter hp set to "clear" or "cipher", the values of the protected Header Fields are drawn from the Header Fields of the Cryptographic Payload, and the body that is rendered is the Cryptographic Payload itself.

4.5.1. Example Signed-only Message

Consider a message with this structure, where the MUA is able to validate the cryptographic signature:

```
A └─application/pkcs7-mime; smime-type="signed-data"
    (unwraps to)
B  └┬multipart/alternative [Cryptographic Payload + Rendered Body]
C   ├─text/plain
D   └─text/html
```

The message body should be rendered the same way as this message:

```
B └┬multipart/alternative
C  ├─text/plain
D  └─text/html
```

The MUA should render Header Fields taken from part B.

Its Cryptographic Summary should indicate that the message was signed and all rendered Header Fields were included in the signature.

Because this message is signed-only, none of its parts will have a Legacy Display Element.

The MUA should ignore Header Fields from part A for the purposes of rendering.

4.5.2. Example Signed-and-Encrypted Message

Consider a message with this structure, where the MUA is able to validate the cryptographic signature:

```
E └─ application/pkcs7-mime; smime-type="enveloped-data"
    (decrypts to)
F  └─ application/pkcs7-mime; smime-type="signed-data"
     (unwraps to)
G   └┬ multipart/alternative [Cryptographic Payload + Rendered Body]
H    ├─ text/plain
I    └─ text/html
```

The message body should be rendered the same way as this message:

```
G └┬ multipart/alternative
H  ├─ text/plain
I  └─ text/html
```

It should render Header Fields taken from part G.

Its Cryptographic Summary should indicate that the message is signed-and-encrypted.

When rendering the Cryptographic Status of a Header Field and when composing a reply, each Header Field found in G should be considered against all HP-Outer Header Fields found in G. If an HP-Outer Header Field is found that matches both the name and value, the Header Field's Cryptographic Status is just signed-only, even though the message itself is signed-and-encrypted. If no matching HP-Outer Header Field is found, the Header Field's Cryptographic Status is signed-and-encrypted, like the rest of the message.

If any of the User-Facing Header Fields are removed or obscured, the composer of this message may have placed Legacy Display Elements in parts H and I.

The MUA should ignore Header Fields from part E for the purposes of rendering.

4.5.3. Do Not Render Legacy Display Elements

As described in Section 2.1.2, a message with cryptographic confidentiality protection MAY include Legacy Display Elements for backward-compatibility with Legacy MUAs. These Legacy Display Elements are strictly decorative, unambiguously identifiable, and will be discarded by compliant implementations.

The receiving MUA MUST avoid rendering the identified Legacy Display Elements to the user at all, since it is aware of Header Protection and can render the actual protected Header Fields.

If a text/html or text/plain part within the Cryptographic Envelope is identified as containing Legacy Display Elements, those elements MUST be hidden when rendering and MUST be dropped when generating a draft reply or inline forwarded message. Whenever a Message or MIME subtree is exported, downloaded, or otherwise further processed, if there is no need to retain a valid cryptographic signature, the implementer MAY drop the Legacy Display Elements.

4.5.3.1. Identifying a Part with Legacy Display Elements

A receiving MUA acting on a message that contains an encrypting Cryptographic Layer identifies a MIME subpart within the Cryptographic Payload as containing Legacy Display Elements based on the Content-Type of the subpart. The subpart’s Content-Type:

* contains a parameter hp-legacy-display with value set to 1, and

* is either text/html (see Section 4.5.3.3) or text/plain (see Section 4.5.3.2).

Note that the term "subpart" above is used in the general sense: if the Cryptographic Payload is a single part, that part itself may contain a Legacy Display Element if it is marked with the hp-legacy-display=1 parameter.

4.5.3.2. Omitting Legacy Display Elements from text/plain

If a text/plain part within the Cryptographic Payload has the Content-Type parameter hp-legacy-display="1", it should be processed before rendering in the following fashion:

* Discard the leading lines of the body of the part up to and including the first entirely blank line.

Note that implementing this strategy is dependent on the charset used by the MIME part.

See Appendix E.1 for an example.

4.5.3.3. Omitting Legacy Display Elements from text/html

If a text/html part within the Cryptographic Payload has the Content-Type parameter hp-legacy-display="1", it should be processed before rendering in the following fashion:

* If any element of the HTML <body> is a with class attribute header-protection-legacy-display, that entire element should be omitted.

This cleanup could be done, for example, as a custom rule in the MUA's HTML sanitizer, if one exists. Another implementation strategy for an HTML-capable MUA would be to add an entry to the [CSS] stylesheet for such a part:

```
body div.header-protection-legacy-display { display: none; }
```

4.6. Implicitly rendered Header Fields

While From, To, Cc, Subject, and Date Header Fields are often explicitly rendered to the user, some Header Fields do affect message display, without being explicitly rendered.

For example, Message-Id, References, and In-Reply-To Header Fields may collectively be used to place a message in a "thread" or series of messages.

In another example, Section 6.2 observes that the value of the Reply-To field can influence the draft reply message. So while the user may never see the Reply-To Header Field directly, it is implicitly "rendered" when the user interacts with the message by replying to it.

An MUA that depends on any implicitly rendered Header Field in a message with Header Protection MUST use the value from the protected Header Field, and SHOULD NOT use any value found outside the cryptographic protection unless it is known to be a Header Field added in transit, as specified in Section 7.

4.7. Handling Undecryptable Messages

An MUA might receive an apparently encrypted message that it cannot currently decrypt. For example, when an MUA does not have regular access to the secret key material needed for decryption, it cannot know the cryptographically protected Header Fields or even whether the message has any cryptographically protected Header Fields.

Such an undecrypted message will be rendered by the MUA as a message without any Header Protection. This means that the message summary may well change how it is rendered when the user is finally able to supply the secret key.

For example, the rendering of the Subject Header Field in a mailbox summary might change from [...] to the real message subject when the message is decrypted. Or the message's placement in a message thread might change if, say, References or In-Reply-To have been removed or obscured (see Section 4.6).

Additionally, if the MUA does not retain access to the decrypting secret key, and it drops the decrypted form of a message, the message's rendering may revert to the encrypted form. For example, if an MUA follows this behavior, the Subject Header Field in a mailbox summary might change from the real message subject back to [...]. Or the message might be displayed outside of its current thread if the MUA loses access to a removed References or In-Reply-To header.

These behaviors are likely to surprise the user. However, an MUA has several possible ways of reducing or avoiding all of these surprises, including:

* Ensuring that the MUA always has access to decryption-capable secret key material.

* Rendering undecrypted messages in a special quarantine view until the decryption-capable secret key material is available.

To reduce or avoid the surprises associated with a decrypted message with removed or obscured Header Fields becoming undecryptable, the MUA could also:

* Securely cache metadata from a decrypted message's protected Header Fields so that its rendering doesn't change after the first decryption.

* Securely store the session key associated with a decrypted message, so that attempts to read the message when the long-term secret key are unavailable can proceed using only the session key itself. See, for example, the discussion about stashing session keys in Section 9.1 of [I-D.ietf-lamps-e2e-mail-guidance].

4.8. Guidance for Automated Message Handling

Some automated systems have a control channel that is operated by e-mail. For example, an incoming e-mail message could subscribe someone to a mailing list, initiate the purchase of a specific product, approve another message for redistribution, or adjust the state of some shared object.

To the extent that such a system depends on end-to-end cryptographic guarantees about the e-mail control message, Header Protection as defined in this document should improve the system's security. This section provides some specific guidance for systems that use e-mail messages as a control channel that want to benefit from these security improvements.

4.8.1. Interpret Only Protected Header Fields

Consider the situation where an e-mail-based control channel depends on the message's cryptographic signature and the action taken depends on some Header Field of the message.

In this case, the automated system MUST rely on information from the Header Field that is protected by the mechanism defined in this document. It MUST NOT rely on any Header Field found outside the Cryptographic Payload.

For example, consider an administrative interface for a mailing list manager that only accepts control messages that are signed by one of its administrators. When an inbound message for the list arrives, it is queued (waiting for administrative approval) and the system generates and listens for two distinct e-mail addresses related to the queued message -- one that approves the message, and one that rejects it. If an administrator sends a signed control message to the approval address, the mailing list verifies that the protected To Header Field of the signed control message contains the approval address before approving the queued message for redistribution. If the protected To Header Field does not contain that address, or there is no protected To Header Field, then the mailing list logs or reports the error and does not act on that control message.

4.8.2. Ignore Legacy Display Elements

Consider the situation where an e-mail-based control channel expects to receive an end-to-end encrypted message -- for example, where the control messages need confidentiality guarantees -- and where the action taken depends on the contents of some MIME part within the message body.

In this case, the automated system that decrypts the incoming messages and scans the relevant MIME part MUST identify when the MIME part contains a Legacy Display Element (see Section 4.5.3.1), and it MUST parse the relevant MIME part with the Legacy Display Element removed.

For example, consider an administrative interface of a confidential issue tracking software. An authorized user can confidentially adjust the status of a tracked issue by a specially formatted first line of the message body (for example, severity #183 serious). When the user's MUA encrypts a plain text control message to this issue tracker, depending on the MUA's HCP and its choice of legacy value, it may add a Legacy Display Element. If it does so, then the first line of the message body will contain a decorative copy of the confidential Subject Header Field. The issue tracking software decrypts the incoming control message, identifies that there is a Legacy Display Element in the part (see Section 4.5.3.1), strips the lines comprising the Legacy Display Element (including the first blank line), and only then parses the remaining top line to look for the expected special formatting.

4.9. Affordances for Debugging and Troubleshooting

Note that advanced users of an MUA may need access to the original message, for example to troubleshoot problems with the rendering MUA itself, or problems with the SMTP transport path taken by the message.

An MUA that applies these rendering guidelines SHOULD ensure that the full original source of the message as it was received remains available to such a user for debugging and troubleshooting.

If a troubleshooting scenario demands information about the cryptographically protected values of Header Fields, and the message is encrypted, the debugging interface SHOULD also provide a "source" view of the Cryptographic Payload itself, alongside the full original source of the message as received.

4.10. Handling RFC8551HP Messages (Backward Compatibility)

Section 1.1.1 describes some drawbacks to the Header Protection scheme defined in [RFC8551], referred to here as RFC8551HP. An MUA MUST NOT generate an RFC8551HP message. However, for backward compatibility an MUA MAY try to render or respond to such a message as though the message has standard Header Protection.

The following two sections contain guidance for identifying, rendering and replying to RFC8551HP messages. Corresponding test vectors are provided in Appendix C.2.5, Appendix C.2.6, and Appendix C.3.17.

4.10.1. Identifying an RFC8551HP Message

An RFC8551HP Message can be identified by its MIME structure, given that all of the following conditions are met:

* It has a well-formed Cryptographic Envelope consisting of at least one Cryptographic Layer as the outermost MIME object.

* The Cryptographic Payload is a single message/rfc822 object

* The message that constitutes the Cryptographic Payload does not itself have a well-formed Cryptographic Envelope; that is, its outermost MIME object is not a Cryptographic Layer.

* No Content-Type parameter of hp= is set on either the Cryptographic Payload, or its immediate MIME child.

Here is the MIME structure of an example signed-and-encrypted RFC8551HP message:

```
A └─ application/pkcs7-mime; smime-type="enveloped-data"
    (decrypts to)
B   └─ application/pkcs7-mime; smime-type="signed-data"
     (unwraps to)
C    └─┬ message/rfc822 [Cryptographic Payload]
D      └─┬ multipart/alternative [Rendered Body]
E        ├─ text/plain
F        └─ text/html
```

This meets the definition of an RFC8551HP message because:

* Cryptographic Layers A and B form the Cryptographic Envelope.

* The Cryptographic Payload, rooted in part C has Content-Type: message/rfc822.

* Part D (the MIME root of the message at C) is itself not a Cryptographic Layer.

* Neither part C nor part D have any hp parameter set on their Content-Type.

4.10.2. Rendering or Responding to an RFC8551HP message

When it has precisely identified a message as an RFC8551HP message, an MUA MAY render or respond to that message as though it were a message with Header Protection as defined in this document by making the following adjustments:

* Rather than rendering the message body as the Cryptographic Payload itself (part C in the example above), render the RFC8551HP message's body as the MIME subtree that is the Cryptographic Payload's immediate child (part D).

* Make a comparable modification to HeaderSetsFromMessage (Section 4.2.1) and HeaderFieldProtection (Section 4.3.1): both algorithms currently look for the protected Header Fields on the Cryptographic Payload (part C), but they should instead look at the Cryptographic Payload's immediate child (part D).

* If the Cryptographic Envelope is signed-only, behave as though there is an hp="clear" parameter for the Cryptographic Payload; if the Envelope contains encryption, behave as though there is an hp="cipher" parameter. That is, infer the sender's cryptographic intent from the structure of the message.

* If the Cryptographic Envelope contains encryption, further modify HeaderSetsFromMessage to derive refouter from the actual outer message Header Fields (those found in part A in the example above), rather than looking for HP-Outer Header Fields with the other protected Header Fields. That is, infer Header Field confidentiality based on the unprotected headers.

The inferences in the above modifications are not based on any strong end-to-end guarantees. An intervening MTA may tamper with the message's outer Header Section or wrap the message in an encryption layer to undetectably change the recipient's understanding of the confidentiality of the message's Header Fields or the message body itself.

4.11. Rendering Other Schemes

Other MUAs may have generated different structures of messages that aim to offer end-to-end cryptographic protections that include Header Protection. This document is not normative for those schemes, and it is NOT RECOMMENDED to generate these other schemes, as they can either have structural flaws or simply render poorly on Legacy MUAs. A conformant MUA MAY attempt to infer Header Protection when rendering an existing message that appears to use some other scheme not documented here. Pointers to some known other schemes can be

found in Appendix F.

5. Sending Guidance

This section describes the process an MUA should use to apply cryptographic protection to an e-mail message with Header Protection.

When composing a message with end-to-end cryptographic protections, an MUA SHOULD apply Header Protection.

When generating such a message, an MUA MUST add the hp parameter (see Section 2.1.1) only to the Content-Type Header Field at the root of the message's Cryptographic Payload. The value of the parameter MUST indicate whether the Cryptographic Envelope contains a layer that provides encryption.

5.1. Composing a Cryptographically Protected Message Without Header Protection

For contrast, we first consider the typical message composition process of a Legacy Crypto MUA which does not provide any Header Protection.

This process is described in Section 5.1 of [I-D.ietf-lamps-e2e-mail-guidance]. We replicate it here for reference. The inputs to the algorithm are:

* origbody: the traditional unprotected message body as a well-formed MIME tree (possibly just a single MIME leaf part). As a well-formed MIME tree, origbody already has structural Header Fields (Content-*) present.

* origheaders: the intended non-structural Header Fields for the message, represented here as a list of (h,v) pairs, where h is a Header Field name and v is the associated value. Note that these are Header Fields that the MUA intends to be visible to the recipient of the message. In particular, if the MUA uses the Bcc Header Field during composition, but plans to omit it from the message (see Section 3.6.3 of [RFC5322]), it will not be in origheaders.

* crypto: The series of cryptographic protections to apply (for example, "sign with the secret key corresponding to X.509 certificate X, then encrypt to X.509 certificates X and Y"). This is a routine that accepts a MIME tree as input (the Cryptographic Payload), wraps the input in the appropriate Cryptographic Envelope, and returns the resultant MIME tree as output.

The algorithm returns a MIME object that is ready to be injected into the mail system.

5.1.1. ComposeNoHeaderProtection

Method Signature:

ComposeNoHeaderProtection(origbody, origheaders, crypto) → mime_message

Procedure:

1. Apply crypto to MIME part origbody, producing MIME tree output
2. For each Header Field name and value (h,v) in origheaders:
    i. Add Header Field h to output with value v
3. Return output

5.2. Composing a Message with Header Protection

To compose a message using Header Protection, the composing MUA uses the following inputs:

* All the inputs described in Section 5.1
* hcp: a Header Confidentiality Policy, as defined in Section 3
* respond: if the new message is a response to another message (e.g., "Reply", "Reply All", "Forward", etc), the MUA function corresponding to the user's action (see Section 6.1), otherwise null
* refmsg: if the new message is a response to another message, the message being responded to, otherwise null
* legacy: a boolean value, indicating whether any recipient of the message is believed to have a Legacy MUA. If all recipients are known to implement this document, legacy should be set to false. (How an MUA determines the value of legacy is out of scope for this document; an initial implementation can simply set it to true)

To enable visibility of User-Facing but now removed/obscured Header Fields for decryption-capable Legacy MUAs, the Header Fields are included as a decorative Legacy Display Element in specially marked parts of the message (see Section 2.1.2). This document recommends

two mechanisms for such a decorative adjustment: one for a text/html Main Body Part of the e-mail message, and one for a text/plain Main Body Part. This document does not recommend adding a Legacy Display Element to any other part.

Please see Section 7.1 of [I-D.ietf-lamps-e2e-mail-guidance] for guidance on identifying the parts of a message that are a Main Body Part.

5.2.1. Compose

Method Signature:

Compose(origbody, origheaders, crypto, hcp, respond, refmsg, legacy) → mime_message

Procedure:

1. Let newbody be a copy of origbody

2. If crypto contains encryption, and legacy is true:

    i. Create ldlist, an empty list of (header, value) pairs

    ii. For each Header Field name and value (h,v) in origheaders:

        a. If h is User-Facing (see Section 1.1.2 of [I-D.ietf-lamps-e2e-mail-guidance]):

            I. If hcp(h,v) is not v:

                A. Add (h,v) to ldlist

    iii. If ldlist is not empty:

        a. Identify each leaf MIME part of newbody that represents the "main body" of the message.

        b. For each "Main Body Part" bodypart of type text/plain or text/html:

            I. Adjust bodypart by inserting a Legacy Display Element header list ldlist into its content, and adding a Content-Type parameter hp-legacy-display with value 1 (see Section 5.2.2 for text/plain and Section 5.2.3 for text/html)

3. For each Header Field name and value (h,v) in origheaders:

i. Add Header Field h to MIME part newbody with value v

4. If crypto does not contain encryption:

   i. Set the hp parameter on the Content-Type of MIME part newbody to clear

   ii. Let newheaders be a copy of origheaders

5. Else (if crypto contains encryption):

   i. Set the hp parameter on the Content-Type of MIME part newbody to cipher

   ii. If refmsg is not null, respond is not null, and refmsg itself is encrypted with header protection:

      a. Let response_hcp be a single-use HCP derived from respond and refmsg (see Section 6.1)

   iii. Else (if this is not a response to an encrypted, header-protected message):

      a. Set response_hcp to hcp_no_confidentiality

   iv. Create new empty list of Header Field names and values newheaders

   v. For each Header Field name and value (h,v) in origheaders:

      a. Let newval be hcp(h,v)

      b. If newval is v:

         I. Let newval be response_hcp(h,v)

      c. If newval is not null):

         I. Add (h,newval) to newheaders

   vi. For each Header Field name and value (h,v) in newheaders:

      a. Let string record be the concatenation of h, a literal ": " (ASCII colon (0x3A) followed by ASCII space (0x20)), and v

      b. Add Header Field "HP-Outer" to MIME part newbody with value record

6. Apply crypto to MIME part newbody, producing MIME tree output

7. For each Header Field name and value (h,v) in newheaders:

    i. Add Header Field h to output with value v

8. Return output

Note that both new parameters (hcp and legacy) are effectively ignored if crypto does not contain encryption. This is by design, because they are irrelevant for signed-only cryptographic protections.

5.2.2. Adding a Legacy Display Element to a text/plain Part

For a list of obscured and removed User-Facing Header Fields represented as (header, value) pairs, concatenate them as a set of lines, with one newline at the end of each pair. Add an additional trailing newline after the resultant text, and prepend the entire list to the body of the text/plain part.

The MUA MUST also add a Content-Type parameter of hp-legacy-display with value 1 to the MIME part to indicate that a Legacy Display Element was added.

For example, if the list of obscured Header Fields was [("Cc", "alice@example.net"), ("Subject", "Thursday’s meeting")], then a text/plain Main Body Part that originally looked like this:

```
Content-Type: text/plain; charset=UTF-8

I think we should skip the meeting.
```

Would become:

```
Content-Type: text/plain; charset=UTF-8; hp-legacy-display=1

Subject: Thursday’s meeting
Cc: alice@example.net

I think we should skip the meeting.
```

Note that the Legacy Display Element (the lines beginning with Subject: and Cc:) are part of the body of the MIME part in question.

This example assumes that the Main Body Part in question is not the root of the Cryptographic Payload. For instance, it could be a leaf of a multipart/alternative Cryptographic Payload. This is why no additional Header Fields have been injected into the MIME part in this example.

5.2.3. Adding a Legacy Display Element to a text/html Part

Adding a Legacy Display Element to a text/html part is similar to how it is added to a text/plain part (see Section 5.2.2). Instead of adding the obscured or removed User-Facing Header Fields to a block of text delimited by a blank line, the composing MUA injects them in an HTML element annotated with a class attribute of header-protection-legacy-display.

The content and formatting of this decorative have no strict requirements, but they MUST represent all the obscured and removed User-Facing Header Fields in a readable fashion. A simple approach is to assemble the text in the same way as Section 5.2.2, wrap it in a verbatim <pre> element, and put that element in the annotated .

The annotated should be placed as close to the start of the <body> as possible, where it will be visible when viewed with a standard HTML renderer.

The MUA MUST also add a Content-Type parameter of hp-legacy-display with value 1 to the MIME part to indicate that a Legacy Display Element was added.

For example, if the list of obscured Header Fields was [("Cc", "alice@example.net"), ("Subject", "Thursday’s meeting")], then a text/html Main Body Part that originally looked like this:

```
Content-Type: text/html; charset=UTF-8

<html><head><title></title></head><body>
<p>I think we should skip the meeting.</p>
</body></html>
```

Would become:

```
Content-Type: text/html; charset=UTF-8; hp-legacy-display=1

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>Subject: Thursday’s meeting
Cc: alice@example.net</pre></div>
<p>I think we should skip the meeting.</p>
</body></html>
```

This example assumes that the Main Body Part in question is not the root of the Cryptographic Payload. For instance, it could be a leaf of a multipart/alternative Cryptographic Payload. This is why no additional Header Fields have been injected into the MIME part in this example.

5.2.3.1. Step-by-step Example for Inserting Legacy Display Element to text/html

A composing MUA MAY insert the Legacy Display Element anywhere reasonable within the message as long as it prioritizes visibility for the reader using a Legacy decryption-capable MUA. This decision may take into account special message-specific HTML formatting expectations if the MUA is aware of them. However, some MUAs may not have any special insight into the user’s preferred HTML formatting, and still want to insert a Legacy Display Element. This section offers a non-normative, simple, and minimal step-by-step approach for a composing MUA that has no other information or preferences to fall back on.

The process below assumes that the MUA already has the full HTML object that it intends to send, including all of the text supplied by the user.

1. Assemble the text exactly as specified for text/plain (see Section 5.2.2).

2. Wrap that text in a verbatim <pre> element.

3. Wrap that <pre> element in a element annotated with the class header-protection-legacy-display.

4. Find the <body> element of the full HTML object.

5. Insert the element as the first child of the <body> element.

5.2.4. Only Add a Legacy Display Element to Main Body Parts

Some messages may contain a text/plain or text/html subpart that is _not_ a Main Body Part. For example, an e-mail message might contain an attached text file or a downloaded webpage. Attached documents need to be preserved as intended in the transmission, without modification.

The composing MUA MUST NOT add a Legacy Display Element to any part of the message that is not a Main Body Part. In particular, if a part is annotated with Content-Disposition: attachment, or if it does not descend via the first child of any of its multipart/mixed or multipart/related ancestors, it is not a Main Body Part, and MUST NOT be modified.

See Section 7.1 of [I-D.ietf-lamps-e2e-mail-guidance] for more guidance about common ways to distinguish Main Body Parts from other MIME parts in a message.

5.2.5. Do Not Add a Legacy Display Element to Other Content-Types

The purpose of injecting a Legacy Display Element into each Main Body MIME part is to enable rendering of otherwise obscured Header Fields in Legacy MUAs that are capable of message decryption, but don’t know how to follow the rest of the guidance in this document.

The authors are unaware of any Legacy MUA that would render any MIME part type other than text/plain and text/html as the Main Body. A generating MUA SHOULD NOT add a Legacy Display Element to any MIME part with any other Content-Type.

6. Replying and Forwarding Guidance

An MUA might create a new message in response to another message, thus acting both as a receiving MUA and as a sending MUA. For example, the user of an MUA viewing any given message might take an action like "Reply", "Reply All", "Forward", or some comparable action to start the composition of a new message. The new message created this way effectively references the original message that was viewed at the time.

For encrypted messages, special guidance applies, because information can leak in at least two ways: leaking previously confidential Header Fields, and leaking the entire message by sending the reply or forward to the wrong party.

6.1. Avoid Leaking Encrypted Header Fields in Replies and Forwards

As noted in Section 5.4 of [I-D.ietf-lamps-e2e-mail-guidance], an MUA in this position MUST NOT leak previously encrypted content in the clear in a follow-up message. The same is true for protected Header Fields.

Values from any Header Field that was identified as either encrypted-only or signed-and-encrypted based on the steps outlined above MUST NOT be placed in cleartext output when generating a message.

In particular, if Subject was encrypted, and it is copied into the draft encrypted reply, the replying MUA MUST obscure the unprotected (cleartext) Subject Header Field.

When crafting the Header Fields for a reply or forwarded message, the composing MUA SHOULD make use of the HP-Outer Header Fields from within the Cryptographic Envelope of the reference message to ensure that Header Fields derived from the reference message do not leak in the reply.

On a high-level, this can be achieved as follows: Consider a Header Field in a reply message that is generated by derivation from a Header Field in the reference message. For example, the To Header Field is typically derived from the reference message’s Reply-To or From Header Fields. When generating the outer copy of the Header Field, the composing MUA first applies its own Header Confidentiality Policy. If the Header Field’s value is changed by the HCP, then it is applied to the outside header. If the Header Field’s value is unchanged, the composing MUA re-generates the Header Field using the Header Fields that had been on the outside of the original message at sending time. These can be inferred from the HP-Outer Header Fields located within the Cryptographic Payload of the referenced message. If that value is itself different than the protected value, then it is applied to the outside header. If the value is the same as the protected value, then it is simply copied to the outside header directly. Whether it was changed or not, it is noted in the protected Header Section using HP-Outer, as described in Section 2.2.1.

See Appendix D.2 for a simple worked example of this process.

Below we describe a supporting algorithm to handles this. It produces a list of Header Fields that should be obscured or removed in the new message even if the sender's choice of Header Confidentiality Policy wouldn't normally remove or obscure the Header Field in question. This is effectively a single-use HCP. The normal sending guidance in Section 5.2 applies this single-use HCP to implement the high-level guidance above.

6.1.1. ReferenceHCP

The algorithm takes two inputs:

* A single referenced message refmsg, and

* A built-in MUA function respond associated with the user's action. respond takes as input a list of headers from a referenced message and generates a list of initial candidate message Header Field names and values that are used to populate the message composition interface. Something like this function already exists in most MUAs, though it may differ across responsive actions. For example, the respond function that implements "Reply All" is likely to be a different from the respond that implements "Reply".

As an output, it produces an ephemeral single-use Header Confidentiality Policy, specific to this kind of response to this specific message.

Method signature:

ReferenceHCP(refmsg, respond) → ephemeral_hcp

Procedure:

1. If refmsg is not encrypted with Header Protection:

    i. Return hcp_no_confidentiality (there is no header confidentiality in the reference message that needs protection)

2. Extract refouter, refprotected from refmsg as described in Section 4.2

3. Let genprotected be a list of (h,v) pairs generated by respond(refprotected)

4. Let genouter be a list of (h,v) pairs generated by respond(refouter)

5. For each (h,v) in genprotected:

    i. If (h,v) is in genouter:

        a. Remove (h,v) from both genprotected and genouter (this Header Field does not need additional confidentiality)

6. Let confmap be a mapping from a Header Field name and value (h,v) to either a string or the special value null (this mapping is initially empty)

7. For each (h,v) remaining in genprotected:

    i. Set result to the special value null

    ii. For each (h1,v1) in genouter:

        a. If h1 is h:

            I. Set result to v1

    iii. Insert (h,v) -> result into confmap

8. Return a new HCP from confmap that tests whether (name,val_in) are in confmap; if so, return confmap[(name,val_in)]; otherwise, return val_in

Note that the key idea here is to reuse the MUA's existing respond function. The algorithm simulates how the MUA would pre-populate a reply to two traditional messages whose Header Fields have the values refouter and refprotected respectively (independent of any cryptographic protections). Then it uses the difference to derive a one-time HCP. This HCP takes into account both the referenced message's sender's preferences and the derivations that can happen to Header Field values when responding. Note that while some of these derivations are straight forward (e.g., In-Reply-To is usually derived from Message-ID), others are non-trivial. For example, the From address may be derived from To, Cc, or from the MUA's local address preference (especially when the MUA received the referenced message via Bcc). Similarly, To may be derived from To, From, and/or Cc Header Fields depending on the MUA implementation and depending on whether the user clicked "Reply", "Reply All", "Forward", or any other action that generates a response to a message. Reusing the MUA's existing respond function incorporates these nuances without requiring any extra configuration choices or additional maintenance burden.

6.2. Avoid Misdirected Replies

When replying to a message, the Composing MUA typically decides who to send the reply to based on:

* the Reply-To, Mail-Followup-To, or From Header Fields
* optionally, the other To or Cc Header Fields (if the user chose to "reply all")

When a message has Header Protection, the replying MUA MUST populate the destination fields of the draft message using the protected Header Fields, and ignore any unprotected Header Fields.

This mitigates against an attack where Mallory gets a copy of an encrypted message from Alice to Bob, and then replays the message to Bob with an additional Cc to Mallory’s own e-mail address in the message’s outer (unprotected) Header Section.

If Bob knows Mallory’s certificate already, and he replies to such a message without following the guidance in this section, it’s likely that his MUA will encrypt the cleartext of the message directly to Mallory.

7. Unprotected Header Fields Added in Transit

Some Header Fields are legitimately added in transit and could not have been known to the sender at message composition time.

The most common of these Header Fields are Received and DKIM-Signature, neither of which are typically rendered, either explicitly or implicitly.

If a receiving MUA has specific knowledge about a given Header Field, including that:

* the Header Field would not have been known to the original sender, and
* the Header Field might be rendered explicitly or implicitly,

then the MUA MAY decide to operate on the value of that Header Field from the unprotected Header Section, even though the message has Header Protection.

The MUA MAY prefer to verify that the Header Fields in question have additional transit-derived cryptographic protections before rendering or acting on them. For example, the MUA could verify whether these

Header Fields are covered by an appropriate and valid ARC-Authentication-Results (see [RFC8617]) or DKIM-Signature (see [RFC6376]) Header Field.

Specific examples of user-meaningful Header Fields commonly added by transport agents appear below.

7.1. Mailing list Header Fields: List-* and Archived-At

If the message arrives through a mailing list, the list manager itself may inject Header Fields (most have a List- prefix) in the message:

* List-Archive
* List-Subscribe
* List-Unsubscribe
* List-Id
* List-Help
* List-Post
* Archived-At

For some MUAs, these Header Fields are implicitly rendered, by providing buttons for actions like "Subscribe", "View Archived Version", "Reply List", "List Info", etc.

An MUA that receives a message with Header Protection that contains these Header Fields in the unprotected section, and that has reason to believe the message is coming through a mailing list MAY decide to render them to the user (explicitly or implicitly) even though they are not protected.

8. E-mail Ecosystem Evolution

The e-mail ecosystem is the set of client-side and server-side software and policies that are used in the creation, transmission, storage, rendering, and indexing of electronic mail over the Internet.

This document is intended to offer tooling needed to improve the state of the e-mail ecosystem in a way that can be deployed without significant disruption. Some elements of this specification are present for transitional purposes, but would not exist if the system were designed from scratch.

This section describes these transitional mechanisms, as well as some suggestions for how they might eventually be phased out.

8.1. Dropping Legacy Display Elements

Any decorative Legacy Display Element added to an encrypted message that uses Header Protection is present strictly for enabling Header Field visibility (most importantly, the Subject Header Field) when the message is viewed with a decryption-capable Legacy MUA.

Eventually, the hope is that most decryption-capable MUAs will conform to this specification, and there will be no need for injection of Legacy Display Elements in the message body. A survey of widely used decryption-capable MUAs might be able to establish when most of them do support this specification.

At that point, a composing MUA could set the legacy parameter defined in Section 5.2 to false by default or could even hard-code it to false, yielding a much simpler message construction set.

Until that point, an end user might want to signal that their receiving MUAs are conformant to this document so that a peer composing a message to them can set legacy to false. A signal indicating capability of handling messages with Header Protection might be placed in the user’s cryptographic certificate, or in outbound messages.

This document does not attempt to define the syntax or semantics of such a signal.

8.2. More Ambitious Default Header Confidentiality Policy

This document defines a few different forms of Header Confidentiality Policy. An MUA implementing an HCP for the first time SHOULD deploy hcp_baseline as recommended in Section 3.3. This HCP offers the most commonly expected protection (obscuring the Subject Header Field) without risking deliverability or rendering issues.

The HCPs proposed in this document are relatively conservative and still leak a significant amount of metadata for encrypted messages. This is largely done to ensure deliverability (see Section 1.3.2) and usability, as messages without some critical Header Fields are more likely to not reach their intended recipient.

In the future, some mail transport systems may accept and deliver messages with even less publicly visible metadata. Many MTA operators today would ask for additional guarantees about such a message to limit the risks associated with abusive or spammy mail.

This specification offers the HCP formalism itself as a way for MUA developers and MTA operators to describe their expectations around message deliverability. MUA developers can propose a more ambitious default HCP, and ask MTA operators (or simply test) whether their MTAs would be likely to deliver or reject encrypted mail with that HCP applied. Proponents of a more ambitious HCP should explicitly document the HCP and name it clearly and unambiguously to facilitate this kind of interoperability discussion.

Reaching widespread consensus around a more ambitious global default HCP is a challenging problem of coordinating many different actors. A piecemeal approach might be more feasible, where some signalling mechanism allows a message recipient, MTA operator, or third-party clearinghouse to announce what kinds of HCPs are likely to be deliverable for a given recipient. In such a situation, the default HCP for an MUA might involve consulting the signalled acceptable HCPs for all recipients, and combining them (along with a default for when no signal is present) in some way.

If such a signal were to reach widespread use, it could also be used to guide reasonable statistical default HCP choices for recipients with no signal.

This document does not attempt to define the syntax or semantics of such a signal.

8.3. Deprecation of Messages Without Header Protection

At some point, when the majority of MUA clients that can generate cryptographically protected messages with Header Protection, it should be possible to deprecate any cryptographically protected message that does not have Header Protection.

For example, as noted in Section 9.1, it's possible for an MUA to render a signed-only message that has no Header Protection the same as an unprotected message. And a signed-and-encrypted message without Header Protection could likewise be marked as not fully protected.

These stricter rules could be adopted immediately for all messages. Or an MUA developer could roll them out immediately for any new message, but still treat an old message (based on the Date Header Field and cryptographic signature timestamp) more leniently.

A decision like this by any popular receiving MUA could drive adoption of this standard for sending MUAs.

9. Usability Considerations

This section describes concerns for MUAs that are interested in easy adoption of Header Protection by normal users.

While they are not protocol-level artifacts, these concerns motivate the protocol features described in this document.

See also the Usability commentary in Section 2 of [I-D.ietf-lamps-e2e-mail-guidance].

9.1. Mixed Protections Within a Message Are Hard To Understand

When rendering a message to the user, the ideal circumstance is to present a single cryptographic status for any given message. However, when message Header Fields are present, some message Header Fields do not have the same cryptographic protections as the main message.

Representing such a mixed set of protection statuses is very difficult to do in a way that a Ordinary User can understand. There are at least three scenarios that are likely to be common, and poorly understood:

* A signed message with no Header Protection.

* A signed-and-encrypted message with no Header Protection.

* A signed-and-encrypted message with Header Protection as defined in this document, where some User-Facing Header Fields have confidentiality but some do not.

An MUA should have a reasonable strategy for clearly communicating each of these scenarios to the user. For example, an MUA operating in an environment where it expects most cryptographically protected messages to have Header Protection could use the following rendering strategy:

* When rendering a message with signed-only cryptographic status but no Header Protection, an MUA may decline to indicate a positive security status overall, and only indicate the cryptographic status to a user in a message properties or diagnostic view. That is, the message may appear identical to an unsigned message except if a user verifies the properties through a menu option.

* When rendering a message with signed-and-encrypted or encrypted-only cryptographic status but no Header Protection, overlay a warning flag on the typical cryptographic status indicator. That is, if a typical signed-and-encrypted message displays a lock icon, display a lock icon with a warning sign (e.g., an exclamation point in a triangle) overlaid. See, for example, the graphics in [chrome-indicators].

* When rendering a message with signed-and-encrypted or encrypted-only cryptographic status, with Header Protection, but where the Subject Header Field has not been removed or obscured, place a warning sign on the Subject line.

Other simple rendering strategies could also be reasonable.

9.2. Users Should Not Have To Choose a Header Confidentiality Policy

This document defines the abstraction of a Header Confidentiality Policy object for the sake of communication between implementers and deployments.

Most e-mail users are unlikely to understand the tradeoffs between different policies. In particular, the potential negative side effects (e.g., poor deliverability) may not be easily attributable by a normal user to a particular HCP.

Therefore, MUA implementers should be conservative in their choice of default HCP, and should not require the Ordinary User to make an incomprehensible choice that could cause unfixable, undiagnosable problems. The safest option is for the MUA developer to select a known, stable HCP (this document recommends hcp_baseline in Section 3.3) on the user's behalf. An MUA should not expose the Ordinary User to a configuration option where they are expected to manually select (let alone define) an HCP.

10. Security Considerations

Header Protection improves the security of cryptographically protected e-mail messages. Following the guidance in this document improves security for users by more directly aligning the underlying messages with user expectations about confidentiality, authenticity, and integrity.

Nevertheless, helping the user distinguish between cryptographic protections of various messages remains a security challenge for MUAs. This is exarcebated by the fact that many existing messages with cryptographic protections do not employ Header Protection. MUAs encountering these messages (e.g., in an archive) will need to handle older forms (without Header Protection) for quite some time, possibly forever.

The security considerations from Section 6 of [RFC8551] continue to apply for any MUA that offers S/MIME cryptographic protections, as well as Section 3 of [RFC5083] (Authenticated-Enveloped-Data in CMS) and Section 14 of [RFC5652] (CMS more broadly). Likewise, the security considerations from Section 8 of [RFC3156] continue to apply for any MUA that offers PGP/MIME cryptographic protections, as well as Section 13 of [RFC9580] (OpenPGP itself). In addition, these underlying security considerations are now also applicable to the contents of the message header, not just the message body.

10.1. From Address Spoofing

If the From Header Field were treated by the receiving MUA like any other protected Header Field, this scheme would enable sender address spoofing.

To prevent sender spoofing, many receiving MUAs implicitly rely on their receiving MTA to inspect the unprotected Header Section and verify that the From Header Field is authentic. If a receiving MUA displays a From address that doesn’t match the From address that the receiving and/or sending MTAs filtered on, the MUA may be vulnerable to spoofing.

Consider a malicious MUA that sets the following Header Fields on an encrypted message with Header Protection:

* Outer: From: <alice@example.com>

* Inner: HP-Outer: From: <alice@example.com>

* Inner: From: <bob@example.org>

During sending, the MTA of example.com validates that the sending MUA is authorized to send from alice@example.com. Since the message is encrypted, the sending and receiving MTAs cannot see the protected Header Fields. A naive receiving MUA might follow the algorithms in this document without special consideration for the From Header Field. Such an MUA might display the email as coming from bob@example.org to the user, resulting in a spoofed address.

This problem applies both between domains and within a domain.

This problem always applies to signed-and-encrypted messages. This problem also applies to signed-only messages because MTAs typically do not look at the protected Header Fields when confirming From address authenticity.

Sender address spoofing is relevant for two distinct security properties:

* Sender authenticity: relevant for rendering the message (which address to show the user?).

* Message confidentiality: relevant when replying to a message (a reply to the wrong address can leak the message contents).

10.1.1. From Rendering Reasoning

Section 4.4.3 provides guidance for rendering the From Header Field. It recommends a receiving MUA that depends on its MTA to authenticate the unprotected (outer) From Header Field to render the outer From Header Field, if both of the following conditions are met:

* From Header Field Mismatch (as defined in Section 4.4.1.1)

* No Valid and Correctly Bound Signature (as defined in Section 4.4.1.2)

Note: The second condition effectively means that the inner (expected to be protected) From Header Field appears to have insufficient protection.

This may seem surprising since it causes the MUA to render a mix of both protected and unprotected values. This section provides an argument as to why this guidance makes sense.

We proceed by case distinction:

* Case 1: Malicious sending MUA.

- Attack situation: the sending MUA puts a different inner From Header Field to spoof the sender address.

- In this case, it is "better" to fall back and render the outer From Header Field because this is what the receiving MTA can validate. Otherwise this document would introduce a new way for senders to spoof the From address of the message.

- This does not preclude a future document from updating this document to specify a protocol for legitimate sender address hiding.

* Case 2: Malicious sending/transiting/receiving MTA (or anyone meddling between MTAs).

  - Attack situation: an on-path attacker changes the outer From Header Field (possibly with other meddling to break the signature, see below). Their goal is to get the receiving MUA to show a different From address than the sending MUA intended (breaking MUA-to-MUA sender authenticity).

  - Case 2.a: The sending MUA submitted an unsigned or encrypted-only message to the email system. In this case, there can be no sender authenticity anyway.

  - Case 2.b: The sending MUA submitted a signed-only message to the email system.

    o Case 2.b.i: The attacker removes or breaks the signature. In this case, the attacker can also modify the inner From Header Field to their liking.

    o Case 2.b.ii: The signature is valid, but the receiving MUA does not see any valid binding between the signing certificate and the addr-spec of the inner From Header Field. In this case, there can be no sender authenticity anyways (the certificate could have been generated by the on-path attacker). This case is indistinguishable from a malicious sending MUA, hence it is "better" to fall back to the outer From that the MTA can validate. Note that once the binding is validated (e.g., after an out-of-band comparison), the rendering may change from showing the outer From address (and a warning) to showing the inner, now validated From address. In some cases, the binding may be instantly validated even for previously unseen certificates (e.g., if the certificate is issued by a trusted certification authority).

- Case 2.c: The sending MUA submitted a signed-and-encrypted message to the email system.

  - Case 2.c.i: The attacker removes or breaks the signature. Note that the signature is inside the ciphertext (see Section 5.2 of [I-D.ietf-lamps-e2e-mail-guidance]). Thus, assuming the encryption is non-malleable, any on-path attacker cannot break the signature while ensuring that the message still decrypts successfully.

  - Case 2.c.ii: The signature is valid, but the receiving MUA does not see any valid binding between the signing certificate and the addr-spec of the inner From Header Field. See case 2.b.ii.

As the case distinction shows, the outer From Header Field is either the preferred fallback (in particular, to avoid introducing a new spoofing channel), or it is just as good (because just as modifiable) as the inner From Header Field.

Rendering the outer From Header Field does carry the risk of a "temporary downgrade attack" in cases 2.b.ii and 2.c.ii, where a malicious MTA keeps the signature intact but modifies the outer From Header Field. The MUA can resolve this temporary downgrade by validating the certificate-to-addr-spec binding. If the MUA never does this validation, the entire message could be fake.

If there were a signalling channel where the MTA can tell the MUA whether it authenticated the From Header Field, an MUA could use this in its rendering decision. In the absence of such a signal, and when end-to-end authenticity is unavailable, this document prefers to fall back to the outer From Header Field. This default is based on the assumption that most MTAs apply some filtering based on the outer From Header Field (whether the MTA can authenticate it or not). Rendering the unprotected outer From Header Field (instead of the protected inner one) in case of a mismatch retains this ability for MTAs.

If the MUA decides not to rely on the MTA to authenticate the outer From Header Field, it may prefer the inner From Header Field.

10.2. Avoid Cryptographic Summary Confusion from hp Parameter

When parsing a message, the recipient MUA infers the message’s Cryptographic Status from the Cryptographic Layers, as described in Section 4.6 of [I-D.ietf-lamps-e2e-mail-guidance].

The Cryptographic Layers that make up the Cryptographic Envelope describe an ordered list of cryptographic properties as present in the message after it has been delivered. By contrast, the hp parameter to the Content-Type Header Field contains a simpler indication: whether the sender originally tried to encrypt the message or not. In particular, for a message with Header Protection, the Cryptographic Payload should have a hp parameter of cipher if the message is encrypted (in addition to signed), and clear if no encryption is present (that is, the message is signed-only).

As noted in Section 2.1.1, the receiving implementation should not inflate its estimation of the confidentiality of the message or its Header Fields based on the sender’s intent, if it can see that the message was not actually encrypted. A signed-only message that happens to have an hp parameter of cipher is still signed-only.

Conversely, since the encrypting Cryptographic Layer is typically outside the signature layer (see Section 5.2 of [I-D.ietf-lamps-e2e-mail-guidance]), an originally signed-only message could have been wrapped in an encryption layer by an intervening party before receipt, to appear encrypted.

If a message appears to be wrapped in an encryption layer, and the hp parameter is present but is not set to cipher, then it is likely that the encryption layer was not added by the original sender. For such a message, the lack of any HP-Outer Header Field in the Header Section of the Cryptographic Payload MUST NOT be used to infer that all Header Fields were removed from the message by the original sender. In such a case, the receiving MUA SHOULD treat every Header Field as though it was not confidential.

10.3. Caution about Composing with Legacy Display Elements

When composing a message, it’s possible for a Legacy Display Element to contain risky data that could trigger errors in a rendering client.

For example, if the value for a Header Field to be included in a Legacy Display Element within a given body part contains folding whitespace, it should be "unfolded" before generating the Legacy Display Element: all contiguous folding whitespace should be replaced with a single space character. Likewise, if the header value was originally encoded with [RFC2047], it should be decoded first to a standard string and re-encoded using the charset appropriate to the target part.

When including a Legacy Display Element in a text/plain part (see Section 5.2.2), if the decoded Subject Header Field contains a pair of newlines (e.g., if it is broken across multiple lines by encoded newlines), any newline MUST be stripped from the Legacy Display Element. If the pair of newlines is not stripped, a receiving MUA that follows the guidance in Section 4.5.3.2 might leave the later part of the Legacy Display Element in the rendered message.

When including a Legacy Display Element in a text/html part (see Section 5.2.3), any material in the header values should be explicitly HTML escaped to avoid being rendered as part of the HTML. At a minimum, the characters <, >, and & should be escaped to <, >, and &, respectively (see for example [HTML-ESCAPES]). If unescaped characters from removed or obscured header values end up in the Legacy Display Element, a receiving MUA that follows the guidance in Section 4.5.3.3 might fail to identify the boundaries of the Legacy Display Element, cutting out more than it should, or leaving remnants visible. And a Legacy MUA parsing such a message might misrender the entire HTML stream, depending on the content of the removed or obscured header values.

The Legacy Display Element is a decorative addition solely to enable visibility of obscured or removed Header Fields in decryption-capable Legacy MUAs. When it is produced, it should be generated minimally and strictly, as described above, to avoid damaging the rest of the message.

10.4. Plaintext Attacks

An encrypted e-mail message using S/MIME or PGP/MIME tends to have some amount of predictable plaintext. For example, the standard MIME headers of the Cryptographic Payload of a message are often a predictable sequence of bytes, even without Header Protection, when they only include the Structural Header Fields MIME-Version and Content-Type. This is a potential risk for known-plaintext attacks.

Including protected Header Fields as defined in this document increases the amount of known plaintext. Since some of those headers in a reply will be derived from the message being replied to, this also creates a potential risk for chosen-plaintext attacks, in addition to known-plaintext attacks.

Modern message encryption mechanisms are expected to be secure against both known-plaintext attacks and chosen-plaintext attacks. An MUA composing an encrypted message should ensure that it is using such a mechanism, regardless of whether it does Header Protection.

11. Privacy Considerations

11.1. Leaks When Replying

The encrypted Header Fields of a message may accidentally leak when replying to the message. See the guidance in Section 6.

11.2. Encrypted Header Fields Are Not Always Private

For encrypted messages, depending on the sender's HCP, some Header Fields may appear both within the Cryptographic Envelope and on the outside of the message (e.g., Date might exist identically in both places). Section 4.3 identifies such a Header Field as signed-only. These Header Fields are clearly _not_ private at all, despite a copy being inside the Cryptographic Envelope.

A Header Field whose name and value are not matched verbatim by any HP-Outer Header Field from the same part will have encrypted-only or signed-and-encrypted status. But even Header Fields with these stronger levels of cryptographic confidentiality protection might not be as private as the user would like.

See the examples below.

This concern is true for any encrypted data, including the body of the message, not just the Header Fields: if the sender isn't careful, the message contents or session keys can leak in many ways that are beyond the scope of this document. The message recipient has no way in principle to tell whether the apparent confidentiality of any given piece of encrypted content has been broken via channels that they cannot perceive. Additionally, an active intermediary aware of the recipient's public key can always encrypt a cleartext message in transit to give the recipient a false sense of security.

11.2.1. Encrypted Header Fields Can Leak Unwanted Information to the Recipient

For encrypted messages, even with an ambitious HCP that successfully obscures most Header Fields from all transport agents, Header Fields will be ultimately visible to all intended recipients. This can be especially problematic for Header Fields that are not user-facing, which the sender may not expect to be injected by their MUA. Consider the three following examples:

* The MUA may inject a User-Agent Header Field that describes itself to every recipient, even though the sender may not want the recipient to know the exact version of their OS, hardware platform, or MUA.

* The MUA may have an idiosyncratic way of generating a Message-ID header, which could embed the choice of MUA, a time zone, a hostname, or other subtle information to a knowledgeable recipient.

* The MUA may erroneously include a Bcc Header Field in the origheaders of a copy of a message sent to the named recipient, defeating the purpose of using Bcc instead of Cc (see Section 11.4 for more details about risks related to Bcc).

Clearly, no end-to-end cryptographic protection of any Header Field as defined in this document will hide such a sensitive field from the intended recipient. Instead, the composing MUA MUST populate the origheaders list for any outbound message with only information the recipient should have access to. This is true for messages without any cryptographic protection as well, of course, and it is even worse there: such a leak is exposed to the transport agents as well as the recipient. An encrypted message with Header Protection and a more ambitious Header Confidentiality Policy avoid these leaks exposing information to the transport agents but cannot defend against such a leak to the recipient.

11.2.2. Encrypted Header Fields Can Be Inferred From External or Internal Metadata

For example, if the To and Cc Header Fields are removed from the unprotected Header Section, the values in those fields might still be inferred with high probability by an adversary who looks at the message either in transit or at rest. If the message is found in, or being delivered to a mailbox for bob@example.org, it’s likely that Bob was in either To or Cc. Furthermore, encrypted message ciphertext may hint at the recipients: for S/MIME messages, the RecipientInfo, and for PGP/MIME messages the key ID in the Public Key Encrypted Session Key (PKESK) packets will all hint at a specific set of recipients. Additionally, an MTA that handles the message may add a Received Header Field (or some other custom Header Field) that leaks some information about the nature of the delivery.

11.2.3. Encrypted Header Fields May Not Be Fully Masked by HCP

In another example, if the HCP modifies the Date header to mask out high-resolution time stamps (e.g., rounding to the most recent hour), some information about the date of delivery will still be attached to the e-mail. At the very least, the low resolution, global version of the date will be present on the message. Additionally, Header Fields like Received that are added during message delivery might include higher-resolution timestamps. And if the message lands in a mailbox that is ordered by time of receipt, even its placement in the mailbox

and the non-obscured Date Header Fields of the surrounding messages could leak this information.

Some Header Fields like From may be impossible to fully obscure, as many modern message delivery systems depend on at least domain information in the From Header Field for determining whether a message is coming from a domain with "good reputation" (that is, from a domain that is not known for leaking spam). So even if an ambitious HCP opts to remove the human-readable part from any From Header Field, and to standardize/genericize the local part of the From address, the domain will still leak.

11.3. A Naive Recipient May Overestimate the Cryptographic Status of a Header Field in an Encrypted Message

When an encrypted (or signed-and-encrypted) message is in transit, an active intermediary can strip or tamper with any Header Field that appears outside the Cryptographic Envelope. A receiving MUA that naively infers cryptographic status from differences between the external Header Fields and those found in the Cryptographic Envelope could be tricked into overestimating the protections afforded to some Header Fields.

For example, if the original sender’s HCP passes through the Cc Header Field unchanged, a cleanly delivered message would indicate that the Cc Header Field has a cryptographic status of signed. But if an intermediary attacker simply removes the Header Field from the unprotected Header Section before forwarding the message, then the naive recipient might believe that the field has a cryptographic status of signed-and-encrypted.

This document offers protection against such an attack by way of the HP-Outer Header Fields that can be found on the Cryptographic Payload. If a Header Field appears to have been obscured by inspection of the outer message, but an HP-Outer Header Field matches it exactly, the receiving MUA can indicate to the user that the Header Field in question may not have been confidential.

In such a case, a cautious MUA may render the Header Field in question as signed (because the sender did not hide it), but still treat it as signed-and-encrypted during reply, to avoid accidental leakage of the cleartext value in the reply message, as described in Section 6.1.

11.4. Privacy and Deliverability Risks with Bcc and Encrypted Messages

As noted in Section 9.3 of [I-D.ietf-lamps-e2e-mail-guidance], handling Bcc when generating an encrypted e-mail message can be particularly tricky. With Header Protection, there is an additional wrinkle. When an encrypted e-mail message with Header Protection has a Bcc'ed recipient, and the composing MUA explicitly includes the Bcc'ed recipient's address in their copy of the message (see the "second method" in Section 3.6.3 of [RFC5322]), that Bcc Header Field will always be visible to the Bcc'ed recipient.

In this scenario, though, the composing MUA has one additional choice: whether to hide the Bcc Header Field from intervening message transport agents, by returning null when the HCP is invoked for Bcc. If the composing MUA's rationale for including an explicit Bcc in the copy of the message sent to the Bcc recipient is to ensure deliverability via a message transport agent that inspects message Header Fields, then stripping the Bcc field during encryption may cause the intervening transport agent to drop the message entirely. This is why Bcc is not explicitly stripped in hcp_baseline.

If, on the other hand, deliverability to a Bcc'ed recipient is not a concern, the most privacy-preserving option is to simply omit the Bcc Header Field from the protected Header Section in the first place. An MUA that is capable of receiving and processing such a message can infer that since their user's address was not mentioned in any To or Cc Header Field, they were likely a Bcc recipient.

Please also see Section 9.3 of [I-D.ietf-lamps-e2e-mail-guidance] for more discussion about Bcc and encrypted messages.

12. IANA Considerations

This document registers an e-mail Header Field, describes parameters for the Content-Type Header Field, and establishes a registry for Header Confidentiality Policies to facilitate HCP evolution.

12.1. Register the HP-Outer Header Field

This document requests IANA to register the following Header Field in the "Permanent Message Header Field Names" registry within "Message Headers" in accordance with [RFC3864].

Header Field Name	Template	Protocol	Status	Reference
HP-Outer		mail	standard	Section 2.2.1 of RFCXXXX

Table 2: Additions to 'Permanent Message Header Field Names' registry

The Author/Change Controller of these two entries (Section 4.5 of [RFC3864]) should be the IETF itself.

12.2. Update Reference for Content-Type Header Field due to hp and hp-legacy-display Parameters

This document also defines the Content-Type parameters known as hp (in Section 2.1.1) and hp-legacy-display (in Section 2.1.2). Consequently, the Content-Type row in the "Permanent Message Header Field Names" registry should add a reference to this RFC to its "References" column.

That is, the current row:

Header Field Name	Template	Protocol	Status	Reference
Content-Type		MIME		[RFC4021]

Table 3: Existing row in 'Permanent Message Header Field Names' registry

Should be updated to have the following values:

Header Field Name	Template	Protocol	Status	Reference
Content-Type		MIME		[RFC4021] [RFCXXXX]

Table 4: Replacement row in 'Permanent Message Header Field Names' registry

12.3. New Registry: Mail Header Confidentiality Policies

This document also requests IANA to create a new registry in the "Mail Parameters" protocol group (https://www.iana.org/assignments/mail-parameters/) titled Mail Header Confidentiality Policies with the following content:

Header Confidentiality Policy Name	Description	Reference	Recommended
hcp_no_confidentiality	No header confidentiality	Section 3.2.3 of RFCXXX (this document)	N
hcp_baseline	Confidentiality for Informational Header Fields: Subject Header Field is obscured, Keywords and Comments are removed	Section 3.2.1 of RFCXXX (this document)	Y
hcp_shy	Obscure Subject, remove Keywords and Comments, remove the time zone from Date, and obscure display-names	Section 3.2.2 of RFCXXX (this document)	N

Table 5: Mail Header Confidentiality Policies registry

hcp_example_hide_cc is offered as an example in Section 3 but is not formally registered by this document.

Please add the following textual note to this registry:

The Header Confidentiality Policy Name never appears on the wire. This registry merely tracks stable references to implementable descriptions of distinct policies. Any addition to this registry should be governed by guidance in Section 3.4.2 of RFC XXX (this document).

Adding an entry to this registry with an N in the "Recommended" column follows the registration policy of SPECIFICATION REQUIRED. Adding an entry to this registry with a Y in the "Recommended" column or changing the "Recommended" column in an existing entry (from N to Y or vice versa) requires IETF REVIEW. During IETF REVIEW, the designated expert must also be consulted. Guidance for the designated expert can be found in Section 3.4.2.

13. Acknowledgments

Alexander Krotov identified the risk of From address spoofing (see Section 10.1) and helped provide guidance to MUAs.

Thore Gbel identified significant gaps in earlier versions of this document, and proposed concrete and substantial improvements. Thanks to his contributions, the document is clearer, and the protocols described herein are more useful.

Additionally, the authors would like to thank the following people who have provided helpful comments and suggestions for this document: Berna Alp, Bernhard E. Reiter, Bron Gondwana, Carl Wallace, Claudio Luck, Daniel Huigens, David Wilson, ric Vyncke, Hernani Marques, juga, Krista Bennett, Kelly Bristol, Lars Rohwedder, Michael StJohns, Nicolas Lidzborski, Orie Steele, Paul Wouters, Peter Yee, Phillip Tao, Robert Williams, Rohan Mahy, Roman Danyliw, Russ Housley, Sofia Balicka, Steve Kille, Volker Birk, Warren Kumari, and Wei Chuang.

14. References

14.1. Normative References

[I-D.ietf-lamps-e2e-mail-guidance]
Gillmor, D. K., Hoeneisen, B., and A. Melnikov, "Guidance on End-to-End E-mail Security", Work in Progress, Internet-Draft, draft-ietf-lamps-e2e-mail-guidance-16, 16 March 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-e2e-mail-guidance-16>.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/rfc/rfc2045>.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3864] Klyne, G., Nottingham, M., and J. Mogul, "Registration Procedures for Message Header Fields", BCP 90, RFC 3864, DOI 10.17487/RFC3864, September 2004, <https://www.rfc-editor.org/rfc/rfc3864>.

[RFC5083] Housley, R., "Cryptographic Message Syntax (CMS) Authenticated-Enveloped-Data Content Type", RFC 5083, DOI 10.17487/RFC5083, November 2007, <https://www.rfc-editor.org/rfc/rfc5083>.

[RFC5234] Crocker, D., Ed. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, DOI 10.17487/RFC5234, January 2008, <https://www.rfc-editor.org/rfc/rfc5234>.

[RFC5322] Resnick, P., Ed., "Internet Message Format", RFC 5322, DOI 10.17487/RFC5322, October 2008, <https://www.rfc-editor.org/rfc/rfc5322>.

[RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <https://www.rfc-editor.org/rfc/rfc5652>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

[RFC8551] Schaad, J., Ramsdell, B., and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification", RFC 8551, DOI 10.17487/RFC8551, April 2019, <https://www.rfc-editor.org/rfc/rfc8551>.

[RFC9580] Wouters, P., Ed., Huigens, D., Winter, J., and Y. Niibe, "OpenPGP", RFC 9580, DOI 10.17487/RFC9580, July 2024, <https://www.rfc-editor.org/rfc/rfc9580>.

14.2. Informative References

[chrome-indicators]
Schechter, E., "Evolving Chrome’s security indicators", May 2018, <https://blog.chromium.org/2018/05/evolving-chromes-security-indicators.html>.

[CSS] World Wide Web Consortium, "Cascading Style Sheets Level 2 Revision 2 (CSS 2.2) Specification", 12 April 2016, <https://www.w3.org/TR/2016/WD-CSS22-20160412/>.

[HTML-ESCAPES]
W3C, "Using character escapes in markup and CSS", n.d., <https://www.w3.org/International/questions/qa-escapes#use>.

[I-D.autocrypt-lamps-protected-headers]
Einarsson, B. R., "juga", and D. K. Gillmor, "Protected Headers for Cryptographic E-mail", Work in Progress, Internet-Draft, draft-autocrypt-lamps-protected-headers-02, 20 December 2019, <https://datatracker.ietf.org/doc/html/draft-autocrypt-lamps-protected-headers-02>.

[I-D.pep-email]
Marques, H. and B. Hoeneisen, "pretty Easy privacy (pEp): Email Formats and Protocols", Work in Progress, Internet-Draft, draft-pep-email-02, 16 December 2022, <https://datatracker.ietf.org/doc/html/draft-pep-email-02>.

[I-D.pep-general]
Birk, V., Marques, H., and B. Hoeneisen, "pretty Easy privacy (pEp): Privacy by Default", Work in Progress, Internet-Draft, draft-pep-general-02, 16 December 2022, <https://datatracker.ietf.org/doc/html/draft-pep-general-02>.

[PGPCONTROL]
UUNET Technologies, Inc., "Authentication of Usenet Group Changes", 27 October 2016, <https://ftp.isc.org/pub/pgpcontrol/>.

[PGPVERIFY-FORMAT]
Lawrence, D. C., "Signing Control Messages, Verifying Control Messages", n.d., <https://www.eyrie.org/~eagle/usefor/other/pgpverify>.

[RFC1035] Mockapetris, P., "Domain names - implementation and specification", STD 13, RFC 1035, DOI 10.17487/RFC1035, November 1987, <https://www.rfc-editor.org/rfc/rfc1035>.

[RFC2047] Moore, K., "MIME (Multipurpose Internet Mail Extensions) Part Three: Message Header Extensions for Non-ASCII Text", RFC 2047, DOI 10.17487/RFC2047, November 1996, <https://www.rfc-editor.org/rfc/rfc2047>.

[RFC2049] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part Five: Conformance Criteria and Examples", RFC 2049, DOI 10.17487/RFC2049, November 1996, <https://www.rfc-editor.org/rfc/rfc2049>.

[RFC3156] Elkins, M., Del Torto, D., Levien, R., and T. Roessler, "MIME Security with OpenPGP", RFC 3156, DOI 10.17487/RFC3156, August 2001, <https://www.rfc-editor.org/rfc/rfc3156>.

[RFC3851] Ramsdell, B., Ed., "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.1 Message Specification", RFC 3851, DOI 10.17487/RFC3851, July 2004, <https://www.rfc-editor.org/rfc/rfc3851>.

[RFC4021] Klyne, G. and J. Palme, "Registration of Mail and MIME Header Fields", RFC 4021, DOI 10.17487/RFC4021, March 2005, <https://www.rfc-editor.org/rfc/rfc4021>.

[RFC5751] Ramsdell, B. and S. Turner, "Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification", RFC 5751, DOI 10.17487/RFC5751, January 2010, <https://www.rfc-editor.org/rfc/rfc5751>.

[RFC5890] Klensin, J., "Internationalized Domain Names for Applications (IDNA): Definitions and Document Framework", RFC 5890, DOI 10.17487/RFC5890, August 2010, <https://www.rfc-editor.org/rfc/rfc5890>.

[RFC5891] Klensin, J., "Internationalized Domain Names in Applications (IDNA): Protocol", RFC 5891, DOI 10.17487/RFC5891, August 2010, <https://www.rfc-editor.org/rfc/rfc5891>.

[RFC6376] Crocker, D., Ed., Hansen, T., Ed., and M. Kucherawy, Ed., "DomainKeys Identified Mail (DKIM) Signatures", STD 76, RFC 6376, DOI 10.17487/RFC6376, September 2011, <https://www.rfc-editor.org/rfc/rfc6376>.

[RFC7489] Kucherawy, M., Ed. and E. Zwicky, Ed., "Domain-based Message Authentication, Reporting, and Conformance (DMARC)", RFC 7489, DOI 10.17487/RFC7489, March 2015, <https://www.rfc-editor.org/rfc/rfc7489>.

[RFC7929] Wouters, P., "DNS-Based Authentication of Named Entities (DANE) Bindings for OpenPGP", RFC 7929, DOI 10.17487/RFC7929, August 2016, <https://www.rfc-editor.org/rfc/rfc7929>.

[RFC8162] Hoffman, P. and J. Schlyter, "Using Secure DNS to Associate Certificates with Domain Names for S/MIME", RFC 8162, DOI 10.17487/RFC8162, May 2017, <https://www.rfc-editor.org/rfc/rfc8162>.

[RFC8617] Andersen, K., Long, B., Ed., Blank, S., Ed., and M. Kucherawy, Ed., "The Authenticated Received Chain (ARC) Protocol", RFC 8617, DOI 10.17487/RFC8617, July 2019, <https://www.rfc-editor.org/rfc/rfc8617>.

[RFC9216] Gillmor, D. K., Ed., "S/MIME Example Keys and Certificates", RFC 9216, DOI 10.17487/RFC9216, April 2022, <https://www.rfc-editor.org/rfc/rfc9216>.

Appendix A. Table of Pseudocode Listings

This document contains guidance with pseudocode descriptions. Each algorithm is listed here for easy reference.

Method Name	Description	Reference
HeaderSetsFromMessage	Derive "outer" and "protected" sets of Header Fields from a given message	Section 4.2.1
HeaderFieldProtection	Calculate cryptographic protections for a Header Field in a given message	Section 4.3.1
ReferenceHCP	Produce an ephemeral HCP to use when responding to a given message	Section 6.1.1
ComposeNoHeaderProtection	Legacy message composition with end-to-end cryptographic protections (but no header protection)	Section 5.1.1
Compose	Compose a message with end-to-end cryptographic protections including header protection	Section 5.2.1

Table 6: Table of Pseudocode Listings

Appendix B. Possible Problems with Legacy MUAs

When an e-mail message with end-to-end cryptographic protection is received by a mail user agent, the user might experience many different possible problematic interactions. A message with Header Protection may introduce new forms of user experience failure.

In this section, the authors enumerate different kinds of failures we have observed when reviewing, rendering, and replying to messages with different forms of Header Protection in different Legacy MUAs. Different Legacy MUAs demonstrate different subsets of these problems.

A conformant MUA would not exhibit any of these problems. An implementer updating their Legacy MUA to be compliant with this specification should consider these concerns and try to avoid them.

Recall that "protected" refers to the "inner" values, e.g., the real Subject, and "unprotected" refers to the "outer" values, e.g., the dummy Subject.

B.1. Problems Viewing Messages in a List View

* Unprotected Subject, Date, From, To Header Fields are visible (instead of being replaced by protected values)
* Threading is not visible

B.2. Problems when Rendering a Message

* Unprotected Subject is visible
* Protected Subject (on its own) is visible in the body
* Protected Subject, Date, From, and To Header Fields visible in the body
* User interaction needed to view whole message
* User interaction needed to view message body
* User interaction needed to view protected subject
* Impossible to view protected Subject
* Nuisance alarms during user interaction
* Impossible to view message body
* Appears as a forwarded message
* Appears as an attachment
* Security indicators not visible
* Security indicators do not identify protection status of Header Fields
* User has multiple different methods to reply (e.g., reply to outer, reply to inner)

* User sees English "Subject:" in body despite message itself being in non-English

* Security indicators do not identify protection status of Header Fields

* Header Fields in body render with local Header Field names (e.g., showing "Betreff" instead of "Subject") and dates (TZ, locale)

B.3. Problems when Replying to a Message

Note that the use case here is:

* User views message, to the point where they can read it

* User then replies to message, and they are shown a message composition window, which has some UI elements

* If the MUA has multiple different methods to reply to a message, each way may need to be evaluated separately

This section also uses the shorthand UI:x to mean "the UI element that the user can edit that they think of as x."

* Unprotected Subject is in UI:subject (instead of the protected Subject)

* Protected Subject is quoted in UI:body (from Legacy Display Element)

* Protected Subject leaks when the reply is serialised into MIME

* Protected Subject is not anywhere in UI

* Message body is _not_ visible/quoted in UI:body

* User cannot reply while viewing protected message

* Reply is not encrypted by default (but is for legacy signed-and-encrypted messages without Header Protection)

* Unprotected From or Reply-To Header Field is in UI:To (instead of the protected From or Reply-To Header Field)

* User’s locale (lang, TZ) leaks in quoted body

* Header Fields not protected (and in particular, Subject is not obscured) by default

Appendix C. Test Vectors

This section contains sample messages using the specification defined above. Each sample contains a MIME object, a textual and diagrammatic view of its structure, and examples of how an MUA might render it.

The cryptographic protections used in this document use the S/MIME standard, and keying material and certificates come from [RFC9216].

These messages should be accessible to any IMAP client at imap://bob@header-protection.cmrg.net/ (any password should authenticate to this read-only IMAP mailbox).

You can also download copies of these test vectors separately at https://header-protection.cmrg.net.

If any of the messages downloaded differ from those offered here, this document is the canonical source.

C.1. Baseline Messages

These messages offer no header protection at all, and can be used as a baseline. They are provided in this document as a counterexample. An MUA implementer can use these messages to verify that the reported cryptographic summary of the message indicates no header protection.

C.1.1. No Cryptographic Protections Over a Simple Message

This message uses no cryptographic protection at all. Its body is a text/plain message.

It has the following structure:

```
└─ text/plain 152 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit
Subject: no-crypto
Message-ID: <no-crypto@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:00:02 -0500
User-Agent: Sample MUA Version 1.0

This is the
no-crypto
message.

This message uses no cryptographic protection at all.  Its body
is a text/plain message.

--
Alice
alice@smime.example
```

C.1.2. S/MIME Signed-only signedData Over a Simple Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a text/plain message. It uses no header protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 3856 bytes
  (unwraps to)
  └─ text/plain 206 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part
Message-ID: <smime-one-part@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:01:02 -0500
User-Agent: Sample MUA Version 1.0

MIILGQYJKoZIhvcNAQcCoIILCjCCCwYCAQExDTALBglghkgBZQMEAgEwggFCBgkq
hkiG9w0BBwGgggEzBIIBL01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04Ig0KQ29udGVudC1UcmFuc2Zlci1F
```

bmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtb25lLXBhcnQNCm1l
c3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtb25seSBTL01JTUUgbWVzc2FnZSB2
aWEgUEtDUyM3IHNpZ25lZERhdGEuICBUaGUNCnBheWxvYWQgaXMgYSB0ZXh0L3Bs
YWluIG1lc3NhZ2UuIEl0IHVzZXMgbm8gaGVhZGVyIHByb3RlY3Rpb24uDQoNCi0t
IA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMg
UlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
TtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDH
dZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy
6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMC
BSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdao
x644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtl
uLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vR
hZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
NO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwID
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
JOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4P
GHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6a

```
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkq
hkiG9w0BCQUxDxcNMjEwMjIwMTUwMTAyWjAvBgkqhkiG9w0BCQQxIgQgrhyFjywc
FLYzlCbb/xsgb5+a0sgYLUg094upq1ZXLWswDQYJKoZIhvcNAQEBBQAEggEABOi5
kcjRmMF4LK94svcfl92padnfUTSyjJtrIf6R6C7xy87VzsmPOPCmHgZOmTCuvY2D
iKuMId6WPVdjuRUaW6xkgYtgYjPDhy80NY0a9wXEQtjn448G0UHdM21cJyu9LTAg
orSzcT2pwEuGzNdsHW8LB5GtJKYct3RS0+jlbSr7WpZFY1mUrwpsm2r8za2KoOcy
t/E7Qz/8hT4HU52Na7pS1ZnxrasLr5prSjDSSKs4QK3ncJR8jhF9by0pDCoYgswy
zYaeJt0N+8uv7ab/kBaE3wfZlipMSFRJIlh+QeXCkIHo5fW5bn/REZHxMMdMfdPh
bqYT1i46156CSOqyxA==
```

C.1.2.1. S/MIME Signed-only signedData Over a Simple Message, No Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-one-part
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a text/plain message. It uses no header protection.

--
Alice
alice@smime.example
```

C.1.3. S/MIME Signed-only multipart/signed Over a Simple Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a text/plain message. It uses no header protection.

It has the following structure:

```
└─┬ multipart/signed 4187 bytes
  ├── text/plain 224 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="253";
 micalg="sha-256"
Subject: smime-multipart
Message-ID: <smime-multipart@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:02:02 -0500
User-Agent: Sample MUA Version 1.0

--253
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-multipart
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a text/plain
message. It uses no header protection.

--
Alice
alice@smime.example

--253
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
```

```
   hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
   zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
   jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
   zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
   A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
   qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
   7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
   ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
   cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
   MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
   A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
   AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
   a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
   /evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
   SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
   saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
   ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
   BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
   ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
   VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
   8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
   G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
   RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
   bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
   7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
   OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
   MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
   RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
   cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
   9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTAyMDJa
   MC8GCSqGSIb3DQEJBDEiBCAB+IATfw3+2kO9hwjUYxzW+Z12sfFp2dTb1pmXGS+7
   DzANBgkqhkiG9w0BAQEFAASCAQANJdfU8DtOpINW4FeIWpdexndYvHYy7jFg5ICy
   wIkh1DcqmbdvB4PXcksbJ0zKSVjdjXPdYQYRS4E5ClAEevEe+OkFd16UoGaadoaq
   OjyGnuiEJJbRG2UUZZWMyJW2g8OZRAGZjYgEgvbVflmxqRjFRaeLGUorHaHoxk40
   LomKSVRTUG11eEhmRmxIY4wKhwc0U9PKjCQFrhu3t1ZkGSfPn9jvdNTJkg85WUpk
   WqmOyrup6DH4Gb84By+0IMk3vflrOyAw3kbsj6Ij+zymAlH61YypnAvddFBIuZPL
   2LYdIHPLmq8KGrzcgjkjP+Y58hf9U+6gp0KPuS8DAGOvxYs0
```


C.1.4. S/MIME Signed and Encrypted Over a Simple Message, No Header Protection

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses no header protection.

It has the following structure:

```
   └── application/pkcs7-mime [smime.p7m] 6720 bytes
     (decrypts to)
     └── application/pkcs7-mime [smime.p7m] 3960 bytes
       (unwraps to)
       └── text/plain 241 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: smime-signed-enc
Message-ID: <smime-signed-enc@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:03:02 -0500
User-Agent: Sample MUA Version 1.0

MIITXAYJKoZIhvcNAQcDoIITTTCCE0kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGi78TIbx6BFPvdJW+VbgXY631bpi8XsHhD0
vTxHFViwRovgyH6v1vvobDE1xv6VdbyzVT4LEsiGbDzr0tO22oXSBV3JkzJez5fw
umUNX49fx31aXa7GDlp0G7YHzfxSCskt7rREceVzbp3qR46nGGbreosgbVqpiuUX
m3+ghxULxFZBggDJAFhWwH1cWtQ5lp6zAiior+Fc0A48OHErdNCqEO+21j3/3wIP
oQR6Aqx9beav1jJsjTVGm2BaCpCvLI4aooptm4LqMxXIe33FkzUDexJclwXJgx8y
r8yW3MroptDD7zJQMFu7LMgUYZ2VqTlbJBvpST13ZNQ+wxWHRz8wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAcBM/QDMNvyAPHlG0py8AovZ7
NHpupXUiRN6AZBINXb9rbgM5bv3XAuWKIeNg8cI4I+TF/RXYLnwTr8YSjThpl/+Q
DvcV5T1DyJBlHU5S7VFZHsMrJFw9+14nn83id60n5MSEqtn+Ec5DZaeKoOWXdfXx
Q/QqLoQVxlOX5awyChHk6s/oIdgXPAiF7ZJkT35FAGuv/Dx9o2chl7o1SIcgfOej
8K0txmm2e2ez8bluhZw1DaGDBiYsUIjw3VF9vQqUnhEisQZxOg5jOxGc2kE7Mk3q
wiH8xydBCzKRQfq4ze+ml3uyPPgMDJi5OpJqO0rarsKz4dV+YWbz/5YVKnlMZjCC
EC4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEBRNCCx1UMI1OKK9qZck9jaAghAA
cC8Gt6ZgbCpV3HWObyl0nE4w+Vhxs8Z/1+nNlgrtaL6/ZDHZkfdc+lhk9LUeAr09
QfHkfqGMYxWF5BqUk3l5BI4OEyL8kU/dcqTFpWt/Fa4yWodfNGLThjoSfryHJFeC
vBjBcaOkiL9EsFpeFB4Qe5DY7/rcAGnCM5N6N3eRTPsIzguArEWX5fz7ulLuI3dt
/c3LsaGlmeHCB9bKhewhqa/jj3fxntB8CRDoSAUwt0t1lzx/GjHNXboz1vH623Oo
VPABjb/fqf6lzO3gszY2RE6wI7zHydlz2DgkpFdjyVk1Jub2+QkrQA7Brn9gES/I
gshjTIF+OL3me4UBxww0Bxtt46yz8FpVVOK4MunYel4U4p1SR1WEZGRLPDL+bydN
vXdstX39Eg8YChAdt5o5pPQ7bUo3Qkk0X9glJdyVNsTpWREj+F+/6do/JPStJSQt
TYgnXdjkHP4/w6+xqOcogfEVp6in7KkwfZ0v+SdZK++IPm/rMOsZlP9MbM9LkOA1
6xAB4MmPlOUDs5KQB5NYWvt034PQv8NRqfs7mlS7F4gvCaaAA1SZdqRn7kIdiNqg
RUFYTkhF5/g+pJ/Ysw9lVIvAOXHtnrbsTOxbrsIzL5wbkvCDW6ZTQIQ4kP9D0NTl
1JcxNVj10GprUztmYgqOy+wIJj3DlXHSSdugy3S/qEjiCCZwN8zAVl+c8AiifgfP
zpI4QU1552EC8HyoIUZSQP5O/dIy6ABLEDcwZKJ8nGJdSLurpD0V68p/hWk+Q6mu
```

I7DqidlNT0yehBKvZRE8jr7wclUm73xX/PhOqY158N6wNsekUHOHYERKU0BzRScQ
+YJ9tcsmPldE6jAzJB/vjjgoiLxIMci0PAXVdGjisxY3QhLh4DJTwKwhIr4kMkv0
OdciW3q2+9sxT4fbFMrOIXLUahE5qGbIyyvpPgwRmP/otP4jEyCgHuBxHKar630J
q381rmnb6Cqybc/Gmfxb0hX78DTn9hWag7fYh6u0yfMuH2bWvXW+ff+yeAy0/PCR
hxv0jZ+e3yx0Z4d8Q4Jk6kT6+HaP1tAMvJc4dubvP0+nQFZsHcxdLMrmBel+xpg5
DP1cGVtwQicVbCYWPkJINDcn9fExd1BiooF6yfaQ6a2h9zFpaevu5EqxRso57zpL
fv9PpPiuT9xQvFyYTg07cD8negTwJxVZwhP+PXdctwuwOkhCaW8I65SnKcvyYZpG
0t+Rr4Ul0oXs/0ERZLxQQbJLIRIxwsfekwvFBZ8QXp30mfQ+4M4lCO/f6cNO0TpF
LlNM6YyjWYQ38UDpirxgrp+ySOmCCFF+OjVC5AHsS+Orozv8IOWG8A8KKgryfNMs
tLrLctIOXLL900J4DOP3noqEQnYOI9Qq9X7f2Zv+f1G2sp0qrA8+frrxyB9H1VKu
Nqo+S2qq/c3d1EvDtVG8YYU4gCFeZzUq2nAsZcIoD157z7M512cQrCabLcZAYG4T
/PwRQpb9EqPwzuEBPZq997VbzzWKzqOuJPx4TeT8ksJawZzvs0/Gi5YL8inCV0Hx
vz2vmsWlL2sDDCus6vcl7X5pOqckNW5A7J/uGOXylkb2ZxTR0xP1wd4P3Ncw0S8m
3TVIiSKsNDHd3/ZEBkTeVIcmkprNeApZ6toTc3/izJO2OgLDtdjfu85nEVTIsalg
Syq8uGagBIQPpNb/EmICF1s78/b7MPu/NtF47Z0j8LIljS5xac1s/mT9XOEPw28z
ZmL6/5I+UKMKsJuaoSAJ5TcK13TONCdOteBt0dxMZHbw4Ix/YKESkCFu9B3IyoLq
kuCKtuGG6KNyIDYhkrLHs4wvQrhuky5r+wuzIE/HcM8mDWSaX+qEsGpOBUvFaDQZ
oNxuupslwKXsEO3I2WYOT4vVu6FbkQxVusmxL5KcXqJzaPu7bfaA9YpEyc0b0psC
YXMyUoplAtGQFwptKKxbhjBNoaIK26hnhREHgaOcD1YWTAU1p0bwTTRCqsYi0Vr9
iHmXjOrI3Hzz5Nks4OiF1tATULhL3dNzpZjIfdfMWsY6rFIfo+CaC/VpXFFvl9UD
1TDD7NYmSLNKgHMQ4yDBOQo9TyfiU4p2Asq3T+kFcS6X5WqdXeM2KwaDPuULl3J/
6ulUm5tm+8rQ5hf3jbxSmoC73HYywM0pdnv4BwghDetE3mdcVcSWYS38H5pOZfh6
NhTKY9PT7poeW2U/rmlfuOwKP97bIWVYiUM+F47fukbGymGztGJVqYtOJoLC3HT/
cVZhUaAqFkgbDBpGA+bANkzD1jHl3wZya4rb2LmhYSZM1xNqkKolQ+t3VhZ9FpgD
FFA7UWxGGjW2N2k/zJLdYNLjMtBRb2idEh0KXmxadRWRazIb1IJwGiXRtKmPRvWS
IPN138WtWF/fTpV5XP+Knk7SDZYzq2AZ8f98QDimmopz0N2cBDQRMUD32t4hFzHz
K7IBAx+fkQdw8JkX4JDJSGzMKM8glO5dpONZYSNb4ucEcmchi+7nMKszz5A0Nsjr
1V/khpZapoTjcTH9WZegiJMsaiU+sir1SadRTdnYxiwkJH5g/XfOe+3/+1+BDPb3
ac0vB86womwCoUgRnnFjWPLO7Dky5+p9BqYvKkmHuhzkL2O8+/gy+Z/aPnfZ1Syt
dz0gzSgvFrmRPKASmP3KVGmM6w/UwEhldO3HjNoOdv6qyQsy1dY6M4IA2tsCvKYg
qCwlzzZMs/P+PSkZtwwsQ9Zkn1b/wq1AFDqxjs3cysQeBLt0wAGBIRtnetvsWht9
yxAMLanLX01Wh8PtNewJY2LZZkhkOWCxP30VSqrzmwhGyX6lwMH2AAv+mu6hD3ci
tyhD44SvQUVVOVSCSyPSIcDZsdHL+XjuY7WDuiFh6v9Jb3KKZqbuoXoet44BtouY
RTit8UQJBGqReS9YJGh14U2ra1dvKLoZHIZdyxob12fu4QkTDAjGIvDzYuxuVaZL
W0NaHpBNIlOQUitx5e6JvyjIKtwM6Y/3/0o9pInhXDezk3t78NYctFR08xFQY3LJ
DN3S2EgXj1jWmd5E0/z+Tccg7d8hEn+0vVCRRQksqiPIEcZ1f/xgfm01FOfnI1Pb
OJfUSuZpTvnWtvCTOn62XmWj+4jzxBmopauAqf9XzDj6NsHGkrPVrdotEhFoYYRu
OHO0K4dUQf57JkVv56tuHkCAGUUgqVRzf9h2wcXP77vsUx0gpjXSKv4SMx7IUlW0
jCz1WNqQXPFny6j60BJzZ8wd6nFshHcYbvCP+BKxx7WB3j5Pqxr3/s9S9daCgMQ4
gWiPMOzuSgoTz2ggjqv31QMAXvkBSE+DIauh9BPw5pwoMsdMYT9eV+DrbN4dhy6t
P/4zCB4NQcyU2vP8P9piBLhcjunadSdITTna3D/fA6VdhidmuF5ieCzo1sTAGH6H
/VRPjxvA9gBeDtko120xoIaLpBF7I75UuFziIzuGuSE1lAf1S+I4NOD9tw0Gw+xU
/lvzqk4NHZ/j91GvRxTRj0eFWRuTKXDvVj6Z07vW1l8tJs+IpslaZgo5/sE7Ntx/
kTpAFcckTfz4iG0ngjlbVv7Do9fM1ndyUz8KxxznxBkS5kWw63rsobmlLpfks9zD
qIcxIldwnbKDufmd6kKgu66wjtfxKcGK+JQ09r2G+E0vDHLO3CUHjVafLEN1Rwt9
4Caj4WW5dcVQh+r3cYNeM50WHsKQ4leBxdVHLswnLa4PsIH5LqUDafFUVEOXbDOI
SnqIMMCdqGsGGsBIEDjopOrYj8rqyUP85j43/eTE2Jv7mQsvcyeAqH5fOzb8MkGD
8AsdOxVIbgYYalaB01pWcQE/jRv4D7cO0D2OM1DQzED9Ydzvl51jHE+71LVUbSkA

```
LQoYXJzLNj16DRYbSynXXFiRPmgAq9sfPEf+CoR47zpQUVXACRPLieRSDajlnj/U
XaoLV6JVFLY7+FQeW/W0YElIz4R2NJXdBXtaNNBjLnrS+8sW99cVY/yzMUjsohys
5Vjun8GPVRYVyAx003J5bdzefPLxoUhy7Of46lJxL0kBELzWAtCMm+MwBbrJCphS
0PlziAmYr5EGUEhA2pmv5O5Ok83Z7C4lmdbrRDraw++N0fq7mSm9ZgJRwbslrP+D
efLWEfWIeOz333XsmbJSi1E/MhJ3dCevVc33rEwaUvOJK8pOSMQj0ftl3yPYs+V1
YU/spQFYsXMhF8I4ZKQwGErIQEY5erTLbnhCRZgJgteQ0CkiQwB+U9JVnaJByjTw
DpY21mtfKIvNdc5rrThpDDI2uEiS+u42z5UxZiXiTYthWvrx7HQaCF9JP4INCe57
tvuGXDdfN2Hu5Yfnu6CdTqrovkbEzYt2kEzCXKvNZGcp58Nhbybt6Pw4Iju5XsA+
bptyQfmSSW6Ph6dXub9VJQKlFO0nhyyq6+Th+DXaNeRnXxl2jfykX+mUUFN6KHkK
9Td5k+yyIOGWe6oEeG4nwwytaDqduK9jBEna65cOBh5RulCvabCEXsHT3ovdvgrL
oJUO5WjAGGpdHpXUTlCwZHLo2zgD9L86zaZdi0fe9EcRxI/4NcbWkRhSoZTBur0+
KwuMH5ijXlI4Bb6YGt8Z9VUsTQr/QjdlnGVkIWSOqkw+3EVuHsB+ukx19hTXihCz
TDPgBaI8twdD5UfxnlglmM88304Rt4JsraLb3YtX8SD2p0g4GFfkEVKMJXYjWz6M
cTyDUBnyyShRHtInBjnn6alMBkq0t1vulRmUwOhd1Ua7ripH64qJFe938SJBu3yC
7divmSGh36en0ix6/hwq8uYVvO0RiyuMQmGs3KVVIByIL43RVhlthvccOO6I6l3s
U40BsdC/zXG4iZr5PT0LhAUgmX6OcPy2INFx+E/Idy45sN0pj7zfTSxrg5br72gg
dIZQkGYe3KJhMvHvkA40IEjGljU95Bx+bFoojWUaMUI4wlhhz0bppZF/bkENLhGq
IXVMYUfa0GFSvfhfXN7r3VvRpzkh7mgJrsIFwG035ZhZq904Z1Yw11N9pns8X2s6
PsSOZAO/E0NOMLSrOonmHy2wqGY7kSMprd9FI7ESe1hwLgqh2pVNesYGqx1Aw0AD
9rDktHKChXqAQDYElV/D1239rxc3tVFzoXtkk6BcNlwq/hvksAjk1/sMNA9x7OAf
gfE/zFZQNhWFNzuGd6ADf4Io+Wg9+L60JZmgBx6A9IiTygG9D38yREzQl0BgfGx4
xlkbs830dOgKafDVTMWCNomvOqIcU9kdirLuaOYl7N5yIR3TMH8p2kkkyYH0hMdX
TQ5v4K/OUYQteADMquJIJQiIfsOEdfd6to46yWIWlCQSJpN+M2iw0QoOPOjevCkC
RVZ0xXALDuEEuUJLjlSrwRVOx5drsqLoClAeH1Li/ZFm+I6qA2pVKrxohwndGimR
3FVKgLzC1srGGXsIGqoq5ueeN2ZTIQ6OyJh/ERLFd0uEeVCv7UIBRwQ9WrNaaFY1
1OtoJc+0XZ617xSFoKWnyA==
```

C.1.4.1. S/MIME Signed and Encrypted Over a Simple Message, No Header Protection, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIILPAYJKoZIhvcNAQcCoIILLTCCCykCAQExDTALBglghkgBZQMEAgEwggFlBgkq
hkiG9w0BBwGgggFWBIIBUk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04Ig0KQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYw0K
bWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlN
RSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2ln
bmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbg0KbWVzc2FnZS4g
SXQgdXNlcyBubyBoZWFkZXIgcHJvdGVjdGlvbi4NCg0KLS0gDQpBbGljZQ0KYWxp
Y2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJU
h6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTha
```

MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5B
bGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqV
KfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfID
lB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdS
NRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1
ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv
9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIB
aVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxl
MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQU
olNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpn
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9
eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLv
Lir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLro
r2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSY
kGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzS
WHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIIC
t6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTAL
BgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUg
TEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQx
OFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEB
AQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oulls
k4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpX
mFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2
GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wX
VgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7B
tZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYD
VR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYET
YWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8B
Af8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQY
MBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2
p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzh
W/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqEN
t1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9C
Dr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0T
zPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+Aq
J5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQME
AgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0y
MTAyMjAxNTAzMDJaMC8GCSqGSIb3DQEJBDEiBCDlUvgsJW6j30yo/fAeR1vd2Kst
erfZdXyjSKu5gnNGRTANBgkqhkiG9w0BAQEFAASCAQAYPeerPzpSeDL0FAep2p3r
y/xmN2pXvMsg1OQI/r6H/WIUpXga0Z3Z5Ml/VsZtKIbFGv/3en7GoqKc0w7/R26B
qKvtjt+0K7CW1BaWKRqcx7hTIVJXQhT7UnQLnT5daf/BiPbf73FEKoOE4N0cvsVY
237ni7VR/Rz/uz3TnheOsBk7H/AEmKIaPBnJj8wFoc6E8Vtusy5ZIrhX6YEq6e3A
YIJ01cm+cNWBa7kORT2pyKZ3yF2IIcoqyEfw/QkPkh6KM5hKSOUhvbQRPdKOv5u+
r/KmOuAbX04XzLZY+RYFdPG/grj+YxeJEgZlUfLgx8pJET9J0RkTImNh1zVVU+r4

C.1.4.2. S/MIME Signed and Encrypted Over a Simple Message, No Header Protection, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: text/plain; charset="utf-8"
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses no header protection.

--
Alice
alice@smime.example
```

C.1.5. No Cryptographic Protections Over a Complex Message

This message uses no cryptographic protection at all. Its body is a multipart/alternative message with an inline image/png attachment.

It has the following structure:

```
└─┬ multipart/mixed 1402 bytes
  ├─┬ multipart/alternative 794 bytes
  │ ├── text/plain 206 bytes
  │ └── text/html 304 bytes
  └── image/png inline 232 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="e68"
Subject: no-crypto-complex
Message-ID: <no-crypto-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:00:02 -0500
User-Agent: Sample MUA Version 1.0

--e68
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="f70"
```

```
--f70
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
no-crypto-complex
message.

This message uses no cryptographic protection at all.  Its body
is a multipart/alternative message with an inline image/png
attachment.

--
Alice
alice@smime.example
--f70
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>no-crypto-complex</b>
message.</p>
<p>This message uses no cryptographic protection at all.  Its body
is a multipart/alternative message with an inline image/png
attachment.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--f70--

--e68
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--e68--
```

C.1.6. S/MIME Signed-only signedData Over a Complex Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses no header protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 5253 bytes
  (unwraps to)
  └─┬ multipart/mixed 1288 bytes
    ├─┬ multipart/alternative 882 bytes
    │ ├─ text/plain 260 bytes
    │ └─ text/html 355 bytes
    └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-complex
Message-ID: <smime-one-part-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:01:02 -0500
User-Agent: Sample MUA Version 1.0

MIIPIwYJKoZIhvcNAQcCoIIPFDCCDxACAQExDTALBglghkgBZQMEAgEwggVMBgkq
hkiG9w0BBwGgggU9BIIFOU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjUzMyINCg0KLS01MzMNCk1JTUUt
VmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdGl2
ZTsgYm91bmRhcnk9IjkzMSINCg0KLS05MzENCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21p
bWUtb25lLXBhcnQtY29tcGxleA0KbWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25l
ZC1vbmx5IFMvTUlNRSBtZXNzYWdlIHZpYSBQS0NTIzcgc2lnbmVkRGF0YS4gIFRo
ZQ0KcGF5bG9hZCBpcyBhIG11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdp
dGggYW4gaW5saW5lDQppbWFnZS9wbmcgYXR0YWNobWVudC4gSXQgdXNlcyBubyBo
ZWFkZXIgcHJvdGVjdGlvbi4NCg0KLS05MzENCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1
cy1hc2NpaSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOiA3Yml0DQoNCjxodG1sPjxoZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVh
ZD48Ym9keT4NCjxwPlRoaXMgaXMgdGhlDQo8odG1sOyBjaGFyc2V0PSJ1
bGV4PC9iPg0KbWVzc2FnZS3A+DQo8cD5UaGlzIGEgc2lnbmVkLW9ubHkg
Uy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWREYXRhLiAgVGhlDQpwYXls
b2FkIGlzIEgbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBp
```

```
   bmxpbmUNCmltYWdlL3BuZyBhdHRhY2htZW50LiBJdCB1c2VzIG5vIGhlYWRlciBw
   cm90ZWN0aW9uLjwvcD4NCjxwPjx0dD4tLSA8YnIvPkFsaWNlPGJyLz5hbGljZUBz
   bWltZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tOTMxLS0NCg0K
   LS01MzMNCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVy
   LUVuY29kaW5nOiBiYXNlNjQNCkNvbnRlbnQtRGlzcG9zaXRpb246IGlubGluZQ0K
   DQppVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFB
   QUFjRWxFUVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95
   d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1w
   TDJqbzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldS
   V00vdWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0K
   LS01MzMtLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQw
   DQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
   V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRo
   b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
   BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
   bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gB
   UCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXP
   mrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEF
   XgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41ko
   aZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX
   +TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iP
   sIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
   AWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
   MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkV
   fAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJ
   KoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtK
   tl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3M
   RsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0
   LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXw
   fDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyu
   OfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3
   QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElF
   VEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNB
   IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
   OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEX
   MBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
   ggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo
   7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+95
   0MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYW
   Tut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfC
   n+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9
   COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
   ADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21p
   bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAw
   HQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwH
   Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4K
   kkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30Uxf
   yrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HV
```

```
X524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP
0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+
JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSz
NnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkq
hkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzAx
MDJaMC8GCSqGSIb3DQEJBDEiBCDw/DGldVr1aM/U2iIYH8C6YHSKLUihv8FIEUZC
JPECvDANBgkqhkiG9w0BAQEFAASCAQA/sn8ReNdvJH8O3Ejzs7eF6tBy6DYD5dFE
aLVxB6o3G6qHcupmwvHvL6zouALUoh+zkYRxuWNcPQGfbUqXoAC2cQ6ejwtz3Qnm
4L6amZZQC3NnwFfytOrIvGrMdT1M/39igmep2ZUq9BQS7vq0mYQzSgkGm148yOfI
QDeuJZGcw1EcFZuFUZPX4J9kvUu5twvDQoPnTitPVGJ9C2lB6PRkYjKW7JAmNtBL
qRbwZbtOjbrhAszzkRG5P8jR+35FIkG6abSF8hwYix0fJokUn3YnU7G6pRM7DSGg
S9MtDUy34GTkdUQ7OXFlLa5kpQfUFBbQ5qflKUvIrBsYX6qjWAVs
```

C.1.6.1. S/MIME Signed-only signedData Over a Complex Message, No Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="533"

--533
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="931"

--931
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-one-part-complex
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses no header protection.

--
Alice
alice@smime.example
--931
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

```
<html><head><title></title></head><body>
<p>This is the
<b>smime-one-part-complex</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a multipart/alternative message with an inline
image/png attachment. It uses no header protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--931--

--533
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--533--
```

C.1.7. S/MIME Signed-only multipart/signed Over a Complex Message, No Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses no header protection.

It has the following structure:

```
└─┬ multipart/signed 5230 bytes
  ├─┬ multipart/mixed 1344 bytes
  │ ├─┬ multipart/alternative 938 bytes
  │ │ ├── text/plain 278 bytes
  │ │ └── text/html 376 bytes
  │ └── image/png inline 232 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="4e5";
 micalg="sha-256"
Subject: smime-multipart-complex
Message-ID: <smime-multipart-complex@example>
From: Alice <alice@smime.example>
```

```
   To: Bob <bob@smime.example>
   Date: Sat, 20 Feb 2021 12:02:02 -0500
   User-Agent: Sample MUA Version 1.0

   --4e5
   MIME-Version: 1.0
   Content-Type: multipart/mixed; boundary="0be"

   --0be
   MIME-Version: 1.0
   Content-Type: multipart/alternative; boundary="cb6"

   --cb6
   Content-Type: text/plain; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   This is the
   smime-multipart-complex
   message.

   This is a signed-only S/MIME message via PKCS#7 detached
   signature (multipart/signed).  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses no header protection.

   --
   Alice
   alice@smime.example
   --cb6
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   <html><head><title></title></head><body>
   <p>This is the
   <b>smime-multipart-complex</b>
   message.</p>
   <p>This is a signed-only S/MIME message via PKCS#7 detached
   signature (multipart/signed).  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses no header protection.</p>
   <p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
   --cb6--

   --0be
   Content-Type: image/png
   Content-Transfer-Encoding: base64
```

```
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --0be--

   --4e5
   Content-Transfer-Encoding: base64
   Content-Type: application/pkcs7-signature; name="smime.p7s"

   MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
   hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
   KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
   MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
   dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
   BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
   ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
   acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
   yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
   Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
   N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
   B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
   arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
   AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
   CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
   8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
   hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
   zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
   jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
   zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
   A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
   qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
   7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElfVEYx
   ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
   cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
   MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
   A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
   AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
   a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
   /evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
   SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
   saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
   ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
   BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
   ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
```

```
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzAyMDJa
MC8GCSqGSIb3DQEJBDEiBCDQTcb+2QaMhBSlslOnLpojyHSnq4gNzFYU45gwqAHj
7jANBgkqhkiG9w0BAQEFAASCAQCYM1/HD0Ka4aZwwLS4xMGoyFzGn5G2C3ph0jKS
mCVbpfAxeHnsnuFjdCYzgN/mdBCOQs4P2/rBGWy3DpDHnKdaB+Q2/IZmI1UgyRTM
oclbWWQfTLX1BuI/mJKqHBhJn0y17UXCUAnvSoYGFhjmqTQStR3k4PsdJod78pEa
9+Yx6lBGVyznuhHaGuB7lh/S9pxAYtoJFUuIVq+frSN5xhmisPXluFHC3UPu3Hyb
3w6gm+bTL4NDNWwXXSn5wfm9Ru05b3eAEv9pADPZ2TKZPxzrfe4wPNzArgYwdn3k
6NdLvgw4mZmSSiOyOlfKo3cgo4rZuN6CeLCgqZ0GjIJS43v+
```

--4e5--

C.1.8. S/MIME Signed and Encrypted Over a Complex Message, No Header Protection

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses no header protection.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8710 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5434 bytes
    (unwraps to)
    └─┬ multipart/mixed 1356 bytes
      ├─┬ multipart/alternative 950 bytes
      │ ├─ text/plain 295 bytes
      │ └─ text/html 390 bytes
      └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: smime-signed-enc-complex
Message-ID: <smime-signed-enc-complex@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:03:02 -0500
User-Agent: Sample MUA Version 1.0

MIIZHAYJKoZIhvcNAQcDoIIZDTCCGQkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAAWNP5pH9dbDPUdHQXSo0/ngHl7DGuH0uRFS
i68xp82mLO/liolbzronottFipHvmMHYZ+dL6fqVLlqY85FtCp/6r6iklmuQzP3g
TGRtiY5SvNBnm9bqSMcfOwHRaat7gKVKLktFXeQN5vUmaxW4H+RXBQHFXpoTljF7
z/z2oPxLYiazyV+srwrlSF7N8NvwXgtewhV/GDQZKGZEqQlX4XPRy1XDPdi+vHwU
0gxqwRzAhAkN8sAIs+82yMFf+OE60fqI+pPWxrR0YIEXEK/DBl4e1yA0u+keo/eD
NWFKE7g2BihWcp10wDEZHqEupPPN52LCHihyzpBdG0ubSpqYm3AwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAEALPDG2li48vBIODVbDuAZnJ
AIJPGuV9pVAU6AQq3+WWPd7kx8ct2WJPWpUOoKsvFyyNsTc8n6lVTrwflR1AcGhj
kkX7VGb71lpnC8ygaSqPF6KtkMICcW3nNdXBuqYR2n6npGD1z7CzElQbMgC53Ell
VqC56yHjeSiyLJKyyZBq/0bDjveFHndHCWoIQG7f1HcA8CY4bNNTC6YzQhQNbc69
hS+S+WwjOtpmNXLVZq491Rs1zPOUN2XjwE638rUqe1M/McBAwAXFQ+YBPdjWhiDg
SrAjN8xnTyi4XJIdabs5RIVg+NWDHuhdiTlzU8M5kY2ShAuGHY0FO445l/e/CDCC
Fe4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEGsnW1gQI42Orjxx3Fn9pySAghXA
P71fxkSiJhQ9hJFUk1VtxPLYVxD6RroosTILpBn/eB28fOyA1z5pIhzx6CH35SuL
MzuFsnN99/LmvOe9z9Dc1UCrWLUhod5uVQilrdouxXljMdZlNGDj1zc10+82ahAP
KotYU/8AmtUHiGGs4BVr9tl5fBF2l72KYhlh1MHIU8x0C99vqOq41vBqtC9cmCzS
ht9TxlwRACQgAxADyzSKMc2rtqkAEqGRNBHxq09KxI9pJ6qkj3rQ5aL+epnkYoGN
B5thIQCoG7x/jNzN+mRdtvi3LhM7Uce1TU0N83VoBxpiH3o04re5CUb8ELEYssmO
4ZN/5AFQ3RQyZS0z1tgWzahrzo91VCvbdnM0irtXZPjpS/NoR/0ZokjE5Iw3SnJZ
35gdvu48eGStmKDFiTs/TXkuPQcMd2aO/joDD+/XNtuSdatXWp+PvELMYR5Z4Pbz
KMo1jMj5n3j/O+6WF8Fg1Dx8vr9JwHTP/4FFjh3qC1aMZxh4PjLEB4dD8rWJQdJA
p/3wS3+d+0kSkhnjG2dT5/6MtRwX5HFQlrVEAbdBIJee0GTAlLn974Li9JiutWzz
sVxTyD+6IBTYSoKQVbL8Th29J081sh5OV2bZ7EFpU6iwWMTEjKQBML9PLs/BO3ME
ZOsd8Lh3+RLMm3hsCh6ixAyDBX0xJUpW5dbbnKMffsUwdRxBBoO8rMFjURSSfJ4G
HzqXh1Lr5XEoKG7UQxW/2brMx7gf3OXsKq0YWQ7t6eniMkItu/lcndywe58q9nZF
h5NmmXH7Wf/YhcH3HywFXRv/0tSs3EgpjIgwGbeggwrND8LKx15kdRpT8egu6sOr
b4D8PhzYwKz87V+6fd6rDBvarWD6Oi+t847eVdaGPZ3qVVaMlQs5llAzLPUsqkU/
zLIL1c1SxCSoFWebd81CJ/6khs8tWpoiEQugHMrjyLykbax+jHeA7UD4+XZhgaBN
j6VJxeiQ3Euaqs6NdVe5KLGQVcpRayoifbsI/NogUY2WM0pfccGHtLA1KbZga5nX
ba6kox8cLSgf2w4B2CGEFAyl/yCXIvEbJE+L5vMYLd5dtW2UsR5HeD5i8NZ2+hYC
oDq8hcNYSCt1CX2BTd7bCrCOaP38pl2Q+k0VV6J2y+lyL+P5hVtcYOXaOfQqWjhf
7tpMXmMGqiaHP/Megtx5x9pudrERLHpJNnF57kx/YoiDOfKPSxNmKMfCWkJFOr/H
9PPYERlir51S62YQvqW9s2rwhjCSiL/YQVXpGoR16JRmcIBOVMsT4a9ArSFUdKNt
```

```
   7x30W+CQ0ff4U+l0sfE/jfLwtPB29h1i5JFvbrzc9oyi+xDa4Iy/St4bbS6wulQ9
   lo7PgPM/Oo8/Crav4vd20tKhNQQuR9YaC8a5n3fnclF256tcZunUg2G4MVm1ZJt7
   oVslu/jaywsluQWdpA8ldSwnDq4wOFN5y9xCj0UgCaYqRSwB5auAlCUo8WXyIkyn
   rhO+TwOigrJvZ2AgJjxh31CqClADwN2jBYkooDE71YfOOXjR6a8LBWrS4jCyInqu
   ykdEdDcr11peNN0AhMKBfD670Qp/eQWtcrjWuM3qOsZfSF6YuKQJb1t0yRQontpo
   dWFHw5RNI5p5lx4bl31XfpQ+dg6JECpbgNjcP03tVRMzAlvlj8m0P3dzr8XBr/8F
   c1128rmsvIGNWPtU8N6sAzBvWC3hnuq0fmiyvlnF4+lk5DJWfXVPHtMTc24xOp0z
   z1gM7+x/v+SIQuH3VvmEtQCCKtEXUHw+sSYRhAlwG1h8Ii88RNgg6TpTqicX2OpX
   WICs5PLwa9BnYk3IAgyWfHhYEqY4ZYbq3lMnkaCZ0G30lXRqIZtumMTFK0j8RFt6
   YI7wtpXImenNYZ0VSqSlS5hwLrYR3BjxjVO88ZhUao2cA+c+Gdown3j/v+BpkJgf
   5AvNcx4z29oJmYq/lCcHU1UHIuKdu/zyMgljgJoTbvtLB/HoIYj1BCgIoknhrWz8
   Rxsxdl+TUpdzN0fQw9jmzsQdwpalTL9gitqjeky3Lt8mfw+rl1aTiPSS667pZebq
   fBdh+FlokKqhprCFYZbD8lV36anMHWkbDxj4/E1Ba58jZbC1w6GDdQ5uSLSXgbGw
   vb255hmcWco8N78G3nsWtvygR9P4zRjfu/KM9IPzReHeQkE1CispMCf7Zx6+LJrF
   wlW4Vl7l59d5qlKODKgInUpjGrBZo06/rb/QJYmh0CvAGbKVUnX7sWzoGIbzTN3g
   zGEV/yAlROQDEAnmCoIKieVlThjDf++eUKiDbdbkhRP4OP4+b6DhSSdk3olNCQ/G
   PO1HfVna9diWNUb35TsUy067EsNpNFlbAJ4/3/e46+h8JxSiD97umeFDeNECO0JA
   0PcKX7x6kdFYZ7StiQWIgkK8lXrSv22vjdrHAUx0FP2m8mgnkWrOTeFRnvAZdYem
   qUTR6g+eqq6+H9cE+VYutjzStfx5b8y34VEr6SmqH09yBggTG82zYii0o5d2qmbE
   riuRHabQEt9ybAeY4BjaBR/o3iH2G45KVVUrOPlvXvAoGCcgzCMHqRC1zOZzcDO3
   fXD2LSPHqf4IcqQcPetejTSiLjdzjkBsw8EZBCfEtZN3/BFyZRm7giiL4qLb6dM+
   p4yzwC2qHe8g1AFhUx9BwynN8iSRgBQzCIgA6A8kdXXwWAGJCygs3FUKZ4mBO0LR
   YxElYI9gaOBifFWOmdmLauNc3Lc9zORmd8X9vjLsEWcY5vQWQ1Ao/Yfj5cdBf3lS
   jrDwKQf0B+Het9Y64x9wHrzsTyF337+PPVtw6PIru52GBk/Zcn/sCMmgcS4R7igf
   eIyWagLmtwKrlZRGb8KYyElMDM5gT86ptGJyoyAhRz2dlvuHBXuxYZPlIAg1Rtql
   O+rj/0d6b0ZfJW8fLhba957Gf0xLldXuuZIMqyJ+yOK20rsVWyYsR5hE4kXqXghs
   aIZFbIsbSIfhRZopjKlUuVx6IPrcQ3qMmwlhnmGTTmDR//N9GRae8OulQmWkexdw
   VzPflEjb2gTpBhNTEFvP4KePmBoKtFVjfSOF+OezE6aKDr1RID0ux5k1HgpS1gMP
   CKFJmgCs07bKgnWiAYgEiYKIocXMvJAOZnzlXVuly6XxZk+SHqUggDnINxKusWwy
   a+SrV4vgeQWs3qTFGvTKRGuRfygPergdA2h/Ra9VSJVARv08Ifo9e/H6kCq/ZaaM
   qJoXVKRUp4QRtHdEV3e2qUcGBS00EGlxEpNBT9kp1RHnGzQGKDPQGTpeSwkZrVzP
   NAW+cgRaCq3ebuGWZYddUpRH6cUhv9+/GYxA+g2LNtKu1544vmar+96nVjLkscw6
   Elyl/xc4q5ADYEErCjgJTx1bGBH/lKdHGanC0JVKld+sImlXGy2BVAzR+fCYSAII
   Z8WkZcu/Xkv3pVYIx/tnl8Lx8kktJltyxkm482hUnzZy2O8knv6lJr+BbzkvmV9D
   mQJpjowoqG79tLqaJVuJtFm9IleTMRLiMxQ07TgHpd6GTpy6OSUks/F3Yn4ZYOa5
   5lPDfuqK6yB54qXjCCGKuRWji/z2B+qdE+hL8RCUXBlKfr5Cvs0SpNKn4ccFrVAa
   SX418VQHSlJZtwmRVeyX5LuCznF+g+vnn/g6h+fwGqzVLU4napv2IdU0ULxSB3eU
   sWEzhcI7JRUsygOEeseQ/0N8WydYwYU8CSGmygTPfl9SIOojZowc8dZ1yaU037GP
   /Y+7O7LyOHZXxheMVBomZTenvyfhRsHiNXgYRIRkL3YSCVmzh1oTN+IOXoLYxWVK
   pHhzOselv4Tcy9wPzKdMOh/YBl1LLyskl6vXElLo45jTFpUr8SQ1OIxH8eeeUfw8
   PJ6yfu/w8gwk6R2x9VbJTrYHuI451oKNZ89jHhhPH1x+PDjOV3ugKabNM0JD9u1G
   t5fN+kFz8A3jKMAtkaBHHFmBJD8Y1lmRPazRSX8EF7hvtU+YgIc2z5yULwny2LWL
   VTRQyGoj/NDDRRt9MsPf0ZBLvVBPHcJWdWY4kLQDPCE5CrH8F9fsIuh89icDUMUP
   yOjI7rCydpceJdvOv65SSscf63MRdsZvYwOm1JgRdSqki8e+qy77o12qXw5eTeIV
   7T+YWRbO5lWuVOZOJPv7tu3rdTCGslsTAe1FISU3AzrB9fNG5eHNmPnjZ1yqOlpL
   J9BXVvNmWN2cVLutEfimcVRW/aeWuY3+HgSMHOhiqR92mRN6VY6PbdQ+rT914fUz
   Vmy5LIN/kZjdeizQyTdgfrRG9pGDEimdlPPia5nCxhCwGqxkGPezjzNEWzHo/C4W
   knfRMJpMbUJqZVe5uOSE466nhOKIF8nmR2fMzYYpnayCsJoh0AgghIAh94OFGz/T
```

```
   Fp8hKykir4JuzspCI43sGwqZFVICfGOEtisIjZhPUn4VTvxdXsjMoC8ebVUpiMsw
   /IihAFjMc5GdU5bP/F2oHiRh+B4e8OnSTdzS7PXb6tZ1g7ccazZ5ezp3rEOc5Q0X
   yJ/UBiy29VmvLNPV5JBsZQdqCOkOHfz5zqXqnZLdp9XjuW/DD4uahd/t7fWkAjk1
   IN82Om8GTMjrKSblbvSHRXXQk4sDC7+4K8a6M6hcDXZ51ggDdJkqgGDeyoquA2Za
   +AX0XQPozqryfKggqqLL0kmBtfz5PJzDkgXof1VrbslAjQ4VsFjsIKeb4igc3IcS
   snPjPC0ujVK/UpKOnci30yo6EreEsxvoRml1jUZ2NZycdJ+qGxL9hK5GWfqFxGDp
   6eqt5X/bHLs+BK5R6G7qZRgk11zsMI+OLj9wkNRf65yxdWiREO/+0gewAX1sWbxI
   soA6zPzvjk1hnz+rOHnip/ak+QIcdEBMWfUIpJXd92MW57IH5g93CL62vO/w2Kom
   AoBVbHSbzFj97vbc6umT2CTM1F7NS4Rxb8xvuwgLAk11Li9QBhMcm47u1l84Jcuu
   3IW6nC1v8SH77deDefBYZQJaeBH1HiBoC5Md1LgwP2EKYPEACnn0oPXW4hOjBRT4
   yNVviniI7/4Pwdux39cDeXg4GbM3FDRtD/4srBF02pl9A9UsADNE6h83bCBTrZXb
   9SNeObOhZ4sVXQ8Ofj7rr5oI8NmcFeI5wcogypd9esWitWGcE5i5wC+3n9nuFvfT
   X8yOkEDXwDzR8qWgG1rl6A6JZnCL1N2fYJHkiOpu/NuFDCCXrlA4tvI8/E2ZmYy7
   PtcEuz0NmkxK28pxKXleGX07ioVVMy6iHhEtGuotiFXjT6USG66KenDcXXRSle+O
   T3ICsHy7b29G9D6ZKxgPA2KlOa8oTvvaea5ptclHchK5WCyRcvdpoei1Vz75K52p
   HThqwLkRD7blE/iIva2R465ghWQLV/lc6L4jPIX6YQXE+uLt5TWQkWZ4gNsBVKds
   KMgUQdy//yqmqxjImRsB/3wVcp947YOzbuQNKHH4Yn2cfsofnuWQRN6O0glCtX7i
   HH1WTu4d16i2oDzWkgBhvfgJMwRFXfytDvc2AaHeBvzTsItyW6dV2YkX/P3Cx51e
   8zTSzM/+ZLF02Mg+kY0+GUaJohjx06dt45xKSbUYq4beE22VVZO44ObuDgNPv7by
   dp86PRFz7yLNKvglqD3XFg3EtQsG2YlS5TpGHqQe2ZxY7inlFzdnktxYAfJrXwkb
   LGLVPNM0OipwTpPnAAShzwy763OX/Lh5Ou7MT2B7C08tCihanl3gQqvZvQ7ufNUF
   3edpbAkvv23lVXIMPFCssgMpGFFnG9NogqXHJc5PzTESr+p7QuH+gvySHvYYkulh
   w7ZtNiBBd7qu6ire1igXaYN0gVizoIyDintGWxHTaL6fN0AYf2CJRzvragn03t86
   IkVIStrRaKh2eyZlwmG84wN4Vuj7dNARVcyK1HTIiz+zjReh2ouRW6ZMw4SVA5Fk
   dUlQAHMmM4NG+BSek8qxIG02VXkaD+Bw9Z9oLcjE2lRfxc5QYc0smUD41m/dqbs8
   kDYc8I1ONlf19073hZmAvqpDSIO/R2OF6v2rHpxRGgoY3GGz3vz1U+sAzwCdT25A
   rqPwvAIS3ocPUXbzbX2BpoItIhM9GR+zy0DVxZ8rdGuisokRNaa67lzEsn3yTHth
   3firVDH9ASlmKYJ7Igf/51Ms2KNm90x5794cE4KJG6k6I2exALrWJXEjdm+A2br3
   O8kfGY7mi6PrkKyFLdTx6m84bSkuIstdfXvq2rrdS1eTqmEppIEuSx5i34L9AlY8
   qMiUbQUpThLhoQ0fdfrKAAdJRPEYH8nn2yoiZnmEKaH3N97cRiYDZLa/YBZXGnny
   O6uh3wezJRYa9QpSQH5mubiNC1fBoHzHGQEyTEZUaYJqqjAc4bx3yyacYnFTEPtX
   mOT2S4o9Pz32f6wvOBT6xJzOFEMoh25gURmymISZKMU1pFePNNTmmP6x1K4pI2Pi
   VAJUuyS7OARkdnjKwciPFU7VB4JubPvsdOTpihU4MzngSuohAcUhvRFYDNB7CwgU
   igyOSURUVw0RnNslCSJxnalxpenfouN6vfuE48wkOtq/vGnJkiepuyuDm7b+qO0Y
   j3iTqIJYVDlo9sNj1zjFN7T/zWgu5w32TU70eJ82PpBtjOFgWyaSi8dQGZgf4oxt
   OhMKjRQAXPJs9f/NZzrR80oa04EZrTGoYu4+T97e5S19iyxKD4cLciqsLVAPISbh
   BgYR+K6yHPT86vhql4dOrg07l9DYt3G1RiDHrCe12YA5iuNBBF2Wxbt5wZl29cdr
   PFmHJvYg+jIC37UYBw9qv2ABsUI8AUJc8gMqvylNIuilwBPz4hYfo/AAYZe+o40i
   cKwLe/UamiqdfPOVQeeN/BkXXaqr2EPDKUSeaShDrui+VKTvgKbJDbImWJjdhjQd
   6ugnYd3ahi8Zk3+v6Taz0a7ZUtnGqvarOX6S4EH+h8H+CnLyuOPron5wJIssCMD2
   cNDVB8a/n26EiQUG+fsakGyCIEqin5nSSdzgBlDiM0ghav5onizmKyqxHtHjZvRP
   /1tGNa0yDwgfSDycM5QGsMD4JUFmozQ/NZsNeGfJEjyZpsI4v64jzcs4QxEbJoDP
   /K8v9kiCQZ3NtkHGDRcUBWNDbKij8wgOPAJmHweFIA6UnHoqJdbPzNwsAAjMVN2Z
   vtvsfFtuDu5BALHyKAlf67WbdKfFYqfktnmR2rPXa5U/3WWiS6cOLly6h+cseQvS
   bPn77hbn6y2tRQOIMstJ7pBIlim6m/duKc7PZz1u/tANP/gKkHzthMyAErEOPmqM
   Plfvt8ju0UpwGpiF1T1E3SRodx5/q8NV6TSKANWeKN7nahusiB5CVO2EclhjATXR
   XmPo08kyxwYYK7P+oBOXsE2gM/uZy3If5hIEfmxxJ+5F19cNiotTQwJM7Jmbag1O
   MtW7IWC7g+sDYln9L8hCxnCjoH331ss7c3470XB9pTy8EBnRdX5IRW9QuoRcMcZw
```

C.1.8.1. S/MIME Signed and Encrypted Over a Complex Message, No Header Protection, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIIPaQYJKoZIhvcNAQcCoIIPWjCCD1YCAQExDTALBglghkgBZQMEAgEwggWSBgkq
hkiG9w0BBwGgggWDBIIFf01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjUwOCINCg0KLS01MDgNCk1JTUUt
VmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdGl2
ZTsgYm91bmRhcnk9IjgwNCINCg0KLS04MDQNCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2JpdA0KDQpUaGlzIGlzIHRoZQ0Kc21p
bWUtc2lnbmVkLWVuYy1jb21wbGV4DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2ln
bmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQpl
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMg
YQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIG5vIGhlYWRlciBwcm90ZWN0
aW9uLg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLTgwNA0K
Q29udGVudC1UeXBlOiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlN
RS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQN
Cg0KPGh0bWw+PGhlYWQ+PHRpdGxlPjwvdGl0bGU+PC9oZWFkPjxib2R5Pg0KPHA+
VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleDwvYj4NCm1l
c3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMv
TUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQg
c2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5h
dGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVu
dC4gSXQgdXNlcyBubyBoZWFkZXIgcHJvdGVjdGlvbi48L3A+DQo8cD48dHQ+LS0g
PGJyLz5BbGljZTxici8+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9k
eT48L2h0bWw+DQotLTgwNC0tDQoNCi0tNTA4DQpDb250ZW50LVR5cGU6IGltYWdl
L3BuZw0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50
LURpc3Bvc2l0aW9uOiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FB
QUJRQUFBQVVDQVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzcz
OW5PM1RwUncyMGRxcGJmQVJRWpPeXdpd1luQ3RrREtuYmNMMazY2c3FsVCt6dDlj
aWRrRSs2S3drWg0Kc2dyemZjVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFm
VFBSaWNpaEFmNVlKcnc3dmp2MFppXUldNL3VsaQ0KdmRQZjFWRjJrREQ5eHBwZDh3
QUFBQUJKUlU1RXJrSmdnZz09DQoNCi0tNTA4LS0NCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMg
UlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
```

TtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDH
dZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy
6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMC
BSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdao
x644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtl
uLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vR
hZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
NO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwID
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
JOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4P
GHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkq
hkiG9w0BCQUxDxcNMjEwMjIwMTcwMzAyWjAvBgkqhkiG9w0BCQQxIgQgXYQxbGVS
YbD1RRyrYjMaj8vm0wJceMeGDm9qv/JsQlgwDQYJKoZIhvcNAQEBBQAEggEAbtxK
BK0ie88UC9KGR0/nHIWpXJOnN1/tXtEWsLoypwYiw8XKgcN8zgZ06RikcGX12ijW
Gz2wgA2yIRfnzWBvS6zmBc9r37klP8uhB0GgPrPFTtq+GeLn9hUApYQTb20HlSKM
e34oCU7qv0lYFfN0sDlwxkha1X3AAg4QFcUrnLJRkYFWDH6XvxsHNiLznwsF/+B1
uNiPIi7rhKgG3oLYu4H8qGolM5H+gyl7+h4t8hUHZVTxZ6QyTO0K+D2JO8aazcor
PgJsa85BUfcx0JXsixcqtLzTAfsPOAQBl1CUHEied1qX6nlMb2gCxP6psFEXPRGM
rxSLzwv5QtKJCaDfYw==

C.1.8.2. S/MIME Signed and Encrypted Over a Complex Message, No Header Protection, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="508"

--508
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="804"

--804
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no header protection.

--
Alice
alice@smime.example
--804
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses no header protection.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--804--

--508
Content-Type: image/png
Content-Transfer-Encoding: base64
```

```
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--508--
```

C.2. Signed-only Messages

These messages are signed-only, using different schemes of header protection and different S/MIME structure. The use no Header Confidentiality Policy because the hcp is only relevant when a message is encrypted.

C.2.1. S/MIME Signed-only signedData Over a Simple Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 4189 bytes
  (unwraps to)
  └─ text/plain 233 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-hp
Message-ID: <smime-one-part-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:06:02 -0500
User-Agent: Sample MUA Version 1.0

MIIMEAYJKoZIhvcNAQcCoIIMATCCC/0CAQExDTALBglghkgBZQMEAgEwggI5Bgkq
hkiG9w0BBwGgggIqBIICJk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1vbmUtcGFydC1ocA0K
TWVzc2FnZS1JRDogPHNtaW1lLW9uZS1wYXJ0LWhwQGV4YW1wbGU+DQpGcm9tOiBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJvYkBzbWltZS5l
eGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDowNjowMiAtMDUwMA0K
VXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXBl
```

OiB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1dGYtOCI7IGhwPSJjbGVhciINCg0KVGhp
cyBpcyB0aGUNCnNtaW1lLW9uZS1wYXJ0LWhwDQptZXNzYWdlLg0KDQpUaGlzIGlz
IGEgc2lnbmVkLW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWRE
YXRhLiAgVGhlDQpwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbiBtZXNzYWdlLiBJdCB1
c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbg0Kc2NoZW1lIGZyb20gdGhlIGRyYWZ0
Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQqgggemMIIDzzCC
AregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0w
CwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxl
IExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0
MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMI
TEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeN
SiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+Ithj
LeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/N
kug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSw
qpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQ
ury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwG
A1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWB
E2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0P
AQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSME
GDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4
oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIu
s8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2
AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gz
nbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqH
rg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RH
NrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcw
DQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/
T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5G
Otz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnf
itOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjG
sgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/
N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ
45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIc
l64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xii
dfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2
lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh
2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2I
JCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcB
VyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUx
DTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1w

```
bGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/Qqmi
XDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0B
BwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MDYwMlowLwYJKoZIhvcNAQkEMSIE
IHBk91pcJj0zJrTyROHOdfUnQMoctIHVb6WXTpS3gYxlMA0GCSqGSIb3DQEBAQUA
BIIBABWhy/yIy9RLS3OdZZTlUNChBhzNHjpSSoL3v0JmzOHeYJVblzBgpyPU33Tu
JALxlGuGp4ybO16yQREHMXNFZJkrqWcIAMZG/4tG7WIHXm0AGIcxl8BKKEpn8t1m
kiOO/NWzFY9TW1pYd/+CC7Q8Asc+S2Nd269HGrFFpL36r74Gt2xJDxn11N3coBh3
khaFt+p5GkqqrNUtfGeo0ifF+66x/oW9A/AtNE+iKwx7mEtukOhBgTXgyr3bi+ev
sEQzWYVLyVS7TCsCM5A1LxHZHv5gVcX1EMTZi7rRaNKKEmUcA9vbJYBSOWlmR/o4
FeLYNUvUvFXvV9YCb/0R0pgp9Aw=
```

C.2.1.1. S/MIME Signed-only signedData Over a Simple Message, Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-one-part-hp
Message-ID: <smime-one-part-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:06:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="clear"

This is the
smime-one-part-hp
message.

This is a signed-only S/MIME message via PKCS#7 signedData.  The
payload is a text/plain message. It uses the Header Protection
scheme from the draft.

--
Alice
alice@smime.example
```

C.2.2. S/MIME Signed-only multipart/signed Over a Simple Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a text/plain message. It uses the Header Protection scheme from the draft.

It has the following structure:

```
   └─┬ multipart/signed 4435 bytes
     ├── text/plain 250 bytes
     └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="78f";
 micalg="sha-256"
Subject: smime-multipart-hp
Message-ID: <smime-multipart-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:07:02 -0500
User-Agent: Sample MUA Version 1.0

--78f
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-multipart-hp
Message-ID: <smime-multipart-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:07:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="clear"

This is the
smime-multipart-hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a text/plain
message. It uses the Header Protection scheme from the draft.

--
Alice
alice@smime.example

--78f
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
```

dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNTA3MDJa
MC8GCSqGSIb3DQEJBDEiBCAIw1Q7hUXhrDaz3lXMFP0A3q3nvlhWh9ejLg/g9kjk
vDANBgkqhkiG9w0BAQEFAASCAQAcl0M6ZwFAzFvsP+/siWSN0EM0YWxuOzvCmSWC
0QwnAQ/dSwXcKMcej0wWMKTDTQSYBUjxFVE0chcK6FMH2gHDVb/PztWrSECmvh6F
utJ2SRxs0uGrFkee3hR0kowuOu9pDXasLtWP2MnB5pSMWX5QMpya1UxYcbIoaUOx
Jeu5zjbYf/Oo2tINvZHP+r+wxQZ7qTaEzviQ+IV0KoJanfU3Qd/giS6MuySwozwP
r3E7YAy3O9dZT7zL6AR5CsC1I0coo7X1PRNnBXXLMEcR/v5cXniGV+GNf8xYaiGA

```
iT9IwijZa6psfTSFjzUWTIc0jGx3GcLZr+BIm+MEBCSRzDum

--78f--
```

C.2.3. S/MIME Signed-only signedData Over a Complex Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 5647 bytes
  (unwraps to)
  └─┬ multipart/mixed 1570 bytes
    ├─┬ multipart/alternative 934 bytes
    │ ├─ text/plain 287 bytes
    │ └─ text/html 382 bytes
    └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-complex-hp
Message-ID: <smime-one-part-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:06:02 -0500
User-Agent: Sample MUA Version 1.0

MIIQRQYJKoZIhvcNAQcCoIIQNjCCEDICAQExDTALBglghkgBZQMEAgEwggZuBgkq
hkiG9w0BBwGgggZfBIIGW01JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1vbmUtcGFydC1jb21wbGV4LWhwDQpNZXNzYWdlLUlEOiA8c21pbWUtb25lLXBh
cnQtY29tcGxleC1ocEBleGFtcGxlPg0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1l
LmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6IFNh
dCwgMjAgRmViIDIwMjEgMTI6MDY6MDIgLTA1MDANClVzZXItQWdlbnQ6IFNhbXBs
ZSBNVUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L21peGVk
OyBib3VuZGFyeT0iZTJlIjsgaHA9ImNsZWFyIg0KDQotLWUyZQ0KTUlNRS1WZXJz
aW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZlOyBi
b3VuZGFyeT0iMjAwIg0KDQotLTIwMA0KQ29udGVudC1UeXBlOiB0ZXh0L3BsYWlu
OyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50
LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRoaXMgaXMgdGhlDQpzbWltZS1v
bmUtcGFydC1jb21wbGV4LWhwDQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVk
LW9ubHkgUy9NSU1FIG1lc3NhZ2UgdmlhIFBLQ1MjNyBzaWduZWREYXRhLiAgVGhl
DQpwYXlsb2FkIGlzIGEgbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0
```

aCBhbiBpbmxpbmUNCmltYWdlL3BuZyBhdHRhY2htZW50LiBJdCB1c2VzIHRoZSBI
ZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbQ0KdGhlIGRyYWZ0Lg0KDQotLSAN
CkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLTIwMA0KQ29udGVudC1UeXBl
OiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlNRS1WZXJzaW9uOiAx
LjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCg0KPGh0bWw+PGhl
YWQ+PHRpdGxlPjwvdGl0bGU+PC9oZWFkPjxib2R5Pg0KPHA+VGhpcyBpcyB0aGUN
CjxiPnNtaW1lLW9uZS1wYXJ0LWNvbXBsZXgtaHA8L2I+DQptZXNzYWdlLjwvcD4N
CjxwPlRoaXMgaXMgYSBzaWduZWQtb25seeSBTL01JTUUgbWVzc2FnZSB2aWEgUEtD
UyM3IHNpZ25lZERhdGEuICBUaGUNCnBheWxvYWQgaXMgYSBtdWx0aXBhcnQvYWx0
ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGluZQ0KaW1hZ2UvcG5nIGF0dGFj
aG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9t
DQp0aGUgZHJhZnQuPC9wPg0KPHA+PHR0Pi0tIDxici8+QWxpY2U8YnIvPmFsaWNl
QHNtaW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZHk+PC9odG1sPg0KLS0yMDAtLQ0K
DQotLWUyZQ0KQ29udGVudC1UeXBlOiBpbWFnZS9wbmcNCkNvbnRlbnQtVHJhbnNm
ZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdGlvbjogaW5saW5l
DQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZQUFBQ05pUjBO
QUFBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3MzluTzNUcFJ3MjBkcXBiZkFSUUVq
T3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3a1oNCnNncnpmY3FW
TXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmljaWhBZjVZSnJ3N3ZqdjBa
V1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9PQ0K
DQotLWUyZS0tDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaK
tDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExv
dmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP
6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp
1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6h
AQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXj
WShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2
lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/
WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpg
hkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0l
BAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyA
KRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTAN
BgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1
u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZ
ncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fF
o/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmG
pfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO
7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQIC
EzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChME
SUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBS
U0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1
MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdH
MRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOw
I2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD

```
73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aR
phZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65
x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL
270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8E
AjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBz
bWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIG
wDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCO
fAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3
/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffR
TF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9v
sdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkK
TM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4G
Wv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s
1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExB
TVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24g
QXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgG
CSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3
MDYwMlowLwYJKoZIhvcNAQkEMSIEIGbRm8jphDRUXRWIk4vxhAup+YZsmtrednWv
3iPoigWSMA0GCSqGSIb3DQEBAQUABIIBAEHG833PIy7iky9Ok2pN22fjSF6xtjlt
h1Pi4Eh9PSjQ5Rdrsv9pJFFsBhSLOXv+O8fwYfS1rUrgwsCVMO64zz5MT1Kj4Y4Z
a6ztE9weXTlciQydOWER6lV1BDP4GwUaz+BBCoKKB0DTHq+nPNo97XtTCUfo55Vz
55vmNXxqWQ952hzw+qxxTxKzdYApFd9cZYzvV4otZgtvZDu3sn6GWFCtVpN4+6TR
xClE93q+LZwvJyXFRFWHcKqpUfQ16ZAomBadrJ1RU3BmRXnC6DAI/J/yhm7OegdN
0Or/+EuyWAzp0r/GCsSGXt2owaAkGPuZf6kPc0mLhb/VFdeY16wy9J0=
```

C.2.3.1. S/MIME Signed-only signedData Over a Complex Message, Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-one-part-complex-hp
Message-ID: <smime-one-part-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:06:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="e2e"; hp="clear"

--e2e
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="200"

--200
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

```
   This is the
   smime-one-part-complex-hp
   message.

   This is a signed-only S/MIME message via PKCS#7 signedData.  The
   payload is a multipart/alternative message with an inline
   image/png attachment. It uses the Header Protection scheme from
   the draft.

   --
   Alice
   alice@smime.example
   --200
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   <html><head><title></title></head><body>
   <p>This is the
   <b>smime-one-part-complex-hp</b>
   message.</p>
   <p>This is a signed-only S/MIME message via PKCS#7 signedData.  The
   payload is a multipart/alternative message with an inline
   image/png attachment. It uses the Header Protection scheme from
   the draft.</p>
   <p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
   --200--

   --e2e
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --e2e--
```

C.2.4. S/MIME Signed-only multipart/signed Over a Complex Message, Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft.

It has the following structure:

```
└─┬ multipart/signed 5520 bytes
  ├─┬ multipart/mixed 1628 bytes
  │ ├─┬ multipart/alternative 990 bytes
  │ │ ├── text/plain 304 bytes
  │ │ └── text/html 402 bytes
  │ └── image/png inline 232 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="ba4";
 micalg="sha-256"
Subject: smime-multipart-complex-hp
Message-ID: <smime-multipart-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:07:02 -0500
User-Agent: Sample MUA Version 1.0

--ba4
MIME-Version: 1.0
Subject: smime-multipart-complex-hp
Message-ID: <smime-multipart-complex-hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:07:02 -0500
User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="b14"; hp="clear"

--b14
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="f1a"

--f1a
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-multipart-complex-hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
```

```
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft.

   --
   Alice
   alice@smime.example
   --f1a
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   <html><head><title></title></head><body>
   <p>This is the
   <b>smime-multipart-complex-hp</b>
   message.</p>
   <p>This is a signed-only S/MIME message via PKCS#7 detached
   signature (multipart/signed).  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft.</p>
   <p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
   --f1a--

   --b14
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --b14--

   --ba4
   Content-Transfer-Encoding: base64
   Content-Type: application/pkcs7-signature; name="smime.p7s"

   MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
   hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
   KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
   MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
   dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
   BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
   ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
   acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
   yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
   Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
```

```
   N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
   B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
   arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
   AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
   CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
   8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
   hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
   zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
   jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
   zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
   A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
   qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
   7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
   ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
   cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
   MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
   A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
   AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
   a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
   /evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
   SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
   saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
   ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
   BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
   ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
   VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
   8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
   G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
   RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
   bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
   7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
   OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
   MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
   RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
   cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
   9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzA3MDJa
   MC8GCSqGSIb3DQEJBDEiBCDKNV54rM1AYevevF+c3DI/JjX14STIx3nsp5B95mHf
   gTANBgkqhkiG9w0BAQEFAASCAQBWQxNUY6IG27ju4XS4aApRfPoBUjk6m7uUMIQF
   /VC9EpXLvWRkn6B9k7L9MMrMJPRKR03oCzimaPjTKH3JKTxdj0gWtb2eELmIaRWY
   nOTaAK/3/h2dqMbPXYXgmWRQPsgFs42m6zWF4CH3YpurTvQC5gB0PSEPF0BOHdcm
   77bRs4AcPf1mfGThUG3YUNXuJ99BKb3Zz3lQiTohvhti9eHRYAMXL/XdP7TLiGVm
   Ee7uoUREekXvLmj8C6B3z8fiTfiWlqENU7J2BkrVF0KgW5X9ANwhekNROEx6X05R
   NVcBYNKNxCxuKMbHcE47Ytt8AuV4NoDWk2yumc8T6sM0Wkue
```

--ba4--

C.2.5. S/MIME Signed-only signedData Over a Complex Message, Legacy RFC 8551 Header Protection

This is a signed-only S/MIME message via PKCS#7 signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 header protection (RFC8551HP) scheme.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 5696 bytes
  (unwraps to)
  └─┬ message/rfc822 1660 bytes
    └─┬ multipart/mixed 1612 bytes
      ├─┬ multipart/alternative 974 bytes
      │ ├─ text/plain 296 bytes
      │ └─ text/html 394 bytes
      └─ image/png inline 232 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
Subject: smime-one-part-complex-rfc8551hp
Message-ID: <smime-one-part-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:26:02 -0500
User-Agent: Sample MUA Version 1.0

MIIQaQYJKoZIhvcNAQcCoIIQWjCCEFYCAQExDTALBglghkgBZQMEAgEwggaSBgkq
hkiG9w0BBwGgggaDBIIGf01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG1lc3NhZ2UvcmZjODIyDQoNCk1JTUUtVmVyc2lvbjogMS4wCkNvbnRlbnQtVHlw
ZTogbXVsdGlwYXJ0L21peGVkOyBib3VuZGFyeT0iZTY4IgpTdWJqZWN0OiBzbWlt
ZS1vbmUtcGFydC1jb21wbGV4LXJmYzg1NTFocApNZXNzYWdlLUlEOiA8c21pbWUt
b25lLXBhcnQtY29tcGxleC1yZmM4NTUxaHBAZXhhbXBsZT4KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lLmV4YW1wbGU+ClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxl
PgpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjI2OjAyIC0wNTAwClVzZXItQWdl
bnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjAKCi0tZTY4Ck1JTUUtVmVyc2lvbjog
MS4wCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZlOyBib3VuZGFy
eT0iYmJhIgoKLS1iYmEKQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOyBjaGFyc2V0
PSJ1cy1hc2NpaSIKTUlNRS1WZXJzaW9uOiAxLjAKQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdAoKVGhpcyBpcyB0aGUKc21pbWUtb25lLXBhcnQtY29tcGxl
eC1yZmM4NTUxaHAKbWVzc2FnZS4KClRoaXMgaXMgYSBzaWduZWQtb25seSBTL01J
TUUgbWVzc2FnZSB2aWEgUEtDUyM3IHNpZ25lZERhdGEuICBUaGUKcGF5bG9hZCBp
cyBhIG11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
CmltYWdlL3BuZyBhdHRhY2htZW50LiBJdCB1c2VzIHRoZSBsZWdhY3kgUkZDIDg1
```

NTEgaGVhZGVyCnByb3RlY3Rpb24gKFJGQzg1NTFIUCkgc2NoZW1lLgoKLS0gCkFs
aWNlCmFsaWNlQHNtaW1lLmV4YW1wbGUKLS1iYmEKQ29udGVudC1UeXBlOiB0ZXh0
L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIgpNSU1FLVZlcnNpb246IDEuMApDb250
ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0Cgo8aHRtbD48aGVhZD48dGl0bGU+
PC90aXRsZT48L2hlYWQ+PGJvZHk+CjxwPlRoaXMgaXMgdGhlCjxiPnNtaW1lLW9u
ZS1wYXJ0LWNvbXBsZXgtcmZjODU1MWhwPC9iPgptZXNzYWdlLjwvcD4KPHA+Cnp
cyBpcyBhIHNpZ25lZC1vbmx5IFMvTUlNRSBtZXNzYWdlIHZpYSBQS0NTIzcgc2ln
bmVkRGF0YS4gIFRoZQpwYXlsb2FkIGlzIGEgbXVsdGlwYXJ0L2FsdGVybmF0aXZl
IG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUKaW1hZ2UvcG5nIGF0dGFjaG1lbnQuIEl0
IHVzZXMgdGhlIGxlZ2FjeSBSRkMgODU1MSBoZWFkZXIKcHJvdGVjdGlvbiAoUkZD
ODU1MUhQKSBzY2hlbWUuPC9wPgo8cD48dHQ+LS0gPGJyLz5BbGljZTxici8+YWxp
Y2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvY+T48L2h0bWw+Ci0tY+MjhLS0K
Ci0tZTY4CkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nCkNvbnRlbnQtVHJhbnNmZXIt
RW5jb2Rpbmc6IGJhc2U2NApDb250ZW50LURpc3Bvc2l0aW9uOiBpbmxpbmUKCmlW
Qk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZQUFBQ05pUjBOQUFBQWNF
bEVRVlI0MnVWVE94YkEKTUFnUzczOW5PM1RwUncyMGRxcGJmQVJRRWpPeXdpd1lu
Q3RrREtuYmNMazY2c3FsVCt6dDljaWRrRSs2S3drWgpzZ3J6ZmNxVk1wTDJqbzA0
NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00vdWxp
CnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9PQoKLS1lNjgtLQqg
ggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0B
AQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UE
AxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0x
OTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY
60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6
kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b9
7enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMs
wt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5
chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQAB
o4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4G
A1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUH
AwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3
DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0F
AAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX
/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U
8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXs
U4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZee
gSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo
2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJc
OvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNh
dGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MTha
MDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5B
bGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0
iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7
pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rB
X7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQV

```
tkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/
2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVC
CpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQ
MA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxl
MBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQU
u/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpn
HGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40
BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeq
AH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ
2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYTo
j1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6h
noQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB
/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYD
VQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3
QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzEL
BgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3MjYwMlowLwYJKoZI
hvcNAQkEMSIEIPo6cfj2PNIuP7W8SRv7KpxepLUu9zPgalLeN0BNuSo/MA0GCSqG
SIb3DQEBAQUABIIBAIB0l2cJSO2iAJg5nB/+gal+wZn3hOPlWW6n8YQ957q/TxIj
Iny59ctj4CokVaRb3uAm50r1TpK1h1x/hse1MsZgWQ0ew+omUQQkJg3RLZ9R8wsv
Ol8SN5WMNdiNSRNC9a3MFtSVPEOCt90XdQdQ2kqeRkL/fthatcF8gI+p4+pOP2+U
dOfnKCjP9nPobyBcXkljv0pRriu7snqQi1O0I1aqd4VwocIm8YV65la0/9522f6e
/4Zi30oBLuIz1+pT2z6frPzUJfd6UbGtSiAwRHyfIJHZ2PAYt94iMv7U0VmK3GmJ
TkzFm1if4dpFLofdkEtUX8Is+DPf+/ZB1MvrrQk=
```

C.2.5.1. S/MIME Signed-only signedData Over a Complex Message, Legacy RFC 8551 Header Protection, Unwrapped

The S/MIME signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="e68"
Subject: smime-one-part-complex-rfc8551hp
Message-ID: <smime-one-part-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:26:02 -0500
User-Agent: Sample MUA Version 1.0

--e68
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="bba"

--bba
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
```

```
   Content-Transfer-Encoding: 7bit

   This is the
   smime-one-part-complex-rfc8551hp
   message.

   This is a signed-only S/MIME message via PKCS#7 signedData.  The
   payload is a multipart/alternative message with an inline
   image/png attachment. It uses the legacy RFC 8551 header
   protection (RFC8551HP) scheme.

   --
   Alice
   alice@smime.example
   --bba
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   <html><head><title></title></head><body>
   <p>This is the
   <b>smime-one-part-complex-rfc8551hp</b>
   message.</p>
   <p>This is a signed-only S/MIME message via PKCS#7 signedData.  The
   payload is a multipart/alternative message with an inline
   image/png attachment. It uses the legacy RFC 8551 header
   protection (RFC8551HP) scheme.</p>
   <p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
   --bba--

   --e68
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --e68--
```

C.2.6. S/MIME Signed-only multipart/signed Over a Complex Message, Legacy RFC 8551 Header Protection

This is a signed-only S/MIME message via PKCS#7 detached signature (multipart/signed). The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 header protection (RFC8551HP) scheme.

It has the following structure:

```
└─┬ multipart/signed 5624 bytes
  ├─┬ message/rfc822 1718 bytes
  │ └─┬ multipart/mixed 1670 bytes
  │   ├─┬ multipart/alternative 1030 bytes
  │   │ ├── text/plain 324 bytes
  │   │ └── text/html 422 bytes
  │   └── image/png inline 232 bytes
  └── application/pkcs7-signature [smime.p7s] 3429 bytes
```

Its contents are:

```
MIME-Version: 1.0
Content-Type: multipart/signed;
 protocol="application/pkcs7-signature"; boundary="a61";
 micalg="sha-256"
Subject: smime-multipart-complex-rfc8551hp
Message-ID: <smime-multipart-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:27:02 -0500
User-Agent: Sample MUA Version 1.0

--a61
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="91c"
Subject: smime-multipart-complex-rfc8551hp
Message-ID: <smime-multipart-complex-rfc8551hp@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:27:02 -0500
User-Agent: Sample MUA Version 1.0

--91c
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="b87"
```

```
--b87
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-multipart-complex-rfc8551hp
message.

This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 header protection
(RFC8551HP) scheme.

--
Alice
alice@smime.example
--b87
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-multipart-complex-rfc8551hp</b>
message.</p>
<p>This is a signed-only S/MIME message via PKCS#7 detached
signature (multipart/signed).  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the legacy RFC 8551 header protection
(RFC8551HP) scheme.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--b87--

--91c
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--91c--

--a61
```

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-signature; name="smime.p7s"

MIIJ4AYJKoZIhvcNAQcCoIIJ0TCCCc0CAQExDTALBglghkgBZQMEAgEwCwYJKoZI
hvcNAQcBoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
```

```
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzI3MDJa
MC8GCSqGSIb3DQEJBDEiBCAYyptCVBhIbjLhlQOKunV/81vEiJSGLmos08/AoumM
FzANBgkqhkiG9w0BAQEFAASCAQCSBglwkJFZNTXSwtDjldQxDo4n3twmJl9VyZSO
AlO0EiVW2+9Tqu06G+mTSePraLq4L2BvutQ1rKW9jVXJXJ8klx3Y8aY6TGvJ5/RH
3GpwQPjfjauEVAplxnIeLdtUbwJJvaColBr6bPHUibtvXS14JqfHvEu7uTgHlxpv
KFZ/VEXf+Lx62gINfpie22d6UC3Nxif6EwPEDLmIjOYILjfMf9McQ2KzAPr6t6x/
hrz6NDG3LeTeLegQ4+onLotaBFsa0QPat0nSFjcaH8j9hFb4RB4avMbT1/5nRR6/
B49YO28fRuAztMvesvs4M8kW6DAJjYj2fFAgT87CdWErzM7r

--a61--
```

C.3. Signed-and-Encrypted Messages

These messages are signed and encrypted. They use PKCS#7 signedData inside envelopedData, with different header protection schemes and different Header Confidentiality Policies.

C.3.1. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 7825 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 4786 bytes
    (unwraps to)
    └─ text/plain 329 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:09:02 -0500
User-Agent: Sample MUA Version 1.0

MIIWjAYJKoZIhvcNAQcDoIIWfTCCFnkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
```

Boq0MA0GCSqGSIb3DQEBAQUABIIBAERRjmiJrN88aVGFS2yaskouoeCwZ++b+Xx4
pJQ1bIG5PzkUkiAqDWKhdwAJT+f74rJIneIhgYQkL1NWefgCuO7UBT+ciHEBDEhP
+3jciOFRP3Hnynxdiw6DpGaUfyyk9WnOGjePADIipvHDkRJXWIuuHFCXpQPQthB+
mwYuv6G5Wm9MxHSpAid/UXMkUAYK2zkVMSoDM4BfG9TpmIUqjBm+uo0d3ZjIIcAM
wzDMpEEZyZc3ZO7jdC7DC1eQBm09co/RnhwpI56kEp2rtQqmRi1waXS3jqHf8EeC
u/X5xskoJlVakhdHteSMObqJ1v0cNnsSMYbHb3TLQRF+BhPIWt8wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAURM6vJvmBdyw0kwK73GhkCBT
DN26jSUwPbZg9MYXICPROANV4oU9gFTF0E/CA4JzCPhPeIyqGA9KHWEpEr9dljFg
HwFIg+jo0VVqa9yHyQ3NvPN9Bmm2fc9JFc9hCj9id/35tEfCVO8dUw2KctQaEPKD
OvoJfHrq54FwbCW5u+I/QszuN2U95gqNXg4R3GD3NFgB5vtUPk/hV26H5n0U98Wk
6Fqd76iQbY9SbqOqxQpdbDcNwdDWYHPDoyuXmmsgGIyCn17PdTcEURrPTCS059OL
oPJy7h8LA9QLdOjg31nF7sXtsJriCIpJ3CFht0fRdi12dVMevhTx3S0cQK1lVDCC
E14GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEECsbOPK1Byo8Yr3SVUeSGAOAghMw
Kd1hOujWtOvKraLc85HbQ5Lx9Z64dro+3EJj7zNUjPx33hYU+m25DXgdjB+ZsA2Z
1QtUO6MvLqsJKjC1Z9n3yrMc7gsom8PjF2KAia6F9x43EyNv7hagnPvawqKEFPCp
QLF3TTLs12i8rIcn8FwjrDlMqSmVlBIz1dvLD9JKiOKQ4IJxl6OjETniZvFZgsRJ
/PXZYzqq7cWoymZrPSX/UksUFr/8pc2AyQR0Ly3JvDZQ+3EykHcXQgRzqtT8TYyN
HB0e+Feo65sjxYQvwMYJJeMRjzercDgAwqYQ3XGroFtDTw+tDJdhIR8/yuXHeWuU
8PxAnaM1QnoZpRvHdIn3zLD6BalgMW98VSGFL54HQL8P6O888LxBvstfl5lTEyev
EnOUwa6Qx+B777Lzt9n6rvIrJQ5T+rIXBhH/U1RfOQtMxfZC5tSc3Lux5LPDSGdc
c5rM2nh26JCEpoY2FjdrikIJOBK+NUdkyu/mlCmjCFO3c7jQm6Q7JFdpG0qmjoQy
gZo8VL4g6gxq0mlaOG+pYK/3QUBAampxnx8kJ9zQ2NdVBEjdRxk7JD5fqVWa5tZb
RV4IA6bm+mfZzAviibnXI55m6E07wOfHHm/b+KKUmyB17WeKvNm3Z3iTkOtViqun
tZnXjyhVA9fGdwaNYs6njkQSuwQjGmjmLtokR0dh6LMOXg8cgX6us34BHfP0yNe6
HUzXhL0wKLQmTuvbLBqZRcNZxVgeSNRViL/n/O8DlLn3kXJpNL+1WUJZQhBLXVIk
T7Fucb02kDhDXufsjRed/uMizdX6lNHjRFObGARZp/SD6rn3X+WzJV2BwX8xpEph
iEr6I9hrVDytdoBFsGt/z9FVM04kwp+n6U02ipikVQdKPt1CpsBYkBzwfDaPFOmS
kbwuLZhZ1nj3tkAzv9sx5a/z71v92S7LVHDycnUcuvNK4AZB8wZvSXz/8WPxwk3O
zmdeeSsn6dyZ5Q9o203Zq6/7k9YhkYD3LDS3XWRkpJMfNmjDL5WEr5ifxVrIq3KM
MAEOs1tqfBMWF4AeA0KOoHa9NAhzLCMsfxNEtXd7l8Ur2JKkUGxtmCKD/3ep5e5S
smIS/Ty3aD47LQYD0kjWhvTnQF61v0vQHrEKLmf7rlrnAwL2fEwfnMvNZTTiTN4I
nfL1m49CxxzffSvlOECTlKs/RZq7JxcfvuW4qN3yjMKy1dwtRZm9pU5+R0p2Hn9F
C4nZQ4Dre2cPdM1JmvimOnVEyc37O3Mi7hF3Nuf7H2j0g4yTMu8Tuk+8J0OKukQD
dNz95Bzj89cCb9FJyq5h4Sk+TeVqJzhONpL0Q6f7xrJeJZVefq4RhMMtfFYgNAeZ
/G1f4xHGXFug9okJXFSZCcoLYv4qek5OjJrbWM3GeY7lj9ClxFbs0bqrtBXAImul
60G7uEJdsFR2wBLyv6i9lCwAVKeBSJx6FdfzKzRqsHYUFsMVeNw3kYPbbsXyj3Mx
PLCrB8lP71NHtIEHPkKFgTPvEaVWzXMvz6YA0g6mKxVjI8iVFSE6JBJHtaTX49kJ
w2XXS/eI4DD8y5exJVt1Rb6l/88eh9IiN60UXbUXmtDm/cKnnMD3Nt4H0weIygvU
BHMVw3+p6Uoj/E3lDExSGIX1BTveRZVGz11AOaz63UGz18KCzOhow+XJrLILJlnH
8MLEF/BarmHe5+O9XHF8otpOYPmdhL8RnFfvtStTthxhp2smd5IIblm13hj1CuV7
KTnVbyBxKX9utmIRmlSyOdvAMR2+jzloNCUTzWYCu2/IcYw23gW44pFQdUosKmyf
0gyFSNQVQJ+CKADEID9sHWm7yBWkkNEk5jExDn00qyU6B0Wr0i4RYY/J6LrQGMWG
YliQtmyVOfhDjzUATEAGumxVBWbCycDAl1DsEp0hSckgowk8aTlXo6tWPeXv5iMq
bCfxUGLY8gmHEf7n+v2yLoCJmZSyTMT0Bh0PjINnNYRWQnsdR+CELSxgmbE651K2
abaYEX/jBZvCvgILPuAHF14WVVHj/BbfMZTfxTRSnjZIKhcP32Bk42WIuo+Hkhtk
sG6xsLi614VAqqtRvpDzMK+HsK8YmyCT53d0mb9JEokmuOV4GaMRluaeBGxV88UK

t0tTQB1VZ+/kcSy7SBBuGtNz2kSapRDUjWgXnWDzMdQeMc5rI16WeCRgwVTiRBRb
EWrsrPtG5u/krSm/wwBdd3m9VDOmlTj+lUoH5+OXeReZjb0se7uQt2W/V/IWpGMy
EK/M/rThL4q8JjY3SNmlzYv9mtrUy+eoFgf+efOiGSfCynfnK4A12K9LPFvaPnS3
qcTH4FVjufs4THAfCp5rEoaefUzEY12DBYdLVTNMfKr517bnCs4wp82XGvf4kHJS
y5tM/H456uv1wQRDNJQ321Fbi6xkCC/KujRMYsDsfLgo0VSlKi+wVOIH5cvpem57
cKrgBwNyUYtk4l/s6tlSWNyDQvFYqCrhN5TEHu+JWCK7poGBdCLzUTtSHJeMOH0x
Jr9K+LiBnscmgDstq67x0rLwhe3r4PM8OcgSuV+Kz91j23RtksSghpeWe9vxCnkx
NsZ/ZddX8ZdNk7uihJZJ/M9/DWEGx4Y12Mk5XI0Shb53ZmlO3KuLlkN7qj8mdOp1
3tfr/FB82zXo5Hk0C7U3Nej9gmqr6SO9kSxwqPa04om342FJuYVZgsfwO09gSM11
Z5bYKrQ2ml+/oRawRLuU03fCM2tV+thgi8M9SIwl3FUZnGevyuGyudbktckRa4FF
wGkERAzpAag836wt3zUWbP4WyZpY0u6soeARvaaeYHpxNW3G8nI53fhwKlHeK0ac
geqC9Z7zdkDZRL6gqDjqZjU+sQZDoFPIRh39zC33YkOVm/0CRg02NSIYQ7C2tgxy
uE3UO6V1L1wbXcBkEJQ653/JYqUkLAOZ3bKRp7FhgJBblLg+Qe1dvg5zFPoOBRDS
b7RNyc5ItAJnciqpH5048PvvUgNwY8fNuKojNeK/9a1GLiE9YBeorWVb+rzkenxi
OgfS0LdgszpxfYs7ag/y4LGCN7IOa3rZ2Kshkq0uD+TUbcdni0vWPVco0Qa9VPjC
UVlyypzJdT6cale8SLK75/ABiIo8SEuqgQLbz+diq+AEPY1TlDW/isd9hCGDexFq
ZrPY/rBXLqA43l+EwqfCdN0lZLOaEvCJ3T71Fwt0JoW+/nn5iG3qfj87mzGbMLK2
wEzxxJnFYW9w5IWjL/YlplPRnNZUm6zsGZDd5x10tW+CE+FoklgU8p/MceR0oEwo
BLXknBDjaq0EDLocgmqIUrSvtKOnDgxgDCCqy3+DNt87YwunGWUFhjiw/SwSH7Dc
ONvvTVsJbMVS8r7G8oJXMGJ+OKpslVhQ0iZYILDHeX8hoUYyCyzQ/istgAVJ6Lvu
f2nhjw04Dg4ldYGBPVgpjwPO7dYaaPmn0pR7qbl7ui+FxLwGKZi3BQk0h9AUY/n/
BkyvsSJgx4TEL4G8JVgEm8+Zz+yDmNu/wDrxQrdIhzd+ws8D9kENuceuM1xM543n
nMOv6d20FygJFaLEQVgVGz+HlsfdHHa79vzSP6kz93+1naS3j/0iNThy3e/rrAAq
ORslyqepsr8XtZlCynxKrmGOpDHWF12iKXJdrN6YYgfhBgNXPuhwlVgfhiPny39+
j1SB8vXpYP2EW0EiiY9iwk/OsYxqsZz7RfvtYobZVBC2AuYFxeK/FfBsAMtFIY04
qz8/vrw7KviAAf/bAASBIAGfre9pwE3w8YF8OdQVk/3mHDs3Z/9v4TO5CKRBO3cY
5fu+GpSBS9EzuKvDmLOIYdq8SyGN/Q0emK3D4omiiklffzGH/Pj6pH50LCsCBhwD
PnathlA7jZ4+NURX/y487w4gATjTv1i/N1gwHxotOln5dC5X/ZrTWLcywS7GATko
2/y+8X5IE/0dWiv6tBkRTNIdBuhsuuKEe8H1rJIAoMfhy1xWIgGrfdWZNgeO8bJe
CZBfDI4NEoO2nOs9wPOWNHkkaTu7dRTKvxFiPqbwb0K7O2s0vGtnLb6TWqdVE4Bz
K5DmQXob00qX+srs2ULKaE9VhK4agziDGBIy7jy56PmDTO71WG5mGYZOLnVjiAbR
dnvia5+QGCcmwNHNg5EaKWOqul2ekrbN76wcT+e5indntAK103nrw82SR/jJIHCD
B+bS9FMoP6aIh04UWR3NQ0YCbxQzAqRQmJK7aFeBK1k7J/kzX0kEaDcRlqdFv2fs
QyiFnY04Dj+lsfGpdP3rTx9cfi6+bM0VY4aDonF1YZs46bLN2rdMKvG73fFZiCnq
R8yVA8gBre3x52tTvRqQxHAKH8CeBGBO5IZGYbA/d1uFpix1cBef8gpD2zFrfR1J
E0cd364G14p9vD+ItE+hHV+B504UmDeyN8r1ACUcPcYXwN9uWwqh1NAsPPgA72x8
bVC2hNGHzAn0p7X7CDK5Jj14lwxdRkOqntAeDZMaYdKzhS6MVRVVXn5e/0g2pX/z
V2rvaDPBWiKgLQJk64OJeBGVXOnLAJUqyKd/JkFwu0ON16lyG0kZ/YBduLK3xguG
YisTXzkYZod+4sbOgoix28Q1iYzMvtwqZ84qW5VcjM3nkdUa0UivyQXwyXXJ/Wyf
WWJkbLKfHZOtJP+Q8RNMYj9oQpqNl2ANd1+PBc86tPKi/u1V25EcDFgM3FFOcgr1
BKNNw3R9WCXJhP5ym1op3hQv/gI+45iyzsP1G9EtMcHhajM1hkagpKMW9naT1aFy
oi6h3jMatP+EQkO1fDYQo5bAkfvVJ/qDiVjLkz7CDNQsBcgx/XhV71iJkUhQb44/
KVGuAAuaYogwtIcM84doJvxEeuPTSObKUunYNHD8tAjrcmKwhhh7c7ihkGIn3p0Y
nDKb0sri0yQhiswNEUo4/lZkSoCYUx3xYyxJaUdkMJ0vuD98Afz5hIwD0WnTYQNT
T2YdoZO+Q2WotvcFyeVgamczb8nsMX0p1QFmbOoeEOwovWWLdYAH2uIIEecKs2Lo
1JfP5SOK8BtM08pdiPqycmf23sEkQVVI+EhPZNbmQUVrYZmYSHeaJPcrXjDK2gIE
997lSp8Iw9bZuQHg6E4Zb3AgIwQlkAJM7Li/VFnh31x5PivT9om1DDqQEUlQshZH
FudrMJlJ4Tn0i1whm33rC1LBElFh5e473ir7kFDhrQlztOgb0yRztTecyk8512PL

```
UuHX0SCmSCjzoLtpdyvwoVNjouKatxP7V7lrofI2HLqAVCbOdtdGsFREn4cGhi0r
g/l1rl+xac85KVf1k9SN0C84/WaSnylVU5/vNzD9ycargmIU3RE0DwU8X0C8ECUg
P1e6wdpuqpYK1bgtl9lG+2dsoFGBdq4b1qRry6reI8xMJwdcR9BWVKksRAMbSPBh
5gFhER4dG8cKiO0NGuL08m74UKgA6vsSz3rJJ5NyXvTGt1vP3j/EuWOUbOFzOSv3
Tq7q4N3yEgLSayg0YEvO8JY+0R2+1EQMTu9I9sv8dCRw+ALR+JI6vJ0gYTLM7A22
l3v7b1FlDWouT+RGrokL//Pnt99uYolCKnRte+LsGZ1/zk87Wx3jxdPHyrWXPzqt
VUru5O+u2x+xDAsyKiEzMvq6SICG5MT95vNQFiMcM/1cSrSsl5eahhigcdpuK+3s
gCkMyScHvy0iGrk+VAaarrdSwpMT5poPZbudr0K+K3MD7Y1Cp9o7ZBT1rjvKCNIW
vpwQdfVSZV+1Ji5sfyC2RLy7+2vwRU72yB3DJs9rFLk9XfjLHiv+BmVW6Ql4tovY
mn45thtn4zYQEtdANkR8aufQg0A+BDQg3XAQicCb2hhyH6j5VFACh3MPDj1tjy+r
YNi5VcHj1ccnXsk2EaYW2y+SkgcGg/ywmPZ50B/I8GLJWNeb7Ai5VBXCWfMeCIz0
NIPzxwdN+mceK4MfBFWM3GDi0hZM72hzMN4pFN/4GeLPEdZUNlOkNWT8hKEreX+W
PcL0faa1xbpEUTfWv6Vviq9VCVkc5q/wxdL1irkqLNR5Ht8PyZUjCH9GsVntgPu+
UDswKkNICxi0rUppHp0Nzr7HRH1Y76htABrX+wyFVtA6ttwbm8nNqSVof7wb0pYa
cHYMfJDCVJvCLCLy/sePxzwGbH8bW/Va4ebVQfNBgS49ATHNbv2HfjROYqgWAINJ
l8L3IqyUROBveA+3+a0wEZ/kJnlIJppNGqIhuS7SiKUBXN+lHvxoGAfeJFN8uQ2B
C5KuodUGgcTbVsxkVDweTfBdS8bG06OIAklSXvgE614E146DNKKlqD3nc8xDCzbN
+YZ9VjShMxepn6pJ06xOKW54NVTa3zy/R+HZ+/WixdzkAcn8gog93ybxg/9PhAi4
VauRPmbhrasLdiZwGyQ65shkUaJMwkjY+BpTK40M5KUV4yLr0ddkzbmKWo4Q50FY
NMc2AtCg1A8e9ziRU4Y2MD8abcs5S8rOKk5/R7o5gJGNHjlHpn9Xz+7fTpqtYqIf
UY+YJhE+LyJW2uu8Gu1tTe05BSdy13E367FpALD0ZTeQHQWKmAckvwjsQ29YcKFM
n5+AmwDhDdpWKXih4nxFgQ==
```

C.3.1.1. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIINkgYJKoZIhvcNAQcCoIINgzCCDX8CAQExDTALBglghkgBZQMEAgEwggO7Bgkq
hkiG9w0BBwGgggOsBIIDqE1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lDQpNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1iYXNl
bGluZUBleGFtcGxlPg0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+
DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6IFNhdCwgMjAgRmVi
IDIwMjEgMTA6MDk6MDIgLTA1MDANClVzZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVy
c2lvbiAxLjANCkhQLU91dGVyOiBTdWJqZWN0OiBbLi4uXQ0KSFAtT3V0ZXI6IE1l
c3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lQGV4YW1wbGU+
DQpIUC1PdXRlcjogRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpI
UC1PdXRlcjogVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjog
RGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDowOTowMiAtMDUwMA0KSFAtT3V0ZXI6
IFVzZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlw
ZTogdGV4dC9wbGFpbjsgY2hhcnNldD0idXRmLTgiOyBocD0iY2lwaGVyIg0KDQpU
aGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZQ0KbWVzc2Fn
ZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNz
```

YWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0
YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbg0KbWVzc2FnZS4gSXQgdXNl
cyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0DQp3
aXRoIHRoZSBoY3BfYmFzZWxpbmUgSGVhZGVyIENvbmZpZGVudGlhbGl0eSBQb2xp
Y3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6YwggPP
MIICt6ADAgECAhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUx
DTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1w
bGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2
NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQL
EwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3
DQEBAQUAA4IBDwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnel
N41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i
2GMt4jse2Dqs165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNH
T82S6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+
ZLCqlLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3
qFC6vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgaww
DAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcw
FYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNV
HQ8BAf8EBAMCBSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1Ud
IwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCB
SXignLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9
Ii6zyBZVjdaox644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz5
3PYDBh4zE4Nar2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/
eDOdu+F2MVtluLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744g
qoeuD9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXz
lEc2tUpAr4vRhZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp
1zANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExv
dmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5N
mn9PkrYo0jTkfCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDc
DkY63PQWl+DILs7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFt
md+K04s+A8TCNO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJ
OMayCQtws1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFec
N7836IPPdfTMSiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq
90njlsJLOwIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpg
hkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0l
BAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0G
EhyXrilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTAN
BgkqhkiG9w0BAQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7
GKJ19naIs3BjJOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd
6XaVWHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7a
gyHahiXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazg
PYgkLD59fk4PGHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jM
hwFXLJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9C

```
qaJcOvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3
DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwMjIwMTUwOTAyWjAvBgkqhkiG9w0BCQQx
IgQgX3dswDsmGjwXzejaB+kh8kzNOiNjkHpEtBXbJ8gjT5UwDQYJKoZIhvcNAQEB
BQAEggEASC6sf2ioO3Y7yVOzy/6sbjR6suLfigryPkvaOvuh1aHCP/I071/j3LYL
nER9aCGoEFXzxXzI1aiTjwlQp+Fg6qNz8avFRbSvecUpAsbihlRbbOSirvNwW6F4
McP6cbA4UR6M52M4mE8buxvDtwf6caf8gwtx9XbZy9a/FSr1YqQoB9ebotZDadDy
sh0hjzMTjvHbq6DTPytem6Dy7rBP7F32Z1SHNC1Wc2MaW4NKejRxubh4kKkpopRvk
diHHADbm6WUwa3IsgU65HV7X/BkE4vQcYsWzYjqyA3WjpZZWlYus023kqug5sHX5
G5uhNtW6SURCQjN+d6PNa182OqCW3w==
```

C.3.1.2. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline
Message-ID: <smime-signed-enc-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:09:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-baseline@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:09:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.2. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8085 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 4968 bytes
    (unwraps to)
    └─ text/plain 414 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:10:02 -0500
User-Agent: Sample MUA Version 1.0

MIIXTAYJKoZIhvcNAQcDoIIXPTCCFzkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAFt/SL+2acYbbnElaXwsZy3nS97+v4FjebWx
L8Q/BXPJQQFAqPwXiBMf2vbpBoVz/mq7OOwPiCUbgG6IT2e432SJ72N+FsZhClLH
WSRu50QqqkFTrSzomm0iCcPEeU6dOL2THdDH01Ltp5zRarFzEFzXmjEIqVfHXFQH
2hmO7af4Usxt8cJWsLaQ8px6hm4KqSpwKSLEeXK7kiDYKJDsLlVeSHDfqiJfkoCt
iajW1C0MfjBTvD6upSlusILp3/wju0ZR3Axjr9svkyGBqkwQxUtNUev2JXxio+9m
A3xYUsHLgDjVNlImBN3q4yQfyTg7Byl5aS/WjdRZd4kB9Poj31AwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEApi17wPDNLbvOE+snTdjrgHyQ
V4DGBR/WTMW8Tzd7Zm6nh6h4jX7x3FX8NkyE380HkFgzZ5yitz+kB7WtcMr2Gij2
VBdJi9ey3pZyTZ1TCkwnF5q4ghqD0vfoPmKXIoPOyQUP7Ak9+EXA91QPYaMcTRxM
jvibAzsbnwQmmvnuuvlLhGqqDjv4woTJ8F/yOxrWaidf8nfWmCEzMP6kYl4sDxFT
xxm329jXEQ0olqYHzyIgYhRklLW09h2TpC7T5Yov7NfWZyQZA0F4j4TW9gCfmcfb
pwP5tcbzkxpclkklBBlnbezpVEMbMsaLCcY5c5RDRLPJPdhYKcUztCeZKbei0jCC
FB4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEHMz0B+KARgbNWCbbkfBkqqAghPw
J7tgZJiuXvnsaLW0qpJfTfd1NW11Y6uUmPGbbp6ukBFi4Ri+coXutASHHc8pgQMd
```

In4vIs48XWLTlRUuotY2JfBWrq67pCjsfv/s5TyRzEaBDC/lwYV0m7UdWiko59tY
+yOXqz0R5p/Rjj7U6RePNBv+QtQN0zXbECJxJ19IGExL14ziddgXGejQcMOJuxk9
9AfoctdteTMV8H3Keg+LGhbUhwhsHv+o9CQfWo/kEAQ9On20Zhb7ORggCLRJSg3c
G1kdv+ph3umi/bGZVupvdpKqBQe5nSJazx2Ej9jkcBX+W58csvteME+bYexzK7X2
v5d/ut/lmd+Ah+POkU+ZVYIAPHE5ORDrLSZjuUC3prtksHneNqx+DwA9MnjwRa4p
seLZWRCoEzgubftMk1zKBDRUJ9WCHxbvK7hLmpGRKpNHyHUAt4uBbHWERXBqvSG7
rmsN8rl07panMefhNZAf2r1wc3dEVtwoV315RFboof5sPyVaiTXkP3KlGC4JeKsn
3nqiP8sgNlkX8FLj2i6GDJYdcUCyzfURMGFGMqwvtqFIgN1TYJW35gFCitJYCAvW
MhUseNGQzlqigkbOjuHxSsgGt/OUwJf/5mhK5cV7KTYstnbF8tvxGTo5MFaRJEsh
s/WSxSQcr9P1T3i3bLQ3lYO63j28cWvMzrt/vZ671WnpivPawpSQlMePPKKHOqj9
ZLtf2iIc3Yn76ir3v8SSWpGsOBES8s1lhM/jEt1t5H8xUfVNz+WyhhnnL/3kdhv2
xXpnuSscxiQja9I4KOhqw5gHW0t//vnNZRRCXhWiVL5rEx0kK3UUnSJm63kkn+Q0
y/EykyK3sLCTSDQIwdbe3CoXq+smap61qDQeHgpBnOSz0/Sp1PvPS09g6fOWn6mj
ocXbrifW/y/uafC2Bs2rLEtfq7Tts0T96urEOBI95bEF53OuYj9xLahALFmIHi8p
DgHNaOymQcXwkooCT9JG5h4c/pZcM6Vbde1v0a4Nu9eoXC/ZIT7zloVV7e7aYvEz
QXaABEmmmHAySmPpBC75SegSLUsHwRbpS/AGQb8LStZAX3mh3fsDfHqcWiKAkin/
QZ2TwDanvMca9DYlWFX3WeWte/fQk4uXEEQdPnLu6c6q3+ls3seauYpfg7pnr+bG
50msWCSg5HDBZqlsw07/cp8VXSXYlI0xOiKZ6gWFtkqcDkAEX44eYW9OQ0V34fz8
yec/JTUTvLVoVRRjQCsg89Hx4dejSma2bKIjIdrF6HJfTwhs+XbDMxG5h4t2++/S
KFFDsmPtYjgcbQEas0ELKMdYTtTWy5jq2L2nVLScheryfIN1vq1y2lUEpK33c4U8
vCpOaVaRvylCi6TaWKjh8JlfJ6e/Sx6/WGOY0wmN9pYeBbRsUmSkjtV6TofOodGf
9tP2VXt/2jsO2RbDCKp3cC/VNgttVU3l6H+R1DvasOJIcVVeDVCQGiKnKLrAoUoQ
6ZOGLhfhT0xSufMPUyvZUqmgbvWn4OcQSYMajot6TCwQ6YSoN8LlH3CX1vZR1tCG
STXkEQ9BIL6TwQQcyraRuBUnabv3oS45HNIZo6uWxBDfS7jHYgdvtJVko6rKc+yB
nXoB9MufZfK0RalSFG5n6hh6wh5DK1/5BLbWvym0Xwp55fhiel82juyG6s5m4LFN
VpeDA1Xyu7yLIHwfMrKaKuzo1YWNU4mTjy1Y+v8WmVFlg3jiDLJGBN9XKsLV9tBp
chbN5lco/RJh7A2Z5FUU71sLFwbBpmSdjK3/H9jtg61QwqozKwIAcPt+NCUdiZE/
DUz9L1ul4qWd5FkoiuXVt7i6/FJUhtMWrP1xBtFXJDx1QQcYPgy9NRzJ07DpGWMK
XYB2aVIf2gGHVoSlO3HGdqMJ/eciaRNUT0le35MkIpLh3Myv3gv8xIG2ue+uiiJ9
tG0tmbpsG4R310t/KV/L59AaOX6y8dtrCoOIyD8SI5QburVh9FcXUxphMxgKle9h
scVHp+KYSLp6cx1zlE4OMUL3ipU+ZLpDKCM12VQS6gdv8xyr38c2IGg23QCk8Vfw
DBmKjJ32FaFJFgjMKcnEqpSJC2w3/i6odPJDNCV5kOQuQ6RTUaJpMLYcUTIlVtiq
5wGVlXF0PR6va7B2IE4zrjst2pQ1elwtQDjR3bwIQgL7/scNeTzmgzcTwWP71HkL
+xSoCu5bCxALqGOzZplcl/v/290M8sN8vDB1OR78YM+dbxej64BzaGaOGDinIJeH
o9hjjifOUcwrKuVRifpTdct+rPpKXkXbI/IyFMEeVLx1JZTLi2i7BcChty+JSUUV
Lb8RHEyRZcx/O3iO+kVqfGUjaEw3S52A69A00/tvFDzE+Yxe/1M6RZrG7VanhtwC
WU3XzKhg2Skm8KNTcG/c7cRw7tzZVwHpXHh16at+9GoIsXA9tiT5keFKJvNWWdV1
U7EswrW557JnqSa0V9WwhWastP3LaAGDsMuseIRDCg65CUMEVC239q6eXX6YBE8O
FnlxN+WluVNp5Q2MAX3nTt0Z4B5R7E2qP5jBL1L6sqzChyIBM7BBi6Z9Enz9lqzY
gLZTW7s0r2Gx9513voz5BbPyM8S9f+XzURH0LBbrhoIR9yk6QswNYS7RaGJREDL9
zv0Ird6mvTzRC8G47lbOY2q6TzU+SNVu1RVUdWj8X63SaU3p8F6HPqdItIfPc28C
NpJDpeMiAoMFt/Zd9ewDUbCV4aPMniYUNQBhVvfX+CFbtSY3Nn8MVD8XN4jC9UB3
+sECae1zD+hAG7j7vqvryKksejsX4tLrN8jIL+PhpU4bsTdC5kg3TAVQinf4Umc/
RcUaaMZItTuy+FG48sewznCd1E/6eBQxXRKfoHCnsBSgimiwqX2wvd+qvpgEzr7v
UTJgy+OMeTcbmnRz+UYIzUQrYYGGtg/vFYiKBM15xTu0qlGGWqC++l5V/Af11lp6
4wYXNGSwNkUm1L6vqQJPgCfJs4L+onRRzLrzVkBKQfZVSs7jHUyiS9ivoYTP+I7+
zhiW0XYkQYf1dcIXwGmVYD78tdv7ip9S0sJTTQj+WdWfdWNP4BP7H3DGKq3rUbts
y+ti5/9I5Z+k84CBpSO6cd6o2ByrHeAnqQ7Ti8GgM2IYvjijO4YFDxKG1EJAvQVJ

MXKiOVIh54rT/7v75k4Dc+uysC3r/7o1BQESxOC9H6J7dHGlrPOAJh36rhb59SlU
J5ea5IZrsBkqLS+3xMy7hlVcVfhuKu84zwD70RftXUqoC4i7NCmmgGZElrQ14sOf
BkiiIqTgHEAr3A8bYFp/QVdx4UVQAwPsTkN0+Gslhj6WJpr+LHME8tesFg2pY4tt
YVMRWe52oVSH0FKmhz6CR6DheUSiPbB9GZ7aYpodNZlUgGB2iyl6qlBHZvH0scFQ
tupRY3EtfZGe26Rh2btS+xrSwph9n2/2apD3jlPCdJkj1yUA3iVybjD0Ks5NCsTB
7hO+V5xbMChDb9PXHx8i9981YLInLjfkGgDA5V4HfwTeZNSMHYpKLQYaFRFyn0ud
ecgQCVHXnC0amgU+bQfreBpMB+PI8ouxR/W4jIrovx2iArGVhvcLdl66IvOO/GF/
Bwa6nJ2VoAfmbH4DF0Q5U6KjJklTCE6oGp0K14ONKy5Kw6nVAmvIcONsYHLDVAY9
ba+0Tjoi+cZAuKLmK4dXK3U2fMOb+tPqqomwaEkQVba9F8lUYdX7wywVTwcqDS/X
hl9CWPW3LKlW0LfMEfqWTwj87SCoT5wF/thc0nm6GTAKwEmP94AbUFtb8kqUxADq
yqvuLKo9tdab+ehAz5V2QZa7ObwuvmWmWGMU6g9i4zEXL4DTVrJJK9buA0SviZc9
v+OIc+fEiF3KBH8vqbfHkYdACn8ElbAYPmDIVbdNGN4+sNmSpCWT+vet9xcTUcU6
17g88jgc4vEEaWO1AA8G1khzRJNNzrbFZusDSGPE0CRPjOEo3zu9/nfAN+yXKuBh
zgAXM3VJmCbcVd95NaaYaw/D9/mm+buZf39tMVlPdUY36pbwgQtT95hfoyw0SAIM
fo4GyIEpd4KgQZdXycC0JJd3T4WPV7SCla6ErduMwJ7qBa7MG9x8HfX0kPNGIGiu
V2UWih9UxvY7wNLfqnX2CV+XLW+iwaeJo3zYzKIAcuFEz55FEl++mELC04gwmAkd
Eexou8/Vig1Cv8y/S++bS2YwYm9qZFRHk13zMS2QdcUBkqaAGF+/dfBka4lDlHVi
jqIAI5d5tXPq512OV3bJtqP5QNb1GvMwO1HrXLgN+OocomZfUKY+XejI2mrgF2rR
QhPYDiUfog/tjpsoZZLSjPfscqUkg3gCqbw7CXOgyU+Qi3o7u/p1cXeBdGDYbqfE
V8dG5owCq+LliK8PP/mi3M9hxvC8NizWmuI0MsRRZkcGB3R7E5MomZxKilhfZgSI
JRsPDYZmxwvtPdVo8kQPpVvbmJsLhp6AE4qoN9pGam8jEpFKD5ju1KoGGeN4Yrrv
3171UGMD8VdJJ/aNWucKViU3jYCNlcL/yOMy40M/KDT4pJt6ipol0O6ZXRDcLnXB
X5wuv/nV6tc/Qa8kW8L0dqcHyD94/Hyt2dtkepQVS3YBOdimvz1htXtlbR8XM07K
iYlF66cIm8dhfV93DhJcyInJhMRNCjSrTZ3saDQZGeJPzOa2kI556YAazjlNgAQ/
+/fL/mDldK+p9euwIevg3xeOl10jqdpTqe9D0PjtjjnVWEW9y+0zv4tFESMh8g5t
q9W9RJ5oN/C1vEFS69BFkSNP8gGiMngv3uxEXDmDNJQUCfwoStlItxIxcV+DjoS7
EDI3qU0h4Cdf53o2dfpc4+yjbvNSsassRr85dH5GmuMoYQa95y07YhiZFSOVRasS
bpcNbTtrqYgLtl2WyyvWnmKS4+IZPeIePdnOtu33nh8OouE0srONNDQM2I8BWE/Z
PFRXHPtlIDrPqciGG13snBoGfzCbGI2IYrBONgaETvBlBa7AV/in8I2oPClWTmNr
LxzJzI7l6iRHKxT9SmLNAZ2kUnolE0B08+DWWyn6+bVmrBv16XbaZmo0JnTJbCSk
IIJGz+yGlXHaIPLdIn3/ouOKdwDtBRwCGdE6DgcH0TCGJO0A73vsXIym45HxZ74n
Mv1mdrdyuIZr78JM5EOlD1czqspcCM73XZnRgT1DAfJtDj1HT2z6jsrlepJHAzxo
pBrJikkl51IkDlJp0IztwRa2a3Nscdr1KKd/FUKQEoj74ga3Lw8cSmOeYU9o3KQe
DzE02rVFbdFvgamhqYmdRiyKrRXLUmI0IpOs+ftAXPWm2MDr0YMlFTIHppaVT6oB
ICc15ZDoUoDdLBBwFztNm2H8UcnplrXLIZQEHOYnS55s72RPMlWcIdIVdZt/+Od1
BDgtMBimGJ7PmN4Qhs26ZxQkAaZBuvceWkiL9ZziIDQGbzJ5cwGMaUGGzF9nhrBd
3bq0friQkI7KcDKwVnyh7sWBgWJfM3+tdRMPCaWDgJ68V8wpd+qvVSQFxozpV59W
SePv7MwQddmvAVot+XtldairyZ29lQtcGPxIPQzyqoke/f78R0UKqG9ugI0cB0By
UR2TcAlpcxwOpEApQBboziLpragIqhd5NtEj2RVD8e1dtOY4CD/jxiVQKqJTTrun
nWBBVWMZOB6pMwoqDJAqjjRPOuaTHBMgI93vjllKfYIDcx0jZn2D21ey8J/LQJjn
rHL/XxJubai4EyhkxTmrafs4VZlZtoc2py99Za1zX90fu1dBXTQ3NdC2qmZ73Syk
SiNy7kOF8aCBcVmSbfcHfCZeKusCGe/KUeGbEUHqHxog8x0PJX0Zp9cMyc8WlhiK
Ky6x8BMTh6/GKHoi4ygDM+wcT06oh5pg8U+gJeDBO+m/TVQkDm9jWcPFqiTm6plb
48KuuU1jexO9/WXIGjYP5rlrViBRIQ1kBCSs/ZGgT+xHyL/U/8YzNtZo48pLtfKx
eKN725KJxEziRXGjKRjDUitJtc0KCYeXWWkgls2hQNkg3vFt+moLgV6UVnZwg+Tp
Kkk5AlXFBLDQUQHIZKBYI6mmzJntMMhtLtE7qR0S31wOLQxgR/KvClwJ41MfqXxS
ShSjgu3ZmAun4TIc5Er8xHtL2fw46cy8NMAAkMZgGRA5Lc0jcbgMWdqz868Uoumn
CABiaM/cw/fLIc9/MVDFrBM+m7GrJJJe+8+GaY9tV+psxo0SVGNI2kqoXVI0yrTJ

```
   WhVik6d6oJaGviNjcZaw4C5kuZ5bKHUCiMLv05uAtQOOyPiddgfZXymBoKCjndge
   MNRBo4MxXU9cYHzi0umhauiw9I3UG4HAKH75L+1DFf1wbbgu165dCSIo2wVTIgOt
   zr3Y03kTJJidclkYzP7o2d80EMGftQQ4uGyEtowWJbEn0yWhss35Vs3Fyy10mwGM
   pncS4Tc1dVGyddkDXyAZ1JvfFzsXnoX+38R5lI25aYHAbfij582/hv48FU1I3XoB
   WXR/gIKr/hQ2cFLwHsiJlGRw6smfBGOzk/x4JhG7sCR2E0QmM9CYzmyhZAKXORaX
   Ur75d8x99mIJdEO4uu4avHvaRouG6D9tPJWYIRioVDTPD1AU6qirN32hOupGwcz7
   t8q70Jbv/tDpcLmLNX5VxsQzUfjpsGGvuz/Eq77raPG/TByissRMTjUuFv4BxS0x
   wh//p9l2sJA4FWCA+Sr5YLFublQqRF1C3Vv0h2YEEz+sFA44u4VMmcCrwGBoJob1
   4we46RXwzH3K7gRV/1tv2QB9pK4G8KxsbHXNV5RwVJ6xXI6JRvIJru3/w4nRPnrA
   lRXXfx7senJDd2tXmXvYkA==
```

C.3.2.1. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOFwYJKoZIhvcNAQcCoIIOCDCCDgQCAQExDTALBglghkgBZQMEAgEwggRABgkq
hkiG9w0BBwGgggQxBIIELU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lLWxlZ2FjeQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMt
aHAtYmFzZWxpbmUtbGVnYWN5QGV4YW1wbGU+DQpGcm9tOiBBbGljZSA8YWxpY2VA
c21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxlPg0KRGF0
ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDoxMDowMiAtMDUwMA0KVXNlci1BZ2VudDog
U2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KSFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5d
DQpIUC1PdXRlcjoNCiBNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1i
YXNlbGluZS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVyOiA8c21pbWUtc2lnbmVk
YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBUbzogQm9iIDxib2JAc21p
bWUuZXhhbXBsZT4NCkhQLU91dGVyOiBEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEw
OjEwOjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGxlIE1VQSBW
ZXJzaW9uIDEuMA0KQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1
dGYtOCI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiOyBocD0iY2lwaGVyIg0KDQpT
dWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lLWxlZ2FjeQ0KDQpU
aGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZS1sZWdhY3kN
Cm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBTL01J
TUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJvdW5kIHNp
Z25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4NCm1lc3NhZ2Uu
IEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIHRoZSBk
cmFmdA0Kd2l0aCB0aGUgaGNwX2Jhc2VsaW5lIEhlYWRlciBDb25maWRlbnRpYWxp
dHkgUG9saWN5IHdpdGggYQ0KIkxlZ2FjeSBEaXNwbGF5IiBwYXJ0Lg0KDQotLSAN
CkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQqgggemMIIDzzCCAregAwIBAgIT
Dy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJ
RVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJT
QSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUy
MDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
```

FzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8A
MIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cx
Qq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeu
Xq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7T
HNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3We
ag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukg
n+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQC
MAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNt
aW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUg
MB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58
BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAyl
OvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeu
OA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9o
pwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4
oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPf
qmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY
1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcN
AQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNV
BAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcN
MTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr
+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7O
xsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTt
dg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZ
DQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj
0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEA
AaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAe
BgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUF
BwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBm
ZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQEN
BQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTn
euK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qN
uz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt
9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh5
2MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4
DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMg
UlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnX
MAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZI
hvcNAQkFMQ8XDTIxMDIyMDE1MTAwMlowLwYJKoZIhvcNAQkEMSIEIBmb56ZODWgP
A1SVa8da67RsNicfHZ2zJVUWYLTKrF07MA0GCSqGSIb3DQEBAQUABIIBAAou3+Ck
FB6wTfWUVq1ABIBF3AFS+wBR2+mDSQKXxlVCnt/cfY07qKDX2YsVkj1uXq3I1Ptw
6RHEtqtbY3iwAqB5pzgfcw7qZHDpRMMEwobNLzHBdSZwW+ljkQ3LvDAZao5c+Cmt
gSUCdnQ9Kvzdkl+xgtJQnjGGGNBiiWDb7NkZhlHYesV7QKNHTP+qP+awE1ZMrOP3
qBgIS1UH9nSNSmOfyTprD8MWoUKPkzFI1YUyPByE/QKjdV245YvYuZjz0cqn4VvV
2Y6t9DI4EmJJhay+P4EJwiggTjH9mJeeXIHyKpyELVSC5KCaIghQpTHV/pIH+fNs
WxxyPU2C+RwECSI=

C.3.2.2. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-legacy
Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:10:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:10:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-baseline-legacy

This is the
smime-signed-enc-hp-baseline-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.

--
Alice
alice@smime.example
```

C.3.3. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 7760 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 4732 bytes
    (unwraps to)
    └─ text/plain 319 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:12:02 +0000
User-Agent: Sample MUA Version 1.0

MIIWXAYJKoZIhvcNAQcDoIIWTTCCFkkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACnWkzPI3J1YHJzg+y81VoDKI7z5vg2c74uE
gBsxorvh95LsdB/zaB4nLdCgQhV+XW5s1srqRKOioiQYbQi9txvMOzBb8ddZeIqw
1CGTLr7OXx5STs4flwJTYFBXOSrbAOYPGrWpHT1M+yIzDO3oAWJRy0Q3eRJW9O0Y
bC5+YSAjTdzdhMnn0483TQNyAun3CV1dTvQPEgrZUZi5/932YEN+sEA06SEPa8Dc
q8aH0843aTttnoRZGm+MGWOw3LWD/82EwRhucvLPhvusoKGIqGuEnvd0ETfTe3LV
CwoVEYotg57+Q1IW5dvio6fmXuvBARHVPOEf9K1Jp4yKgJ0Cko0wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAIYzFIRtcEwk97gg4gObZn6Ui
HpU7Sa/VV4edmxdBjOdBx1BJzDOhwM1kUXSqPgOZvRz9ehSGujeemC9uYfXhXo1J
AWf6ZW2i84zmQXkc23JlUwWajzraVfq6lJ17gy+iv//EtUvka/p874YRKnW6rDSl
PZzdYxcGKh81dDmwRWcvvNQbyMT21EgvjWxm5/Ca77aSseERt2LjnonrKRvSfwsa
j6NZDC95Pd9GplsvgZD1GfNmPtymQaK1VhRy53D3+Ne1xHr97C77XYdJQefaZH/h
qIB2PKhjo3hLpP4dCvBDLI2TwC2wIphQ5azqH3Lcv/imBYuVqZM5UTJlpK58pTCC
Ey4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEF5qWn/RJwrmJiPW9ewiei2AghMA
LYAJ/u8gGEAJbfFuXOTnN0ztW+UHE3nWkbWmNf2rYdRCTrt6/DnH43242t/LkEbh
2fk2eOyffUFnrHglZsRWqfn4UT6dqMFfmNDzgCIx4ZlqMUbkBRvn66S2/L/Sr1iM
wGZBfEAKhFo80ldzkl/aCaQUYVQfZkoI1clDg5ZxUGTVV55kirvTs0+PPir2ZVCT
aUhvZIZPsW0fJAqGjDxq29ByDe2hSxYftpiqequ+PHQuRLII7TEdUnZs8rOprsWj
gn/BkPUiYKAuwIE/QCgd1gBW+TPZRYO8TMeZHaFYx9F0MqDpOLjpgH5msFj973KK
cds0rJVZ2c3Ei/2VuxUvN0nEcRsd6Nfk+lny29hXuLCENLH5j+LlO12n59H81F5B
z0+29a1wRTJNt7ibVzrM/Bj9SDSPFzWrtaZ98UjnAmhTx/4X4O9XS7gEZBdbveYy
+c6Zp/3cUcWFHp64gN9Fyug+cTV6U04Y8X+DzxbFEeOjKfx5nzCy0m2c045cchGx
54vtFwihMrS29C3SXfZTRFHBT/zTG4PXkqKgw+ZbQYG8917ej2UqNf5+EDdK17cY
r5HGlz709hDJ8lMfDzfzW0PZ/60aE+OyvfZITLOZto3fUHM82+kZt09p9Gd81fVu
```

o4mrRTw5CAFbeqv0OpIKeHc4Buq0CnOQyAIJ9W2AEzhr13DuEHHBBB0hk1q+UOlh
AfHC00arooIC5q7wc8sBLJju35AO9msXje6mYGNewzZkVZWLYYHlwURtYbEkonJh
nct0ZA37gL9Emwi/byUScChMlx6IhPrWdRCAuiTWaJfmYR+Enq67wGrGPkU2U3eH
5XOLto815AtoouXP2C9nAvdGfwyHA8GvD28Ch8oDdof/xa4rZZGdLAsBxiUd7OJs
CBBfbSusJqoPvC4yfeR+66GLtvVpFtmVZ+mTir1ZXtckkn5Dn+NakfV2wWvQGTKF
/dzk6OQlu/cCqwBt2/Rr3+CNy1SgJLYstMPWJezWK5ATzmtTKZZ9snyibsskWXlW
QDjZO48lgWaeK3hh+EZ9B1P7tsvgR/E3owHaODrxmTgRGx/CCqlnZr0HPmPBg5h2
bSMYFybxr2CPgl0jrlNWvyZq9g8nFeVg3bqCncumOB57j1Rb4jtadlQRAHuvlpbO
mGcl/KzYqYUVq7/AcV/39O/09mW7xLzgpD9F7KSpC3KxRutZPG+f5o+AGTT7moxD
hqVtwYnZByekNRU/dcakGieb4ksjyeVC40c39Xf8QTfQWm2u7cEjnfZ83D6kwrdV
701NCvs3VCyJahysjUnzA4gRXuKzTI+GJungjP5PlO/DR2C3rimfqoEw+A6mpTga
SuTJQ6IruIlZTxfgAE41lF5RLkyAsMkFOHLuDIfaj6i7u/x1aDAY/9IDlwE+pA6s
IKx6dCyt4XIvTLNDkcQkjLMdl+i4B1O0eLJxanJdm3Ph+k50Xh1zNySbyy0NkmE9
uBJuE5gjjLCovq1o9rPR5l5YSZv0Rx6E2GuFkcbjCEh4WcOixb5CSDYgZSGZELGi
7smZ9W9WM1eadb8gCQIp00zdo1A7slnmG02ff03WAAXV1GYzg2c7UdgQdqhuL/eI
Q/eZhGeFFwA2m2e2H2tCIza1Ezmzd/xaeqChfjqxjanEUwBjtEuvi4B8hGGX4+0n
J8/7bKkNwibVQYHdEy+7fB716NJHrGTI7dzevIyqOWsZLIPYuIhn1SP/02C+Y8bp
ChduQbWqUq/EOm+miVEI2z13i/wWR1vT1ripJP9U4tgENzcjyiZBhzAIL2Ionf25
M17kjHQhxS54DGZJxiff5cxBWHG0vvuu4W9M+3zGPER4yWZML+5VrK5wNejz1PPW
5kt3i2QY5al5UjSL2NIKI81ZNJ9IkNGT38Hb+jSobs3pvkPdnUbl++TjAX1RwYgH
Bgr1XpD+ek8xoImLNcymaJDqApW/Cs/9I1GvVlXIT6BQi3eA0uy7LpaECi2gWMRJ
a0R0lNt31UGHRez6rv8G1VthzVLNOXYlRKD8p2/NjN/Giaa1yJPGAu+z87G04j/P
Zg82+8SWYM3A4crGKjk9bBAlm7Hk3qTVu1SeyBA0dcNyuVHlLYInmzkvo+KGhDhl
rGuM3SVRQdVay286AqX27HUiyHZ39ebqJwMWY+qBVKSjwBOI6z19JOBrMuyBOdzV
TH2ck9dLF6+fQzfLLspnBjbrdc7KwbjuIX2Nj1R9DQLMC6JpnByGeo9ctrVeC3Z7
KE5MbppSG7gcXTMdqohjauu8Ru+PjxPggjtazUymKoEoMJFY0kaww5dqpYuPxtjE
YRgYyMfRFYO7qnAU7+mdW2XzvGJAyVO8o4RcHnaiXenlZs+TAfQ0GovOAKyBwrtw
ob8B35Z/XPp3trlRuGgWaD7TDYSP9Sz3SvPhIpPUbScCFlHw+o5GsF5eoDGE63+g
N/ibjajDNHp3Dk1mIfMXAmErP8bqixSKXuPltf4U5L60pqhIsmk6rNdteKdlKBGi
/Xn3JXT4Qj2PicodzWDJDiaEjn9QKlFQyOXxSCdT8Em5kfptHcclRiNgsaIxOvpw
3RRsPNjG78iWQugl0XAK+HQUP2KxyGwWQX0oET7M5PLhPGhkya+hT14nuK3i0azy
ULFRCtnSFowW+q81qmJYUUfrcZ0QJf0ABVPbnVmLY9kOfG036N2NsPT1Q8alEzVB
/CmoRmtnfJnKJUZubbgTvdqaQnH/mBTg8FiA8i4MZAeFBRJcSRLE+hfL54uA8GNf
6xr4D5eWIMXmvlWKiQdOO0DW5u/c3leWzVyQFqm/Cw58cXnmTFE6mhTrWktkFlox
S0OQB/fzfKTuJuxiB0dFrPHuAIR8smUiWZiyz7NzXC2C7UI60t9FhpfQIlHjAI+i
iktxm9EdGq5cix4RtG6o8lts8kJl/kBLTmuIH95sfyNkbHQ2dYi4LjPR7PKBAZjJV
UyFI6FDvIOMUa6TJfK0kyb3y2eTp+iRzuys1APhEY2sAskL2q02ZCzTldHNJfwM3
qpKciyG0LTg542SfC2GI0SSHEh5jBVHy29liaw1R7ecM0Skjy8Z1MBiiHFn50QXm
5hJ+T2xI/214rUvESBrCpYkMTT8uKnAs6jRxoFvuK5QxcuOVIab1jA+tXsft9FW0
5kSEL3cxfBoXRlWfcLpTty3Um6AukDGMmleopM6iQMoBpeUqdWPmvi4SB8jMJou0
rL2mZcnai3w2tUe+eitwln6AIo5bOMv14NkWcFeArnLyguvjkZ0aOE2nFvaI/rc5
54QCW9/VRU+Ku/S77gleCNSyO/FMOEIwFIWzc0OY4fnQxSGmp90Y1AmB5/eqPD5d
1f7wF4OeNOUSkKCbXOA1VfmumJ+BzKdwZyjxsf5oDzMMfaShmnhtKz8lsfigHEic
1CFzufOwTjw3dnZrNmFIFhWBrcNtur3u8AMEqrmmWCGHnATxL7BUOTiFvtkq1SUa
/VqOk7gbvcAk3UdSVV4Ixr3AN3wiWHaX/Fmta4NJYM4xljrmWPL1nXUH0Nirv7aV
x0xHgzOQE8ftgIzkLjNqvQyuRaz5rJZzmHV20sxyKuK/GipCc8vx1kNrmUTjIjTS
0/9eyQw9I+efnBzydJRzDEoTwSh7Z/v7nJgMV9sxGy9MIX67z9WpCq0L3TuG+r1d
baCymEjFlWf/0l5nkNijswXyEglrgryCZkW0HHogwTAK+5efC+X7ZV0Uiyt8+HRJ

```
+63ZB86gTuKi8gM83p/ujliSjekCm0exPUEdU9LzIcPf+kkEDUZIBoKh558h/2nv
BWK+CVq0GFW+ztgLoGbDfR/iM/0YIUo71+gIR2GDZuVciMHm1wBrQK31BM/sfCcD
KCbCYf3aOJPOu9E44tHjA13pHy9d0uRHHAvLrPxRMCgDkDSi+xNrGeX0dDXfhCgi
iMvg2dxn3C09PkzOYXUQPvtUua/qbZNXZW22sg1u3iKaQ0z4rgNLed6i4jHu9KBS
GjHrN0l4qKrr7C0sD0dl3MSL9M3IRlBJeJBLw43NW7+0X8EE58UWHB1vLemQ9vLS
AXsnXM5YHKBBwxLqxgXFsjISO4ltTer2pl22zdo+Um6cBu4h3mS9AoD8gKhq0q80
MU6ldCmyaZy+9E10HeNNyMt4GU917r+YuEq9CCb7AtpWtJokTCBv0Vr7tLt4Bov7
kinWnCF/JUuxx9QdjEOHzINkQiEq6XyxTkoUcjWM+FdRXF1KKc52JpaMYzeMV+Ln
VSJukwaVCmWMSEeKdOGUo2m/KQO6gX0DReoG7An9cDnTYP5LaNeP/KTliiBkLyaS
jddvEeTizcqKFHFjaanzeEYVavnFASxmdlD1jv06EBQZeovH7NkZ5T3QheRkr68m
lnyBDs4R1xLSd+PRZhdFg5fL/mgdzYCmYNu6P+rwgsQpQZpSbcu2rAu24fEbH9DN
RIe2Woz2tMIx6jTsAOBDRsDtXMWn/bqZ/lc5YaVuGsR0vFf6eWK9jJH3VkZCYK0E
ukwFrEZGSCWVP0dOepYl9tIOU7o2BnQeVBAOas1jnr6gJWueoazZtgQHKtiXo582
nzLC/zS+72a/9JaoChclM97ED534fqkND2SVHPkClxr/wRk0zqSbOOkA/gLzis+s
RGZGMOsv9aCIMMUowMB3XKSn6qEXJvNHeN2uH8p5a0Eml6gm5jyYqJlV0q5a1lhC
6vTbPbFXCWxJS1daqiZWtdVp5RK7qoUJY0CG8etYQGUDKsvUqr2J59RXJKA4mBR7
8beQL7SvDvioaHL7sgoY8Nx9sgCtww8MEAKvRnOkfD6tfURjivu8qz1tGAF/INQ+
RvGuw514o8giG+WU4Jcoz+QUMpL7SBSekiGnPE6iz5gHIXNtM3FUTgHTaCVa87aL
HH/idVK0/uV3Bj774fJhBrfLRxGfOPiaPwjdnE6W8p5colXpUw4MshD2zk27e2cH
W7hpSl7FI427vSKu+9CYDmn71FNkb3JRP2Sy4uBWGBftObmJKVvuwENpiL8D2QNH
f/tvY1zTXJTLzwWiV9vk82p12BKR6BdLY1hyUDEft+MOulXR5hFmuPdbnEdDUX9G
pvvYvb9y9SdwjheYckd3F5R5TTEHTHDyf8+zYEbtCazNNmboKgpvd9z4Xy2RUJK0
4+BCmCC2n4VDN9Ztaf8zVnBCA6vxBf8kSCIoFyMXazCukX11pDN7qhvkQG+BomwJ
AK0UY20qhfKpBRCmiGkglpjaBeyDsX8Bd27lurTRuVry6/YR1cw9zAhoOPPqE3bn
yFrSkQNaVCpAoqB1UitC8NWNsdCQ2h94w5Ai347vQf6SOR7SpT4zd5RNWXwVOlFT
UkBkocfG9JIFKsOapOpXeRc7J3quZEyo87to4U+12UGt1g77Q0aPT/n+StZJcNnu
MKQlj6UB2yQjv0FWBtjwxay4Dn1CKbgLFBT5qntcPBJ3gRq/4Wa4MOlkbDRdWVxO
LoLCgJRWI3aTR9FvjAmAIQjulvwCa8jNnwuXO6Hf0Cgep2/uNeT6BBzn492brQUh
/cpZ1L0yvSY0gCDBGKfcmLXxbm6jVA835TQ456Qc3MX6EEVJvBv0zoqh3EqqGd2S
+fKIGwolruj6Pu7eRDzI5rNmIPbg64OJVDnHxKCH0jhVFBkWGeI7EheYW49b7GPL
w1P3sMlA/67GXPJ67q9k0DZMPDxzTBw/iEnwT35vBaPp1RgW/dXXzdr6hS7kt6rd
Uxb5+ckIzCXX/BF1kh/yaXhQWAGNQy36g5uq77gWY5ypa97GXojuajqpjLrpPGom
P9TWlr1aXH8WOzFaZXMa5xa3YoD9unQIzWRMW3ysobjOvIp+Fmj1gsIlgrfbNI1O
RJaC0WXfX/3WuguukJzC8nAyTVM+Aj/bUZFoPgTCaZ37KXJy8ORZjhUmZ7wMZWh0
lprC6izOj7CUE+UyPUBDn1nIqWRclShIyUIvkGkvsqCPRseMR/K0ObLk7PgHuq7G
VfDTvOyeMGVjrJUPxsydbA9zF6GzTmT6PWNfsLlr4wX38CQkKQzG/8IEGvYQ6xWT
kADeNyrFvVVE0diZgyCcybjTAI1LGj8n36DQBmfpYp1w6T/EyrznwS7PtRftaTm6
bI3eXQqnO+I1HCR6+1gqcS70LK+bX+Cw0sNzLaUy66XVm7/CxYJrohRkNRxTGkHy
cqFFL/wBx1TK/jhARfxm4kWkW7Fsmo5t/ZRAv6jMAlYMjHdBF20HKMNDhZWtf/bC
mEV4/BERSfbHB60aM6ZXWUzBlf486ffAvxsQy5qGjQ/yJIwAMN84qHZvqoA3NwIs
JThbTIFM0Xtux76AITxAYIhtB07ChxXrXC/owJ35oFve+sq1HQGh0fQIGTgTtv60
tq82T7KLO6ervK1UVL6oxHkt/xbr3c6wu4wd2Vh+Kk3xn3wp7ShpT6sopk4GCdBv
mxxbUu50F7e7tlc/sxvCIU1ObwiF6WOJH+7RUJEGmWpvt7eGFZSo/h8oLjnxxvmK
Qyus5nGIIWDZgKWYxxIGpQ==
```

C.3.3.1. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIINawYJKoZIhvcNAQcCoIINXDCCDVgCAQExDTALBglghkgBZQMEAgEwggOUBgkq
hkiG9w0BBwGgggOFBIIDgU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1w
bGU+DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2Ig
PGJvYkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDox
MjowMiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0K
SFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDog
PHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJv
bTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IFRvOiBib2JAc21pbWUu
ZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTU6MTI6
MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTVVBIFZlcnNp
b24gMS4wDQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04
IjsgaHA9ImNpcGhlciINCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMt
aHAtc2h5DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0
ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFy
b3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYSB0ZXh0L3BsYWluDQpt
ZXNzYWdlLiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJv
bSB0aGUgZHJhZnQNCndpdGggdGhlIGhjcF9zaHkgSGVhZGVyIENvbmZpZGVudGlh
bGl0eSBQb2xpY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlLmV4YW1wbGUN
CqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3
DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYD
VQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAX
DTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PH
HNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7m
ZjqQeb6FUH4i2GMt4jse2Dqs165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eD
hv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8F
kyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtj
hflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMB
AAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEw
HgYDVR0RBBcwFYETYWxpY2Ac21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEF
BQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N
83cPMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEB
DQUAA4IBAQCBSXignLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjo
N9f/gsOx/Ht9Ii6zyBZVjdaox644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUh
vdTxDNOOoHz53PYDBh4zE4Nar2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNU
RexTg+z3web/eDOdu+F2MVtluLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyEx
```

```
l56BJABb744gqoeuD9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w
06jaRzWdNeXzlEc2tUpAr4vRhZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kp
olw69Phqzpqp1zANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQx
OFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMT
DkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
tPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJe
STulamNfCwDcDkY63PQWl+DILs7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/
esFfs+E7QMFtmd+K04s+A8TCNO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnh
xBW2RZAeLqzJOMayCQtws1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNX
d3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJ
BUIKkO1zQ1Pq90njlsJLOwIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0g
BBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1w
bGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQW
BBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2
GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9
HjQEQ+v6BdP7GKJ19naIs3BjJOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+x
h6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD
01DZZukKYr7agyHahiXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHB
hOiPU7IPkazgPYgkLD59fk4PGHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN
3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAw
ggH8AgEBMGwwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAv
BgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkC
EzdBBXntdX9CqaJcOvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkD
MQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwMjIwMTUxMjAyWjAvBgkq
hkiG9w0BCQQxIgQgL6N313auMszx5Byu+sPmUUoQvZ6glyBIgh0k1qycdmUwDQYJ
KoZIhvcNAQEBBQAEggEAmHzQqLkVTKl8TKMaeYFFuU9fLrHZbg3aZ5eP+Zt3OkIN
ErSsCBXE2V0u7yCmxk/PdfkTzOoSI9PW/seA5dd/W6yrCVX7EhqWWQx1vA+s+jtx
oZ+Fh5a1GO9W7XmcQBvpjJQL0hyt78UzZt+CL0K5E5oueKj9CxCBkuKlgzzvwtpX
CAK6iYUzwGRWkxqdBaClu1xi2OCEzu5mbpAUY8ra26hGGaExYIZRVbwNZ5uGjfCI
lsrsd5wFdxQbcWOF/M5QIjbed1Gz862IZxaOA/fRY126jdeJyG2VKdD/3XglLNx4
+6kU9F3BYb7itpwqnkY3MiKxLuofNQVx/ZQ1m9arww==
```


C.3.3.2. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy
Message-ID: <smime-signed-enc-hp-shy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:12:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:12:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-shy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.4. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8170 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5046 bytes
    (unwraps to)
    └─ text/plain 502 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-legacy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:13:02 +0000
User-Agent: Sample MUA Version 1.0

MIIXjAYJKoZIhvcNAQcDoIIXfTCCF3kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBADmQPwawzwzPKIJbuLJ1LeeMRHXlIoG7j/r1
tvkHMo9bUUhT8jdexlAgl1L7CKdQmfbXbMq/lAMUe8727BECAU/ZRqw9ZA+a71Y9
NfDivBgRdu0W1qlL0dcRiR3gU/Tbvx5g9kEbQxT4sAqrVVJFBxPxKH1E3NPicFkM
2Cfe18+fM+o6+45xZgKrV3tTO+xsoJe00OBOghFEItp2p9q9+ItOPnBCrFl1Mjed
B/5DmHDigcV/KcJqpQeZGifC9q/3uT5EIqoEq22gyTAg+q+SHASpbrUdtTAI0OqM
MeSl5Ou7Xr7oA++n5nn3KGm0NSbirWQ/luGC8txFEaEM1YCAHzcwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAHFfMy82jaRS88AdeeTpXTcI5
eIWQXlgopLfTZVNWouqoD0UNwE69mNURWUBUqND+ascj2aEc1SlzzZokWMzfAb8U
+HINE78pYcnd4PHC2EnMf6peasmfJwHgrNehJqy4J2WhaQpQD6em7S2wQXfCjxgW
UZdM8ouyXw7VMYd7CDQvY34VGxjWKooTwsSDriEL/CQ1ew2tjsXyznHDkfbFfpxQ
XtUciRQX+WHn6uZHDTGZ5/PArfp+hjsHmegmIttON0Ggk5Orh6Fw62+O56k8W3jQ
Sgtlbqigw4/GnkEYBZ8iYF9dJuQpMV41S3tMcZzwM1FBTwLpW70gMeDtpjOJMDCC
FF4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEG+d1PKP9Bv3wjYhP6kQiGSAghQw
PgNipAhO1AbBIDyP/wL0dgsWwC/KHSouWRESeutz2oMXMW6zDwFHwWVAHUX4uRmT
+ZZVEwiS+wzf3TAfdOXs2kYHfhaiFkrJUxYirdyaqzuT11sVzKLt2F1+uxqud9JU
vLwZo7INJiiUYpredI3plWznCZd0NMhUHiWHv6qT2fBU1KPBEiO0oZ3NZtO/ZnAV
jdMO2PHAUwdnmqPLDNsLnsaNZ7i+b0rRFEgT1qeZ4xhRp0zSsjwvQn7d/WBCNDpC
9KKAP9P+Cr12l6PTjQnFx4NrDNqupw2A6A+qv3NRq/ymn8zR8nm6zGLjje5RfftA
WVGQSajJNLTDir5TUAtb3lo7Cv1Zb8VQZhqxTJJrwW3piWUTV9xjMiVL+h2sqdZ2
LhOnQBNJmFHPhukkdvkCPxbM+vylJU04U+5ma+ZpDOBCgy5nWRgbQbFxcP5dpGkH
dZpcf164e23dKGNrYWK+gjVF0cp2VpEilgZCwJLJYgxnpH+tcoSIM7XfNe2IR1eO
L7pAhrzTrVWiBemph727lAXJM1tWhhgFL9GFWkbkQeJq2ndpGwz6lK4Bk8Ri+9j7
fkXo8qt4xGEcE7hjfHPIHcXr4FhjYRrk2h2bb4LPAeb7E56bEl7XTT9hWCAoAT1I
lcfY8giqsny9xDeb8Bww/i7dVCzpFZCSNKxymnuWybTqu8kmnh4FQttwJFvvDCoR
Xh2j6mMO7DpzGx5v8E74lf4cXwYKdlOer0L7rBCT7worv5OcH+Hf86Hgg5NzvWTn
ZdCioihv4Nh2w5EmLfWLcwP9tnMC+62jNFCIh9k8EQOs6uETEjN0vyFYWMM7aCIQ
JgF8fkEmAs690oU77Na5V4RrGvvyhKZv2EPGUTdwikls6YsYgEHReOQ3hBVqrn/5
/Pm5m3LKe90D3ksmeasjTLBCf29RT+vYpHlLPYNlJf1mTTKZmA6FjMi3yjlByJe1
TbrhXpmSxloX6fHeOMnq9JNqQEgrs2r17gyMULRxDRcVcSwpHYIkAjmjtyfRlVb9
5XfK9/7bwNAH0qoXQ//tppHMFoyK59YyD/aOVvHAFyHvFxY/R63JkYd2lX3AFevV
OHk+a86S8/rlcSW5NMKMEGIR6d3sbUkoTKhVt8U/PNMQgTVbROv6oQQf6wB+VM7b
etSPPJciKCa0zF/m2FU/6HEU8s1DI0lioMgo+Q1YJrqWnAGlJ528Sdc2GTP0LKub
+zMRCZsrYzPHklw0PxuXa3hdyke/c6SZz890Nhhh9jWhlk+1eju7NmNYhz3t9MjB
```

SumAvmHOMoLOy91dBwhcCnp+f4Y/Fx5NdIkj7VJVngCQiPQH/pi2LlgyYfcmqRld
n4ZwC4JZgjvz1Ui6Pd4iL6TTeHeQD/OtwxztqFqiQXZJyRNqbYYJyGZbBz3zFviq
aWahRK9rHYHVDqWKBy9SmyjiHmjVZluWXdK4zDkzWeqcwYHspKSYnymcBcrBneJZ
Hpy/bKK7RVNyUOE4V1duhaz6vUdkXG3KHIWCePPr3crlUHFB/H+CSQ3PXQAA7qNy
DvcD8jQ4TxDMhj3bWSaAKVL+SZiTBSVVXX5A+OkGHoe57TDI9zKqJSmyh1dr6V8P
LiFdSfmGKA5sWuTsta9SMslWobVguXuvYTxE2V1S3zoHgB0p1efJ0IaNH0i+gqJR
NquG2fjiQpMQVYypG6942C6RXNUU1aLg3kH11ELTOmNRCw6EnL7xYA+xwwWQw72Q
6o9xUyrX9AqEv8cH4IMelIpkBue1hhf15eFpvB5y+cUlnv6OjCaINXGXEcNPlrw7
0mvTezWJXIyP1E+x438ZSFkN8EL5DqvbttkzH+0qcUCKwp2/RADofAsRwDdDuIOF
UQby6oDzqLTZHNWvrJiLkgquJ1iXWiKEWPAppgLc1pYzzBDFuOIKb//tjUznp0l5
lyCNpkazuj2FGeDddz9jvWES5u3jATrG85wK4WTH2vjIh16Tk321OpwXeJP6M17O
cG+NuQVPR2r6K1D1IZSGOf9/nsDVtnB5LePXyczIPtPoJYGx20Kt2IUyjJ/00mxt
iGk3/KZsVJdukr8S6U/h5V70E/i5o3GYgG57iLX5DoA6uMTlxi5SEEv1qYMd/fw8
o0PCZw8N1kkkLxP4bKtMJJcAasns68CSu5kxC7bCynjEVR/Ea0YO7bAf6V+pDYYA
ABLNLdZBQuYJ5r4G5TSS6YQQ/uh1zOOg5tcUS3JPb3VYVXSthtpxaR6Z0bMv5tKC
ca4gleLxxv5qWetxcNTKR054tCIREGX9qUX7HhIWV7cd3tiaN3N4RHU17nfy2mr5
geyQdfQRckTzuH66/a7czTqlVMUw/3oXNwqVVyxgyg4TJ7cHwfWx5Em6VCdUAeYA
r/pxcMMlwboDg3gsUuhwBPInGrbs7fQwe2LAJw0zXIjw61dGPF3Q6IJHZuStrGvF
3GHO7/U/KW7P3aaVdBR484uaCf1QGVgkfZYLZNtdATh3uydDrhLot+DYUcD0RI5C
YIrZzUER0Wq2/HskDBh2O3LxGxAB+HAbgzIw7od23AIzrTvwTeyGY0Fotnr8y6ag
a2TjAEHxSItZ7/YT/SiRHJVPDilp8aptPKDQUZJS8POyxCy3zNKANzcDkspdcT1N
R25mBS39o5ab7q6eKiNF6moGRxG1ZU1ghXYFOTp6lHXv4YVpanOK2KKR3efly9x8
apD5Baaoo2tOmQ7Xb6d+NRT6RnrIIB2jUyqUSTADRnVQEsbz2nxd91+HFAChc+tu
7bn9swHrcgaBvC7ynFs1KIIx+UFPqEaOPwzbE0n5xGqja3+VFoEJ3hyOQ58N5Aw8
pgPavMZbWeBHwu8cos+FiTtRsNHY7KxYXPjirYRFU1d03jIWThwP3omjfS6cv0S0
wARwjaiLisgm4g8hj+7bAWjsXYNXbGhqeqbz3pYWYH5BQE0TIGdddXPjAFJs8hih
tn2bOXQqSuywiuX+RVXU0rPPoN8baZIqqLkxeAigsNzgFLhQoiS92hmoCsxgwoXK
EBGZdUd4Tq4V4BjhRXqdFf0OE9jh5pY4xzslnYkxSmemSGqEbYUyJQKQntzx9SdC
gdwsNGOr57z00ySoHMWvChgw9RKZXdLF1MPp3BjIaOXwUhQPOaQPhXxSyogY28V+
j4cGogR4dSdR0YhVT7HeaqjCVHbpxC9BJD7OXE19PEU6wBSInQVwddoYHgxJxEhS
o/GVUO9kqqL3ygV75MtfAOSFuO7RgkQY/geSQtdN6+DZ36LdP2xRdU43aICpyHku
fbUpAyIxpKYBndZAkf/zvDSX67SvhIWrMsuv3VMYZSArW9WWifvQQ3RsYl6Z1hot
NbJyoRPeh0d+18Gj/Nyd2gRlTPzIsfz/jdQqfczTK9d8ewTCAQl1ddTaezlrmT+l
GIniD99EIhouDeH97v46rJRtSTqRv5EtTFktlQHooHJWM/nRmvEFE62YqMrfT1c4
US4JkBI8MBL/oB1I0F0SBol1SWex96Ab1T6XdZihJXStL2gGJgQNQ+Obj9GvFfYJ
uEv+LUP88Cv1MWHV5OrCUXmUnuaGj6RLM27nL6pmXTQB8cf8CwkAlYP8pLzEn7I0
JigRcYCY6eevrctaIPkmmU7PKAB1RF/HUTdvelWzN60jF2idZKn0Oc0ks+o8IUpD
uoh14WwvAZnXbKZBWasPuw3VAKCNiJxik4F8/7S3w75dW2AUmwamSFWNCpU6B5+X
9w083nMsnDbvRai7BHPmpsGmppuH9RHFMFHwiV66UR3Q0aapDoalA6Xo6uFM3KtA
ytx8v1qaqmI9XyWO2CySqGMR+d/Vu1opugr8jIrJCo1FGNhhj387FCeZsBGsKAo/
Lu6DgvgnV/DcipEafi1O8uJrNcqM34FGNL8IGDcWAZGxORNIyIZ3x7dnLpykaoS+
CkABKOMiUYHwEqER1BptchQ7za3nh2IzYFXbPs/dfkLEPE53+RMe7KiDoNDp64Qw
QrZqT8powhIZEVsacVKBe8iiOsFYK1KuAL11zfvSBFWfXJC3pHZOJWqhlYjsATmD
FakLKn5FNuib4PXo52fcqz+EhlqxxxjXePjtIA3D1IzOfH7IofCX/crana7PNGzU
5/KX+1e1srAhSMuylPYSjJFeIQ+Hj63LKp0wisFSq5eAeSh6BbRqCat24xozeMs1
w5285nmwglBHXR9daIEyOZbN67Aa//9V+ANayy2sek4pdsTMyelCtYng/3el+3yS
8eYxeLFW4u/9xJsOg5zKwwKkxWUadRZrOYBBBjZJrwQj+/C/Ydl/xCXdCrzgX5tM
e7NfqrslEd4yaAAG0KfRgOzmhinTnH9xwMk929d/zgcYtcpBhOLXnsbMCpcOsBlg

9YFQTAINMeIXRU5JXUsOxufbDR/XPbLy9bgyKBUUvSvypwEa8yvVaoJvO1FxmC4K
Ne+843Wv0RR8M0QeTP3uDfqcw7Rc1if4Qa0fcZWpDGec5yqoiL8Rx6XpMUhxqZpm
KGw7waMxgP/wXouwXJNFvhUcl2klVG00affvlt5IxJFly6hckkGgsMaDrNduziPn
j00ugta2EgVnAa7fDe9MRXF40PSwR2k62T+OdxrRtC8Fvw5wlQi9etWG0VGuwxPN
kMTVWtOHRPaaySRXwOhw1j2PGUBBJAb/bFfHAFHHLeM3A2M32xWkkVo4y6bNGRq/
50XRISApwVZbpSUm94VD1++LYrRk/u0XUBE0vHUeP16ICKKWXk6W4sFfAqisuPTS
JzqrIaQcOEEcn8c//Jyo4HtmFmqDdVeax6lkNeQekyJDoc9U87Gie9E8bJWZ9F9p
jXod0zX7SQjS+FqXA3vPeSixDq2+4rJhUzsF8aPxm3/HjutoLlylXTi7V1W15oh2
fpyHBPSp9E851ZLlf+c0OXOA2HfixTjg7LVBwtf7jTZhUt9P95PIYQJNu0BhCe2w
TOMcwNVigbKw0ZV63nSs5zOJ7ZjMVr2eAONIYCx5trzS1bplUMdspJVkTUp4bycv
qgAXguOjMqxnS5ACuGIFiGRIyWMi6oVt/999wpSwJ71wV/rWZTgaAvU1h7lfqM/j
GxTHnuqVlpYPupUpNaHE97xbNbJoFTI77EnurLZssekD06jlzErtEkOvBZmj6KrF
StJMuCKE03KZo6BmOagisDD6RF74fMxgQ2MyC3KeWpjbE+VoMEbNEEcQYW61kyUy
Qgt/TuY0WmMyrfyZJf6/xd90zN8tLRqev4FvOtPxfHE4qEGzlRg3IMPKrdt0L/SI
B6nFxLwhsKLCzfoGYl2npk4IaQsU2v5obj7blSgNLhGGD//JQkbwNYp3UgToTsZL
QlpkEnAmardCEj4olwiOqwDWAZOCcicf8PcvZYRuTl8yZVlpndx5eGvmCdEyEayU
2LCf3Iiaoeb5gF9BWQt9c0nFXb4iDjbcK4ijMbpw5IYRHAze1/GMnbkJJwzItJM2
LXbJSyVC8DvUYjyJsBu7CGJpd53lks2Mq03GFGVo3sDp8RlAUddXOqnvKj9je5Qe
pygvaBbAFn9NaHNQOH0YRta9DEphGqMzjTgCtdQWhDHAUZ0P31fR2gcgBred6CuO
gwoiXJxTyhx4Vqeb7G+dqx9/TpFgN0/Ml2p10Bz5yXuDPAP/D3InjewCSgw4rOrB
6/W13FnQfpngWY3Q/HvQRVlArUbROy/qf7amnQ79CPzYKUIW8xn6rD47ssNT/9i5
anPtuUrX02E8Wg5GeB3unBvqsRliK3tbS5u4pBCEHWrvHQuDJF3VenPdAag0pM/a
SRMsrI8ScXsz5XeZwRCCkxIB/8GNwQuHsiVnKQ1tmBg9dn1DyxQfHyN25J4o5kSb
3hj/YtZk5pbOEtWvLOtMs+zBa83RaSWYaKn+sJESrx+pyU7YLxFKNmkbIVdB7m3l
4LXb9m0w5j+zXRPGvoY4hzVz1bTFqhXCKORnCjJdm/2J1vNMjC/FioeAOd/oGwBx
/knz5VWDpbxcl0zeituHT/Y9iZ0TUwDncB3uS/sWn1F5yEIFrgd4emtibETOS0Xb
aweHBTxxZ0IuCYhtbyqFPv+P32bK9dAsO7gVCCgrISA1TmTI9dRRJ7xE/P24OBSZ
Zl2/8xJsMjaxDvcS63hfWelbJRS3U1RRp9vZRbkggnutMrBu61NL/yLxPCS5OR6q
HVw2Pr0MvkRvZx+RHQf9oT8tc9owYhxwGhweF926OMlHwsYW28K/IKyFIaMWwlUH
cxYnc2yPckCN5ffTAdQXA8UNFBIBnSmartVGG5zxc1PoJCVax3Xz7Tgj+vISBaeA
HQHjNSzIa8APRIxE5jVMvzOfyvc6KtPLLgbOmvLmgyDC9rUVAuceVO9oyLS1MsCV
g3j4RmMIswPdagpYELQcwuek5e5ffD5bidL2Xn5BOXkMK7N2S1lXlmWn215NZG55
PoIAeXjgNDjdMmCXSt/frUvTsFOPtcCA2JAcI/e2dsyAF3iIRvPpDPRfUsvEzSQe
gB6OEFYkDOqcG7Lk9Hx5d78ZpJst+XViQAIDlgLHBpPuwkIvh9OOdeP/XKLH/1lJ
yOQ9mQCfuTx6rBtj2216o2L92OKFI27F/Ns4Lcir5VX0/6hrNe4/BlkAnexKnOgs
Ok3hIuQnB6C9Z2vtWt1P0lnsemX+AhIJPtgRs6aGhMUnIwtvb8aZwFsS8WvaA6PG
uLKBUfuv5V+mjt5vNNlnkaaF9bMGQVk9NmK6mgkqmjmoaXP+8MbKHJ7cf2Kt1Bpc
PJ8uPBQ302Qv3PjpFk/YYdi3tmmvaxbOlDkNCJ87xjN7Tlgd5jmBZRCDzxDBmbOs
1USxLB1yDN/k4soKAKL/Ze6rVusjC+GJ02TcWFQkS5eQjxoHNKIkU4fMDggw1vzJ
m5kyP5p5DST0+cko42Ae0yjn05T75MdYP0/l/I8YBes=

C.3.4.1. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOUAYJKoZIhvcNAQcCoIIOQTCCDj0CAQExDTALBglghkgBZQMEAgEwggR5Bgkq
hkiG9w0BBwGgggRqBIIEZk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeS1sZWdhY3kNCk1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWhwLXNo
eS1sZWdhY3lAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFt
cGxlPg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIw
IEZlYiAyMDIxIDEwOjEzOjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVB
IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVy
OiBNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1zaHktbGVnYWN5QGV4
YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAt
T3V0ZXI6IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNh
dCwgMjAgRmViIDIwMjEgMTU6MTM6MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFn
ZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpDb250ZW50LVR5cGU6IHRleHQv
cGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1sZWdhY3ktZGlzcGxheT0iMSI7
IGhwPSJjaXBoZXIiDQoNClN1YmplY3Q6IHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5
LWxlZ2FjeQ0KRnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzog
Qm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTA6MTM6MDIgLTA1MDANCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMt
aHAtc2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQt
ZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVk
RGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9w
bGFpbg0KbWVzc2FnZS4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2No
ZW1lIGZyb20gdGhlIGRyYWZ0DQp3aXRoIHRoZSBoY3Bfc2h5IEhlYWRlciBDb25m
aWRlbnRpYWxpdHkgUG9saWN5IHdpdGggYSAiTGVnYWN5DQpEaXNwbGF5IiBwYXJ0
Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQqgggemMIIDzzCC
AregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0w
CwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxl
IExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0
MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMI
TEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0B
AQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeN
SiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+Ithj
LeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/N
kug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSw
qpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQ
ury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwG
A1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWB
E2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0P
AQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSME
GDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4
oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIu
s8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2
AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gz
nbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqH
```

rg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RH
NrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcw
DQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMg
V0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRo
b3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3Zl
bGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/
T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5G
Otz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnf
itOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjG
sgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/
N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ
45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZI
AWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQM
MAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIc
l64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJ
KoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xii
dfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2
lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh
2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2I
JCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcB
VyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUx
DTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1w
bGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/Qqmi
XDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0B
BwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MTMwMlowLwYJKoZIhvcNAQkEMSIE
INdmPheiziYcbAwKeKaDpmuOQFmVMdAqPn4+xeOFjp3NMA0GCSqGSIb3DQEBAQUA
BIIBAD0aQzYiNU8AycDkBbQVbuAjHzerZmO27QlIZ47Cw9QfNcJ3w40RJAohR487
1NpkFskR79WY6aHuiLxClWV0Jw/iuieAFfBZ8Z9t2hOt+F93M+9v1eoLzrgA7YZG
itp6r5zToKCdwNOc2futk/+dutbrTqYlFI8nnjLNqegBiGMMzVfateMc2fVnIVN+
7/4fyA8ASzseEis/HQTN7sEjw0pUCvU4JvQy2klVYsaTZO4bdKXW86DHEWjoiweF
liiKSueA3WB1jeJRse2/g33dL+5++UUtQLY3kdknM78705WOaFg03V57abGCp2r+
bgcHQNhfe0MXoJHKqYrnG++22tA=

C.3.4.2. S/MIME Signed and Encrypted Over a Simple Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-legacy
Message-ID: <smime-signed-enc-hp-shy-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:13:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:13:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-shy-legacy
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:13:02 -0500

This is the
smime-signed-enc-hp-shy-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--
Alice
alice@smime.example
```

C.3.5. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy.

It has the following structure:

```
   └── application/pkcs7-mime [smime.p7m] 8300 bytes
     (decrypts to)
     └── application/pkcs7-mime [smime.p7m] 5136 bytes
       (unwraps to)
       └── text/plain 335 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline@example>
References: <smime-signed-enc-hp-baseline@example>

MIIX7AYJKoZIhvcNAQcDoIIX3TCCF9kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGpRgu/+AsR287dW3Ygyjh1atM+HOIMy1LVi
g0Kr8xBysv4g5DuAWfNU5MC40hTQC/VzBNQEYq9XKLZojwJCSAz/doygseKYXqV1
I9Mwh3tWaoHHgLQxoP1zY+AI7jWNIwSbTtn9W2YGtZCeZ0oV/7QY18nes26aNDgc
aRdEhx2jmLKxvhTCpFy7scICBSERea5SgN9uRAUihwsEvJRhX9vjngrlKwbGKMz7
ewpe0YcoY+gGRYqUYLKIvu6jyd5A/dDX2Tc8z2Zvv2MxYmMdP0okeAiie7diTHg+
ae9CTZN6HP7vbKHaftgcKcP7JT9x2PfoRLBagy1xFG9sy0DcqbowggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAN08bq23teHvwfECD/cO1SAZq
OJ8aphPZfk0r4yfTge+uSLc/UUk5ipnFTHrUfmf78/BQmqSfaPRwHRhLREaZeFB6
aWgZN/DSe8BpkheW+2Y7L01NvmREQZLP69mwPg1WQ+phUc/NCUvz9XCMDbroiX5Z
XwauA4fjKKRhn25wdrb0EeVa5PRg2CjjpcFrLWUU5TvDbEB1Qss0X467REyFg0QV
mSke9tdTh+M7IL2t2on4DIlxJy9A+dVtwMgz8qd/bw6a5qGC+Hk6CgpskEfexANP
ypqF9iFQW/1lr1NhDOm8OQLgm4PG+/L5nX/xsI3QkgBbpC7N6po06+W8Es5lgDCC
FL4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEAYLQLnmoDE+1L9M+p4U5lSAghSQ
ukiRYivwnbEQfkBN8oIwjd6EBGHDfK53gjhPxRaaY43MwJqWoSjCQtJAzc9to2DA
gFyL/s+lMGXxapd8DHwDXu9Sota0wZ94gJYSeNMBJy+QTjw0rkqMrurVqTrlDs+v
55xulqMYcOw6WEAYdJwMZ9TPsaHb9af7k+KNghTBUpteD+HGozWGdOP/WN6I+zq6
HhwjXaEcideIxg32j8yT0bDHp3lz42eFzlFNCHd42bcHtEDFGKFUTZZVO2B54hcv
DRDqLSIIwAs4TmW7ajD+qcfM3ug5lRj3NJERbZyBjjxwXCDAa1P+3ERBc7KovqWC
0NOgBLcxQL97EA0YcnYuB9qZaNC4/Z9tnPdocCCMXViWkqGhfaRlCHLSKbySVOQR
3lqLSr8S3lzQ5L9+GFw/om/Bto2VJp1AHWa7wdZk9CDdZKHk93eEGPHpMTbzcW/Y
L5kaD2Yw+vRFIM4ZYYgya+WkXh6SQYml+dAKlsXE1aGOnsTYk6odoanC6Jv9Az0l
9FeNSeiH54hSyDNaDjcUvGOIm8b64pZCiZOc11qivKOmc//n3AmUTOk3+xvu/Icm
N+Jv2blnYEF5jf73Hfv/xFm9ZuEfhLsxCtjtUcBmUyKh13vcoMw8iDU5gfUoTtD8
```

```
ceN5XkTFELM44cc9M5Kec28gWHYUM09wpyGiq9/Z1Q8qS+RgRZV210Yikz886ATb
v4+m6kciaI95EF5X790zglLjODR8JY5gSOfbCGdb94XtPouGASa2J0TOO3f9AAE7
rlytRgPHMJyY7G2lNpSF81VhVlfY1RJZpPBbZ88tRvMENsyWQb+6+mMW/PrNy83L
ZxQ1E8gzA2oyOl8SIuRMgfYcSIGM831q/IiMTJI0cA8OX5iVD4KnBLoZlVCuQUwM
0WK/iGjJIgXDTsMLHNrlgZeulkfol/ryWU1M+CwJSetqorE3WBy4HxvUau8v20CO
pABkDZ29evve2X46KVmDDXGICE9O+q+fanmX4ZFzMsVmPS81s3JQhECigYJ62IPI
hl561lXJzkC8lcp25TcpacjjnvB3VGfdqDgTjmALJD4gDDgeGSWZHKWxEdIrzeXr
7yIoKC4H28yOtCwZ0UNQbeIVo6qcJjvTrSJ/ZD97L+jLQ5RMRwtGVoOhlS5tTRC4
l3SmVX7qJbX3I/W1AKBGFCtvY2k/NqzMJ88td0RRmbVvNwFC7iioWYUCmU/97a6x
1v73Kqpc73L7DTkofya+zAgtHqcRlOvZZ3Api3Spa83fYQc8kUA5n/Pq7P1LCbbq
yrv+2Y27If+bW0CNFP+4J8/hFdrQECTBhDgf5PtnizLORXFxCvZbqVdwN7qjocqW
U/gi745fcEOJjIMeECdhpY4sMsAaspxFH21puSdUv/bx/i3Eaz4B2pgtL/t957pT
oATDNublLFP8F/k+0Ml+LFFlg7YsbQG6l8Ki61xHyNp6HnK9XjyluLUIgTMV7KrB
DZwqygl7UJd1IIgBZL6tS5mXOCv/k3Pe9raQR8MmCPNIuQynBB9JjiI8DqcCE17L
siRFtb0SPRR1GNmIIm+30HOB1IaPqPE470J9AprPe+tg2umKnD1MST8qOUQ2c/lt
eSBzmJBHJKpOS2GHHIfOoDz6n6JvV1DUUtNi7LxJOm/cjrTxoviMR5b8hcOTvueh
nHtutZK2jrqGfMylRxPD06tRQ9cRv/svMlfXascl1apce0qwDGVUUVVxI8yvEwgL
MML9qVt8GIC3xMyU8UXlNhAC9iU3VHuU1i/mzIdVQmxXyKz/Csnvwe3jY44iW50z
dRKmrbr5JKf5HFGvucEsmz9Tiz8xziuoxURAensZT8NastY2rmnHqAITbJc1TALo
cHow0MWUUfyjRQgFoSVsQf5LpOIvSxj2dZ0k941MDjmH2M1Zm1ik9MQtbDWx4z3o
w6rlyBnUq9geh7Qt45nK1dyuoUaaueOoVq1HXt2qZ2w8f0DurR6XueEuakpl5ty1
NrxDi3oKNc68s6jBnHbcRjlmqB3g1C/iA/D8gLZRcVDbM8kn+KGDMBJ0J/DHZn51
enlAddnXgI1sEolNGlGWVFFlTCQuZpw2RohTcP1/+6yD3TS1BakjweiXKLAhKNEn
t4yWxQiGurwTO0d0VxUItt0d7s8idH4pxjayc652CK29Ov5Dz8ysKyqT+uIySPJB
yyWURsmpqYtoV8Ox1w11oWisBa/dpk6QhKSValXOU+RJre1p59WL7Bozte21Z09Z
g0uQEezaR38rByfeG1sExG1QJGcSgyELVUYVOFcdM6r5cfHlsqNJN2XMVwlZry/W
JgJKuHaw6LCC6+1gmselpXGkcpPLF02ZLBgDbC2AKZRT8e3T0j+SE53FQIyyZPbr
CjZ0ljtsWru+eWAlaaktJnRfokBpNCJ5GEyyd5asZu+oJXGIFZQNVQYe1FqLbrBY
Z4Rfdcu+cMvz2Viw9f6kgAo4nDEBHkoJzAM7+1h0a5mGfaQEuL+kcMIRPVEbJ9kp
cWMoSE0M9TnLJ926fhtSItZQOEItfO+Xs5y6KOJTLly02KdaCskyyIqju2AYAOhJ
UVdyzulqvURUIwIMCjyUh1jrmpCE7NtUx3/gXcxvEto9RjexlYHw++KCgoIZ5E4q
f/ZJjRMqBDu8CJpT7nHNv0pgRxplQg4x31A9ZDm6pdXF8U/ZNJrfSaSnaBOUrLDF
wbeN7vdJsW/7JssBuyVRIEjx2vIfZ0U5y2yy/hbLjhh01jt2zkJZC2dxLBH64UFD
pGsL+lmQHSQpL3cf00dNyrx5h0wDoz8/rC5w4/axD70KijIbKcssgSHUCd1oWBn/
c+i1hdqXfT/obUCDhgFOMlbrbC9juoSz3Bs1EnjWFt8unm+N8UaNuggTbCeujYvd
Mgh5eazSocQ82xqpwmIxvez7ahN4i0bLI58ZE7OSyFME1yFL0/fnD7B/Dy0ooATT
wFWF+hBfeGaWdXdPIbnOjTXjEpYchaWgN9nUon9DGlKYay4UpUSntUcnqI/CJEVI
U5FVWBaD5BY+nRymkTX9yxuB45z/AixvDMYBn69/LmcchIAYQeldMHwsy611it+T
cZUMtpemQoGqGdxP/uKkC0Pf5TFeq7v+1W9Q5ybxxJh5nrHTAcupH5FJBsqnySg1
jOd3xIO/sQNTfCWBIjN0YuedORUkdieRYuJ6ygazkCBQCr1k7/r/sQiO+F5PD1LB
J26sP0Ly+WXruQ00yA9tTRYiRgwqx/sjcv1Dl86kKMmKBNCVLyUdFPsgjToIhsti
DASDRZXEWlXfAJSwT+dyaDz+HOOtwOH6In8SNr6UPnSsoXofE2Kh4U7DNTot9k39
s1AQBG6FtYfFE2qZ+r7oaHCWfkrkUUCgBUUJcKaGv7mZptf3BS9WEkSHBZboAxse
yOfszNnagBOqVPK6Yi9JLleXEBNSa0CQuxuLDzEadDNLltcEKt/CWWXYcq4Mkqej
FyGNnNGoFRJy/ExL+IbaMVg9wmAhYLXr7vmPFQ0me59CYtbaNr5y8818Gvu5EHba
g7ZEubaE4qFnGX+jQ5te7cgoJ4aR0Aeq6fcV9mwBK3Cs60ejpCv60LYjDXrX5a/w
PMhFtY+KCVOyfgIG69vDh+MSSsRKe7VxIawTJyhDOmiF+iW/LA4zJKXgDdSXk0wB
+hECKChBTlBqF2SHE+8s80olKv3wbNp91cY4m4MV6+Rjo1x5eP28tGQOG/nx3Cs8
```

```
   f/uvxTvOijAc43i3O7Hl1HJTY0keEzEVcmXh7eEhASYJxAELpLPXCVDmuohnIAIH
   VUCx+jiWESllycm9QmCf7ItjnyyI+cQFjzS5hVQDpSVLm3NJVR3hcJey80OI43FW
   gTpB41MR9jVDN/eQ+za+T9wNN16yKNKr1WXcT4Z6j4fMzoUdAmSVITjGGqy2vNX6
   jZFVI21ne81gZifabkpxmmCig6pDkTlhsHA9dB0lywBqOo3KQ6E7t6TIiJ15ULr1
   Rr1vxE9jw09DtSIqJfK670/ERJtIVRwHCeyBgLz7vV/IWcYeYtVyIJhuMpWtPuoL
   BUf/Dnmd22fJh/o8fYrNG/OFwWX805gqsP9gwzN7TySxw5lnmeE9ggr1M8R9+xqY
   hv3NK2I5rcbgraRT83X9qugiFFQtIAn0SZmP2Heo3YJ9MQUrarmvkMOXytKhBI7a
   +WAm3VxW44u1SoduDQltkKVlbEwqDzVp5RSMuNInORSNP+RLYmQFpK8UD4cZb2lw
   uEmx7rvvQMLsmfmjhEnQfh610CXt0q/gtnvZNlcbAPkY4m2T0czYuA9cL2ywArZM
   Ya84vxqvCvXwqlwIK18UxhOyGfYEUCUfPc2vrHPWt0iu/dTLdzYCo8gfA7aWK2MC
   DUg66Skfqxl27pFIUUz96RbXyR0tG9F6mMOdWgyuqZUh5Mr4S0yDyI1r+1ynQV6b
   exdCUobNN+CaRyI7qktV362GBebeOiEe06wjrAAElXqLCbEslXg5myl0jVm+t+1K
   2R+Jv8zcFsUCK9XFaK/O29qElZZPc715bcXS+FukyfR9wKvaRKc6u6WRJE02LzVZ
   0ty5yfAOxFDKjxbYV/xfdUuVIKVA1Z7mMKkgk951zD4yUJYfgP4NKw2IRXTIEi+0
   DSRfmEPIjOFHn5Ae9asKmXp+jfnvAOv9sKezmrrsmMsWpFoFAGyuSy5ZyXgjIEnm
   TnW1kJwqDYMiNgzTM/X+Grac7oXYZq9Lw8vvDSPdn34Zuveul2Q6GlI98UFc5OOH
   V/76smknnphD5Smk6VJEP7bvfvTfJvPQJ0/xIoPP0LFFa5+iZ4x5XsnHkhNXTLb3
   6sDsZ1VX/jPmZRO0XpbO4jNIV4elCNHaBk7+UC50axW4KtMteG4F1mML/6yK+f4I
   6O1UDiEcxxPvJfUDpkhSPSfoWLE43eJgbr0Arm4YKjdLyA2j+jAD1aqXNv81gh8f
   7HlRVh+yiZ+bADj+Y2bYP98ppwMu9+zNEGUMBY7dG2r2WbzHrDBciTKQvy3ZsxFS
   vXcO4p7Y++Zirsxum+o1/sXi3Mz8uIigzE3fUVmbysVJ4ZYWBhS+/NwvOt3ufxvo
   Y3Ns9BalJD/ljbZGSEvFhpgClyNWHzLy0FFpZRvpCzWvV8pKmkbs4dyPFRp+cgKF
   dXmkWfqf1CNh1GDg+0mWO+V1NticcM2aTdWjWR4itvpBPZir41YeSIYCT7blzoCx
   NtlSnxNik0VaYAGNjYL53HS3kfGJuVpu6vwxCWJ6PIhkvJMW0/nrfdrrBLkRj5RO
   NANnLc81IOciOEqE7GDP8c4HD2HxrFYY9CqrGJJaMDFuhAB+CNv4c5nqYBmkYefu
   l/W1N3klgyxJoYP1m09J78zDhv8ZS9M36ofAwya7Wv8JE6UHE/1E1qgxg6vycFEH
   zt0gM6uk7do50yHE3YVuFmsulKXKdzdCEmGxtkFEC4pUN1Tn9sRe3d2CW4MFtriF
   8z1mH3M3uk6BEOkAUgbpF874AFAzGy/r5HWPv8QdSDVsZqEfg0Znh2cZGkXWXEUi
   jSHlaUvVCJzAHXVmHNL7YLqLOU0aZM2ON8NHoAsVXmS1h3IGNIHto1lIFWv5UNe9
   AhVRSP/lUhdXIf7q7UH/kNyUYpOsESB3ai/t4ubt4eoWD6n+BSM6CPGzDVURL7Rk
   fYX28DTcr/fv5HC7XVLSycQ7mEz+QVFXh6gxFTTuxpGBR5Jiv3azwcNmSUlCdlwR
   Nd5hKU8GFFfv2QOQlgyBif4mfJbGHJcYduoiIsTLvQHMZtn7QEQx3k/lvOyjYpqE
   GlPrJ4yineubGfaGAH82fZcjrzsEFpSiQ/UxDOCx6yDWfCINZqXm3AqQDk3DdWMP
   BjlZJJbQOlD37LqPjpB1zk/LM7PJNEJFldcSHKQs0T3kQyMONIJ6ih5Yowo/tOAZ
   l1kKGvhQvYm+FHQow1e2nTFPc2L7QHmEmt0uJJME011PZ8jR/bccw90MTHuOPQPt
   UJCpAcNHlO2D6csRGg0wTH/CXbFVkBfMWVFPndX3n/vypbHTRN+/GOL7wFiS4B+E
   w0Ae1woY5uVLw3EMOwjK8bAEVWhmsZkg6E0XHwNUvH3KQfhR/7/2M0I7jJkaA42T
   Ira7g7PiQ9WzmlOIfSBdQHblsaw6i99Tq92cCpvACUwm83cUK3K39TsXgaokNYj5
   hxbW2ZMhHuxjF/rcZsjcRCA/zncX2OEaL58jWhRBmzpze2C3CPJmAm1eUdzWLurp
   J4ndgRoShI2QkR9rpyNlMEB83P8fl//6vH4Jj/gKS90hMCTSnw6iv4QEAz4cJZEx
   RLSdUEOcuEdgtqKA1XH7beiNs9/66I755G0X45DIiSkWSoNsofvNX5GMQi8KHfra
   Lvkwj/tv9nJ+y1RdNfd19m2yp5kJwyqJvZ4q9CnKvQn1qXHNYbcHeCFLknfl+YzY
   BAhaHwg47t/5F7I1m7CpkdlXuI+ByZiYaCtAZbkYElVYPpNLzvFmblwqA7UjPrL5
   RzA9qsqEXuJBLqP13d0iciEa3AexWFU9om+lDNHc8bIoZfxk3wW4BITDoM7CwO9k
   M3mPHTwIU0zwauzqgWkBS7XNWGuFdyphRf8Oos9nlDfZr5hnQsRDKwusMxQQMpyK
   aamXq/Yhcr2flUZ9hffQwVffGlLT/4h4WhKrDcYlO4XwY85AOB+9MouvPIgUt5Pa
   fyWG4tqcFy5DSKTiGpoO4Y5N51tQqnO0X6j8fd4DuI/WkMfib+84Os+ZnfQ4BM+b
   AnGWAqHzU2mwg1vSR1nBoLNERKLnsTUM8OX0qkhqo4hxCjdh+Dc7gqbCNVtUfBbe
```

```
fqdfr1EdJoe+GEdrT8J3NVl1AYzS3t3zTQdQ5yNzrP0kVyOUIbiyd5MpNBxLquLS
TwpOTnEcj+46IC6cXcIeVmTWtEmnGvGcQHdw95waGV0BrpAyPjyEfZ48ubfY7i6x
eSC4YX5vzM0DEfkz8tXrEkA0PHbOvuEJgJE0iX52fYc4vnMquiEY4GDIc7WRJ62H
j4nVpvjAa34DWgZ+RgQCXF95kSztyoSAL3Jnq1fQOZ8=
```

C.3.5.1. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOkgYJKoZIhvcNAQcCoIIOgzCCDn8CAQExDTALBglghkgBZQMEAgEwggS7Bgkq
hkiG9w0BBwGgggSsBIIEqE1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lLXJlcGx5DQpNZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1o
cC1iYXNlbGluZS1yZXBseUBleGFtcGxlPg0KRnJvbTogQWxpY2UgPGFsaWNlQHNt
aW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkRhdGU6
IFNhdCwgMjAgRmViIDIwMjEgMTA6MTU6MDIgLTA1MDANClVzZXItQWdlbnQ6IFNh
bXBsZSBNVUEgVmVyc2lvbiAxLjANCkluLVJlcGx5LVRvOiA8c21pbWUtc2lnbmVk
LWVuYy1ocC1iYXNlbGluZUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNtaW1lLXNp
Z25lZC1lbmMtaHAtYmFzZWxpbmVAZXhhbXBsZT4NCkQLU91dGVyOiBTdWJqZWN0
OiBbLi4uXQ0KSFAtT3V0ZXI6DQogTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1l
bmMtaHAtYmFzZWxpbmUtcmVwbHlAZXhhbXBsZT4NCkQLU91dGVyOiBGcm9tOiBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NCkQLU91dGVyOiBUbzogQm9iIDxi
b2JAc21pbWUuZXhhbXBsZT4NCkQLU91dGVyOiBEYXRlOiBTYXQsIDIwIEZlYiAy
MDIxIDEwOjE1OjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGxl
IE1VQSBWZXJzaW9uIDEuMA0KSFAtT3V0ZXI6IEluLVJlcGx5LVRvOiA8c21pbWUt
c2lnbmVkLWVuYy1ocC1iYXNlbGluZUBleGFtcGxlPg0KSFAtT3V0ZXI6IFJlZmVy
ZW5jZXM6IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lQGV4YW1wbGU+DQpD
b250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsgaHA9ImNp
cGhlciINCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxp
bmUtcmVwbHkNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5
cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhIHRleHQvcGxhaW4N
Cm1lc3NhZ2UuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBm
cm9tIHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX2Jhc2VsaW5lIEhlYWRlciBDb25m
aWRlbnRpYWxpdHkgUG9saWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5l
eGFtcGxlDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaKtDAN
BgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVs
YWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP6AFQ
J+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp1c+a
uzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6hAQVe
```

A5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXjWShp
lcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2lJf5
NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/WI+w
hUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgB
ZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAww
CgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyAKRV8
ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkq
hkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1u0q2
XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZncxG
wy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fFo/Qs
hlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmGpfB8
PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO7K45
9CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQICEzdB
BXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0Eg
Q2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5
MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcw
FQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCC
AQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOwI2ju
wdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD73nQ
wXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aRphZO
63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65x8Kf
4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL270I
6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAA
MBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWlt
ZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIGwDAd
BgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCOfAcX
DKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3/gqS
Q4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffRTF/K
tmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9vsdVf
nbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkKTM/R
CGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4GWv4k
m3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s1LM2
cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBT
IFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgGCSqG
SIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE1MTUw
MlowLwYJKoZIhvcNAQkEMSIEIKHPvLfnw9dsDhrKZlaFW3+cbW6ewBQ6mkp22q7y
BhI9MA0GCSqGSIb3DQEBAQUABIIBAH3cRn5LOa7nqW8Z/czFCRpkU6j2e8xqaw7/
eCh6GvC4emq/eAgKhqpbhw+QwEOYZCMmTe7GFb/eSl82QjB+zYaR+pGgVhBH57Zp
IOtobnzbOEsgzmUKakI2iaAuQBtOxMPqDRTRjMPLMhc6ddIRBqNeDpC3hm+sOXrj
r8rQAMDBJTck7psP72DTyDWDeVPw7BRMSnxz7FwSbW1CXFeiJ6mWhZ0Va1YgDpJK
Ic2uW2Tq/ob8jTjnPrVIQhq0ZxKOiWsHTMfzxRnH3xyYt/c/huuoDtcf9P3j9GWa
a23tU+PDSpfcpG5MJPe9DBzExWII7Z50Om8g6tZETD0+pOjNTAg=

C.3.5.2. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-reply
Message-ID: <smime-signed-enc-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline@example>
References: <smime-signed-enc-hp-baseline@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-baseline-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:15:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-baseline@example>
HP-Outer: References: <smime-signed-enc-hp-baseline@example>
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-baseline-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.6. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8625 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5368 bytes
   (unwraps to)
   └─ text/plain 426 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
References: <smime-signed-enc-hp-baseline-legacy@example>

MIIY3AYJKoZIhvcNAQcDoIIYzTCCGMkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACjyNrxVYj1Xb+ACrx0kFuDPNhExlQkEjbJj
EZ3Az3gK6rWKIcIfSUIlwhqWJn4Vqa80/fHS0WRkaYuLRR+WBBoXszR6j+cEhHwa
MHYVoj14YCg9+AmGbU1s2GNSrxqPFRFbrLVHCHdM26+7mpjWx6NhbVtPTsZ/+MfC
BPmKulF7rImdumm8nkaqdenbvp+AjPA82P38Ah6FTMUeC5ItSqr0WnvVMvcL6NA7
8BX/WlxEYVmcIL9B/EfRmC9f4nDYudwfMytHELddT9Gv7MejEqOB8B2+b2K0+z7F
DqxBUK3h5dXgIDoPadGkvunqnTLFak1JJyIeXftPK1GCnglXI30wggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEABvIWkrAM7mEjQFyBhNeJwopi
KUcL2wEHZJkKZxQcx1nzWdNXGhF+JCY5H0KmZw3fbcH4VnGPB0olqC1yarSiLuHO
dfaZB0ioUwzLUKobv5u3gJ53vd7LwDvZnadXAWdwSXuxbp5XCRnK3UFE00/djZ6k
K037U5tydzJtCi484Yd5BfaQwF8UPW3/JNxGFs9Kw+jmVGjWJxDToZAhlKNzILmk
nj2OeZcUyQoCtmzXmpTHDENz60IJZJ9KvbLhCpJ6owwM7818kOn/69ffTYR8dV39
Liy0KUISCODAVtTAsioyQQV/wBgwkmE5iTILa6WKPogsbxWmGTjItdQm5Ty3NDCC
Fa4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEIZLVXkwIIvlTRvYBsWvNdWAghWA
/OKrDfplfnq8JqXGW2x4c7ag9bUaeknkbqeNFeWbtYUXuUs/qEjYEnwuGoxs4KoP
14FjMC15o/IFDzURsGR644EvdxjKTgdzDIJ03SoUIz+RgdNgGCkGbGoBbl3t2PQV
645X+7uSfUqCppTceJ5zFyIZKoYlkdP+nqMSKQItXPydmaw01ipeVizufHb09Fqz
FZxZthU8O41z2Glr9y8y8PDHD7EpgZpNa1n4vpma+612G06aIuVFoIxmjMi+Zbbb
yRfJcvpPR/iY0M1H09ZvR3za35m3ffSBdE4P/Be13CBhEO6kRQ8Wpvzg3Hk5vKo3
O/FMT9+EiF4BZ0lIkzUxK7BEZ0VsLK89KC96P1Jsp9PDe18/XbyW1bLsuLdMfCld
XDq+Obdtv236mRpDeAR5TNtcFelr35ZZf2KxFHnnNVl/OI+UEx7kI1w48m8CSvKm
KuMQRm5+oQtDIYTqm0hiIogOmw73q5pS8oXbR+Am6sGu/fbt4ucE9qpU0jk0IkHL
```

4rLHAj4Tg2NOecFBTECvN+Ce/QMPQSqOmBsoPnJO0dWt4veyxFlIxjlkty33PsQv
ulcAF6c6PVef6lFSHx65KJVUUtzbd66h2/LYb5zkV8OICa0UQxGX5hMg1METhVyb
108IwQ2eGbCyHBlErwWsUY4xca7WvTEOmYIDcEtIKwL3HYauTjn2qUkhzfXkrARI
eizjTTkxP2fPFCMRPrMD28nDObKqS8ChYXOgy2U4WY9DyiZ8iKu6C3itXCFW7vkZ
Po+IsclwXmwEqMotPMsjxuMtS4LTy8Wb/KUk4gY7OQeBEp+u3zIBUNl2b8LQ6ZLr
7ktrD9GrEx5l4eGfoNZZNC7+27HHo0wzFjHLSnAHO95iilKTLy7iwhcuu4bHNyOE
rq63jKdaABkDoktAaMcb9EYkXBMx31W3/rGtKK3NnjIimsztxu44aTcGthbF30to
dcKyZrK2s/6/LDYfwyt2zljaoQ1F+ozCpcx2Lv0oR/Qq4M2DY9YekJ33aAD3QsdA
+JhTVNpWvXykQp/UzHzjfF5J2XNGZrJtz7KHzXTATk0b3imqxlct13J7kyuaKTem
HYlH5lUegRyRefOVjAS9rft4fbelCUwzX8MclbLH9buDB0tIZafLHDjlhiLHaYsF
PmYFSDy7NsLPUjrHuxpyY355es2aKpvz3u+38N4ykveAY1Rhh4Z9HNMnSssSnyBe
TWn8LogACMHGp7QZuXqhcHJMJZIH9QX3mxs4hrXliXivQ6vpsNnZDEBapEpcfckR
riujD6mQV6y3mE+wjTiLaC9ZakKosB9W6465ca8F+bmlKuaaH0rJOLf4I9mJw5fV
7IFN6uXMLEb532cUE5bixUrIqWPyeX7mHfr6EOv94bLcuAss9dT9ny/TXlY/FSm9
4DjbaaP7MtF5RO0MyBS3p094dEF6lSkcZykIWMtJsqa7qIynZOBPOKjGgrwMkNee
llwFFD81SESUC/GSOVr6I3WgMp7ZydaZ7KR7p96Gx78j6ZL19HsbauToON6TI/uW
kTSKVzZW8spUz45pzGDVKBnvD7hE2dO3poQJ16VS8YAPrPgbAewmqSA6vYU9TuUy
D8lGbxe+THB7U7eYO8t/PHCsD5MbJNBcmxX2PBJgPUqWIjz4oush8aJ17z12jkTn
yXecwDQAkk4CH7QqHlYgtam4+mK/A9YydDPObCnPQK6KAvGLfNoJEkxe5KUfBP4D
+uzUiTu/WslArHTABROsrnidewhpeUwCZYv5g2gc/i3stk5Dj/M5hAd+TDohWY19
9kYPRMvEfSMVR0OrwwS1wv7gBZnyy+Ovby0skOPgoojnbrQyb8tS0TTeCfXyQ2T9
1HIzR1cdC/58VaM80zQUuajYyMa7JshYl/xz01ynL1YY1uBuGpBIW3Wb+OTTtnbh
CHCo4/NvnSd2eDJPc8/nlQzy04R7ML0wQATBArLtd2L2DqDJT1Kw4ZRrXX7qvwoY
B4VUjtAwCnoR20mzPeioI7dYSf/dIfg11IoDHCt++g26TRPW6RVoaVkPMFEqoaFp
LOnor7UoQ5o/pa1RgE4b0QdJ2PRZ/EvaAams7LkHrb/3HWhBSZ0Z3k1N7M5FFjPV
Euez74xXPKhYnpLFNc72RJ3tqjkAUbhbgvp9Nx7CC3TO94iyy1R7OZhRnZhrcv+R
9PsovDR+HvrFvxIQnFBC5rrkBxKcPMIobPlDDoawun1LJEq1D380u91BUupkMkvz
fdkRr4zGfW5xOFiIHMtoukrWPsxad7Gy0jb/thROWPdSvbtnEKpfvWtEIovnIo/H
BheLoM/6dbkvdagKwg4RhI674DXH1PlYKgTYPKjcoGrn3aYLAkDKK50E16NQSNAF
4j/CkJE8DHVye7Cx7ehNfqmBfgDXCi9pZpqeJq4UOCArNV3/zmMAkQMhFyXGzzpq
7JsZz0EOKhwP8HbLHsV9qpq5ZUjZ3wnvtuGq0Be/itv8DTI5ezuOpX3cemiy9INT
hbFpRvDeGHeq9lwtgkcWNZIS1x7BtvYce8dsDZM9tN/t2d6J1DtpIb7AjpWn7ke2
WlTNl9C3MVMBXn83mwGyHFtW2wfZOJxROWNfDssCGfS0BRodMsm4LRqQnc8MNK+4
A/6g2pMxj0wikABBMke/+YgwlAEt+VKGcIexo/LOAoQDpG+hI2dRGfZnrKz7Hc4r
R1v6gaCqqErVonHFPNX8bGYUPrEwBxPwdzjj8bbAczwC0Y4KsZqfABysXUzQ0nOn
4JQ491uuydJSBjgP0Qr2ZuBpuRKf/m8NamX3LEZUfeixvSNzh1eNVL/98EhdoEas
nT1bfFNSbg5+UmaiQJs2z9tGJokUXtPplPYKLgr6DfoPqUe2yNTrBn0SxDLZwN0h
RU7CoxoKKHQY8QtYdwXQiOh5PGFGCzRloeUaYq4KDYYr6dOD2Ok4Yu0NxqxYrkp5
RyBXAI/p3wpBK1p6lnHmybbpb2gpSY5HGmKDdq54yLZjDHM//A4I6T35Nx47uWS1
Ix/5McCzZP1gFHXjndRU+7Mdj2OkBsSpdVZ0+OemrEtjJGUpXJoC5xHN/cxLQ8jA
gJtbK6WuZ7ShAFe/y946Zh7r5xFtDhNqFTl3q8oHoiFPDW4qafryKcC9faClKiP8
TDBkQZ3qgngiTEvSrVkfASJEKFHfNSl4dgVK41YkUTMT9y04C0rvMBxHGhgxEVFC
eRuWXBV/RPa5y1RT7N1iaMDtlOpBrW2Qq/BLw1jma42QybmDhsfGtgi9O2NBPdyG
SjgsMNQoRHNQ4dUh+kTsDxaz09s9QDASGa/ePVbEPMsBVftbIphOWNkvwpC6+k10
oJZgx6dqxRoJPLXLF8qdaVq9sZJL9ISaLJqFZXflx8541shyyOzP03s8pzAGh9e+
u9oYtl+DwvBB+GoGqBK4zwGDReXBlQ5aJbq8QhzoHPnhlpfXsvssPXIZRX7Trq1d
z7J3iMJav9bDaAbuGWvP5jbMJ5GVypnjgbaDGO94YxkScou2yW+t696iVJaMVadQ
bm+N2pgJDiC2yCCzbEiWGTeMoW1irHPLnBugPxQinB4KQ+nOg6v4K1VbgZkWuafe

```
LbQb9+bwhiZ0YNinzaQ20fEf7qtEUvtJ1P3UkZzW/MD+eFRLHJoN40RDe10PaP2r
aMOwA8Fsj2FpO/8Y6tlGSEfZ4USeiivrd6vw2JWs8jKV+5EOSJwzeCmvi6uNQe8L
iJkkA684/Exp90W/ASQk1nEy8MvDrypH4UdQQ2+Iyef9ukOL1wID7u3BChaikbdw
2l1Ph9caHNGSMxr3CJU98mQo7NytCSHv9tD6BJe+Ilt+s5NwxVg9JD++hEN/agKS
NsYFRdOAW6XPZSN55zA1ypsVHGGUWaSMSvLogxlVDlzBzpnTXsidHavUwHI09fsn
LrD5FXDjjk3iU8O/ara4Vkg7y5UI8RS5SnU/N2MYVvP17Mt83/ax0D+J+hXKRJ48
fk8TP859Ec9g2LMZPUCsK0K85adKh5/ETjNo8stdhWkOfdapisSg3vkdCT1Btr2f
kTrT7z8mX620vENI4EBPO3tX6V9waWeQXA7ogDZ+arjh9eThdS+QZj3SpkAPPy3X
/FbPCaFm1IUO7V8N5qCpMlb2iarjvGVbtNFlTosbBYQuJ/ztSpZcF8lQ+ukTw9OF
4PxZmGtU/bmDGg/nwmIIzUliAKBQ8MTViWe4nk6r4fdr7cpNph7TiRhG8fM9zwVY
QqJP0tvy454q73DqhIbMZixjINeyq4C7HpFp85/m0/cSgGdqfyDjVTV4koQb/RPG
XEEpOSx72k0MVUoRF1hO83f/QiXZWdfIDTBbgjxZMtW4o8qG5xigFfAwpTzy25GX
l+EMbxgD+YSf7N1zdV7zWBy2UgV9OdFkWYd5J30ThaDJ+j6DsDRawz132INUWA00
WFBWH/jspgzIbCThPWt5E91flhm11qrIakJi9ivVjPOZWGVm+L37CA8PxK5cWfg1
v+5a+HuU5k2I5w02C6qvqLhAhQ9jX2VtvuOej3eLNoFbOYrJ8M7ZbRemcitso64r
6rdbFn72FwTiGQdgKp7p+jkSIIdK+GWT6lWVQ2ZPHyREZOMPGeZDtTW8JzfjS6ca
DpxURVz1VUEwQYxd9uCtjjslmInatBKUmWyoRmMMuYWEzsr6RkjZoOOqP0CzNSMz
PJGuRCrU8uvO6/xFu7wnk195O0sqAS2n0He6Ek3Y24JerOYwuaOsLeEymWt+KSZn
uG5LWvVpgot9yfyE1HJ9bIvQl/7qxKbXkKll7c1U+WzMpFQlIW1OgIi25n00Mr+H
YcYr6KdXizAhuPAjRQl7UFKIhT7D0qxHh8e7+gEhX94XPX1B9PJsdSq2lm3kvK2n
f8/MRKW1RphqZdXHkE7QtRanyZMxbC0+Mz85U3iCkkJqfzTnXYorvFNdTC5YBLQS
PFdlrhtUBgx82GlMC/OnDgF5RwIRBZsl+oZ46cgJxVjr0A0pWmYVfQ2mUmV6gqQx
kOOWwRGslcXN0KKfRITPbrIge/+68dwtR0ftuYMPZ5wmCCna2LbvQYGcKZ8NRtQu
Q3/fDGSZMMQo3FC1XHVDVlBRg2qLapJe9VZM08RVx2vBcB5IIVceNPwkZDPATtMd
lPBVNpwHnb5JIM8xiDHomjhPL8P0AuuMMDcmUsjlOJsgwyqJArI/JlhoFsMUh9NL
7jNcpyuk2YzizC5AOYUoa4XOpwLVmRShQ5reedn8v2oIch9KuIT6dewcELGQHdHR
0Y7UCwOsQYWxCIYu3NjkssO7+xrmqrffdgJdq7sf8tXZpBqhOQBtmrqydbnx96JQ
HRtZpwk+X2Lc1d2jd5jfQmyk+m6MyB11rMS47CGs39qWyXs5rMr6cFyHnQYfaXR4
o8rLT1A1f+K70A6JrEM65Ka8YkeUzSiNKDgPq/OThItAFe04GH3UpdBpoiT2oezy
rPL2ddLfMrOoiYIHJwSXPDlHdIYvbfxveZUJoAZcE0USPxneKVyb1A0G7rRj1ahw
bRdQ/voqOLQh+STRCZifHws6JbGfFikLH06TB737Qo4E4XxZegQFIbwgg7Irc/XU
F4fdtew5pMhEpGC8Im02j6QCs2Ls9cJEZo0LAqyjYXTxWgUATvy9gIoG/99AuG8O
wGnqMQmYrX+swf8QAK9wLxE4wSs1ZGyc8oWqyF9mfwdLSx4cfalR94930CgI6hBS
MEFAlTBVDKvEr21D74f1S/8Ya+pUD8Gxxnp4MDWtHEsls9w+Oc4UDgq6S4gcMMAE
sTry3u/D/hFZqRX8M2y7W7Adj21FyvC8Mm3OYCbXOGHF1bie4AQ1wSiS+fjEVVVt
XSzRozuULU9HIjemb/oLmVzs3Bx/U5nOIf5ucCbUxCOA+Ol6rHNMMmYQHwpu4rbu
+d7wMRrtVWLEShy5awYotV9XLI7chZUB+pXhOBljGA9h4DChE9cwvHJGCEwfOutm
63/6T8uNwI9OI0LAPbbbABSR8na9qzrpV0STxuG2TQ9Qh7cCHRnIfE+QRJuy6Xfc
rVhLZB24GlCEPf0kys4RPfrcHFBfC/rAdiF/KIjD2vw3oXdccd2gdn0FrJ9fFPfM
ZMWKFZKSB0vUFUFAyg90jMS+J0MoG1Dnmk9ZtddhLjh/IiTInTdrWU+T02XG6Vlb
/qNEFkIw6vbaPwoLzowSeprVWptogqTnfCaQPPFUv70+14mNTL6wi0ufinwhHtF5
fvuhUkekixn5M61+uE7czfflyZnxoXTzI8YhSdRnVCcrJ+9AV5dyx7Cr3ELipGLB
2OKWNHz8V/GddKLN2Wu+ls0CPiss/bCKW+UJb4wtxJz/fHp5gkH6qc3EqZ7i5crJ
ozY9n7Up6WSZgvgzwET0JCbcHsL2+wStkSaRlhTyczB52cNJTACi6uXEYyl9om8M
7BWq2FvDTeUJDawB+rBm+XzyL95ySrXhLhTN9N71U+Jk1CDbf/zJXVbu+NDPhEpY
7hTg/P/u83DbXkUR8w0Ja1nSjA8ze+Fxt3fbtNPSzG/bC7Ut+rGkJsnzBBYpTUjt
dbDoEdjj0cj2z8B7LSLdEdtlueLKLtIdYFPDdca5CjoEzja+4I3mNU8FxF/CC7Ci
KIGaRgwy1JW9Lsi3Z0QM1jnugR0RgsLisIU4yX9pogO9EvWmo00wj7kuM4OVGggg
```

```
y2/c8YlJJi3JvyBayMj22CrUtBv59fPz+biFloYe1nHh6jGJB+zxsobKpEZ0UMGk
1Q8k6PKznMicR0M8cummltrtNcwk13470zy0VCisjIq4j7YLfSkUH2Wo+3WgHdpN
wUAsTXpE2HR9Amg17uOU7qBqBkCC4nbArddaw9d/Jv6IxfsGx5kyDK1X8Nkalqvh
wT59cOw3GXzOeS3eIfvu5RO9o+d2mfRH+77sRkvPIXOkM/bDwZH3cPtT+YEveqOK
8RJTDQeLMqSX7lo1+VC+975x2Wsv1z1LBpWiw68tXLj4De9Pp8O5BXnfBS80vJFY
JMBtAg6MIVIQyblv+QxnYX09CGCxjqjka1PehmYpafcP10OUfU5tSqJb4kB7MyUj
NRn6yYcJXJBAt1lMRGlLDkUTN/mswR5Bzy4NnzThZb62sUZ23xwKJVOoApexfBVK
rJRaeuUaDx1upyGfMEVuIlmCT1aYIXBb3f/W2zK5219f2dbAFU0goYTKJoohBzGL
tJ3/dO5jLgje9H1AgZS22UVUI+FQo8uG8ApPJgts3AW91fjohjzzYCp7T/zR7x4h
UERWGfMG2fHYje5/QuyobVCKt8QfG2DhvSIMDPBY7KHO7bXJdEmUwb/aSeggmDCp
LHK2foRU983nLGdDrp2q4TWCoMGVSmOwBasUjVHiUA8=
```

C.3.6.1. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIPOwYJKoZIhvcNAQcCoIIPLDCCDygCAQExDTALBglghkgBZQMEAgEwggVkBgkq
hkiG9w0BBwGgggVVBIIFUU1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LWJhc2VsaW5lLWxlZ2FjeS1yZXBseQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25l
ZC1lbmMtaHAtYmFzZWxpbmUtbGVnYWN5LXJlcGx5QGV4YW1wbGU+DQpGcm9tOiBB
bGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJvYkBzbWltZS5l
eGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMDoxNjowMiAtMDUwMA0K
VXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86
IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lLWxlZ2FjeUBleGFtcGxlPg0K
UmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmUtbGVnYWN5
QGV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVyOg0K
IE1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5jLWhwLWJhc2VsaW5lLWxlZ2Fj
eS1yZXBseUBleGFtcGxlPg0KSFAtT3V0ZXI6IEZyb206IEFsaWNlIDxhbGljZUBz
bWltZS5leGFtcGxlPg0KSFAtT3V0ZXI6IFRvOiBCb2IgPGJvYkBzbWltZS5leGFt
cGxlPg0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTA6MTY6MDIg
LTA1MDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24g
MS4wDQpIUC1PdXRlcjoNCiBJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMt
aHAtYmFzZWxpbmUtbGVnYWN5QGV4YW1wbGU+DQpIUC1PdXRlcjoNCiBSZWZlcmVu
Y2VzOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZS1sZWdhY3lAZXhhbXBs
ZT4NCkNvbnRlbnQtVHlwZTogdGV4dC9wbGFpbjsgY2hhcnNldD0idXRmLTgiOw0K
IGhwLWxlZ2FjeS1kaXNwbGF5PSIxIjsgaHA9ImNpcGhlciINCg0KU3ViamVjdDog
c21pbWUtc2lnbmVkLWVuYy1ocC1iYXNlbGluZS1sZWdhY3ktcmVwbHkNCg0KVGhp
cyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtYmFzZWxpbmUtbGVnYWN5LXJl
cGx5DQptZXNzYWdlLg0KDQpUaGlzIGlzIEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQg
Uy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3Vu
ZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYSB0ZXh0L3BsYWluDQptZXNz
```

YWdlLiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSB0
aGUgZHJhZnQNCndpdGggdGhlIGhjcF9iYXNlbGluZSBIZWFkZXIgQ29uZmlkZW50
aWFsaXR5IFBvbGljeSB3aXRoIGENCiJMZWdhY3kgRGlzcGxheheSIgcGFydC4NCg0K
LS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0KoIIHpjCCA88wggK3oAMC
AQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgP
MjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBT
IFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQAD
ggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpM
LcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7Y
OqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF
5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEH
AMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z
5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMB
Af8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGlj
ZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQE
AwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAU
kTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKc
FqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN
1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMT
g1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYx
W2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIe
Morj36pgL19oWZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCv
i9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqG
SIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEw
LwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5
MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJ
RVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2Uw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijS
NOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX
4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4D
xMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3Cz
WruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog891
9MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7
AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIB
MAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggr
BgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQ
ENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3
DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doiz
cGMk53riugAocCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4
ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf
8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+
Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI
364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYD
VQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExB
TVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69Phq
zpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwG

```
CSqGSIb3DQEJBTEPFw0yMTAyMjAxNTE2MDJaMC8GCSqGSIb3DQEJBDEiBCDlm+B5
0QBs78N2wRl0kf1Exib4redr1foUWvF3vmcyCTANBgkqhkiG9w0BAQEFAASCAQBc
m0fLRAACOYr8JymCYS4CYBWzMuTqh1DOat4MTroQLeNXvV8NijRWYdbHFcL1hrdy
uLBoqHTkv29eG3Lp5+Ah+uYLcPeamzoxWgfiLgPBaFSQU8ZyxPqVRj2xLq2EqG16
IW5DfieHgVN0bv9P+gmRdKdzG8+hiZcZXBm2aJtN8oifP/ahgTzePiBiHK4Qvecy
q+Cr1gFwVlT+1t/2MO1tGqif6R14NCmUaHzeOvzEpJs1HlE8W7yUjBdrS3my9KW1
fAv+chp5rIXeSrZGTg7ZhNLcq/uq1H9IpgnYvRXN/f6WhggdVUZ5BJwPqbNcCJFl
zAP8CJk3IK1fzZulSebk
```

C.3.6.2. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-baseline-legacy-reply
Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
References: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-baseline-legacy-reply@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 10:16:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer:
 In-Reply-To: <smime-signed-enc-hp-baseline-legacy@example>
HP-Outer:
 References: <smime-signed-enc-hp-baseline-legacy@example>
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-baseline-legacy-reply

This is the
smime-signed-enc-hp-baseline-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy with a
"Legacy Display" part.

--
Alice
alice@smime.example
```

C.3.7. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 8190 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 5054 bytes
    (unwraps to)
    └─ text/plain 325 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:18:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy@example>
References: <smime-signed-enc-hp-shy@example>

MIIXnAYJKoZIhvcNAQcDoIIXjTCCF4kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAFAk5Jw4mFC+UC84fvpvWVuVYa7lz/mqUPw1
jVB8JIsTrvGAEVoW5Jm9cei83og4JLMUOIxM9WAuJEUbUApScNRBgW0vSyl0qB8E
4VdNXWLA0Hsh2LYySirv0yxb0cGuvoWdgGxlqlUmgoHMcwcr3o0F9Y8HenqQkE/L
aplaZ7E1TW4OGmDmuxxUHUHPER5QcS3UKFHmOrQga7Ecnagzlw7SLiloFNwOFhMb
oqAbKADbMdgn27ThOoroxT3z02GDIHLaYa6uP9IVe/ysFPQTqjKZhd+6TETLh1/p
0SMix7NDaUnm9YiZYIzsqsQwKTCWYqgBhl7uZ0MrrooZNQNn1rQwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEACpVIIC327M39MPcp0ozCdnwC
eLqFcDb59GdezAghfnv5LE38ZBa8cl4Hq010yIE0CQlbpW0NRbQ4qa62PEHsRaHC
hJlBhkOSs5xw/ClO8RRPsQz01t2j5hA1F9Khe8z+OC+TaLBFVjXm7v6SOnp0GHSi
Rcy2QPTCU2xj/4u0wGNQ5SMxMg9v0RmnKs7I5fLHJDTgBQ2p+YLGp55LAIPQIA3Q
QD4TjlsZrCYCK1RK/qj2/0p+llf9X5lVPUe0kttJ2qu+lPWJXQ2+FYB/zh244v5K
fnD5DGok2NK96pr3HToJTRgTTRgA6wKF/6tlE00BZHRqr1xhUL/d4ZMkfsjpdDCC
FG4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEJua4/oTK5pBnB0FVr+FDv2AghRA
NffO6MgeUXY60oPjjAtWmKdtLrY3CCr/iioPo04wnBngRfEHJQNkqJ01gOScql+w
eFP5u+7znmTLC7ib9Y7Wed8KpObxTISfyLmd/xByN1fIuDyd+mejL3c5O9LnclI/
Kng0VGlxbQekkITS14iBrwgIvOSsNDBAKsVpyQDvq2gkOyR+e3fTAKFtDpEovs63
48iKvZu922TkdxTjyp/wQjtB9lVlWqPDnHr+boJ2TjGZomEIAwat3mA4+ESIbOkR
0qPjgLFqul1mH/XA7dvW5y7PqN8WiUKf6dBnesRIjv9Vhq0a3OFqdzYdKy9KpnXU
zI3o2GWC3xdGJ2WhX0L+J5hvW22k+CIgrB02Y+1ddESmC4gsr4LqOSz71erlr7cR
qSc7URAqQefd240iNaJfKv3pkTzUYXBnclIovijegtz+ypzbv9h4Ejr6CyETCqwV
+HNC9216ptAGhG4aobQ4cEgMx6AYgVWk21gXe8/ZsXm7xWmkdqAwCNNBUExdOQNw
```

cSFAVI+0IsyPSoUBTyA9CL5oQkODjviy4lvswBqjJYuQEGQnNZffMuuNKESJpA30
kwBPtVhEba6fK0HpW2XStVzhpgOjr/J8OHqfw4aTWFuHOcZbOqNQ424FSAZdNbsb
mUQWOCPvzdM4tGM27T2MbC0z/ux9PXRqola5/YcLkjm0ji5hntITDmBTY2XgvEgC
yr8UoUFJ5xEWFGQMcyUkN/WNF9MdGRvMqKpyKimRqn+lY3imYDOQlGDbXsufJAEj
9tFbxG58inPfQl9m+oQ4KnMGH1/wZisxJGzZT4mkBl7155+wfATa2Vk35gnHZJ04
8CrdW4k3y0L3Av5uDk4XIoWBrRk5xMUF+ESceQ32NGd/PXaifDe8P5NnxBYw+5Sr
+3+Wsl4v1CUZoDAEvCipqNKIT5MV8wrSADE8WC9lDYsTeRWx7dxeTdiIOQzKhaUL
8rjgmWF2+SMm0HL8eX3ibROVzNl4r6V3BKGJrbztHT9kKXRCPsOmpA5XLsObNCXP
vqcPKIk4XkzLvPgZ/znIa9bhnPKY3BqphyLDMVU5p/1Wp4UIztLmiqEGZLkpHpCM
pa5zd3r/C7Lk8EqOGIA8TmwY0iuiWZX3+Zegsl55QYsOBmSS2/2XKyPGI9+QPond
SOeyEJaxUhtJtXt9mqae9doxL4jzLfc2IW8Sau+WmdVXmyZtxPxDp9fZc5pME/dD
uL9RE774krvPtGvpI45BIAlKVxPpalicEURf2U8QpDBcCAO3hml9nY8t5nPGV1nm
gkV6DViWJkLPCSl3a6l3faIQUWR/ERLku0omu5zFToe1Xq8oxN/fQeVETMNasiTQ
n+ReCFvdcMbR3aD0yoC2obz5BImvIXwde7Tw7VWYRuuOngngluf6C1sv+uvURHj9C
eu7asNze8hCdhvkeVpE02ow+ou3nstMsbTo2xdjXPGlIalFO/kbZjOAlV/6E9GhG
6eSV36Rl77bj6pJW+XIkYM0UHUNNZoSrxwX6EuL/+P0nVA72tyP6T0ZubuJtSSk9
IeWI7Tt6l4PGdFj0UT22v8QXbfSFXSH3A+A6DUXOQn2Foe+pB5sLQBdrD3iJmBpv
j6hN2rZCd+N5WjRANUpToD9f82BE39fm8Cx/DdlZTSsBy7QA5a/Ho4Emu3mt0OzA
gUPPgru48T+/qZs2TAZ0i3Sv1Rv2orXrbUW9UWyv/T8bD5ICggHVRmisFbZyN1h/
ZBkZCAO0vVq7hbPOAyClb5/Fc8bHXk4iKlWCt1+4agzA/TjPZmN+6V4DFdJBLf3L
EPvWW381ejEIIeGx9wgMWiDxc7QZaIGIF7n9yKrtUeGgz8D2NF6P5cweiFJ1U5zz
VoqIyxwE0yySPzlItRl6rkztn69yDBfzUZTaX4oWxLyVW7Lv+F5Hn17HC4H/I8By
3aWPHbYUXuSXvXvXC+R287RjOyNi0efGQm+kKAOn6386fsw7MvJ0tCGIzLWdhWMf
TZtKSTOQ7753xxcQVx+4YDp6TaPx+qgT5MjS6baHVaUR7YX+oFQkY60bhh34fmzw
q5WA0MQH+310MbhadPvC6CcDtdz37iHhaGbMf9fc2OJY2VMMJx/unT9KTtYh/avZ
OD/7sLgkVCkkLbtpHchfHpGvQJkTA9cx0/lEYxKTb5VLo+pC5+x9CdoGvuI/hWve
igy5BF3wxfgNK61pusCXS6VRCJuG+ohtg1iQK5NRJA0W2JX60AlKaiRJawB0IFQu
XUrri1leiCD4zJHNixDMkawoi7X5TtcvKjOfhiRGifRULn73UFLL6tAo8Fy/hWGC
qYIFACU8RjrlvDPVjLiFPQCsDuPrxe5NSt7bI+C8LzeqI73pYGaK4kSNtSMYk0E7
Ls1jxKcRVh602gA2sNoRRxirScQsF2UW0BKWpKXIunzvL4SgzHo4yuS0U1H44M9E
kbR86G/KljXKBnVnW1H/ou9Os5GgCbJn76TxVRzpeRWAKOX5AhU2OQYCJb0MxZl9
wRD7Ehsv68CzE8Dw4VBIjMku4D2jRov3fu2LGmreQG4MJEQjwUNx4xyHNTfr7BDp
5Z87q/rCa/GNZX8zDXi+FrEy/4JjM8j8VV7MC6cGMnbAd8fqQPVPQLtcHUQgGbuv
Db9gQF573Ss8ttWm6n55pb5eUU7wLgcH9YbXdLLQENtJ62HTxeKY/HD206bCEQfA
zqb3/MWyIElvUiIci9hGZCowzcTm9+JCry3/JBr3hkZ8+OSvor/x1HRjRqtlYW3c
EvuyYXFJ7/dD6yHrqdwJG7AhJbzpq47Y4SUTWpDtpM+WHGaQFj1B7JVP2iYtxsDa
nTLg7Ym6GHtH5ZwizjkZlDR9WBWaOPgpknb3JMbI2pYLz8p/69fdOkMwudl4iE9+
iThb9nf2Z6iVhZzxpSei1EGh/5EMQHGLIfcrZwIu/vuk6GGIGYF/ktUAdHBdengs
PqRYP0tEaNQF40nG8RPLPiOPiUlxvOKUl4+7ChD0so5Y8fVDRlgK7GCJ8lfi4LoU
DLGF3sto76A3RgpmCjSh7fSk7IYRiZm92KwTGssRhfPnABqskxw7rXtDcAOg8uU5
sND5d41btT6GqAQHWiYrfAQN8cIZd2WBSiGZG1w7/KPRxcoiatkGDlYJd017ytbH
QI2C3m9v1GpykX3b4sYN3SkHU9GSkeAJHHa3bnXlzbsmudhAL4Ql9YayagABbdA5
VwzGFIZ/43ybp+MQYx5nBl9y7RwxDd2N/kZZXXaqq+9aBKLVhpOpngBbxrvOjiuH
e4SaMN9aOxJ1oiYufu7+azgIcqia6cDTlR8jgYXACPuvZkZQAwkmAvQlIvLjhv2X
O1nogIyWfhNYxJqpxrWexbtg9TYHDnr9JxAdi0dfrMIDx+r10MmF0Sd+Cp/LFMxD
jaR0Z1Gug4CAuypdypVnif+a3FiltDvtjlwaziKG8J5Qcm1X7+7gv+RtqcLnsaxv
70Gd7o1XbiAhNvEUWbM2wxSM+T7zgFdHI8cEjUl5MAT3Vf2gKxGfQibd8z9vmW9r
HZV9eN37qlQY1MS+rO2De5jCLdi6WcMP4CxPaRbbzXPmUm3bDesOf2CZihf+HLru

RPNI4Mg+xy1N9VcMVSXl1SlN1r4yMJdQubdzS722gw7GpIaxVjTQbr6qAtE0xon0
pUmaRwABerAeiFU61t+uAGeP7dCG5MkfL69YrBBVf+jvZeHzcnBNtBuNvBhQy9er
SHL6Gst/Uybdbc+VCboDX0FNb7FgDzD9sN8tkBhP2vYEu1peOqZeVZBIvJpipaSO
PJOVaqmP6Z8Yj/afEIfl5GY7+l0tKifew4gTIYAtdEUqc935yC9dvH2wjVv/OVSu
yfIpxao0AcjGCRdByH/yhl2cwvydVlcjdVjnFi8r0NWjuBozKcjB9urpjVdjoboZ
GHE8L8NGsjGQxzT7oAiTY5VfYnmMlPehsKXNJ84YYsRvK0P1fFk+YG7AATKrQQRC
K/R8v7ymePqfC88281jZkVA9deNoHgRdjdZDxl55vjH5+DX36K8DtSlANLavnZLi
uvltHl0pT0zPdg3XpFyqz1iZZUZe+M3O5EBpbDn7VayM75MwFO2gJhlykEGOBFAA
2XyrEl82tQ58q0pRZy5jW8jcaZhn84NuJGIwhmAoytcW5dqVnDvKMbQZbqiN/nhu
yj57eMnAfR4pl3MtFbI6zAZLnsZ2Re0m0TgNk62F7QR+pg37OMYNvp/P6Gong8zs
3+hDKpj8kfG1GgDf0PNzdnRGsnEcKDx5DpeaR7o43PQAPjIv8ESov7Xrbd+zilQ2
E1haaVh4NWrPT9lFApiDLQY6KFSGHeb/Xu3s+p7xZWmqgML4jgDXzcKCKPTuKDL0
qg+CVAeFLOG95pGrdTo30iUV232E0DV+OzhOF67B5GbDu4M27cAaCJoZN39wlz5Z
C80bYjd3XAJfGiBRWRSriu+HugTDUHS47oe3bJMSRd+qrQaUOy9cCqwOEgvQm+9u
rm1uTM3aeDJzQ8oToV5tc72OxvNRdv0d6sZPOStUD07u6IXSN+S2eSxw+jBl0jQ4
lSkXBKPpi2HW9Zvm/PuDdWA5cYRlgre+rxvztbg7KMzRheKJE9tz52FPybJftvyZ
1J3j+g6u8DC9WLetCA0/HXw3aiGF+vuBeaJM48jMNRxZGd3dRmwALHsRV53mFa5S
d4f8F4kTtXrqBa0Di9qPMKznp8Z+BbXtI602Lv3IdPEaboyFBVJyGMFxINDmuyIt
B3fWbEC8ZsZ6AxZN1nemckf1MEkyhNC4pwZx73nQ/qNleRVsbjXTX6qiGlrTaK0c
PZ5dPJFJuNeoCTtowqnsK7eElb/qKWr9SbjUq/Kmnla3FWxo4+P1goFnaZmacfEH
mhs4vTDHsgKmBB6rkIeUAxxolb6TzLDlZqUS/EWaJCA0gGJSCtdh7W17CwtRuL67
vygwTQqeKNi4P7/DGo45zhCjOsABBAQZ+0i9fVwAP9rTc3MFgb72jTfEIzqDSfzo
h0FE+9X5ssuYZUyPUi3VFCOm4Qxv/LVFCUKa3CskcssjhUQkbXVX4gltDigPRFms
7xV95x9/MEO6RzEZTy5IRmWVImePuKn7lH+TCoTJDxpHC+BmGxuMkuS0qYSLwlxD
wuOO876bUHHdfaJ+JfAs1c1aC76AmL44AfI0eBMoqPxaCD+VdCkDsTbU+vEAOZPe
gi6f6ta4DNMdDGk2unqrGGYaCY6n8ZOWowI40/Qtyq4AgQLT1TtVq7CYq3K+vNVc
vRvbsqwQHVKEwSA5iVVsOkb6YD+q1obEcgJRN+zHNC20jFDZMPaPRJiu5hk/JLTx
71IRKblxaYqfbO/TSNwlRezonDJWTQqvIt5erHXjjGmSYTddadf+dVsaLbuQv7u9
W/XFZzA/zZz+mhGHYeiRmMZ01eyxXCXiLKvc2DnXwT6+MMolOSpgdHgApfpd0uVO
yeiwtlTGUD+cJJcnqkk3rdOv8rm76ew3TpixPYh4xg9HBeeJKhkpIVowg9ihgUge
/L3zH1iMiSk1+fPbqFGmfXbLJ0sy2G83sIgvE4/88MrA4+mKGB8zORJhYdZ8TxuZ
r8GNW3hoXh6ov5v6jEYoGd3XJWsYcJJTtWNtPwMZua+u234unR2sAxwYw3q+w8yX
LjsK9nOXuhcZNTZyGIUEJVOBEb67nMK/UhNiFRYQAKEXJTvO8vAh+gzFgDlHr4+k
z23Z9v6Z2v1zwxAheWcYNER+Jyk04FiP8toA1qYPhx1jttaiffXxdHJWs+soQjv3
/mGD8vTogVJdGjyaJmab7jLTbp2zvMMLKqkN1byjbjZRhaH7rftMxoD06zG9Ca52
ehAhFfsiEjUjZzcUx9ynvBXsEyV4rpRzCREUA6NsL7zrYWIGSVeLn8pDBkk3gigF
JVg2mN9POZYSlZIctw9OhOUXhCViHM5+dceyMcIEUmMyFgN8yDe86sPSnXqJ6cYQ
xAB/TzIsoWddbLUNNzK1WnRaarXx7tU/2iEH9iR3A192b4pZ1126JfURFwhECP/M
cY1Q3lHSMB2Oo9RRWYvlpsGck011EcMwlYYIYxK50RtsmoL7PF1OFK1mYnTvPTyb
NntoJ/mem/T3rnmxTEFP1THxs545BoUFj2fCYjWsxXAlJSht5gH7rQ7cFFmNu3Rv
4dYWF0R9Cb5+JpY7MoAhXk9k4PqgQwn84XUuqdIYPNU/PmB28ObGb3e3zvihZvK5
nHjaAs/k6Z40gQZaAEBFD08yKlMTYYH0F/IO/Aey+mJe1n8SvWTVG0XTFZHm459z
kb9o2JKJmBKTHOPHFOI/dDXfm4kbHvn6T1y70Vke3ORySdHxxTXoEEchkJ65rT01
gJ/cA7EJSIzJ4DpcUlKk+HBVmvl0HX63NSTBEEfWrsWdoEUAktVHmTTMfxnvrtoh
LPnNUdEXJae+0kE+EyEWce9MbSPjsNFddHAdNpxthy04hbvQx6/YrUrk0BHGtzDI
lIdeatVgxlIb6XS3UzfS/DqHx6+FCGZ75ZYM5/IwlYXkNzXXibin6xqAL3UFAGob
kGeAoKE1bo4d4TJdoYafa+9KxU8DH8fQvMrfFBtS9327I4qWFv4fzPG81opU/+d9
kkKOvewfx99h4aMfflT0Y1bs8/mLMABnZiiyPdE4ZDIwoicqGsQgO1u/dRD7pHWt

```
J9Hv77iPBZMmURHGiRkK0hBxYlRGUFZm/6/Y/aX4vG/1K+A8l2ksWdLpqXRQpcuD
kqIBlcn++x8pyWyY1STAOF9w1IFp5wBHH1fy07yNBDj/xKMufz9j6hrYWQV8bjWV
TK3cb8Ar2Qr80TrUUCjyu+d+37kcsi2uMDkiRD/avJbLPwePFTuJZe7nZYdA1A2s
hxnJyBasTI4iMlxH11JYuMGHouu24u5BbCILf654lR+BIQ1d2ogA41eHPlZ7x3H7
```

C.3.7.1. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIOVQYJKoZIhvcNAQcCoIIORjCCDkICAQExDTALBglghkgBZQMEAgEwggR+Bgkq
hkiG9w0BBwGgggRvBIIEa01JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeS1yZXBseQ0KTWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5
LXJlcGx5QGV4YW1wbGU+DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBs
ZT4NClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBG
ZWIgMjAyMSAxMDoxODowMiAtMDUwMA0KVXNlci1BZ2VudDogU2F0LCAxlIE1VQSBW
ZXJzaW9uIDEuMA0KSW4tUmVwbHktVG86IDxzbWltZS1zaWduZWQtZW5jLWhwLXNo
eUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5
QGV4YW1wbGU+DQpIUC1PdXRlcjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVyOiBN
ZXNzYWdlLUlEOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1zaHktcmVwbHlAZXhhbXBs
ZT4NCkhQLU91dGVyOiBGcm9tOiBhbGljZUBzbWltZS5leGFtcGxlDQpIUC1PdXRl
cjogVG86IGJvYkBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCBGZWIgMjAyMSAxNToxODowMiArMDAwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6
IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOiBJbi1SZXBseS1Ubzog
PHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogUmVm
ZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5QGV4YW1wbGU+DQpDb250
ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsgaHA9ImNpcGhl
ciINCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5LXJlcGx5
DQptZXNzYWdlLg0KDQpUaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgUy9N
SU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBz
aWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYSB0ZXh0L3BsYWluDQptZXNzYWdl
LiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSB0aGUg
ZHJhZnQNCndpdGggdGhlIGhjcF9zaHkgSGVhZGVyIENvbmZpZGVudGlhbGl0eSBQ
b2xpY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCqCCB6Yw
ggPPMIICt6ADAgECAhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUA
MFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhT
YW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWU
nnelN41KImVaTC3D9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6F
UH4i2GMt4jse2Dqs165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXy
CjNHT82S6DgCReZuTtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/
```

Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80
RuQ3qFC6vL/PGeWy6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8w
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0R
BBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAO
BgNVHQ8BAf8EBAMCBSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8G
A1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IB
AQCBSXignLEynBakDKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx
/Ht9Ii6zyBZVjdaox644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOO
oHz53PYDBh4zE4Nar2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3
web/eDOdu+F2MVtluLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb
744gqoeuD9YSHjKK49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWd
NeXzlEc2tUpAr4vRhZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phq
zpqp1zANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhM
QU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9u
IEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzEN
MAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNl
IExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4
Fj5Nmn9PkrYo0jTkfCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNf
CwDcDkY63PQWl+DILs7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7
QMFtmd+K04s+A8TCNO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAe
LqzJOMayCQtws1q7ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7
QFecN7836IPPdfTMSiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1z
Q1Pq90njlsJLOwIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAM
BgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYD
VR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syy
LR0GEhyXrilqkBDTIGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0
WTANBgkqhkiG9w0BAQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6
BdP7GKJ19naIs3BjJOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzco
zmnd6XaVWHg4eHIjSo27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukK
Yr7agyHahiXRn/C9cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IP
kazgPYgkLD59fk4PGHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s
16jMhwFXLJtBiN+uCDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEB
MGwwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMT
KFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXnt
dX9CqaJcOvT4as6aqdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqG
SIb3DQEHATAcBgkqhkiG9w0BCQUxDxcNMjEwMjIwMTUxODAyWjAvBgkqhkiG9w0B
CQQxIgQgMahPfXeRTJKDWjCE/0llScBMuyD7DptAxoKsAmAzBdgwDQYJKoZIhvcN
AQEBBQAEggEASJuMfoErHP+bowktPN/yJIltnTlZUibkbJxhHPhR5EgNnn3JyMoW
l0yP6nJyH3sBQ2/CIBkmMSXmg+A0PFv3w40fUtX2oKVzT5TKnNsIDtv2Z7J5JRI3
TbATMRmw8VItmPGFCJsD9nXRc4cEgvrvojXSfv6bWp5hCO+8WNadiiGZNdoZduiL
rWNSwO9nQSxuNkqNo+wwaXF9Rynh1ZcazsVopBB4s5XuJ/Zcbbsaci1w34ywNCHw
5xx9Cgj+6+yUsFp33P2YVgdfK4beyoOZK27Rm9e7Mpi6QxUi+BCR/8DB9svZBwob
K7iaKJzRBDxl4Qt/m6VHxtvkTXjkOOD+7g==

C.3.7.2. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-reply
Message-ID: <smime-signed-enc-hp-shy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:18:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy@example>
References: <smime-signed-enc-hp-shy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-hp-shy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:18:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-shy@example>
HP-Outer: References: <smime-signed-enc-hp-shy@example>
Content-Type: text/plain; charset="utf-8"; hp="cipher"

This is the
smime-signed-enc-hp-shy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

--
Alice
alice@smime.example
```

C.3.8. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a text/plain message. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
   └── application/pkcs7-mime [smime.p7m] 8690 bytes
     (decrypts to)
     └── application/pkcs7-mime [smime.p7m] 5418 bytes
       (unwraps to)
       └── text/plain 514 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 15:19:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
References: <smime-signed-enc-hp-shy-legacy@example>

MIIZDAYJKoZIhvcNAQcDoIIY/TCCGPkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACdv0XrIiYwOqFiCZ4pb4VxZQfPk+g7Kb7bD
45v1z22kXFlsbpOrdYsJCfyleCEN88RhU/gzDpyLHY4ESXAJ6fEvKWJn/1kRZEXO
LFVzbE3f5F1N0x0cLKa7r7Au0ryY8P8fvBM0Z1sgZToOL135JiiKm3RD7IKXCLxg
onz7kgGCrkby51sdsGAQgJ6rvFJlmvPQLdmi9YOOYpKiIR6wfAUu2mHOgBdEtsot
k7UfAloQ+AZXA61VSejFBwEWwKMSk1NiAj6S9Nppn+bOzEI/1qQsVJcNNcdA5kE0
BWRzQFs2f8HzaoitaeLQuI4UPjnasy86sX3kl+xK9MCe9iSASZwwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEACFBy5UfVv+8iiNnM1ZrlMISJ
ygBuyl2da1yDyv3d5J9El31g6QoJPllmkSC8loxIYPQGdAZ1OIEDBWV6bkgPGnZP
tL07RkYkNTAUwLJ5Ug2tKADNfkKWOZ4bNa8SbxKDmgx5CtleG2/u3X6xw0DEA5N6
m0s9vDa218FWKbe5wSKAA5mToCzWxEOzLLlKHL/a/7p5njtYxneRj2iRPSAOFmU6
uZ1c2UJDmd58b2JlrUxTxYf1+jJguej0/j2YannWR0w8LcF/jEXrMUn66CuxOLoZ
JdFTc5SmrHnJrjuE0U0jw6SW/R/IIF32XXEX7/4VFltbjzD8Xr/MeocHl7hTdjCC
Fd4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEH1amtLrDCmloM6pbsnGLNuAghWw
x8bEDtMcmKRFaclsZQSooeU5PEKfwytxagFordfhGUM8tkgm+ZIGq7mujmTz9AmR
rwvoKTU7j43XdwbT4QPzFwNZml2ay7z3qQm13qlR1wNNQgmnH/KWiku3iFYzvF9g
O17Io10kAfgcH02XtPxPUhKxNJxrW2fSpELB4olSyET1qpHQyrCf+4m4BK19M6sa
AwqBO+gj/hv2L5TNq21dqsAsTe7uNpM0++gJZqm8MQOdmTQrdOf1wxr3J6KRIB5o
JAFyLHikD5fKyzLaWfLaUPp36lrISZPOHodnHwYYQUuRZaZ30yABi/5KmPxu978A
ad7SAgBqg3ni8VrVKHPz7b8SngjPVWYOnlCjUC9jQlXZOz2mGeaP9ShiW0+Oh4HC
Czm9z6RJ+4B2pkkDtnPvxZnbB7VeMmuJYW88GfAka4HxSdMU34PQioy+egjdcPml
OwIQ059A+mZBDhEYdaNxLjHvbL7SBrV+AsfuwmOUmGgTXVnzRbd3qRqRt8UIU10+
H/vMN1W/HKeWvjsg3RAjFCY5B01CJO/+bp0I7JBQZn2p2Ke1hNTGThUCaVbX+0A3
9ivwOwws48WoynTr6M2upt62lpFqI4FaXwv6/M7UoprWrtppSMdlpFv5Cun8RPb2
```

```
   ZlOGkcrHxEZJjbCA5uzPu8VrBAj9f0pM4pIcyXBtpboRBRWctlFH+7N6WFN0dojk
   yuODty7pRnbpaZyll6GjzByf0hUsyuWbPp7V7moqTYqIMfkrOWWl8j9G/Ri5LNu/
   gpuGBrEBhW3VDmya1axW3MegAFu25WTxtJ8lIeE+BIKidtEE3jhFpl46KsG9IPc5
   6Ctb4kGm2sI+1O6EvkP4CvMo8/ZGwCSYLCsLwi6OXlRA4LbAHgwCx/UsXNcYXRAS
   oEmVhlN9C4exEvVW38OB9KGIjX7ViCxjwaXpPhrnLNnxLWQLBApM58+4DgEa/jlN
   rHL3c11S0/HFbJ+3RxA3jCE/CVFeOfoszrUNz/tSLqeoLxyeGixIEutTwIag+5RX
   WuIa/vtBI9om6v2UqwgvijipClaFwBZBjZXRDxZjO4wbDgzmXT9uGKSLwgrnOwRM
   Y/k0SITHuRKMYAnRqTj0xTqdiUznIMLKCRTlrqejCLREGUuTowoJGgpYLmQ1OdpR
   Qx10qrtEG8pCMFm/GS2kdMXvSnlNDYFKiJUkVoIDEzjm43DhpIN5KGQwcfChAGX2
   gf4T0PPGHVokXsurrqpLc7Uy3gSajfc9/4VWrALDRfBPh7NsXgWflMc0p5eIU8FG
   i3pzph/J29SSN1+JAiIfeSoIdX3k5oHMgHwhKY4+H7U1RX/XEdNsM/twQpeC5Ri1
   9WPx7ZcaQKRVQT0vBmIlgJFYBJY45emZcPaKMcN+hPue9Yt2+gQXD8xKnh4IGbZy
   a6K+vlkoEpb9VrRhGjSarX8CzsnDlGTYjEfFru+qbYN8XYT8mtSUxbLYsnRo/skn
   BcT3tHz4hi3MS6KjJkcnXw98dyH1IkJgYACSv2GjyEGEZpR3wadJP6Jcig9xX8Ga
   f1OuyyDwTM4ZsMj8PiB+wd0KN/JmgGU5b1wkTcc8cVlRCmiN0UuqNAHsCO4pn2Qh
   yhfdZUO5l8mOcmsZQ6fRu3UbVu1HjZZH1eGjxiPwtGUtBo8mhOQNOCZPbO4a2sza
   QBOMx5uVsZoqB//p6oQFQZdv18nOah4T8JhoSoSnObr2NgJYSgLER/WzucP4zk5s
   o7LgRTlb+IfTYnw9FLUvOHLEs8AB8TWTpkk8Pto+K3CcUyJMKYjbg/57teYT0T/U
   /aYB+CuAatM7HOc03C0XcvfJuZsXEzSdu0Nuw/VYSwibXS7tgIu/w8TsfGZqAdEz
   k+mCDx3NeCukg/t4/7ju3NPe8RqhU3lBer4r94jNoPG1VkCVeO9bUQw/6PAVmpeS
   FkbJsAB1UTSCimrgZlUxQAnndDFZCdU/rmc8ogRCmHtxrgzGyHt803jdlEBQ6Ct/
   rb4PcotIHQALRsc3dyL8BkwxW0N+nuB3Slxfr4ooOv7lEeAvZn/nizGGlxynFynB
   DSeXi1NnMt+8ZeX+jQbPDQNnAONzlQG7LoxuFXS/7AIeF1V5MmWsge0n0SL128tj
   8xVC0X1NUvTGVKcW73AXZ8V7oI7sVee/waRo7SdT4yzg0lSEzvRepNecB10smdnM
   Z7VPXoazVhQJN5QprodedrLOdRD5KwifgrulJsDNHxsMl+cLYym8rx7ajyhofOrk
   OcH2PNRyu14o9ts7jpPhghyqwG0P2A18RNHB7YcsPiy1MUftIRExzUZ2VCyYRK4O
   DTCk6zatynXBEbr9olQdeQJHAYUF+D53RUJzDD/vTD1TpW35D6xY5s7PxajLaybc
   4WMcZwJcLt2u+VznKgwlRCADESBE1XqScu7mfoB3jpc3pepdApHcNj4T+vBX/OwW
   L5IcN7wcMRzdcfP1XlHii+WriJk4GM8Xn8HY4iK15csC1F5TxbPIT6r4SVdRoCFX
   zpxEoYa3JvpAP2ek5LX+nTd2TZU4WcbSLG/Nn6y4K3KJNR+SuinwLqNrwXbXtKu8
   BM7+bshaz35e6klKXyKksXECPS+qPjVkKMSVYoqg6go1VIxqDvPhtlr9IvKjWK7B
   4mSWU4ZTaw61bTRw96bAjrjQA5O/pY7+RGxxAU6K3G1BKzL0z4rGCACokU7i/n+l
   Rj2iyF0a9Qf37CLg5TQXqoDS+zgx2qb2YTos9MQj8jSd9HKS2B7VIXWJgTJf0ZE8
   rlxZZUUx0BwehWBo9fJ1ysBQ/ZCyLV5i0hY5/93Jst8Q42ohT/Jjo/vxsYbruUdR
   tGjePoIs0zY2i6pAhfx816/x5ULolpKBAhtVNByiP2TMDZ8FVSM6JmciNs81nnlV
   AjDixrjl5PCY5sfW/qGhVp+h6PUoRjTXS+ybbJAzkVn7BAHli2sdW7OvS64yJfxn
   2+nj3J+VpMrnH0YbaDzIcK6G1cCN7UaZolUcfgPdYQKdzogyRxBYgr3eAMEUwmrk
   Gu1TLSrLtloSb+w/+mkQDg5LkidqVPpRz7IqlDhWVuZXI5ntzEhY+7DWJEocKSkf
   n8vpIecLWn5wHTaGsjTzvwgZma/o4QDJrNH+pcFj56DBxVR0B9DyUiSBOrZGU/kk
   ts1FOaFYGBg6xvk0S9qFfevizRZ4DTY+VZBtLpk/tvYU864FnSkff3ps3W+bEmlb
   MgvVAW4UpLgVGe20V2z6QmUm+DRmF4/MXSmRJTIEv2eonDZQXZ2/16KaxL6RUTNP
   d+ZgU1ZJfdvesVgoZCZQ/F3lsDlSROqDgufQsaxvbz0eVCTgSEoITfN+99AA6p7t
   xmBblraAIfax15zG0VQAvEBhWZzqkJzdKRr57RUW/UVOqBKgYegKxBtTjdXHgRE4
   pwr1kWlCDqF8GUjC4JX6oc57tQ+Wf6G0db51+jQoJ+XexKUCgyJFj942795Du47E
   tzLS+GswkD0kD2JBz9fXj9iAg06RvN6clJhStTOFj7Ila/6DFL+GoV5d3TCNlZ4g
   lYv+hUmiW8RPpZMSGChWdTIrp160ftE7fpHR/M0cNBO6zB42HtXWgJzGyr3TZ54L
   FmfUEnklbvExdmZN/0G7eI04ZIZvQKZQYl8pSMQ4kZ/8hEHf7BkeHznadb5FGpS6
   +ZTKy/pT5/ulpeyMUDlu0e3p4axhwGGaUnEpNRdUOhFT4jiil/hZzO1GN4GCBDsJ
```

Ok258Bo9xVHOeyDneHVbn6FKWkgASGGBzbJJwCybiEJIM/ixWgd36jg7IpbO35Fj
YPZYoMQjYGyyuq+PoNPlCj6k6jU3wYIbRoNpXso6eacAq1z62l2lWDQBdSSNReCq
gXeX/8S/qVXEGAR4Kju/MiROou9yx8TvWAmJ5RHaiOkDHdFvxRFbXjf4GrVMYpaz
gVLgFuvn3Imt78IYOu0rb53GazUYix9qEa6fdWAHK2RXrgJW0YKtlDRfZTYgjVOY
cdf5kQhYRSAktDOSB4LncLCTY6KDhrkrMshWgCOYgikhoe44enEPXKhWM9y1BVTO
ZvCjYR2uQ4ryIVnpinFhPhT8kZwqdia2mfiJpXmDMClDX+XV3TWTsMWrZ2c93miv
0KfaMJDOiFWK+zhlQrJ3aKpa1iR/+M0YkrxKxx1qOGz4LW0rCn1b2hHjW64fqq/5
rJRFcC1SQM/vYqtk0U6yUeImlfIoRIIUH++f8vd/7Uv6AmOOsgKEYp+pkhtl2nPQ
MtZ1NHw7oNmnLi4TeJbtLRU2M/7mChrL9C6BVDP6CZx7F310RNkxQ7wHapVSiU+A
LmL59uxWzXSyESQYojaV4hcM4pDjzP98X/N/qNwJPnY4K/LVacKBz8GZxi3KOEBa
nWxVlOf8RRpvi0AQb/t48FVGAVzC2Rvfg3MMvrmKMv8SXh/Vj2IsYuhDME9ns1P+
eJs9DCLp9YwJYpnstS6MRT9xcPwWAHT5PwQbqTlTFvAJgKL/UjxYlsjwP0Fa/aCk
CNlSMVHVgQSSAbaR6CN89Yok0tnDJ5VSG4X8CKbVQved21D2UBXPSoCsnuvgw3/y
jc9n7EyD+JsgmIZpbvQmJcoqvO1gxjmxPmFuM6Q4RO8VIY5FHoQZIArHo40brgZw
gpn4WjpGkyWBVunGsBX/WEhNoPlpvNDZHSmH2/j1cG5QWrV0x0ZRsQ/J/cpiOSj0
Ez4ib/yQaZWdKYtGd9SBBvPm4SslOaLm6eSLy88bBDJCRd8j77RMgjZVYzEMkjCV
0A9GHBX1yPcY5X3bxS3+D8QsyjUPNDDk1rwY4MNby6MsEsdwoZ+qFFWLXjzlLW1p
wHYCM+MH+vXwNlxBQE35FCIoNrBgzsuGonDoiawtcZ17LBnHLu9O+mZOw5E89ukj
NvqBY+Xea1jc1RjwAjD/aM+GKL1V7IoOsFwHZYSVADcvrjWBEbqu8Uaahb7YCh+D
5cY36IlaKvWircrjG4ZRLzI79e+lutD6JWASaQMfpJwP0FrY3Rt+KdSf1vXS/EaZ
bI+C3h6JxG1cOW1lJHG0u8rWVNQkN7uYVsw5IBDgUSIrOl5No5hcFbMrslF5X5XQ
lA/4tGJjT8tZVuksk2+P8Sq80Zs67Bsq2J9envNQIe/zXiBacOfpteUnQOBjH7Q4
dTz+NnO0bH4fQwg2jPMjArUvRgjexG0DpC/hbBTX1PEhez2djjXjbsbEoS5N7MwI
PLrI1F9yBhU4I/ZPVVqEXlOrSbgKyyKxzX95jXrfFplFVW+ch3RxPFGVk1gVvRUi
GmwNAjVQzU8rzJtzGKI8aWnQUfwpvEVBsXFWzn816oQxwfZR1aIHHKRQ+aTXyzr0
u+20U0DJP5ibVwSANUbbEcxG0vh1hJDbPGa+zhy+aWIWbAiZFZPHENPG4g//iww8
ol9NavfvvZMhaWNX5jfBr3j4mMCbRfMfq/ZgLtiCfQUXKraVQrDxSVWqzxSGMGm0
iQHoKKEO08DUvFQ6YlJse1N6MxQnL1tUKKPeTE90mXescLZsUg6lf1Z2NaBIVNoG
4UMKGJ1adznOKWVGZxBr/GBcQDA9OYTOOq/ylxG0hZetGixOGQYBsJx3U9fdDWYm
4o+nmEFhH1sr5QvSAEkho8uCZxTXx3zxh547nzzCibuG26uhGpZ/xbFA/PpFvkai
6tXDze0uK2rlz+gf8yRn1Yl++Lq3SFNrK/hisAGY2P3vYSa7p3k7cI4lfsacX7AR
gmkpCfY3gLDLHftoE+XHHFGNwoWo0mkiF/gViRv+rj2m23jtzs2RKckiDpHPryBD
6aktHPrs7ie+4e4Gj/8LEdp/czOG1r+QdhMYANSn2Tls4lQNu72i0BOBeVBszUaI
A1bEyVW7eOXQy1dqTkhTkF4YgoWbxi041p1E1hjGs3lkRuaSkbhW/JDJ+pWEmJwx
EX598fgRN/fnedEElqn99ob4iifPbRWl4gk0n6Gb2R12yzx81U1AJesPAPzwDiPd
rfp/JM69QgRUEs0ady10Xi/LOXehg6BBqcpVLPXtQykK1Vh2n2mlG0szjI2AHxWl
k5EDLIcoBwUdp6UqqZIt2WOtP1o/KT6xvb7oUBbHTDUt5gYrBOwNx+FSAW3MEI/k
zA4zZRgl9cPTSG3Om5dd7WejVxw7YLCd3HULWOCYb38id9//QmEPxAZaEemEFslK
WAEwKbqoiFi2fkTPjZlV+4a3wor+ZpjR8itnknFqMkRGewklmA4Q1hH8cW4L+TJK
5OA1HI8vTeigu3vog0nd8wlRr3hy0zNLr5b1QtpAfv+m3gaqn2DjHNXHU7aYsna/
+fZ5I2Kx4ja4vyDcx+vIEOiJVZ0SabINF4hsAyyF18xdo9Ox/rapKhF4HZcTGi74
YHw30ig+ddtvtRrdpfuZKW8OrEVgmvhIc6Yj/oVc/lTflJ5BEZA/pU45dH3NLWWo
gWqivq05ncRgbqPVNJyjY6XBELWWonQesu0TTq4PGESxKGeSBE9h4S21tYNhm6Un
SDm33C36ARtOljuvdELav8B1wqJNCjNU/PCPUI23txYMQP4lM6RkPWjNd9Z59Zpn
hgHXs4nF7ZWnNxEhnG8MN7D+kXG8UjBdQwyAGwkxUl0wPEbMcwkj0bmBVmEvWUFg
5MoJjt952bgNTa4tNu0UDzKg/eirLXMnlxgwE75ZHeMWYj7OJmDl27UDA2zy2o/U
gU5j1ovrtdMqsLtd2g62ccKDlzDJCVn9gP6nN/KXhKBQRhLATgo6a1lmyd3GNA12
CGizsLjg+UImbJkFUWp4eEZr9E7RcdJ6lC/Gs93K4aq/XbhJMdjfQXWLM03ndF9/

```
r7Cp3Z7TW2emivxYYCk7airndOWeIdZrwxoACNTQ+6IeD0LSet6iMP2EiLRRgfOB
2eU6X7yMWvTwRYbByybrKpqsM2moy4IpMS+DgaThSVxVHf3RbFvIXPUmhRCFFkS4
lmmm2czKN9wUaBLKcmeynBpRaunt9n0uFyWJgSbekqw3cet82vu9MOPSmM2h36UV
WgJDktehhr/gi23ON4kavEwGngVIvlq+Emm0SuUmKacqdaOmATxUhL92IA93L9pm
RvT6xARWsy0DrG/r362C6PDwp1fsTOQju6LkhFAOAvqDPKk+HOIjgBtkynHUPGwv
8EN9Gx2SWwDJahAjPoz2t9kByC7PdG9qyGAAAEU6G/wXjshmzgw3jdw/PRmfSdNs
gbky/4GGewNl06WC9c+6qN4ldDff+m83ABgWonCuamerjlaIFFbfBJEGX/CBz7GQ
QpfxuAEbhi11UloM77povWS5Cl8e0GSD2t2mt7E0aLgMT+L2TZXQx8lZmN8sWQq7
cP6aK8FpkDhidLIc9fneWucvMH5BKXx8em3ug4Bl8MUABR4K03ebuTLfDH+FGkD0
HNeqqUVBSzDveFdaylcw2HkJpm8D9BoC3Y0n/WMW5VE=
```

C.3.8.1. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIPXgYJKoZIhvcNAQcCoIIPTzCCD0sCAQExDTALBglghkgBZQMEAgEwggWHBgkq
hkiG9w0BBwGgggV4BIIFdE1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5z
ZmVyLUVuY29kaW5nOiA3Yml0DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWhw
LXNoeS1sZWdhY3ktcmVwbHkNCk1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5j
LWhwLXNoeS1sZWdhY3ktcmVwbHlAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGlj
ZUBzbWltZS5leGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpE
YXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEwOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW50
OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNp
Z25lZC1lbmMtaHAtc2h5LWxlZ2FjeUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNt
aW1lLXNpZ25lZC1lbmMtaHAtc2h5LWxlZ2FjeUBleGFtcGxlPg0KSFAtT3V0ZXI6
IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjoNCiBNZXNzYWdlLUlEOiA8c21pbWUt
c2lnbmVkLWVuYy1ocC1zaHktbGVnYWN5LXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRl
cjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IFRvOiBib2JA
c21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTU6MTk6MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVB
IFZlcnNpb24gMS4wDQpIUC1PdXRlcjogSW4tUmVwbHktVG86IDxzbWltZS1zaWdu
ZWQtZW5jLWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4NCkhQLU91dGVyOiBSZWZlcmVu
Y2VzOiA8c21pbWUtc2lnbmVkLWVuYy1ocC1zaHktbGVnYWN5QGV4YW1wbGU+DQpD
b250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InV0Zi04IjsNCiBocC1s
ZWdhY3ktZGlzcGxheT0iMSI7IGhwPSJjaXBoZXIiDQoNClN1YmplY3Q6IHNtaW1l
LXNpZ25lZC1lbmMtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KRnJvbTogQWxpY2UgPGFs
aWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4N
CkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTA6MTk6MDIgLTA1MDANCg0KVGhpcyBp
cyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KbWVz
c2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVk
RGF0YS4gIFRoZSBwYXlsb2FkIGlzIGEgdGV4dC9wbGFpbg0KbWVzc2FnZS4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0
```

DQp3aXRoIHRoZSBoY3Bfc2h5IEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5
IHdpdGggYSAiTGVnYWN5DQpEaXNwbGF5IiBwYXJ0Lg0KDQotLSANCkFsaWNlDQph
bGljZUBzbWltZS5leGFtcGxlDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rO
QlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQx
OFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMT
DkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB
8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5
R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJan
Z/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9
yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJL
AgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0g
BBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1w
bGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQW
BBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2
GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD
5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GD
Eu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8
uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K
9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpi
vNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88w
ggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTEN
MAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBs
ZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1
NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsT
CExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6
WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZ
WleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CR
Q/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3
nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0
nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAM
BgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAV
gRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0j
BBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJ
ojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnN
vOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSi
oQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4
z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2Z
PRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH
4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAP
BgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFl
AwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8X
DTIxMDIyMDE1MTkwMlowLwYJKoZIhvcNAQkEMSIEIDUClbNj9mKYodH3vCGfNVpZ

```
jSSWg3QZ6u/dLxbyfbvEMA0GCSqGSIb3DQEBAQUABIIBAHqRG2dp61WFSKrkBcj7
sVy7SmsllIQUOl3EO23T5h4PcL8PjggAJi/GHWaEsGviQEdS0QAbljEnzd2wjgn0
QDtLBAfpQtQR0byQGTzpg7y9Lt5WnuxQaZxsBPvENqeYSFesUVlW1JrJGXcqLH7U
cu1+bdDLEe0p2ITtazvmgJ5NvoHkucBk1v8fwW6uliGJCZC0Gf9WJDP1qay2Jexy
/TUzmr2Egnxq71WlAVql2kfUOfZkgALFRzhaHtonrST83I1sLK9ZxB8ZX8vJX56v
5hHRzhuQQyAVgOeVz7skKIb5ODfBHqJ1vEzvCjf72BgQLYGEzR6hmPXW1Ml4vXtV
lIw=
```

C.3.8.2. S/MIME Signed and Encrypted Reply Over a Simple Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Subject: smime-signed-enc-hp-shy-legacy-reply
Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:19:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
References: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-hp-shy-legacy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 15:19:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-hp-shy-legacy@example>
HP-Outer: References: <smime-signed-enc-hp-shy-legacy@example>
Content-Type: text/plain; charset="utf-8";
 hp-legacy-display="1"; hp="cipher"

Subject: smime-signed-enc-hp-shy-legacy-reply
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 10:19:02 -0500

This is the
smime-signed-enc-hp-shy-legacy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a text/plain
message. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--
Alice
alice@smime.example
```

C.3.9. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10035 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6412 bytes
    (unwraps to)
    └─┬ multipart/mixed 2054 bytes
      ├─┬ multipart/alternative 1124 bytes
      │ ├─ text/plain 383 bytes
      │ └─ text/html 478 bytes
      └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:09:02 -0500
User-Agent: Sample MUA Version 1.0

MIIc7AYJKoZIhvcNAQcDoIIc3TCCHNkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBADDPZm+dVU61KX+lmXLEuKI+W/hu1Uw0QmHq
Vi5HfM9uo9AMrXVl7PG2YzA75ItxhcJMjf8TwnKlA0YbrwGnhJAodi9MHCR+nqdY
A413rxKHU1hcJLn8oWck8ypYwzs3NBDJi7F+8aBmfEolG8xn42o5B1FlKCnKMlNg
NBTQpqruLd+n6iin0vGFPTJV7PBDdcE0VVeqiIoDAsZaTp25PYqEKSsnCO10zRF5
8v2BEAX6h8EpjqE5PX65JKus2NAjnJioN9eUjCQ6mn1XPBw4UYJEUqc834+17HcG
FjwDXIoJY7XuSNd2brm9JFYSmlyR6gzz3bRgIUqWYgjQhqulCRswggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAmxXv7vLaS7vcshZyoM5wgRsY
IUF4iPK6n1BuzbCZnexPwW5TGghgsO8zxA64/hzzqEwbVneZIfcooIij4bdQZx17
nbYpLBCC1Y35+gtsiLGgCyUvqymH9jg7znq617FNqgD6v+Oui7OF4ZX3t072I+4I
HDjfFLryn939vUwMpmTPUQ5Y1ZqKTNjM2jdDQ5/lJ5ndGYcC/wi1hiZt5mz44LvF
```

npGAXXVRn7bcYUtDRsFuuSmHbckCnbeI4C2yUOc2G6fmyHuOnpy5LL5US0hODca9
pMV9dn6cJH5T9bksl2eYiPGS9CrixOL/U+fXHmVKsyzm5cRU/CB3rwUDnLen0zCC
Gb4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEBzMZlGxbLgauF9sIia9KrGAghmQ
avkXlQ62LNzHi7NtNtPLsiqIrji1UwDWe8cYPupsu+3hxQZRVMDHjC1ygNsK8BWA
P86t5gJaORrI4AvyO//4bEzZM267YRWiC3RgxM+p3DB161vETc1cXjZu+7qKJMdE
LbSH9iLue/iNi+xQxD0tGYVzuYPwHypts8br+Cs3Yda3aWK1ipJQUuCILbDCGvl7
ZC5eizwGufBEhje17iJkgVDyU6sAY10E38YFL/saDHjtryJLp+c0cV7R02UEmDPC
Jf/BfdCknCdo7gEu4lZitlkcr2T1h56IAyK46iyPLXZaZua5R8He6/MEdC5Ys2a7
gw3FwSgzjUlxOzIRtGwCqDk5dc1Up7PLOmeZ5PLaQglwB8fXYDkv9f/T/Sh0uJ40
xc/pcK5yjrcpFr0pVzcPVurzBpWtKwRNjiRnwFGhJafPfldxJf96WtgkkZcJNDmW
11yO5SwWHRUd5OpVvffdqipm88nL9tVfp31Jy3jbFR+7XTRPUy3QJ1l7d97aO3p+
aZLKXhgvMWN9R1MzqtF6wihpmPccLOX3Bd8bIwuGFeyZA4FR6iXicdql7nXWDSzw
1Zakfbe4EbKRg0yrRb9X9iMaUBoScwByEopp4jlGex0hGD5omujbvrd/tpR5amqN
Q+cY/J33oo8v5auCWQiBdr3NK9jG6dAyfXrhcvpVi/Ay9sSMGewApCTXkRRibbNS
jY+2szt81uo2Nfp4FWr36rfNmE7KmBHXWTs9U7ZW5yYJvBVG9VZDGk+7vt/KxNqh
JEXdQlW/g8XmuYDqtnx9VL+vAZqHvKkBqvSZqsTrEhOIJ69e4wTu+2/f5Kv5DYlw
pas+TKxRN2VZgGaLx10Jp1OTkyY846t4iud8pVR1v3MxuMSzS3JF6R+Ynk1uTmtD
xD27uKFT5LwS5+jvLOy/a6zk104pr5SvA/EnGJrVnODO+Rszw2JWxRdiE2Cejk1X
zXgLIdDvRF/tytRNN2UOhypvsdkZdjRT+MrT26ypkJSPEA9a/0LdiylkRJuFW0Fh
FDYIZ4TljFMkedTktD+O38TNVFE42LBF5dTm/ATz0Be00YQgRC+QSE6O4NEnCZhX
Xppkk1sFoPJvA8AAZANQyZ10wQuFZA/8S/6mJ/15Fh/pr8c/NU4NyM/vC1T6Pg5f
ZMFx/anra7iUCSyn6Muo7t3vyevh+QX0wn6aHWWe90NPsuLFd25EDYWrokrPo57t
/538uPU47RPCRKtG0tqmuNplh/8HshhP3e9082WKPyFaFixGaVVmhMjzU9+CFGQa
d6oJag2uudjv+e2mpwX5Zm4lROlIO0QH3ubhaHz9ZCU5S5Hckwb2yIvk81gFqmm3
/ykRWX30gl1J4tfb4+WpbcJWYsckwc8mvGizDEQTu6oStblDBqJXzeB+PdXlLZQZ
xsbAc6xRFyD8CJBEhAEzwQ/y9tVG3hLbNhg8IQ1XMCrVp3EypwDRdDEIDnIP2HUS
Iub26/ZnAXwzCT7jt5WGjsM73XHMruiL/4nwSGv+px7Zw59U+D7w3bxncqaJHUPe
jUxBIJadRSUkK0UgIMkshAQsCB6GyTcvddolFZF+keE+cyvn1wKa/pUPBYh1Hwmy
LZ5Niko2jqyuuufTAgB+u686Z7c36E3N+1xGUS6BQIoTKulEXmuvCdwC1xjmC9Hi
uHKb8tvlFaHfsp/Ilo2v8GgIL+pkJsZeHww6cM80qtuJKMMGz35SMdrMbInYK+4U
OdijBsBB2tCk7m5aRn6HVff14RBZDsqN+5xtuPYaE5Wmie/NMTOlKhvuc9Yp+Xl1
rvIe02kKZ5FjPYW5BQJuj3gJl3G6Z7Z9qrEpgqK6XtkMvEjxUbzd5PuhFDklPd9q
PbXD48D8LO3q1rLScuHgrRTaSXy9XfYRvBaNuGrGfD07ucM9LqS3Ugu6MPyV4wPs
2bvQkybHmuav5M+szPnyUVnYvS9LmPlCg3IX5YshrCyVYz2w6zZRF4J+hI3zIkla
huJgUoGumLSlea7qTwr1GS2MuaUfe5PZMn16qOaqXTMk68yEM4ugI9a6O33MJK1o
OTkWQvXFRQpb36NWAVHx5rGlk5+LG0idxGFjyI/AUcpoe14h98QtYROjas6UOIDm
/CVjFKsrzCsyWPjlxL1mLoe+0J8ErFY5X0ZHGYIP2AvgpTMZGReC9X5FZKeAs1Ny
WjiqUjjsxW7f15ynVpdHH2Z7M5rZgTdClC+sxn6qPq2uaOAGeMY5hQR8MfPX+aWk
4I62uThfl4lDECunGX22nIcsgpRfuW6ylmGlkpNZDNGf/ngrEkQEj4uK7CBx75Z9
jNubdl+HYWUQEEF2I+Gp665beYQuF4tpmI2Bh5TTFyF5+0Uj/DeEB3Ol6opPG29i
b4+cuKXFbF4F2ShtKqyO033vVeWKmDyB1TfcmWJx6Z/feQKrVRKJsOIp9KrsNVYo
K+xBtHHnnPuJiQM6HUsA7ttPpTCjQkMWz12trAvGOEcKaXAATfQ/upTBuk3NoiAo
q60bS80irMm1/W63hgPILubiXlMF0H1pQ/1k6FoxJfT8jlcXM8xyNxufux0O/uz4
aTStfUW85RzFBa98hoVGJrg/bKXH1Ffc84Z2cc7VMqsAZZcyKjzGIBso0MFTMN2E
JsTY0HtF3hzUcV/KrEU+4m3mSSauUpudyR4yLeFmPN5Fc4l4MYhh+vU+S/k4AQwE
QChtthYZmWcmhTu3Nmb8IINWLpUT8m6upYy9/YlVApQP4b4HosKdFb9ZTW8FXhhB
ASzt5f4G/cJhw+V2TahvFNyWGMskArEOsrv7Sg9GNRv7IBSGCB7g+c5A3cWBWGt6
xIy+HlHz2wxaIip+A7Rflw0plZjaxRq9hCtMEXM7pq4FK6MUzs+zVR7ZjFD7Xp15

SBlLkr9Shfo915mGbAvjT0/zNj87yPu/6IiZ3BXTF4mXJFh8LjRSf3WaFLmDGeZt
iX6y0U7wsLbkGLHOHvwMDCm7an8fUyCTzpOC6RwiV6gT3QOFhxj25OyTzwIuETXW
3oNSq37nLwZxXzj58jgsDcjPysfngGTld7PxDzRS3BOIk3YbDhCgYXYsy/Z43zmD
AqDqdoh8ab1foLtuiFbYQC+Ons9eAjbLzqdRzXJMyzKWQXkmzNM03TYx5Sto+G8D
tkv2bPbImfD4ElirDT7nquY6hBG3p1O7qUiFsOjq6RS4wb/v8TW2NqXwGoCplSHK
zg9MuzT+srDCY6qSAePqy2HZ3JnAYsk3Bs0oB79yWYLXkYzgeMZADP3C+ees7oK5
sA7X+LV9eA+dIjRSdXsAlnzviEhM7zSq+82V65GqcvNNFZYqkxsli67Kciy12XxU
pKYAc54MdvrJurCWVp3tWvKsqwdXXlZyrx3/a/fdzsiTD1k++REYhRTEwGkyZsK7
okSoR+ZkVAIRv4vto69DpkPmUX+M+56Wn/nmV3XZQ7IQ5CuF1XutC9NXF5mvnnnI
jIAf9HidAV8Xf3+ru0WzMxGzVtkW8qzz5jqJtDpYIa/IJDRC9DRLWaqJ6a3+c7B+
zbqggQd1Sikha96oqoQOC6ulcjWt+MuFvzjcICERkjFpCAgsCAAt8C1a+5ImnlDt
VNfZwvhhnfICwV2BRQDZl00flQwJTlSijK3cRO0OcgogL28a4ydWqVDO7Zmp/0bs
CRUckUdhmLd/vq4ctF+nsRObmtYQ8+By+QoH2NmWkiIyKatniZLBNnoWmQV4rqkz
X4MJxJlQkHznpxxYVJNvvBmjokw9OFeSkwfoAEWUzIi3WgY2TKAMI1kKj0XCsPSh
eFcnh7+HFHGACmBcpJpO7nWQzbIZNQzXFAdmI/jLTJ15SfDiJi/xfKLb8i6Vrf0q
6tk+90HRy44Mni6wCvg8fVJ+fY/UHGpwdWc33r5W/1lLJbo2QugsGkNBO0m18Mz6
IerbrP659NsqYgfXf1GzXQ5ySkkHL/YB0taljpMiF+MYTLbGu/DlxMG65nGyNADD
wbTOY0s6PeeKKvc69LzjugHlA9hgFhdGraNq0LIjX90POOkWbwFSmijELEgbbspv
UI7Oy+0z8iptfSN9P05V5blSYEx0KK7C96tKXcJgCmZlTnuOHJueoaUW18s3lBPk
WFX840ORfcxNHxVn62SQZJLP9fmOAHW5w44ZND5n32U/U7gqNxPZw9bbhsIWufjc
UsHZQns2Zoy9z+2D1f6zXRouU4DxkhJtLZDubYqyFO/yuYeG7P/1nmIzcmQXUX6J
G1BSZGcoFAuurvfJOOCKi6E90pmXPFxdOl0kMMXWFdnDiAa1ND4HpWKCo9SevZsx
0dxl6xFbBNm+ryjTm0pqzpHPo9EOwUdkol0LuYL/pLFE9t2LlGu20ILRp/gZsN0m
GNpTZkP3aNZ8y9tg/IO4DbwbdqYJFyEKmZUjxxdxyBNj4TW4Ih/HisVfsByRJn4e
yMGexDmMrxXTetCfMAISTPGk00hPFZRBLUXn0kOgefXln25xk2XqpgHFqKF8zSHk
9Ke2joNowVQjqvxJ+0VYgX0a+JjNS/x8p6g32HH6ajzHxQDzV9VFqHqdiYFB+ZkI
6ZTSLZesnOjxDmWYH2DQXJLwO5FBeioLJniUq3BzbVcilEZg9erp9KCuM8dZ6mkQ
olZXmAyKG5VSr5Fw3NFTCtFZ29gFAbkmAXHannZsGogAoAOTVegTgR8m9+jNNElb
SBKUxEny1EUtLlH4KaxDZqzHQtwjLldq+b7XZ5QsOG5aoq7UhbpkQboJZesYtqEv
+XaqccW8InSNzUhXcgo2Om16C7OuxlBhF46kxcccmWj0G2sKAL8t4tp825bvJMmy
fE3b+DH120zVQ6AfX4ZRpjDk0Xxc/5h3SX2CmbkO5kedoJrh+USO2uVYMT/TAaww
BlbYwr3R0ikSF7dZK07vnDsvXV1MDZ+6iQHnLkXRmQxMYvcMoyp5uKdSca3hb8c7
lrePfaI8PG5+RQ47JbYjjg91cRzA8GC/l70KU0naxalgvf9FSsl8PLCjmCNuoS57
FB4+JC2u37iGmsDu94eUODwwzrBxzM3I6HZDAlhqTrABLztww9E/+qc43F/L+mgv
ndic5HuFseCHRilbLq/SrQdzWH/t7FYuke9mwqJ5fMozW/TGIGJy6kYcMWx4NGcs
Sgq4H9waeqVdpUCYi2rnBobfxwPp+iFzJLFcYyLYjKB4lPAZdn49PIO0o2cXXMKA
l+B5qMwIumPe5tx10ETUes8wW6Ma2BuuRpjX9YK/mwICAyOCmrUQ9P3hCaKdvkuZ
oW0h9bdZutmK9/eByk8ecjc1aYLuFcAzuLc2UHNhvNpqDntEhcxFOLhgO6FBQVry
n7j7NSc3tTR/PoyMmDXHIubDi8ACm126ju5ioyVxep7/DUzfXAAXY+XI1VkTlM+D
xwG+OZQK1hl6OOFqypmjEhcALxUcD3jxJcmnA0OoYNV+j+CQj2xi+To+fY1gMTT8
6BCg6dT2VwAJoYVaOzBFnFvQ219OvR2EFWnJuLBg28XExos4/4MS9Z6t9thWcu0J
uVoDVjkGdeQcyuG3Ey1YwSnKxapj+ZtQn7m7rR2YTGndDqVLypXZn0SQyrcamlgD
C0/+iW7fbnUevaruDyyXaz+Mlxv2KCPhP62qeAInbwWMdxkVBL7cWLymUZb6i+A0
HkraXcLbadGGjmd7sgoZRVDQzxj0on1B4iIgWigZ3RS+4QLf8L5Dmr3tnvslyeG9
OvtsdJaTJ+jGtUE1BZ6nyOusflL1k+t/PGrkBtv1AFsLu2YWvxnP5Ob1HsD84YXv
XA7ieDsgXXDSwn63VAUhoaMr1hhEFl+2JFwqDx9v1ZMwnmNANJUPT3J0DYKVjBel
nRZeOePzpYQGXxJapZhYshsMNjQpHieqm/yyU61i+NXuap6Cyqifab7xRSc2TQza
txISAuRxg1pfTu+anSmF33l57w3YFttJx/KzjAImNvVHYvAg3AYd11s2gaI7H2bh

MHvkXs2wcBimKSqkanMmzZ2Ds8K1OYsECcvqY7l72xEvxG2yhETAwiuXXgRHy88L
WnftnPJ+x8aWISWCoY7iGIdWTX9nqgd2fvPx76ZMgKDYYhUFU6jhRl8HwQQozesK
2qgMXy+tsMmO6pIK+dtsJX5vtr4FHVq12dE/2VsHqzfOu/dfJSkTYP4qsLZw9RRX
NfFCAnV+ZSrCMzQNS2B/1d6Aa92PC42QYxGtQebmPnzSvBpSbGAaFoQDVF4wCaY6
iRUegB4a52zfjEGmCjOYlllOW89ep113frCrqdual5qPKQw3XvAtQg9taTGM1RW/
kqSlw2ThmmPdik4/JriXTJYBP80b80FQBYFxbrO3H+6cxD9F8YcYCnQQ6RngA6xL
ZPGH+galIYFnp9sOX9iguS+r37pBoPWfUfXIrzZpoYOKL2npgjf9/qdWTF1MzMDZ
PbavWCdWOk4ZUksf8QlkXEoa8Rao87yUhxvyofcKNoX7UE2PBanu0BnvsGJZQq/y
6u9nNm+aB8gSzGaC/FQ5mRXvUU+3SmLW9oWrOD38HEQe7wtVUchez+NQukZfDf8G
uOuE6vBtXtHixn3vZa21Yp+rWpR7i2BOsKGMeUzKLsg9UvZkvfwnP4+zuZvffR58
82nMbLStjTBOZnqNDkLhIZueXGJgGXxO95kkqowlWv8QYyp5XQy2HaGjaULGB0Yt
VyCF+7RErqXvNDycnIc3aumJ7yJ5wygor3/z+SgEqVOE4iEkjaSvsRKard6vVdCK
KQG3LL6fKwgGDTdP+08KKXLyhZMsi8TtGLjye722CQ5wl7dfQex1L/vnHN5avW8B
Qdq+TEQowytWJC5qTe2EtwmRiCcBc1PNebQFM3cT2rX45cl6iiFz3zM2EYvTQBYf
LKkLudvH/4vd8oFWS8oKY6mzPtZKWZ4XgM9gxCsN59HZ/+CsrNFoEx1kTPVRpfD0
rgr/sfNpVKSS7E4hagMUbElSU9GlcyxX6DYoqy0sx23ErcOi+/Dl9MLNAny9+xO+
IplyP9dVbeUCSLBbzQIH57FN64h3iHXx6Q/JNnkmLNKwMXNIi+ekE6e/ikZLSBhg
cMrTtZO+G6P/7bQKOKYxIkdaoFRL6qkqKqzTbHXM9F0XlxcjBP4EhfSzS4zTk2PP
oQs9iebTozmbk2x6xjkW8/D27fmWFbWdjCLjCN2Z4xWkmkkXonwrdesjw4ORGxwk
AsS1VHW5akXeXr0xHx6wjS9y6sGftYWI5fghlJTxvvaSjBY+13BvLZboKLAw0/0j
5JiyQAB/t22zUaHvi/YEwL1aHtpgY/PUEatbHmU09kt7PY+3jiURxPHjae4CelqL
D3dFJ/I6DGPuLhLgxCUkTDXGDbReugmNA9rM0z/aS/yQuwRh+OiNLsJd+iifaX5p
VlDyRq6gOkRej31jO8fPKEHNDLgTToHbDzDhUTBKGcjePhMH0//JrOkH3izTpSWR
6IEfM6Jo8HvcZGPqO0Ra5HSOBPcQ/rEr5GiEtbEUqkJ3PonMEYelK2buI5Lw5sUt
W8/wt9YLuXap2OL4jnVAJrfLf5n3fOPm4F9mCPCzBCNzBv2U+cuASVh9HA4E8+dG
KqR4FEqqv7Mo5DONHdfYk8Sdw5IYx+XGahqk/qvrqR+QXPBbO6oeXLmbIl7TZKus
nqAg6PoENnxf86R3jPwrZOc11jasz0L6zQ6yVQTxlx/Jj3CbzhkYEHh6sU5EPkWu
H2B8lFifdxkn8CIs+cdWcSyVxJlYRU8qwqdUudsXbCfN6bW41/V43yrz4BozVuB8
N3vOTqoDZeLRRAebCaFGRmUGWW03/WvOqqdzMc3UFxBiMDol0Gyr/3tKff2kf/dY
KaHssQYIIC2hh+f5l+Ekp3XjaX6GFtAjM/scJlC0ftupzk9tJG3scEUTbK8MwUxT
pJ59+cj3CtdJHxMVIc904PlPqsocHzK5CpqQD5Clvqj1jFc+eZ9BICZ+s880Ie9B
bFpW1S8AN9UyHl6nCbllDOazUIhdRh5goDv1FRv47Wtr+zZCseGzIJ7oCAE38KDZ
u6QdAe2a16qibKGeOKaZEVm1DDIae6YCIUUJZw/PDmO5Bf8NkRSz2atY8UzyxSxi
K9HYKPDly0ILMF+aQzqvy36IttNYQ22nqN1XVCmYF0HFPnS6RFyDXU+Wa9RATL1p
u/kW8TwMOBveXstkJUm8TBhX5TDEFtg+Y+tyDNb4n4xwpuishLd/pMck6LNK3fO3
cOaqQssUWkpjJSzSeedcA4oonnq833DXP6SPF1ksXlArsDVWB4atlFRqbaUKKrpv
Hinhb+MUjANUW+TcAEznbTyHFvEuNCIX7WU7SlOglcrEjJzGnJZC24+l0KzxF3ed
7PndgDslLmJc4ExhALrKGFw57Muvy1UNd4f6W7AEraj/54FIoZzDRH+R/owcjuiK
Pza8vs8W8792ds1ewGcLs+B1g+l79IbO0+zR4eio1f+6kSsRf+EucrH4RF+lU+ba
w56nBq1EMoBJFuzPrLdAOD9vRVwi8cmKYYf/VgriDvZxqsDsdjC81fUEesG8/iVS
axpAOFhCp8oUQZVg8yRsR7x/m0EjFWZPu9JZwAge76HhwpSu+yg55m5ndeXEy55p
ss6t9jHwuFu7F8q75xTTVE+jBZomyxfYQV0qFvvelF86Hrc+FTobS2AzPRzhwj+p
Wfh8ORVoQaHb/BuAREB/xXCLhzDsirqoUKDcVATLnBUvZIawptgC1OjIaAX3Xgn0
VQXDSeABdtUDVBgI67OgFw==

C.3.9.1. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIISMQYJKoZIhvcNAQcCoIISIjCCEh4CAQExDTALBglghkgBZQMEAgEwgghaBgkq
hkiG9w0BBwGggghLBIIIR01JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUNCk1lc3NhZ2UtSUQ6IDxz
bWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmVAZXhhbXBsZT4NCkZy
b206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNt
aW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjA5OjAyIC0w
NTAwDQpVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpIUC1PdXRl
cjogU3ViamVjdDogWy4uLl0NCkhQLU91dGVyOg0KIE1lc3NhZ2UtSUQ6IDxzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmVAZXhhbXBsZT4NCkhQLU91
dGVyOiBGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVy
OiBUbzogQm9iIDxib2JAc21pbWUuZXhhbXBsZT4NCkhQLU91dGVyOiBEYXRlOiBT
YXQsIDIwIEZlYiAyMDIxIDEyOjA5OjAyIC0wNTAwDQpIUC1PdXRlcjogVXNlci1B
Z2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KQ29udGVudC1UeXBlOiBtdWx0
aXBhcnQvbWl4ZWQ7IGJvdW5kYXJ5PSJlMDMiOyBocD0iY2lwaGVyIg0KDQotLWUw
Mw0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2Fs
dGVybmF0aXZlOyBib3VuZGFyeT0iNzk5Ig0KDQotLTc5OQ0KQ29udGVudC1UeXBl
OiB0ZXh0L3BsYWluOyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc2lvbjog
MS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRoaXMgaXMg
dGhlDQpzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUNCm1lc3Nh
Z2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBTL01JTUUgbWVz
c2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJvdW5kIHNpZ25lZERh
dGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQvYWx0ZXJuYXRpdmUgbWVz
c2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFjaG1lbnQuIEl0IHVz
ZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIHRoZSBkcmFmdA0K
d2l0aCB0aGUgaGNwX2Jhc2VsaW5lIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9s
aWN5Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLTc5OQ0K
Q29udGVudC1UeXBlOiB0ZXh0L2h0bWw7IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlN
RS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQN
Cg0KPGh0bWw+PGhlYWQ+PHRpdGxlPjwvdGl0bGU+PC9oZWFkPjxib2R5Pg0KPHA+
VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNl
bGluZTwvYj4NCm1lc3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNpZ25lZC1hbmQt
ZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVk
RGF0YSBhcm91bmQgc2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRp
cGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3Bu
Zw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2No
ZW1lIGZyb20gdGhlIGRyYWZ0DQp3aXRoIHRoZSBoY3BfYmFzZWxpbmUgSGVhZGVy
IENvbmZpZGVudGlhbGl0eSBQb2xpY3kuPC9wPg0KPHA+PHR0Pi0tIDxici8+QWxp
Y2U8YnIvPmFsaWNlQHNtaW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZHk+PC9odG1s
Pg0KLS03OTktLQ0KDQotLWUwMw0KQ29udGVudC1UeXBlOiBpbWFnZS9wbmcNCkNv
```

bnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3Np
dGlvbjogaW5saW5lDQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFV
Q0FZQUFBQ05pUjBOQUFBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3MzluTzNUcFJ3
MjBkcXBiZkFSUUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3
a1oNCnNncnpmY3FWTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmljaWhB
ZjVZSnJ3N3ZqdjBaV1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJV
NUVya0pnZ2c9PQ0KDQotLWUwMy0tDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5
l0rOQlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREw
DwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0
aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2
NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNV
BAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKC
AQEAmpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2
vWYB8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuT
SxX5R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjM
UJanZ/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1
V9V9yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvw
DhJLAgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYD
VR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4
YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1Ud
DgQWBBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJ
KGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbM
l1gD5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkB
D+GDEu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTO
kRg8uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadR
lE5K9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZ
kPpivNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCC
A88wggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAw
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIw
MDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNV
BAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZI
hvcNAQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XT
vyi6WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4
WHWZWleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6W
z+CRQ/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+
SAo3nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4S
WcC0nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCB
rDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREE
FzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4G
A1UdDwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYD
VR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEB
AHOJojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChw
KfnNvOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNa
ACSioQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMv
cdH4z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXT
us2ZPRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk
22OH4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYx

```
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCG
SAFlAwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkF
MQ8XDTIxMDIyMDE3MDkwMlowLwYJKoZIhvcNAQkEMSIEIFPOmRBiI1gpSbRbrEhT
xW8uQ+V/G/cmOB6495mnsKVeMA0GCSqGSIb3DQEBAQUABIIBADgh7UBYrX+esUzQ
I9zNqk4LnbgdQoUdeJtdY2Jvyl6dlV8cfIFNgng8IluuuJI48a5yJwYG3060AkvF
JC/hq7sSBCLzNVb9UioTixGi+4nGB2iRb7TKsfamuyh5Zdjg4OrN8N1H4rwUQ1K4
Sis2TCi5/TSc+UYG7rH+YyIRSeVxNCII3rEA8E+dDRg6R5bqOTHxInQbBvG9q19e
pelntJeSxvRSOSYwcoNGXenZ6S7eqfB3iln65d0gURSV7hPSfZwh1QSZa47egE7V
9Dgce5pbZYQgeB27mLBCpsgRgYKbQ/+NBPBexT6Kxixd4sND++AZ6kUie+AvUpXo
+kGun/Q=
```

C.3.9.2. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline
Message-ID: <smime-signed-enc-complex-hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:09:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-complex-hp-baseline@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:09:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="e03"; hp="cipher"

--e03
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="799"

--799
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-baseline
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
```

```
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.

--
Alice
alice@smime.example
--799
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-baseline</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--799--

--e03
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--e03--
```

C.3.10. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
   └─┬ application/pkcs7-mime [smime.p7m] 10640 bytes
     (decrypts to)
     └─┬ application/pkcs7-mime [smime.p7m] 6856 bytes
       (unwraps to)
       └─┬ multipart/mixed 2367 bytes
         ├─┬ multipart/alternative 1415 bytes
         │ ├── text/plain 476 bytes
         │ └── text/html 636 bytes
         └── image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:10:02 -0500
User-Agent: Sample MUA Version 1.0

MIIerAYJKoZIhvcNAQcDoIIenTCCHpkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACLgXflY746FTqdLnYLWQE/uY53acAbSNoGw
OY86dFVtfd4kmtKoF6bqyRom13sRj228BwPm4P/SiMKTt40967XTuuuYFzWYOIl5
QV1W+59RRrZnNMD71rG6Cy/t2jcn55iGjpFhVUgD9LMD4YgO2LJfvOoQLFDDvI0w
Q09gy+4+ydc65IKk4qZcn2WfTK1TyVnHAAjc9vLItl0NPZCrPsfrm7JiKLtyBT/1
CsaVp7atHrCNZmUSb0wrcfdXkRYmMYu8Tws/+Ck/5LBKc6FRRv478oqZLpP88Bkh
37OF2AqrfJvdLQZFSfqxeVZbHBO6sx7y9IDQUAN5qCy72w6ULxIwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAOuP/nJwnkTi9bK5viGgKWQ5l
Me5kgUCfpiPFrKfzn98Wo/WeRhNuvvVbK5B+4TT7W2TC9FD+zQOdKtoU9i2EbBlw
V/nSbVJoUjnFyPYRcAKgw828RfQM1PGZ8pRUOBMlZuk+TkCPdUAIJGsI38trL7c5
pItqwKJEEoZqr2qe3/rt2eWStYDbZH6ZCp5SktozKYK2jlLxYZ15K1qQ9tnnf2pV
DIUf8UTHl2NFq9SWC/Vnc1ifoAmzgv/Q3CY5prl3Ucz69LpGI5vAQ25+iZoRyzzT
jsP7xbIHnYS+CHKS8sOIDL2vf3/b/cSOp756tuVd4kGBXYQdA5NV0ghvPXX9BDCC
G34GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEF9OiG3jOvWyOYsEwUhg86mAghtQ
J9wQwdRPPRIjqaFR9ciP9ECMC1tXw3uNHjsjl9tgTgzT0WxgwuKrHDGzYywRPtFD
pEYPXbYKmjH6w8fr2a46v8nQTgErdhO0gPQsc/FDPI4s1uR+aCd1H3pVDB2HJ4lW
uJhtyalcbFT9As8mNk9izHLd/K4POXKc4W7dhv66BbeBMVBseFDbGoqPalblRHsI
c7sjqLUsmlEWIkU6e18/KHFuxW/m7p+HPItcN+MzhsIrOAzpAb8tvy8a4z7FCrRt
BlNLjzGSk1qIswiUpkhWgv95ZjiJ2jX9+BuOGXWDn8c4NNlyQQSSOg7G9H4gS9m1
yx3D1UMHko+nqGuFdECX4yE96LnKFK1hhWKuIRC2L9bVaMB3lhf6D/K+k7A51DZx
mrOnb6q1rkAS6xr/IlUCPvogo8x+bEK8fufZM806AaL8cRPxGHxlhsV1KVC0TGka
```

sGm3koZZrSX4Q0MFYQsl6HHAFlnCN6agVFema6sbqC22oNtjsTd79Ee0S6VyMvh5
04jJJqbdrCNmh7LPThPY7sesrJwMy9VgWh3qHM8q04JLdQOssxss2WI4QFahFO7L
6Ldu4yKChpXME6dvuybeAjmKdiCBUt79BXhE4frn3LKm8UWQXUV0nUrGRdoFszf0
5+l+SEre/4oLtBv/IIKF9+rwZzScLvhZNhaZq/6rK2s1C/UlAPBKP9eP1L3TAp3m
na9wJ7kmaTwo9xKFlYP9yUv4sMe8pdMIZqGGh22ijtw0z8qKhi9AaoqXH41y6wmA
r9eZ/HIhXtTBfCpRxHqU47wgd4Cn02kk8is43xI0QjClAfNpWEGaGvpZjyy3v4jE
REQ0xJiu1nmUkyUorx/9N1uYo1XeErF5oZX2J00WR/YUQZhjvLK1uH8iEdXp59Q/
BLo7yKDkt/TwY/3IdjDsx2OSgVLekKrOcQC0iAchM0Zg37DGIQHZRknff2aAGhjK
oWXXlfb4M2ym+0BsBkgJHrH63Fk7kxgN9VwUyY5HxyWCQDKauMwUKw93I2tNm30i
7PfnkDlS0QmB3cw4XvQGgQWfmBEp8P9q04QVzeiZvOy4IoFqh0jiOLlkaup+WuOh
zk52lU/im2A9MzlW87UNNsFpTz3pP4k0ZA1lkVSH/HGhCIvHqp4xwIiIECyt6U56
S72X4sUedoBFrZgZYEFki8XJgaFQHjFlVSTqbBifQbWELa8l6cJrGy7W+Fb1d2oI
6hLQQP5r//j0cPfsTayrV8o7QxlcbW2bQsPkCttjB9tM9MDwR1ID4iywG80eF/fD
F1H0+6pmvcegREdmSYJr4QgnqY6thnyBBiFVdSGMUP+3Q8jZqHxiJUjYY2BYnNL1
kjIe+0M4Eey/U4/kUxrlNjzxvXd+7KWaVjJaLwPpVqbfBq8cBx03Q1yZPGRx2xVN
4Z8EbSAO1oPsdJSrjfgM6oYwz5k/92795rNB8nXAQTqcEGBKbajJbqEb2IjLXCzR
bvZBuwESmwuzqqiCpf7WYyJVOEfQXEdPzXtBe3TAy34J0RLaXKfCdKZ5oF4coh6l
WFlm1QqJfrsAuwb4L5QeOH0XQLCGnORRGtfL88TFLxd8quUnxHgg0lkO7UuT8VAS
6n3N882CFN22C9BNkR5+3bdpdQZOAxuJY/5jYPVSfX9p2y6gmJ+KLuX1vYyB6CjQ
sA+bQRqWeqHw5kN+gTXT0UHMOAdqw8D8MPHhU77MwRzaFb6DK4Y0LPBZoVUgXxg0
8Mv52yq5cra82c89712+fHaY43onEGJq2VmKnLkiCbQExVc4c6h+6AnQleZQ0skg
5Q8vzFONHIiHeGbuABnCHmmABs8RyWm1Txlr7MUJcm7gR850sZOe1KqRKWlGEM4n
5DH2JWl0cYWOQQpnwTWTl8y7hq2rzcLQEpzfthHQ9Ezu3GDBieiDdmcKDxtq2FrW
Uo4F+VbqnJLdD/h+QoZGNcCqWeZBeSm4qRKFhBZCTXE7pE6DOaJuwlShov+Lej85
xc+FMb81gonG7c3NQajMCOCyjewQULR/qMUURaZbQkQv+GDjkzAdRjZK1cc+JUaS
m6cj1xsZIwyxELtXNBfvtqPkjrjvzNQoatQhAA305TS9QlQAKJ1+LenQb+otDmGP
hQUaw5Db/w6lheBxqhW/rQC1Wk1YHcTl7vQr4kUK06TjRQ9RIV6ds2V5WDrhEFbn
O/KGHN7k+WNanxMmhyN3Vpnlz6J9OEaFTm548ElQUnEHeQ2z9pJc9TGAAzrSakn/
WgWgonMKkXuQVm8jb/CkpYWrXSH6TvofjMn2wL6SeB5ax6cmW/O318aGJ9otfcXe
0kyNGKbiiT+raZlt7Nno7B9JHLJa5estp3dxb3v1J1lN7diERT++8Gqo11cm15uV
cgdBmP0h1hFRSilr4Z+1DHJ3GRjHoDS5yMI57NpmKCO4AsM4ORXOMSQdm+RzrUfA
8j9LW3/5MsLOReNNioIz3/Zz25xpEwLs8VlCP4g8WKncrKlujFc2BECaA8KTCDai
elIDjix6aC9k2t7gwJKaWDmlUjGcrJNnxs462v4INJak8746dSi8rWYpnFYpcl/c
WPEHXmdVDIME6Sdomiju0tKhP+QrGmORQuRCHfyws8cLLDAyyJxmdQxi4Zbka+de
uBlJkntYvg8mFm5fKyZ2iUAPzFpGNVxA/eDYKPE4opLKdOrNtHakF2fhyq6m2LAJ
pGd4PJ6U5huBF1gazcSMDsOcP4vF6mBgUEBlDTUkFCisSgLHmDouZ2CLdsXcJ9ZU
WbjJbXl/ZTX9VWcd83AJW3HQDOvFHkNVL8GejHQLdLC3iln5D1I73CDT9AYINPtH
BsChRv2Au0eYpwuyEolBHX5QzFEUVh4wG5qDgzBBzx28sl2CGKvFsaAxWan/NdAu
g3mcMBeBtinMPxP2ifqaaxsRoRVjjCbhT7ouZMsPtgJ2oFJ9XGVBJ+c1l3bxDnmu
mEbiKmlz2g+TfjsqL7GIpctQKz6Nu9hr5sY1/Zvz4VrQxUOdp/WL+M4vGJRHCstX
n+kLYSnepevLEPPOj7sU9Mokt5jVNx1iEwJ3U4P9g+LI0oKrUSZczoZ+V/+MOvi3
oBS18iTfFR7840zWLD5DWK1lqIrnEzLSVV/pZ6ZmVxFK3zaN/AM4Y82IvzM8vci1
/eNI1Tndd1JAZU5zLak09u5eacl8GYkk840oqxHOX6wsMh1qftgg0BABoU27cJ3D
7xuXm7EWcUXrQMVpNGO/eG9VJ/it8NUrp1k8QP0KPTQs43jJAoHREYb6deyEwgTt
3L+yqE3xoUB0SQCsczkcXGg7ACv/sb0clhUon4PngjT8e+gc6SM1YckQT5KN7dTe
W14Slku9qpSMVJI5+XyvtK4OX2LLuKjUCQDz2tThVu+AhdfgUqyMiSJr1/fCDDy/
w3lQQioXXXU0dwJhgzmHG+016o4uOHxN4iYijfkQW+Zil4AGMF6xNYbw8iKhm08r
ksvdV0g2gCSwiISXH7bfynWXD1QrDSbr4DPW0U7/EfvH/wGX52wh7EprDPTMa9Xh

```
aekbxK3QiE2R/LPrcm7U4li+FmEw/d6cSK9Ge2HYufj6zlPpKX1tyLD+Ucosj+yD
dufxtdKIoXA3iYISLc95pWcAu9V+VO4lRv+OBH3vY4KsLLi35aF7F8xaj2HjFYiO
Q6UjTSxWSOmEFmRQm1KFj9brBWFeZUx+C/kFDdtRg9ZPhUKxjSQTgMuJoZyFq6B+
vIrmQTo07RTaQgZZDD6bY2cmuQAflEJ/4oszywS+yeiyl2KvNUVuQTZ6ofCZcTZh
7iOkjkH8hqM9xYFvHU/o8ymXKclJDDgDHfgN46NNNh0Feq56/ippiLLlIzCr5wtG
Yc48C4WhECxWIrx4TVktUHGgKJGLQYI2qii2kuvqKCavkf2z7NJW8781xZLzgOvD
6+19H0VhVreHwFpjg3axrJOiA4D12Jq7RgdBqTiB+rTqxTTSsvMldOad18IgFUyP
dk9kPP5heCtT/kNoqeMvTCYtv6SGgoT7oX76gUOzHvlbWq5nm8p7mIl+CumgeBoH
xhFUaLIpGVendGWAfqmnxDIHjZ46HvzLg2ANVxfNnxvHXVNHWOyOh7GqknmAWob3
GrFF9Td9/UoFD3+Y1r4FRUpHXUOqaJq6tIY25TttzYWcvJozJF/GK/77XVIqQ/lt
gLajNfWSKNOWv+1l4VkS/ioylcXGKMtPWYsEhyCdqtSnqf6cvcoEIyyjBlLJCI9S
og1FOm9Kul4HiAtXwPhSLEoipfPIVITOTcOpDp0ZtDK3FamrlIphyBe8tva1S0hH
9MOLtdwoRVbMUvSGy2gOgWVvpegVHtGNJ0nmdSpvMEEktjWUawtVQnkBWCvEaJaQ
bx6bH2fWfOvHvt0aLDk+51evRDovLAQof6s54hvdW8wT2RS4B9J8VFmMM2dvK+ku
t/6AhCpr7GCd+9LodG31XETykfwKjc3s+pKQ/eQtlC4X1ownt9IS7t9R1670pR/J
7qe8Yus3cqXS16PmWJRWMr6+qtNKOTwNRKVrg9CgWFSAytcTw1OmDrRLITDvQz+9
JTgvTaQfA6O+QqVyygi/JvU7reNiFJZ4GSfw/fvpfWS2bQuH7HWms04dG74n6ZBF
i3407k8HsNd6PGHDQeiZmKlwnmr79b9pmZfwO72QBmF1zxZ21+K2ts9S4Zjdmp6l
VEtvWFrmjWz/Z3h/yxQkqol+VZ3U6LbLh6MJ3QdVgTXCq0jicb2hs83an949J9SS
cFfibs77cXmRpGGi6QLhRySwfCNtrbFXgvmJXe3am6tlPAvuw+3hg7JzqDi3zanx
ymQ81qgp7I2/xHY17faGyKvOnBvwUTcJ1OYsbnCyLb3zhLPgW3WeWz/7MI6/V0aX
3L6acMB4yyMi0lGyQdCxyccMrqxjw5lq1kMMbJNISDTkCIqU+ROQVtz4f5TZk4Af
U+ATVySGZ23DAWsI7l8vX43wRtMn0Q5zSkDK/ulTGfh89rSbk+4bq9mbCzWNLjG6
fpXTRx0cW8pPrC9JGKDxjss1dAYK25GX512g63g+gWRcEzUEPTjpY48YjEcfonus
TIWEvgrdorecsRmwyBOvPYkEy52JnKjbppPTM2Weow3e46VVsrmgcB9Ev21WbXH7
RqK4EtgDpDKNJtmpw/l4wl+Tyr2IuOHXWOmfWkSz4JLZD6fOJS/v6DqYU8spfRwV
qN1lgvvcmwt6BfxKoym1JMM0kbl5iFxSkFSZLegDYRZmBkp1JRFpWM0qti/R0ngM
f/QfhOps5JLnzigPWk5XdIRE2N/53uDJ5FhGsUy7FnZYgmJiSXcOasNngmdQ9OZo
FQ/uijNReo/ozFhlgEIBU84o4qaUDYdyDAqq349npZt5XxbHpcHY4FwZhiQBmOA+
7rInBdHfrFiR1ZkEZtnGrlGV2KXZk8aPQsbQMzYELU841jSpumlw/NlTdgbzuGus
T8QH8kRbZLwItMQfofo5+VPJoPvldu8m7ezixf7H53fhPiNOjAnklMAM+mCPGBNk
W1G7GVAZA8eIqRoPVdVh6GCBauMrrLLOvjGX/wF+Wb1tR5CobfWFPQy58k31f9S8
AnyXUbuxEqHz1UZV/gS84sE0NxrB7bGj5+pFbOAs74G2qprKVuiCQ/OANa7r4I1l
r+NehvRu1f4piCbk5gutF12kig4pEpvzdfQSI3Zn8Y/nMj7nuzQjkkooh1wdiw1X
8DjTccNQbEuNUaBc4zFogJHIQve8GuXAZvhSlda9YWZtL6JfBw+sjU68I6/Ubc0g
gslspiJ3+EDxXV8UyT8+Nuw/000mGidIwenHENutknl25rgLiTSvdBASsP+Qo+8x
rczJqeqah8MM/IL4WRNI5GMDyGFZDWbVBxur6JuVS/zqYT4Fwk5B5aelCueLzoW2
7FL+9IKLVds9QPGGxz4MoOb1M6uknKllCtUMx4vI1VO8J0F/vtizCu8LqMm9YI8n
++OXIePV/isP/faYsFaLAc+Sv0aBniCWKxkIO6X8S6MpcVswKzFTpvQ7Neuinbij
eOSTpnciebKkKAw5nBtb0s6gPuvJg0ABVD08rYei8Rxp84WvUU+P3nzIv5StGDdi
M3SJ+vSVTZXY3CQGEC76Oi6YFsQFTD8ONz1vdbhgeF9kBQZUAcPJhfhfdkJhnjni
GWRW9ToyO7Iufd2Rqe8qZpl/5e8YeCjraE+8FYgRAmNCIPnl9dvBT0kRS1d1aV29
iZQWcvt5jCULyeCoQ+Qiu772ZlgToKMS6dP8Rzu0CKkLoRNQzsbTctEL+8wIM+Ym
u5y/nDH7Igvf1INUPuU84CghaRaocFfmTF7iPFbOsq2WBq5hvtGXRqh+k9vpq7yj
wIzbo3LbPalddV21gFhpd7ASg8u8bAgEkarf+C9cejIDtk+/WzilYuX/yzv88aiX
KwdXrwk0GLBHaRsNWPipOUxhleyfAOgzSSm57vGB48qsR11p/ZeWNSLabF9cLKJI
eTi7BEg4LjmLYKuLNsTj5ahbjrerLWiMgX+fUkss3mb/tYc5/FS+GL3t5gpt/z+v
AwauFCK5hrlmKqtzFRr0PNycXRhnBz8JKNJRCnhH/7pze40Zax3CpnllK/TmSPjE
```

```
s3X4vRFc2jn3KDbwd6me3AAkHikYmnLlE7I4WHyc14KtIvw6ZUcHvYNzLOrUJUdw
Gn9/wclMLJib02ZIm9JYgXIVYeLTd2zqEdTU8kA0ZSU4fib9yFSPzsTqfK1FWQqb
KxG1EkKMeSOOZXQieebr+V5FxISLdC3iShBCxouDlSVKYETC7O/Cmq44LDDtDC/w
ymdXt/kRTv/Bj4ymTCKzMpKZCKhtWCaEuQucNcVeVO1vj+iHxfZuIXxJE/Xc4+VO
gO/OnaEc+0N73/fNkV/QFrOnOC/u1jeRPSWUWkEK35UYCIx1/wuJXnXDDZMVYy40
GJOIKqOCjOjATNR2m8ParmrywvF+IEQvINz2G5VAyDeolRqaL5azDA7vuS1O5oeu
E0bZ6Ug9KUgmR12ZEu+28oEjrFLBNDP0s2BQQJxOA1kRYi5ba0rcqOoUWDnbXVW2
MywIzRNt5RgTxQEXh7PaauYMC0qSoxb/9lHzp63tnowQ6wSf1+9s6tkmqOcqHuwC
p6Sv+faNqT6VaS38LeQK61hgt9nBOOr2Ozcc2qYoc5QxJH0/dzpPNRutqaf7Lm30
GLvJiAjn16D5+Wm1M/gqTCmG8FRuf+KaOpVFeoXMNhFVjNPtJP68xl5WDOiemszC
qNTjE+Xy/ZOkeHNdPuhPA2BcGOlcnaowchEPibXFBHPlWxqo75f4bLZuG7mDkvdP
63Z3NO8XTMqWiWyuc6EpwIh1XZY8KH7zJApluCdovDjF3CmuwNFP05vGdu2zkx2Z
VMOe34JUy8/YlVfXm4L4gKJbjjByWuH0xCavNOHRknSPZRhrgNWZQ423TYIHjRxU
b5Bzg/bEXZntfWJs/j6mCTHrUepBA0s675njsNfdoiJW7Swa9Rm/XtZnKetNSBju
QcDglGqXmLhe4ELu6wLs7n2gIqHAL0XeHmObBbCGD1ah3SnTpYNkkKKRcbg3D7uW
c5ORsFu5EXiLza2xwlEOXh109Br4YW2aoM7W58Lb1AQ0uDx3wMISdWCcSuUQ75Tj
8XFAHLH4iITwsWvMcNP6+ExA2otAcFhuMCsMHLUm4m8wTh7ogdrkZhxFrd9M9/Qu
MbIbqS36eFtjZshXBU6iydu0jCWHz4r2aXl68XwunN6HSHhEmsU6+WKHbEKNkE9L
NWJsPljtDuM94Axjrf5MLugZge9Y7COkLvmVUn9p0Yl9CXEAGpGFHbSPYQCSkXfO
YZxU45ZwSKIP8P8QaomSD3y2xVFqUph0xm/CLPDwkSZm6Wl3ZYMKNuhROKxeP4tc
DUNFkRkyvZx0OM0atctx0McFN9JrnebOMh+20NEYlefiHI67lRUPOVguMOK/XIT4
weO+LLifJB9bFLDXd6aib3JY3jVf/1nzGKu7+Qr6XnL+Rh1qsBtt1aBWhPjwf960
1b+PbEBlZN+J8EErhbaNJBQFigS9fBE/zk/I90/fUqQxhX1AofJwH+jXH4XAfWTr
04a6dVJThq5yN8kWrdUP5TDY0dUf8gvML2s9BtVmRARquPBQGJLZfhh+6xJXdi5c
1qaCYxN6IwYc1v7ctxQtahSVdu89QXG/SxwmkLuvIbLfhJMnEOSz+xOiVa2tLJFz
2GyJb6NklwwklYvG2QALEaNl7jLP2YcQUdg8LbxKgmPOFhRRPZrwvzXcrgrHIQ1k
No4ZCWBkHs0HZEBzAeGKP0ZdRTleyOlG+RgkHEPgau5dLnlnaKlKUInzbbspvp/Z
Do6Pp1R+ezTkMoDFmiOUgGrHnhiWbrsciYeqCaCaCTHvCq4Yc3dry+nVFlxMqq95
X9LucfCcSAAvD0QA4ecf6LpdTIpNv4LcdlFqR8ea6uw3tQ1gqxUPVIoTsavfV+Nn
xCGcDCoOQqKmYzOWjEkpLqJUJU4B8VkdgjIz1/+kD0DZKWuo7WGiphhqv5M+VJRr
5hlDxDMRhyaNKAS6Sa8yN3tWHYoXmHPgU1XL3MT0QT2GR51QbWq16+lsCkeaFL5b
0jvQqWn6poDbQ0qNzCk+qqiJjD8UzOFkpN66amptse6KXgc71xp5fBE7m6VUHv+e
6yhJ+9NcCA64prKqBxosVOyb5SBWZGofFlpgmbStt+1hvcPA8TS1Y3LlVd8GCNP3
BysnpeELKcGGHjdUovPTWk7v/ewl/dJ1dVgEiRsnSU7G4bMhR1OY3lRER902wjLm
6zdOuNbd7LrTimhtu6lWIFtSgrJpPNKpDTgjGn5X8R8MuAFJFibkS4uMbL1Fty32
bESHzoLqSLRgWgLpZQjmrTyvOgvYyauKjZYslBnVqjd+oBq9JUgxh7xKsG+z2KQo
V4QC4M3z0ppx76fYMETfOMjp9Pm8KyuhEHXIbAXoVE1rer2m1ptaJGZF7wUJAqEL
uJiKSztN5S5sFe+a87BsIlDWkCLZRuDb04aO+ndSd343yK9CMfYKbknZXtC/cAVd
2cwFAg+qix+351gdmGd5L8tQC9V4FO3uy0JQU90g0Twq0nE45fvLj0J4rnivuQkD
NMypJdswmGcd8TWFdb8kQMtZPNWuupbV5w1lF3ibGEhGqtO+4/gu1ua3jg+cHI3o
oKBzUuvYGLXrbrYnPE1b3HQXvxDVd8m/+KLDNiwyQ7UT676iJn7ARCYZCwP/D3g6
zMc3NXJkUZ8KFOHqokaaJ3jleLoMi6JB23bhiv/RRJuYk+TCwX7uBKF8fnt+E802
YOhbKcnThdDUreGM2QrsjZeHZQ6qgIkLUedro8EsPI8=
```

C.3.10.1. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIITdQYJKoZIhvcNAQcCoIITZjCCE2ICAQExDTALBglghkgBZQMEAgEwggmeBgkq
hkiG9w0BBwGgggmPBIIJi01JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGVnYWN5DQpNZXNzYWdl
LUlEOg0KIDxzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGVn
YWN5QGV4YW1wbGU+DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4N
ClRvOiBCb2IgPGJvYkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIg
MjAyMSAxMjoxMDowMiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJz
aW9uIDEuMA0KSFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVz
c2FnZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5l
LWxlZ2FjeUBleGFtcGxlPg0KSFAtT3V0ZXI6IEZyb206IEFsaWNlIDxhbGljZUBz
bWltZS5leGFtcGxlPg0KSFAtT3V0ZXI6IFRvOiBCb2IgPGJvYkBzbWltZS5leGFt
cGxlPg0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTA6MDIg
LTA1MDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24g
MS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjMw
OCI7IGhwPSJjaXBoZXIiDQoNCi0tMzA4DQpNSU1FLVZlcnNpb246IDEuMA0KQ29u
dGVudC1UeXBlOiBtdWx0aXBhcnQvYWx0ZXJuYXRpdmU7IGJvdW5kYXJ5PSJmZmYi
DQoNCi0tZmZmDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlci1F
bmNvZGluZzogN2JpdA0KQ29udGVudC1UeXBlOiB0ZXh0L3BsYWluOyBjaGFyc2V0
PSJ1cy1hc2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNClN1YmplY3Q6
IHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNlbGluZS1sZWdhY3kNCg0K
VGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNlbGlu
ZS1sZWdhY3kNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5
cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTNTIzNCmVudmVsb3BlZERhdGEg
YXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQv
YWx0ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0
dGFjaG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBm
cm9tIHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX2Jhc2VsaW5lIEhlYWRlciBDb25m
aWRlbnRpYWxpdHkgUG9saWN5IHdpdGggYQ0KIkxlZ2FjeSBEaXNwbGF5IiBwYXJ0
Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQotLWZmZg0KTUlN
RS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQN
CkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1cy1hc2NpaSI7DQog
aHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNCjxodG1sPjxoZWFkPjx0aXRsZT48L3Rp
dGxlPjwvaGVhZD48Ym9keT4NCjxkaXYgY2xhc3M9ImhlYWRlci1wcm90ZWN0aW9u
LWxlZ2FjeS1kaXNwbGF5Ij4NCjxwcmU+DQpTdWJqZWN0OiBzbWltZS1zaWduZWQt
ZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGVnYWN5DQo8L3ByZT4NCjwvZGl2Pjxw
PlRoaXMgaXMgdGhlDQo8Yj5zbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFz
ZWxpbmUtbGVnYWN5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGlzIGEgc2ln
bmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQpl
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMg
```

YQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVj
dGlvbiBzY2hlbWUgZnJvbSB0aGUgZHJhZnQNCndpdGggdGhlIGhjcF9iYXNlbGlu
ZSBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeSB3aXRoIGENCiJMZWdhY3kg
RGlzcGxheSIgcGFydC48L3A+DQo8cD48dHQ+LS0gPGJyPkFsaWNlPGJyPmFsaWNl
QHNtaW1lLmV4YW1wbGU8L3R0PjwvcD48L2JvZHk+PC9odG1sPg0K
DQotLTMwOA0KQ29udGVudC1UeXBlOiBpbWFnZS9wbmcNCkNvbnRlbnQtVHJhbnNm
ZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdGlvbjogaW5saW5l
DQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZQUFBQ05pUjBO
QUFBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3MzluTzNUcFJ3MjBkcXBiZkFSUUVq
T3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3a1oNCnNncnpmY3FW
TXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmljaWhBZjVZSnJ3N3ZqdjBa
V1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVya0pnZ2c9PQ0K
DQotLTMwOC0tDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rOQlSHoe49NAaK
tDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1Q
UyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1
dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsG
A1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExv
dmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAmpUp+ovBouOP
6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB8gOUH/CVt2Zp
1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5R1I1EXGt8p6h
AQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJanZ/VmS4TgDqXj
WShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9yu/3DjcYbwW2
lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJLAgFpW/jA/EB/
WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpg
hkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0l
BAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQWBBSiU0HVRDyA
KRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTAN
BgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD5H14EC4Muxq1
u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GDEu8uKveERRXZ
ncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8uuivZfg/m5fF
o/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K9JiQaJYOnUmG
pfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpivNJYdTPUXTSO
7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88wggK3oAMCAQIC
EzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChME
SUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBS
U0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1
MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdH
MRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEP
ADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6WWyTgBK9LCOw
I2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZWleYXFKlQHJD
73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CRQ/YbHPKaw7aR
phZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3nBdWCRYV+I65
x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0nsG1lyyXt1TL
270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAMBgNVHRMBAf8E
AjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBz
bWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIG
wDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0jBBgwFoAUkTCO

```
fAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJojanzqmgaSN3
/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnNvOFb8lV1iffR
TF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSioQ23WxHGVy9v
sdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4z0IOvg6mrYkK
TM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2ZPRPM8JXNQC4G
Wv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH4ConlB8f7R7s
1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExB
TVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24g
QXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFlAwQCAaBpMBgG
CSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8XDTIxMDIyMDE3
MTAwMlowLwYJKoZIhvcNAQkEMSIEIDe7/NLwTkHNon7IR1M1xiObMU+8qMIZ1No5
ANcjz5C9MA0GCSqGSIb3DQEBAQUABIIBABi/HvXTe3Z+LaltuFv57ZaUvY6kegwe
OGiZ5UPa5FBpQxoE/1vp8xG+UVIUnpdV/1THKPjKFr6bZZff1/4u4NFeBYwI9yg+
tK1cYz+B2cscX6FDAGjUr/6QxMOwd+ol7bnlzJJDrXvv8B5AOdHFosyOrDSrvn2k
Pzc6ush4JvS3aee5QFEgtd1bQx9fx3t/QhBsn5kGMC+3FzvKtmAYUlz0unqvk4HV
I40Goh/Fm3uzNxwTQ3/rzE7ws1Qkrp0VlBxVGgUa4dZ1VXVIizkRz1PRtis66F73
EXJlygf9Btm/TJDUivXGr7fCI2i+njByX9vqUf/0UANsPevCy0HQWCY=
```

C.3.10.2. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-legacy
Message-ID:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:10:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: From: Alice <alice@smime.example>
HP-Outer: To: Bob <bob@smime.example>
HP-Outer: Date: Sat, 20 Feb 2021 12:10:02 -0500
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="308"; hp="cipher"

--308
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="fff"

--fff
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
```

```
   Content-Type: text/plain; charset="us-ascii";
    hp-legacy-display="1"

   Subject: smime-signed-enc-complex-hp-baseline-legacy

   This is the
   smime-signed-enc-complex-hp-baseline-legacy
   message.

   This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_baseline Header Confidentiality Policy with a
   "Legacy Display" part.

   --
   Alice
   alice@smime.example
   --fff
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit
   Content-Type: text/html; charset="us-ascii";
    hp-legacy-display="1"

   <html><head><title></title></head><body>
   <div class="header-protection-legacy-display">
   <pre>
   Subject: smime-signed-enc-complex-hp-baseline-legacy
   </pre>
   </div><p>This is the
   <b>smime-signed-enc-complex-hp-baseline-legacy</b>
   message.</p>
   <p>This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_baseline Header Confidentiality Policy with a
   "Legacy Display" part.</p>
   <p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
   --fff--

   --308
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
```

```
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--308--
```

C.3.11. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 9925 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6342 bytes
    (unwraps to)
    └┬ multipart/mixed 2003 bytes
     ├┬ multipart/alternative 1104 bytes
     │ ├─ text/plain 373 bytes
     │ └─ text/html 468 bytes
     └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:12:02 +0000
User-Agent: Sample MUA Version 1.0

MIIcnAYJKoZIhvcNAQcDoIIcjTCCHIkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAIT/yEi7AoxOH3WdBU9Ff3ge5PZyEKHiXwCp
exVEZRgKm2m1PHvc8STLe9siVkz9OH+MbPfTQ9RYRw+xiOmvK+mwpCPfAf9QDCWw
4dU75zCBVQOPy/m6+SDQRtvHyesEe4taEjnI07DcGj5ENoE8ugCcjr34HmBsIILF
+OLJQ9fTXTYjeXQbXjP0InPjQk1GgHnfNXgtIcTM4XEA/EEjPSrphXsifgnBf0Dm
smBfCKe7fSPN6tEeP+DIQkuQVZIrBZd7f+nzM99ixMH7kpI23Gl+BCLeSr6M4fjf
gMoL4tuj8WgT8kr1W6x3583fOonWNsVDW+9FJp5iefg5ou9g/y4wggGEAgEAMGww
```

VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAIN4h5gziR7BMQ587FEgEjT0P
M8QJzMfBPlgZL/POdBeNvMqLMABEZOna24NjftAZw887hhvv5nHujIBtEO3ezN6V
wZn0tzznuqMXBExxOHq+h47VahUNmg5zrlVYBVg5O01vXXPVoIWjW24vwZo9Q1hp
0QqGC0MItLN81RpwG9FTgvtGMx/uDs37IxHQDDH81VqSu50BbuDEYPgD6U3NtzkC
uVlW9aSqA0scGwib7bVLdmIoL3f++HUWD+YDKHnZ3M08E2u/trYTc3ofiU9RImKo
SjMLKQVGQYXg05sXb6IUWSXxKi43BfeI1YcQsHE6TMCcBN5v4esQ7rDyIKlzXTCC
GW4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEGjqoAw+Ed51rHpzWgYvdraAghlA
YTD4kIjvM0Lc1TM5w1rdgJ4hoLTX6BDFIUPye3MkOg20XYl+XKES4fW60C0vad0j
2A6N6TbJoxrHQFy3tSCnLScUqF0O4BY0Y8u300s7HMKV0cQFKFAzv8STtpu2uOUA
2pKrjK/BCYQ89GzGvhSInN+Lx475Hh8l11B8Ue3JrxI/x73cNufYsaPUmRQnYxPV
F0TI4k7kxaELKwradV/owDJnulGKq68tX5/GRoQMhFAZHrYDyDzvlG7FHRVQx8cK
2BZeCEFcCVbpYFu31hVmu+RB2MRFSmKt7FedNnc2cqNLTaCJURE6qSMcsBfxoGME
TjZJUVtB2Fsoe02UvVzOQvoJ9odB6oihKRsaEUe14w6aIpgwGS8h8LJiuG5yFlmj
j0kG4sQul4wc9zHGlP3MZ0ivrvUCxag9OOY/qI3aJNj/KgyGyx2ncuYps61w49kA
6QSnvPBtcoVGmu+VlmtSS5AscvHnUFcrj6HYIO68gVdJF5zW88qF7qN9rQaL62rF
Llt5TXz6TaM6+S0Q14QXA0nGk7Eeliy9e5Anu2DPm0jRZfujwouvzj+hBtelMX+G
kx7f8HiaSZP7wCAkw219gnaRQbyUvDaYDWlAS+lDbKk0jX+zH33T19F//aKw5grY
qAcCO8rXY6755AubfhUk1xmuR2nDeNIKx/q+ur/BUhrXH99788Tl9GHJVCqVUzkO
R6wAULl26kqU5HWrFxQtz6yjoWC+YU4tZJQrYFZmyU6BvSJhcKck38lwktrvXuvb
GBQ9Dmu+0qUk53SXEtbnxgpO54JyNRBpX+FP3MWqiMcQdlY+iI1eSNoatXEeLrTE
IzMiCYgx67jI3rgAshwBDBfxhXnqlbdby9/IJWsmfYlnhiubdlZ/wJMDnPMbE88r
pMw5IccDR2jM5PvQsRJrmPfUDkFXBio2KNUVMJy3AWpCUKu4/JxnR+Og1fs/ffbe
m1b794TlEctK8iXRzDp1CLGFTpsHtA3RYHHPd3DM2RPeYl1FYWILyuHTbZB7soKG
dJR0gpL6V/zpxo7y59v7yl7FEvq8+OwVkKgx8pGrAPPd9R/7S0jlqxSZVSzgIEWA
9fawyV7IcaSH6FhBSUgbQRm+javR4RgPHTSHrenFUm0/hPT1PL8GFDdZFnNhHZ+w
ktF9x98Lf/RlSwqT+01Hdgd1Hk6EytYuLRhT6h7YxBIb0iKPe21hVV0jFqnAqAlI
YhAACYQ32SJGZAfPQ1+tP6g9bGxKWb6hxn+wEhNR4BTbSujrR6dkFIQW7FfBZwDE
PMTZ8tJ8V2E1DgU0gD2RJabZ+FKa0DAArT4dFs5RsmCJBCBrydtE1Qn1QjoWsdC2
8HFI9h87fxcAs6tSTNtV6dLIignDCu2kBWKEMaAbuO7E0OUPV8708WbXGy4889CE
4SuGldMTX/h0r/wzSim+HFndJF+ocLL/7R/ynV6V70wYsGy3Qba1DrG6AHOQzIMY
uOtK2R/y6KDxKTQUOQpt4TBzDJu96D48b+BxIQpB9KXSbNsNQuHBql9A30FlZhxb
kELYZmenmi89slmRgdjQ6r5673r2kGAD5601XLhtT67QsrBNMe5FX9EKHIKdamSY
a8weblLDrpHI8K7tnuJiBPIF0/vAiJRkJ2ARDcuhEAHVu6ONX3+0dylxiwMkR8/o
ae7dI+RQWgl94g6kd1AKT7pOyA4Paah0fZZ0SYwmR0MTXMt74Xl0/AWgL0K/GunI
4eCrBCT1ewUae109F4ue/2vmO1wt590GApZM5N48LvTjLo77KYK1w5RlFawWCnGm
MHw5osNEEcntNcukumQkoNVbYl1PVH27L51Psm6g6sZJlaXuFz3o1k7mXUUjdqPZ
TPem/JqObrkuIAX01b6fYasm4eYZ4Jj0GvW0xZSVP3dcEj0+kWiug9/8UVjPqd38
GAaxDn9qoH4sVfFg0Qm9HLnZ4ebSePb5xe/kb1ft5iPv63T/1tWe5IOkqRlkTKbS
WqhiksIPGv2nruMokawTOe+lr+CCE64epfClN6YzE5zcx9ZzY67iUNljG2cBYXKR
028Ik9ayqjuwOYbFBET2yreVT4GK7Xn3fWAkqzkCjVt0I0w2g0pL46hq4got/D//
xT/xMCEnLSz9hZB0KAwO5FAaLzbEpPbS6HsfPAgithbCHSOLAXN/+qQtUrS2vtiB
YBF5sgUTtpOoYdOu5Wqnu/XbHmHvi+uBIMoTbASO5+D59mcIwVGdutjJ0lwWITQk
OliBQwd+OFe2Ro/yE28nsIg+sMzvYVH5gngAmS9+gmwNNr6j/MMeZTJeIdqpkjJp
98cAJ4iNRve1yTYuHAnBoxwl58RNpl+GBGB0NP25MWVs0pTuSc5MlyoufMB59hjj
SMboejGK2bBxRfSTGZ7BdDM7+7KY5mQotONOCpMQW9ubklhOkUUSlUeawRSr6pYk
Fml7mUWMUP23PESDEgNq8j6OGsZVT5fLxo2Sn97VhUXnXPCAE27GlN4VYu9U2CKF

G7aNU7GWnm+pz/Bf+VJ8VRIKoFwYNSHAajmhfizhz4SqipwLhfRMp3jGXA8F4cmM
lPKqqUZ6eleRH4bWUGPm2hynM2A9tFG6W03e+Z8PsCnshABKq/XBzkavRClK+Ry+
rH/D3L2RluVHbejNWR9qbumAAvwQf6CZX0yZc8FVXKZd9sPSn3h5u6Uub/01kl/A
kPN0aX5ld1+ZG623O1uO8OFFj9EMK9O5PJ9iinzeCFKHVjfdR23imO1WOF3QSRIM
iUyPGqsnlC2yg/CA1mZTmfnKg6rwUO4Zhd7bf9287jEOInJwrhFIZg5aFSn6hR6N
15eNF6CY3m6icjaT+Km800YjxcMNw5MmgPu0qXYC6J2NG8ppSpR6czacZJWgPKlG
XdFFfOQTcyh26KlP3P47Dp/ZK/ciDQ8ZoSxIhT7e8gI813SdwkTSy7e2razbi2vA
ZxDaqLpN1stx+doOIPjWiFrDWlWLwzcS9iOAZMHDnXY54l8zNXG70wwivj0t3nIl
4i/EQX6SF7W4o9wjM3rGdr9lclKpRMR5dWB/Viflyoe+9UdiC4emnXosdRxK0Umz
nJ/ej+oZGsTQ2QYgWvMFgKRrOP8tD7L6l1LMThXEvjff+HVILH7lPZioML2znenC
j4SGhvqQ78/vgAKSIsXCNy67bNY8BE+vUWDSoYpQ3JTuv8af6ou6LVSPmjIQRxP+
VCoyVS0ymqt/kHFgaNI5UMDQCrKX7gDD4E0RoM7t4o34MN3HwNVTriz5SnqjQxkt
r+3aUWndQchUHAmH3Sre3Kr+U5+VGSuRRVa07FqKXrbaGD7IYNmfBuaVOaA8CJqX
/0vxQv3F3zNmFCh8aomVmQcQdgI0ZRfso7t/sbT+/FpgMV9xXSzp69LwrpDME771
TEP3J4L1S5flNuy12MYr3Cfgq058erDbs9x6L172nP4WgQUDyJ9RR0wWpNUPyqlM
2YnFt1iwsGSHSzgv32ykbfHqcPujklZHm1omk0x+2KUkToYZwTa+OMvC7uXPxGkS
8vuBzJzQlX3fZYbsaiyJK5uQxMj2Yp2WTLsPFEkg0xSKl5i3vmCWq/kyZMwnrVr/
Ty/xHasuSlBaM+uZEVorN0yFdIwZF7aeAp2yi1j1lIzh52xY/hwOcDhoo0OX5a8z
V2gsdQQJ5FS1KjJzfs0nsKfxkQCLkzJPCdyzWFlmaUuotGvV37qoCqBWALzsw9l3
8zB5gTGDAvIZkfO4/HL9971ZcsxuPzmrv9u9NoS4lRM4OuGBqlhVaXnPPTSKW7DG
zwpOocCWhhJE5UrhDxWCZHYDmyBqxk77uGn18UzUQQ17t70/EZueLIQZROZG/701
IGaub+MlYXtBlPXPd8whCsd67NVSlqMkLADbu/S+Nr8Q/K0oVVC2kwrqb4dfHf4v
W224JE3WnFjtvkc6vDBIEx+QdO2yw5nR7Zo+XqVyoFoHgbUyhbeWTbM8hqIFUvfd
C+BY1wU8jvWCM15NNY8R2ZwUgyfeshwpmNUbuguwy6CIUHTblwJpYBw1juOggXp9
qESnDasfuZ5dIzuWMxxRwKn/GtmFejYuf4G5MVqgzH8GLB7bHMur6yEVhZjhNAWx
khcDD2o2+6vufzxbbOmxfsG0vKMgTwA43MhFJYnw5aX6ikQiDPl8HpQaJLZ5A3Ve
g9AeNhHqnB7pTz/4ZXy776K9AmyBxSXDz/9AJfdEq1bQDWlSldX9UaQjNIhCpKIt
wfulvdx4b9Fdrqo4Fm9V01uIioQ60xyahrS+ekBjPTl8oquDj1IgfeWWZQH206VV
ch/9mJmqJLKuqMEkhzVm2RQsbCwvALS2bXmBnIu68sAdrKY+G4Ph/QzoGpG20jJ6
XPGID2SHF1fYKhq8bpqgtzncLXtfCps2v5dr7ZMeKVBGC0zR/0Xr/YFHCW+E0CcE
MI6PJrXbwj3Vo6rGE6Akvi9t7BCVg+G02Lbh/cLTnClmebaXo2K7CV3913tFbeXw
FruMZbmU8aneltETSrH4BDL8pnZghhQQB+6zynFH71zRUhUSZGl3ko5GJ/XmjnUW
lMQkaUfWnLWUQNwvRDn0yO6q2hkPkNzJhhUwzPJfC3PhXJBZENVPSVzScX13GmAD
RFJL8HqvTdCXVlyz0HacK6Qzy5QR162gF0f+I0A70QQM8KnRKZvpeLAr+q3Ecv/z
WCWKi/c5RoTsF6U5t18oVTYZpJPuXhzlWgRPcEa6FH03nNkLdXCsYpd3/I3HqRSH
0ic92uDPGcEM9+zvV4IEwesAfKkgHpfbNXvl3QIk3hMdhjJ8Z04OOENThDGXimiT
KxXfIcujc5MGGPsSCIkRaQ0pOYIQkB+DIyEdJHvx2YDE0QFWuRm4ukFWN52LgaY4
s6SCHseFczVZ1Uh+dXJi6dadYf7zrEEcZWyQo2mzYqHqs7l9M3OuCOrmT1Akol6E
ewgMFhENK2hzCxCPQvKCN5sZBdq7UXYrALalxhVzPP148S4yYoFx7R37GZBB8Lmv
dCHESeIEXQ+Mk1gPo6TIgn8/0JGcFfYBlXWDzNSNtphIzN9o3TFsmicL2ofWfidi
L4QOa3qhvADS/7rV/cu0GnG1NUaLVgF532W6iMEHMyW882iGjp0D3rNm8sDx+jRI
FBbDAIrvFlHZwTfSX1v0umSCE7a4inm9n9xUWPvNGE1zIgGJ1y/1lKD3nQs6V89V
o6J74qxrJZpM+mrSkzPcXuIoa44vCiNcyfCceSSjCNSV2KQs03n0iCbC7HF/lDJp
BJR81nccq3A2i9UJsh0mv2tPtDVFWEJ5DORn1EdtMu1rHg4HYJFA4ZEEZAACPoKr
VvwVlGaYSEMYE/C4vMHry65qk3JiHkPL+ceFvlzxyL43F1xuZ0rEfUykpIuChCMA
I6NSfW/ykTdeKu3weFTDCEX0NxTfhqYLjUnmJwrHwdIVRwlKK0ixDTblNKDef0un
4R9LwN+nXpmbQYp3n+UIBqQn3+b98H4rBTyDPq30hkzK2ZkVsfnHKe5WA6x95RQm
zruzY5a48PuGAcRbGUt8Ne/lv4A5JFcliETkBCXOzSDdWrZpAwDUXnwYjwUc9Hon

aWC2g90gTT2DwFBdOWHJoDr0SfquNsiC1LWee25QoG9yP+AByxppJJDTyXae2PK6
tC8wxO58N4LnYIZhC0EoUEX5IqbNoNFWTjNeAScWXdBnN+NgvYkYPR/ATVH996aj
VpOdjJGVCFVaTphqroqer+f9PUk27qXbaK4tplwnNb2+zK6IVQsK81+7Bi8VBYKv
3jOgo23Cp+276nQbZthzfO1T8DkYs1E4lM46DFegPoTqFTn9Y9/CyFxQ0K/+uT3Y
yDqlmgJGCRj7LkyOgcZGW7OTkgyZar5VM+uW9M6ASqeNj61HrZZ7e1NMuHqNe0w3
cIERFOT6q/njz01e5VaWWqrcPudO0CPcTXzFfG9M6gEgUjzLkEg7E40XPiNFfrGZ
3RRLFP6qYJ/LFccRsD2gFQFGmOFmbK/rVGPn9c5mjfO74Tqbl9VvzGPyYHZB94LH
6hboBD4gH/DVKJmPnl57LZhj1ytsmG5tGYBzBaG5QR+C2VlYwNBFrs9A8m0hsIQu
srundztS8LickI6eR6hVp09bclXmxfA/YYPQs8pUIi2evAemdXPa6kZdQcU3bijA
nlsml4AmYNF1w192wDTZ9oVeAzH8AjSGRghRAa2r/G77oyge4EmmhqwWBxdshuii
N/2bpdiuYOGknJEoOSxTu9d6EncSxwwVhAudZ2mynG+AYgJx+LM4ZriVZ7DjuPo+
gU7XLwsEZY8towvuDZsht2/6UJTtaUtr/2RGUYH2zuy4fCeREJKu4wissg9vA60e
ucAGOJg3vnnZKy5hxgNJjJhJCuY3QZrEqbsWavqCuc/Iee/rBEdQ5gNZ4AZIEcvM
idqXhp2gLSsg2O+nUEVxsiQRCQZqQHwCRXjaienkctMxEt2rnGjvCz/ZDnEivLfD
a6vRTZD40Gzxgmk5brcltFvUJs9AY9dfEE+MlMefeb78pDbjwBb0CN6A+P59h+Z8
6Tz8US9RLWK0rr78voT8P0v60FVHiQhAKVjAHh1HRfGe/ic3utAY4YT0Yx9B8QIL
oSFZpCSyk8stO0JtmcXd10WJVTYwPzoFtR1Ebi2MvRqKKUHKPAuuVsk0s6ZUyzLk
z23Dqu73fvt4lDV/lvHXoFuTOdcWV+V3zo/fq63efD3ZKqtw4eEoBv6VRt6xpPdy
14YGOmI9NuGsUhUTsdNV3BiyjK8KBS43Vp8AemViMfaV0h8gjgmAs3kt6UPLNlUy
xfdfcAJlQ+j6NS7VsQ6a3VeDq6Om3qn/v+CARGFh9SG/sh+frkbtLd6wAdD033E8
4+Y/LJWElksOYfZZkJ8Pn94yE/kvRLRIui4gPosJkMmuhc/hCU0exFlkiqOdRJF8
qs9H4qmtEHCIMCK4tl/3/UA1dw4+4H0Gx5F/8mH6WTASSfQlPGzbBfNHBXYhE4Jm
JYdhpaz8rY5djEGrwd9gx0J/x0fuZQSTMQA4DAyb/keFZYY/obXoCpzTb3uASmm8
SGAiurgRPrzOlXUBz6eR6LGm5+TYJsf4tXF7ylURxM29ArS8Fao9K+RTZDRhWs31
uYaxGby/QFmKovpudaT/NPgVtpv3OihUgrEnMvh7nvAS2rk/2+tAsLAIpxm/l+HC
4zemv+joiSMzCKEEGy6Bj7amYpWlU+Ohr5thU4N2MyL4GRy4XEAfyfaqShRAcrAF
aYChXvfiQ4V2ld57/P6XUaKn4zn9FxzRb/b1y2ZOqCEmBI1n0sStaPiaYXfbIbt9
NtwWB7pFvdwwz84QXdEzEKfM3BRF4P0OvEyYqraFtDUchLi4jj1Cyk/Tpl6L1teY
q95nw4Kk/bY6Rce/cRzwJKBlf/33hw0A7aBxonntxl1qsIu5MKaoi7xhgQP73C9/
xQjlUsKIIQXw9u8G8I0BhWOAGFFRhfoYIjwXYD8VKcdzstOsCRPMZiNUsK+ElS38
NqCo9+09NZvyPF6uBErZMP/5CcX3r6owSfcSkOZXFvbQAUZMyBnyGorQ8MS4AQ/S
9RwND4aAsnsMeNIWXTavNDCHIaez5HsiGwhppqY9h2eCWegfreRe0diP85+xo5ro
+7KLUI0mW8B6zP5T2VSdFYQbg80jI4sRKa0EHWg1eFlrK3XXOy8+v5u5RUV8Pclc
C/6o5Co4VEogaY5mhimizvF7u0wV7lKNKGQUvBqsbXe4MjBj87pecPNKp7J9MkeW
rbG8Tqk8ZxFGeu3Wp5WAzIYV688tw4rZ0B/jQMsvjW/uueVXNA4tyLMfYuEFrDjm
4+1NTW/ynviO9Ztoc5rATj29mfqSX6pImpP/CeL3oSnMVSS+SfYOWT/p4tKYc/ED
ydKyUhr3fH7YsnC+m0xpxiHO7V8V0p5MP2+fq24mMco3O1aZqHboHm+cC4i30qNJ
t0yvxCDFt7UTgEJ4FEfq1AIpNtA1XtXT5vLSnBkX2UOqjL5FkhwEPHe6Wqw1l67B
x8uzVRuOsCSgLpo9Ljgp56ly2vEr7gDSWgqIit0cVIwXZlUcOzzaVrDWtDDfmXYF
stpjIHk4BsJGwoqJN8Gf9IGV6Pi6DlpUtifBcDEpCoBt7wkMUCHp/Bjq5lEsTtZA
86yRqNOZKLuyW7tqDfOPYQUsUpbAM4E8hrN84EDgLYMCg6AC/Qs3H/wDO7cJ4LCk
M5Hph06hiyehanuMCtUVyvyfSb1hWY5LELyr9UKLYHXMdCRm6SI4lhkcD/yd7YRc
8xXJwFVSBSXcuRFQD8ViGo84HNNw45Oa/kcT0tfJLNDk2psDgMICjWkiZDcOJ0fF
ExXO65SCDaVSK2a2hScuhLb4o87nkHPTtmCwse92gYQlgEJqhAUCe4tupS3Tlced
rYx5p0TRq0a4saxyQw3KOkvCYb00vr3e5ywj+I7FJmdT/3FRepXHAdJgeymSmelh
MUnQVvRetUv+tbsHk96DXjMHUfvCArWcjf4NfuweEud6JAtmIxZhmBFTlg/j+oB7
L3+nunA6/dDrIlBNCCQ/WWW3STpAhFC7jBCzIZMJMwyP7tRk6KL+PptfMMWD2rJy
QpFXwNDVCKOca+JCuhJ3lhlfjrexPJKD5/hhqGdKqc8=

C.3.11.1. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIR/gYJKoZIhvcNAQcCoIIR7zCCEesCAQExDTALBglghkgBZQMEAgEwgggnBgkq
hkiG9w0BBwGggggYBIIIFE1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5DQpNZXNzYWdlLUlEOiA8c21pbWUt
c2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeUBleGFtcGxlPg0KRnJvbTogQWxpY2Ug
PGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JAc21pbWUuZXhhbXBs
ZT4NCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTI6MDIgLTA1MDANClVzZXIt
QWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOiBTdWJqZWN0
OiBbLi4uXQ0KSFAtT3V0ZXI6IE1lc3NhZ2UtSUQ6IDxzbWltZS1zaWduZWQtZW5j
LWNvbXBsZXgtaHAtc2h5QGV4YW1wbGU+DQpIUC1PdXRlcjogRnJvbTogYWxpY2VA
c21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0K
SFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTc6MTI6MDIgKzAwMDAN
CkhQLU91dGVyOiBVc2VyLUFnZW50OiBTYW1wbGUgTVVBIFZlcnNpb24gMS4wDQpD
b250ZW50LVR5cGU6IG11bHRpcGFydC9taXhlZDsgYm91bmRhcnk9IjFmYSI7IGhw
PSJjaXBoZXIiDQoNCi0tMWZhDQpNSU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1U
eXBlOiBtdWx0aXBhcnQvYWx0ZXJuYXRpdmU7IGJvdW5kYXJ5PSI2MDEiDQoNCi0t
NjAxDQpDb250ZW50LVR5cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lp
Ig0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6
IDdiaXQNCg0KVGhpcyBpcyB0aGUNCnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1o
cC1zaHkNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRl
ZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJv
dW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQvYWx0
ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGluZSBpbWFnZS9wbmcNCmF0dGFj
aG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9t
IHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX3NoeSBIZWFkZXIgQ29uZmlkZW50aWFs
aXR5IFBvbGljeS4NCg0KLS0gDQpBbGljZQ0KYWxpY2VAc21pbWUuZXhhbXBsZQ0K
LS02MDENCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1cy1hc2Np
aSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5n
OiA3Yml0DQoNCjxodG1sPjxoZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVhZD48Ym9k
eT4NCjxwPlRoaXMgaXMgdGhlIDQo8odG1sOyBjaGFyc2V0PSJ1cy1hc2NpaSIg
aHAtc2h5PC9iPg0KbWVzc2FnZS48L3A+DQo8bWltZS1zaWduZWQtZW5jLWNvbXBsZXgt
aHAtc2h5PC9iPg0KbWVzc2FnZS48L3A+DQo8bWltZS1zaWduZWQtZW5jLWNvbXBsZXgt
ZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQplbnZlbG9w
ZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMgYQ0KbXVs
dGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUgaW1hZ2Uv
cG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBz
Y2hlbWUgZnJvbSB0aGUgZHJhZnQNCndpdGggdGhlIGhjcF9zaHkgSGVhZGVyIENv
bmZpZGVudGlhbGl0eSBQb2xpY3kuPC9wPg0KPHA+Q29udGVudC1UeXBlOiBpbWFnZS9wbmcNCkNvbnRl
bnQtVHJhbnNmZXItRW5jb2Rpbmc6IGJhc2U2NA0KQ29udGVudC1EaXNwb3NpdGlv
```

bjogaW5saW5lDQoNCmlWQk9SdzBLR2dvQUFBQU5TVWhFVWdBQUFCUUFBQUFVQ0FZ
QUFBQ05pUjBOQUFBQWNFbEVRVlI0MnVWVE94YkENCk1BZ1M3MzluTzNUcFJ3MjBk
cXBiZkFSUUVqT3l3aXdZbkN0a0RLbmJjTGs2NnNxbFQrenQ5Y2lka0UrNkt3a1oN
CnNncnpmY3FWTXBMMmpvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmljaWhBZjVZ
SnJ3N3ZqdjBaV1JXTS91bGkNCnZkUGYxUVoya0REOXhwcGQ4d0FBQUFCSlJVNUVy
a0pnZ2c9PQ0KDQotLTFmYS0tDQqgggemMIIDzzCCAregAwIBAgITDy0lvRE5l0rO
QlSHoe49NAaKtDANBgkqhkiG9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZp
Y2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQx
OFowOzENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMT
DkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA
mpUp+ovBouOP6AFQJ+RpwpODxxzY60n1lJ53pTeNSiJlWkwtw/cxQq0t4uD2vWYB
8gOUH/CVt2Zp1c+auzPKJ2Zu5mY6kHm+hVB+IthjLeI7Htg6rNeuXq50/TuTSxX5
R1I1EXGt8p6hAQVeA5oZ2afHg4b97enV8gozR0/Nkug4AkXmbk7THNc8vvjMUJan
Z/VmS4TgDqXjWShplcI3lcvvBZMswt41/0HJvmSwqpS6oQcAx3Weag0yCNj1V9V9
yu/3DjcYbwW2lJf5NbMHbM1LY4X5chWfNEbkN6hQury/zxnlsukgn+fHbqvwDhJL
AgFpW/jA/EB/WI+whUpqtQIDAQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0g
BBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1w
bGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYDVR0PAQH/BAQDAgUgMB0GA1UdDgQW
BBSiU0HVRDyAKRV8ASPw546vzfN3DzAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2
GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEAgUl4oJyxMpwWpAylOvK6NEbMl1gD
5H14EC4Muxq1u0q2XgXOSBHI6DfX/4LDsfx7fSIus8gWVY3WqMeuOA7IizkBD+GD
Eu8uKveERRXZncxGwy2MfbH1Ib3U8QzTjqB8+dz2AwYeMxODWq9opwtA/lTOkRg8
uuivZfg/m5fFo/QshlHNaaTDVEXsU4Ps98Hm/3gznbvhdjFbZbi4oZ3tAadRlE5K
9JiQaJYOnUmGpfB8PPwDR6chMZeegSQAW++OIKqHrg/WEh4yiuPfqmAvX2hZkPpi
vNJYdTPUXTSO7K459CyqbqG+sNOo2kc1nTXl85RHNrVKQK+L0YWY1Q+hWDCCA88w
ggK3oAMCAQICEzdBBXntdX9CqaJcOvT4as6aqdcwDQYJKoZIhvcNAQENBQAwVTEN
MAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBs
ZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1
NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsT
CExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcN
AQEBBQADggEPADCCAQoCggEBALT0iehYOBY+TZp/T5K2KNI05Hwr+E3wP6XTvyi6
WWyTgBK9LCOwI2juwdRrjFBSXkk7pWpjXwsA3A5GOtz0FpfgyC7OxsVcF7q4WHWZ
WleYXFKlQHJD73nQwXP968+A/3rBX7PhO0DBbZnfitOLPgPEwjTtdg0VQQ6Wz+CR
Q/YbHPKaw7aRphZO63dKvIKp4cQVtkWQHi6syTjGsgkLcLNau5LZDQUdsGV+SAo3
nBdWCRYV+I65x8Kf4hCxqqmjV3d/2NKRu0BXnDe/N+iDz3X0zEoj0fqXgq4SWcC0
nsG1lyyXt1TL270I6ATKRGJWiQVCCpDtc0NT6vdJ45bCSzsCAwEAAaOBrzCBrDAM
BgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAV
gRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1Ud
DwEB/wQEAwIGwDAdBgNVHQ4EFgQUu/bMsi0dBhIcl64papAQ0yBmZnMwHwYDVR0j
BBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAHOJ
ojanzqmgaSN3/gqSQ4cbbmdj/R40BEPr+gXT+xiidfZ2iLNwYyTneuK6AChwKfnN
vOFb8lV1iffRTF/KtmVEDMR/sYeqAH83KM5p3el2lVh4OHhyI0qNuz5oShNaACSi
oQ23WxHGVy9vsdVfnbhsplrWg9NQ2WbpCmK+2oMh2oYl0Z/wvXMt9cG6jbMvcdH4
z0IOvg6mrYkKTM/RCGnumghxwYToj1OyD5Gs4D2IJCw+fX5ODxh52MbNRYXTus2Z
PRPM8JXNQC4GWv4km3M4rKnJDd6hnoQ9rNeozIcBVyybQYjfrgg4DRvw9Ksk22OH
4ConlB8f7R7s1LM2cSYxggIAMIIB/AIBATBsMFUxDTALBgNVBAoTBElFVEYxETAP
BgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRp

```
ZmljYXRpb24gQXV0aG9yaXR5AhM3QQV57XV/QqmiXDr0+GrOmqnXMAsGCWCGSAFl
AwQCAaBpMBgGCSqGSIb3DQEJAzELBgkqhkiG9w0BBwEwHAYJKoZIhvcNAQkFMQ8X
DTIxMDIyMDE3MTIwMlowLwYJKoZIhvcNAQkEMSIEIOk6rjm9vW4yAFhPqraTwTSM
poDXdAk+kSVCc47Smx1DMA0GCSqGSIb3DQEBAQUABIIBAAURi5oouLYIh9YruNpF
Se6sDsPTGmIcZsDjQ/MZV55S4pmhVBQu4SoVZDVM9KHKxqfBbj+aTs1Cyas8R88h
cWqd8xhiU9ufoC7p6qEMVIyMvyppeupRyjQWUCH+2XtQ5sAVmr+F+l/Valuj7JZw
JU8XS84oinCF6uApu7eucGblt8t7ek7j3JXoFVE7g8a/O1JKg4ezNV2RduQeNXLT
m/lBVIfeiiOsmgmJa5RTgbgAakJtdo3odHj0cI31eANSbQlE3XENz2E9L8JWxYNP
bBceEhIvu2AOtV2PYCBfrVp0WTVwWHorm8GG/DyvsAsa6eGJI55hA8VeBg170gT5
nzc=
```

C.3.11.2. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy
Message-ID: <smime-signed-enc-complex-hp-shy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:12:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:12:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="1fa"; hp="cipher"

--1fa
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="601"

--601
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-shy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
```

```
   with the hcp_shy Header Confidentiality Policy.

   --
   Alice
   alice@smime.example
   --601
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   <html><head><title></title></head><body>
   <p>This is the
   <b>smime-signed-enc-complex-hp-shy</b>
   message.</p>
   <p>This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_shy Header Confidentiality Policy.</p>
   <p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
   --601--

   --1fa
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --1fa--
```

C.3.12. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
   └── application/pkcs7-mime [smime.p7m] 10920 bytes
    (decrypts to)
    └── application/pkcs7-mime [smime.p7m] 7072 bytes
     (unwraps to)
     └─┬ multipart/mixed 2519 bytes
       ├─┬ multipart/alternative 1597 bytes
       │ ├── text/plain 564 bytes
       │ └── text/html 736 bytes
       └── image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:13:02 +0000
User-Agent: Sample MUA Version 1.0

MIIffAYJKoZIhvcNAQcDoIIfbTCCH2kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBACgBnn7CPutWy0itfe5dCraPlDXBE+WvvHIX
EhTzjfwj8Oy666bZWDo8VCr86IK1Ul3/OR6f1a/FyLJ04yLW+1Zn7WVxxS8PKGrO
oaE56/oJxgqRRL3qnY01rMIhqfFrG2DNh6rjRnd03witWba76ifzdWdCz3JRCsrC
3hlh5SMSLYH5O0TDFEJ9tGDGmxFZ5+x4FJ6D+lJ7OLRo64rtpHthyuO5N1NXPBXU
NIxSVFQ4f8j5AS7Z8oo/79IoX1wUlv7IEkq0mfrx8sXrcqZbkmw9bPRGZrWRZLDf
7EYCc0IF+sn6USXf6nd6G1vRAgWaUd1kiZChjVRwgo5SRsAk9nUwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAFOKeyT8lWzqPQF4leLhROrAI
pTb21ahiLRjfX4mWuotY32k8fCLeSEmH5bHrjdtn5FNI/jLC3t9bAtFMEkz7VPZ+
FgjlBT4Bteuw4g8miNcIU+xu7gL3n8HlkTxOOkAmGPZg/m0BYJZYUFXCSQB1OGja
slGNtLS0Km11f/u13p0CLRV0+nasldZxM7Rt7Zd0Uis0PDZfMeVWTS8s8l9ifpjA
YGRJpKwzty4BUMvxbgUBzySofIH0pc/DlcFIB+s/S0Dgc7xAU8CxU7xvo36dicgK
qm6TqyYQDvBBXfnc8MWfVmE64sWIQS+nWJIpvTzXh4pZ0FgjKhNUdOYEV1Zz8jCC
HE4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEMVrSF0MP06N6O1pRZNHTXmAghwg
JGppsM+z42CDVWr/cZdmJAF0qTh58Yba5feUKKVha+SVHfhjgaW4v27XT3kKnraH
7tkFxwXRvPa/qSYKSgCS8LZeHEj0mh6HX7mJjbWIeEogBw9CH7kUUsq+YDmZ4ReE
+teYWio5HaP6aXoiy8qSyu2kbzz/EmIUxEIHwDGtbZ4f8Hqpo9/j2cXR59xGspg8
0u588sbXipWzBv1gxN24aRgpBov48l8XHqw9JzLozzOG0bZwdGMwZeKrtSPjtE5K
Qt2Gonk30Ri3LmLPVHQ8TKv7ZeEUw3mY/95noB2rDvIfm3sX/bBIWTttWj2pnzQv
dWl8byZ0otx1QjJcaLbmL1Vxd2U6Lo5RNsyHL+BsfoE6roSBwk7UacD0tR/tiMKQ
aDeOsQArMHC8+OGV7uKV0p6puZT1RGEkVLW9Pz3MvHYfVQCn7UU4HWz3vjUoCCFn
KRj6CG7xKUHAdQDTmtfKf1F6t3ba7Q3sGi2Lw7FH2RG9u8SO0RUQvYTxWo0okb1Q
```

```
   H163f7DLzIgyiiOaZmtrSOE1rHKhs3utQuYqvBtR7fvUWFC4GtqXTEThwYF84YLi
   vvYhVQqP5TWF7uxxJUyW8cgYqAjNnqi4Iif+LXDtrbf97fP7cAmcE3rNxvDn77lY
   Z2e+Khh/FgaMEFRzNN8P9itpd87YGY+mwde3bBw3fdzVInel1gFaxplGebabqpup
   rko9Epu+i891NSkwnKYMDqb3azOUW7OzGbWOw2Fvn5VcD0FK/eTVLwpn6WHhg7zl
   x2yZHQ7QMUCtKiAv78kjLuumezciX3Df4KUjYidPFF1lLI91tmZAn6exO9vtq55n
   W9A5fznObqeN/xhBv47IWaHTYozgbCY1SoqNqSmpqax+WG1EivO9b7w4jn+yxFkb
   smZ+WJJoMzJpvUCfZ5QeE6bVZhoFMPsDWa4UzzWhiwxFr2lj5guaWqJduQgv3qHE
   qF82ovG4Q4gR35gGHebJ6dxV5FOWD/3Z53ZrYMZUZxdwW+bWr504UgFHOA7ngvau
   vHgOyTnnxvRzvKSkhr3uRItr8jM4+yOa18HLUOmi0+/L45xJJwf8A8GKL0BCNabG
   giTHu+/5KYG3j6foE8mf4x1UAVG1dxp6QfEXZG1mFV02/w4vGJTz0tOrYSPJ3bXF
   +HahaZ0S7KXpN69rRqyFchtTC1Vbm7b75q37+lzLHisVebzvco92TyClaoKooLfZ
   sifJRf8KudETwNkNGFIj3oDmmSUrJ+0YiB3h7zJWGiVGiNd9UBXOm63/7SpTIaYZ
   eOUbCM+nQ5/SFTg4gqjQ2PPh7QSoOzioilMyosOAwWQ3E9ThEhKLzoaGzPx/dLri
   HL1ZBjjdtGC1lSCFcjdYLC7sP3W2nbnyBMG6dqvwakWGlaAuXPZ1yl15jn7yJqPL
   Pnp/eVU+9SlUfuqBfZQbVWPhIUmYg1KL23HzV0blIsKqbi1sjxo7DL4RrC1axRFu
   E5gKB1VaUCiDkZhiKj6vPQetaCD3bTi6Zr/xjj8rH6G0Rr8aWI3HIVgFtwrtuAxh
   D0YNl14Zm2K26c5FcrTVXh1XCpbRCjj0RqqsVUX3onamxH0nEdxSKObegqfBQwjA
   rn8jWSo7jm40wmpiEjg2Szi43g9C31jwMps0Eu1zAg67/O0n/ft/+75/y6j1lSb2
   thJp6L2z0VTMJDNbI75POhY1NPoqHWIZOV9PlOLOnH6hcUg5zt8JvXBeoxQdMcjG
   uY9ly1w+gLMuFA7KdMO/sEH7GM2OwpIEU5gqzoDresGUCE9gAC8kz/M5QOw4dOmW
   t85JlsTwmUbbYGcWjjZiDT2Gb6MrNUa14X10bsPO2hcceuvvEvLt9bBgYywVJcRO
   uE7snAIXXHEXodMkwAxwhSlQLcBjDSVUQm2C8+lVhw1W662ogb4yFJNJc0H7c+9k
   qTP2jJTSyMxG5ibmzF+apc7u3eL5/OU/prUmnZJAlr8DkfB1opYx/sCBQqJMJyIJ
   /ixMsHyqcNUGCD0D4+qibWS1vbUQ3XZOmdN3qIUdvwzgP7YpX1MEUYnb39k4pe18
   fH8fwkSpK3j2qJQ6mLPFMRRIL0zi0nkOEtFa8OUQgG0LpZKH2+Hqiyr7Zmparl0O
   Wc3D/M0Kksp44y5hYt3Hexnz6t+fuUedb4N6V43KjFK+DAuU3SZZ170B8vPRQNft
   s4x/AYMAcsqGieTau1uVEnqwUBoHgm8IRfgGcAwn02XFk9S1UXS/iFmKCl7dEfsH
   OrIvM1d4R/+a220epCUGEcmr5653LtMOoQM3Tupdit58Rxv43pg3KOvzTKygJ4JW
   02qBuNtc+B+llkKoilnQ1YJIqk6Fh7mOE31qo2isdLBd0niDp3vfQDBiFlTBHI/C
   e/5rUmwND2ub3pd006cy79GrEUsDSedhciN6ulsrXONhBr7FtK8oO5IyNVFVHI27
   QSiO5TNKllvyV7hWqCVIIuOVYwEvuaEI/TOMok7Pf7yUnJN0Q04t8co2BT7TiH/8
   NcyZtmGJaf35R8s8YMLnbg7LUb9wqo1V6EPnLfCkt8M8fcnpOlnQ8+Ynpavvz81h
   wd4v49COf5512ptCgdg5YZR/Q9v+T0c+fdeaF3jhR7/vV/D4NNN8LsthODqQ6Ac5
   kzz4RbsLLXbK9ZELjgjyyIB0Uome5ytjDSuAPeqWgEo28DsTJ0vIECRZg25ZhKeW
   cN8uuKI6WezjxeIRM7ZmDN3wvd3amjOSDvK5ASslaO3CyGWpZ3RJ0SknCRCo9Oxm
   aSn9zuHGD1ZtYL8P5kfTNmhCq14ktAdH23Lhjqwr5FNbhEGI9rxT8CsXUweaqRuK
   KeX3UdWOiLBTpcncaaN/3knX8EYdyOvNhQsqBtqu6gZhQTIZB8QiydFvf8ztCDgb
   5IfeDoZUru8HzhMXm2+COxqMC+FKoFjVc+2s81MIrhpMnFXL5M9iPnUKL6f21q9m
   c4KjLQdP20Btgeq0WKPdos9ZWTHyb4wWNZhbkq8AQ12MkThrHymiA2n9EaVO76sh
   ceQwORLinfQVbkqja+tN0u2jDfKVrbI21h93kvK9ZLP/c1IEt3f7u3J4KgCr95kQ
   SBNlSCpzALiazPSWB4Cbr0PKFU+mozln8IvBoYJWryoc4pbX162AFd7dUzXYOWOm
   41nXvsg2jKtor6j/CUIeIog+GrPlkfuesFKihydC6oCEjpGI68qU+JG8AhM4ZCvx
   4VfB75yJHJ7ch2hytw/UE7K6Vjz8lEaxS2LZ1DqiHoBo58QwgPbmmYUU/Mf5PlPH
   ybr1KTSeNyFT1Mky+GmpcN5tX5aY+qeLQ7mu6rfYLVk8wA0aoc3N0sRGO+8eigan
   01Jq4QeBmRbo5SDbe8PuRqGuGtCi1sU4vXbKBvBJt0DUZ+u7cTKHdZ20s08/JLVv
   Ys+SYP6OSwgngI+E0c85XOkREcp011QymxOiJT7ulUJHISB9P/NFoA6ovCYBZyRQ
   SfdYEKvW+0KpVsBLVdYEouJteWd1Utc6Hi96Ej6OS+WtFyV4YUE8MtDzLk1buy6E
   YIOFJiowAWYFVwNVw6JPMF0yoHdk4FIj/lEChCLKNUgL0iABgkYOBpSnxov+Ur9N
```

0V7FQtTJ6/d4szAWZbApUeFqXliOb/py9El/DOTGy6oLUnL/iGVfTf+Ajg5+emCh
44Ahob2UH70VQ0HrMT2GDMizGvgzSPnMk22PAYcePvREiu4wJk2tue48CXUkVhKQ
l47MUmBKnC6gDnyjsQLB7WZ7PkizbmGC3d6vS4N3CcopEyDK7zBaWppewVagIKd4
qOMn6Y9iKm0y97Doc/y8VADYTN/EDQvji4j8Sg8I95cx1VInn46YDvH6HZH2zJGh
4xUC31AfOrBVe/v5oQEHDcCjFZKa72vc4ieANqQPX4G2j0TegJG8JzxLnHifud79
d+OPxcxM8U1w28ybRNWkP+TiDZZQ6L6lCib82fyMcXxeUiGRYRAhSNOQYzblDBfH
Z1H7gMFaWfJAa5XJtJSpJHEstbiWVOrEOY/kNEBkmddEP54uT/bcxkiQs/f89CfF
K9ShqAb7GEmdQMlnv6rf3dTiG8GGNBsztaZAx4/LK5IeoYQUTSrkGFgah0qsQO9I
TaESQK44gRjCe5F9PXjpPK5zpZA0Ti0yBJDPA1h+v2zNj5PklN3V4V02oWCwG8vx
XwaF5YE3dKcS6BVMnxy3lARxKtp4MIZRXpgma6qeIL5DrAXDOLMoTqZA3fiNguuM
Vn/LIEQxpbxhGpzVi3jcDCthvzdVWppl+VfG58ydngch1PuWNfkkA0oEt55ub78I
AGQRhm/QMgYkeXOWrZelfpIKGUFt/WkmhMPpl04sRaJLjRIo+lKXV39TYrlegf/s
2Js4HRz4IIdWufUQHdt0mQkNKnssMIVI30Lloli/0R+hPv1sAc7XshfPzqbIXXd5
ThQXoiSsPBVTy4yHI5d+0LLsx3zfSA+Xq4XRF7bxq4xoaDKBY0CoZe2qVi35Hz5i
sPb2AHT9qHZEV63YZ55+pCmH5kiVsgrlj0pQo8QUzYjCbGq6XOw60SbBUHmf0//0
aHB++zb7IsnYHNeEJFCiRCJxYAcHTVWc2RLyfxJz6tx6GidcnhgDMqw/h5Du4X+q
3WTRxMfFJVNjHkHiD9JsNUNQ1liu+I6LREW27IHaxJ3urfJggpEv7nNZKoQ2Fwnk
Hinnc1Wc1ZXZBoXpos6zQkmBbxOO9ciJKPvfU5vhkjgO2Ja7eMnvaGem3xw6ubLa
dMCW8zT+Y7lOAY3L5jfW6B4wKt55c0nJELUDrnLqR6ITI+b4Nq8+MuPPGkvXIosV
umZ6sg0MWPQfoGgR0i0F80QHkHylMA9L8cTXiC4B6lei5GvTHfoad+7OIzD6ygzP
4ITgaeSC57pB+3ZNrjNn1T2iELlXZZb4sqxwxDf7mw5FdcI3R2VNGH2Hu4krCWqd
4yx5laRk45ChF9Ygd7VexK7ELSRAd/Q3AvkFAyj6oL8Isy3AqruaGzvLPoqQGrTv
uT8DajAOtfV8r6EHf/im61Dwtk2ccGuBoP3qYXJ3uLqGQRyXW5KrPEeq2UxlbSra
nDGYPQ7+OBB2dg4exQ6ewCBAs6HaX3fHsAKJcOFCf49LClN7yu7ARvXZ/yUaGaHq
irEWffl4IC0FvYzMv5MYPczJA+c8G+vJZa3qeBm3ZAZWFMZ0zdkjz9joE4Ox8syE
7ME2a9uBwneLHTx0GGORZsrL4NFxt5wCG09nj43civVgBLwbjsya0i0/RH+67lfV
jmsvZ1M6i9LzhPuvDKe7Htvv6/wJGqBSAsY3PFoEMKQ7n7+Jb9Vk+29O6Ivi5+Zp
SVwmHH7KL7Z7/73U5PSjmuGtyPlvQT7RRr9kqk7BbvEbdpyIGHLrMPTf02hIDc26
BsuVkZ0pDrY0AsUHvIaEZWugmWfF5Dub5osg7S+lZEaZG1nr9jn7ZkFyBynC9eci
qQeh17PBaSPLBeAFgvsfoH5ynBiJMLnuWw9Mmw/G+mw2RMEeV4wMJqylB5mP2hR0
OD32KWcDtxx8NPHULbFtiAZ067raGGWkWYI3iIeBYpqCSJo0bFxcch1CfK8VR/WH
YDFwItvBvQ5k/ntvniCeh1JaP2UwelVV6mafH7qrmXmvqtq2QEFVbVB+aBnRK2KO
uFKbXka+PbZ1b7311HxAz+xsEAe1UXlnKi+aASl+Qn+pS3YKyuH0zg19pOAmCf1t
5OhS7j+0DBgHYFajNfLb7lJy30MceP7gkj6gW1vHMKHRSHVOC0KlbMyQ8JAgMJUj
8yfO9qgbXWzMxyFxJvHX5CyJ0KHA1JfQNF1yl3Ml58jUHUqP9Ys2gDMPrJv6xTsq
T1tvxFLT0IiOO7WsUOyV4LCGi+wnrUk5dbhfwV6FhdZKNpfFnwpdeLak/2ccMMMm
OSZ7WBFFKHBmmWMfozq5359OgGE3sf7/C45x/9SDiIsfWQZusA25XiJ0nrJxwoho
5mN97+DUx5nhbKzD/ajTg43kSldRJFvtbDHC2nYaIl6SLXg6HwhCk6qnAnb4Fxau
3M9M5XZuDwXQ0Z21yjh4Yckfi69GUO6qK3Dgc9wugvmz2WI6lT5oE2Od/4HdTf9e
LNEWzR67qvyUy6tILZi9R3LdAN3HukfmJjXCbaIOUFtQQUgRgCEdM5NbSp3UhTZO
3trXdXa0lifRJ5VfsJmGUiaZqD+yi/p+sYuwRDMu/sSPaSCBf70OtxsLRrScJ4+B
yqg+AOUxxWYCH/A7kAQ5Bxyyj/HxRRH7KlJRTxTxZChuad721D84Y7OOFjaRAx5G
yug48Ls6jJugo48ce0zVZKDQYW6cAoufc+xz4BLZobqoIjGn2vu+9pIvED6+Bud1
p4wsgVS0fM2ZktBIM39RDedb+90NxvKw+VO9Gdo2XmcMQtig2oTMLkUbNbiPC5Or
diokCwEwSAm/+uXU280GhFo8zHwIMpcfzs88kKHCInrTqS0mNFnXm1bGydDdtMqX
Mz0c57+8uCrQvFAa9yXcY+dCIxMNj595lldBMXCVzwUaJF3ITCJ0Juk0ZJE784+A
e+MSqOBm1GPHya7f7wnAnEz3d1qZ5yFgBV0B4kcXpAaW5lgt9xWk8TZ0K+o/+R5S
4VR+wb7cQnYHQNVbMrPCF93Btqw0d9fFDkmvjxAfG8IyPMyuEzfSRqhH0qU/K4Y4

```
fbggbxq1520vax+foW/nQNKFL7Bj4GqLKTLdS0ChQxT1YnwEuQ0cI2oQ8zzo9fFC
AiDYruczd8dA7mPuC4FQrCQjNXp7fzi2GKE8rN1aC6/EsZGFZujmVq48+yMQ6Ufv
byymZlAhAbFXNJlQjQ98rkyjooQr1QIjHpFn6wH6OfSt+1ncOVL1DMRM+8KpPp9+
U+khHu2wKDtFoOhw1+1seImM0cuIxGLfBQ3fTlpl9p9PcN/Db+eMuPjXv1i/jPyf
z3m8EIOg1YqsSX9IulrvH6OhslS5FLSvxG+tT+9U1pytiijH8M1UHUCYRd5++yZ+
VwS3SlyGFryw4u1vH1CT3rUbYpxbVkk0aW0e1HFbJST6WvSkB4OdxYmha2HK4mKb
aOc7QFDwDveewOfOaEXiLVysKhSZusmsIvS5l/oAZDdeC+qmeEH9yctRIJS3910E
DkI0HpM1QEuc/abzIJx3/KmKMHmVKfbVvwpzuiwByvxkIv0Y/enWILBWXQWLzpid
h1AzKiewpDZesdXXCw2pRgafPZRrjuAwInpakuU6AuU9TmhHeWgRD9OtpleyI5Xs
VimkL81rcuCBve5dXtziFZOYj1TfG5VzWAiSX7tajl5tvlhSiCmQN9Yz8CusOfP9
r2kDAroyIts2OmukqRYoavOC3vZVp30vUaxnPcRw7o+0sOpbCWRQen7PVtT75vz0
7YZLrXN2fBhzx5kxnBPD8Ucv5t9ixepy0/pSyztdejHfyTCT9twNeoDKfqkzJ/Mx
HWy3AzlNpSuT4Brqjsja7D1QJenDuCqcMsz6xVL1DM4w+JS5TMiOejWuIu5Ck9ey
2QIQMqEdYmIRyC0zevw260WsbCdwPMmYInUwoTFifcvtC+JLZvfFp7LgzKa6XCIk
dM16z6kOVZKKTjUfJewBdG6ezIecOQZdKlYcjSPy8R1uEPvqc94MTJ5uTdbh5sum
EYIkT6h6DHWjfBjoCTYpbFavprnqXmOPVvoTcifkUemh3sOu9Hll0Oa8wtIAZp13
gVqQXS1ErvzF6Sy4UKSqAu8liM2WUSZH4bmW36sEBEOykXh//19wqHW17NqGHrgG
AVMmRB42waFaTLysx/yNwyrnpNFIRQoRKi9DgfFvDCu94Q/4YfWojNgcooYC5SAr
lSLt6sjIWSp6neP603RDOXq910mbrM6dF9JAL3BAUK0Pn5/+zaaVva5IWyaL9KsH
2mJBvC+WIk40v9k+n9lH0c1eIkJZDCHVeqfM/FEafdhD7teusBcvxDPhZVQ8l0mH
phcUd3u0GEZC4LOfEYar1A9BOKEYslCodnDC2cKT3quqtWvhwej9VttZQgGNOn6w
GLeOsBP4x1pQ5apaSKJa3kVl+Gq+zZs7A+tsl3Z2BlkJ3quYpBkW7/39KTWPniA/
Sx++STetToLGYA7UuVndESoTbHMgjGbSOn94taPNmqejT5aSL/v4SKw3nUGnIeb4
kbuS7CHdTP7cNpo3DC8X2xprJJ3ffZIPH1HvIqjTA27lgs62676XJSG7BIgIrBiy
g6jWTh5X+zG2dRcjTafyPSzW+jf1U+cVFlvW2/cZKz//ku7W/1NOuMjvJGbUbjif
1m5R2PkjvwAYiDjvV8QmD46Xyh9lIumO1YYpUKZahTC+K7w3qs9gWweP+aUYOL8Q
0x7RFcCmWKvm6+u2SOfctuYWd9e57R+q555PanLTReyS6FaHDdqpvuoxxrkPUBT+
gtz1nduPat0SKm0+0253AoFFqozyJpMiDOmEbDKmQO5PHAfOX73ZIiUxAmyHFyNc
FJQwYiy/BmQ3H19wq9/0aSmt3CK06ouUPvTBhCQmwuw24e7X2LxY8J1rOdOSKt+s
IGsp1dVMh1bmiCQE5i1UZBxoBHLMx46ahaMgcd28B+pCoRkRUMUhZXcB59Jf2/qI
z8EgUqGceYMmA6XT13FvGqkc/MGo9MWC/Gt7yXO1Asr6iWzd3wCty/Pd8emwK3wq
rWq3BzmsCqFjtdMlBF5juAUA6WhMc3Hfj5RwCGgHr2fV9M49uYuZziG+aVypIKwI
fdc+hL4XrM+XL/QfcV1lpQo9+Smt+iLHwblykdWRBPKUJ4KXIR5jJel93lD12zuK
dQCUerq3hDVwsd5WWgQlaG8Iwf4misPoAAmpZpbp09XASCK1C2dQr9sX81+3AeQh
TPQam+QzlsR9lKDHlm1an4F7k0t2+xRcZu+YpVocsYeBCzmx6FsKKFJ7eGC9wvFr
T/XUAdhspNbo2OlRQuy4ixDC8gNxMuF/eQoI71ecHShiSsB3pThX9Z+sOCqYu8BZ
3q2Yerkjrz+/Lnbc+XJgtNYErzK00b2Yl+wSivCvgs2CZwHAWagb40ycaJcp1rGs
SHSAyMEe3+9g2Xd9Y5UyhPCePnIFtfvThUUWDMBbl4NkTZhci2Q+NGhwSfd//i/q
0dCdTZHj3ucJsNkCtfW7DtIykpy6Vld5smayE1zu5WjE2EzfumQHHqkOrfCNBBbi
plJwXI0WLdVCJrSAUoOTlZbE22r4tJnar1DA+V3Jep/VPZ1mNxa5Dh0fseI4h63q
eudtLO5NBMLMQxz762u9uB0y1vuFmKOX0VWz2aXZ6jHmN0z4zuwrqbS6yHYqEX3Z
4NzaoFOD7eRJbH92yFb1owGjPsb7QcRykQfBhmiIHeNJUoja5xZdk9M7vX5ygB8w
AIk33yHYWOumHHFeSPvHlTTsNvLel422gDyiDO0fXmJfGAsauqcX11jNB7RI+HM3
HnXNeubb3y3aA1bl1djZxngAwOQ1Sr9aLobmpbL/zsKrFXG7/fiz2DmachOLJL97
PU1j9MTspdH8VtBXX1KFyOSQKBRoGtYmG/OK5gilSXSSevz84KJiZw1ReIMXCa77
8Qxgzs7bIccDSBVzfzxjFADQxFY2jm+g8mr5b17byqO5wiNlLaGyneQeGMsI6H4Q
```

C.3.12.1. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```


```
MIIUEgYJKoZIhvcNAQcCoIIUAzCCE/8CAQExDTALBglghkgBZQMEAgEwggo7Bgkq
hkiG9w0BBwGgggosBIIKKE1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeQ0KTWVzc2FnZS1JRDog
PHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+
DQpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4NClRvOiBCb2IgPGJv
YkBzbWltZS5leGFtcGxlPg0KRGF0ZTogU2F0LCAyMCBGZWIgMjAyMSAxMjoxMzow
MiAtMDUwMA0KVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEuMA0KSFAt
T3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjoNCiBNZXNzYWdlLUlEOiA8
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4N
CkhQLU91dGVyOiBGcm9tOiBhbGljZUBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjog
VG86IGJvYkBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjogRGF0ZTogU2F0LCAyMCBG
ZWIgMjAyMSAxNzoxMzowMiArMDAwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6IFNh
bXBsZSBNVUEgVmVyc2lvbiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L21p
eGVkOyBib3VuZGFyeT0iY2Q1IjsgaHA9ImNpcGhlciINCg0KLS1jZDUNCk1JTUUt
VmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRlcm5hdGl2
ZTsgYm91bmRhcnk9IjU4MiINCg0KLS01ODINCk1JTUUtVmVyc2lvbjogMS4wDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQpDb250ZW50LVR5cGU6IHRl
eHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIjsNCiBocC1sZWdhY3ktZGlzcGxh
eT0iMSINCg0KU3ViamVjdDogc21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNo
eS1sZWdhY3kNCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIx
IDEyOjEzOjAyIC0wNTAwDQoNClRoaXMgaXMgdGhlIDQpzbWltZS1zaWduZWQtZW5j
LWNvbXBsZXgtaHAtc2h5LWxlZ2FjeQ0KbWVzc2FnZS4NCg0KVGhpcyBpcyBhIHNp
Z25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNzYWdlIHdpdGggaGVhZGVyIHBy
b3RlY3Rpb24gdXNpbmcgaGNwX3NoeSwNCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5l
IGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3Rl
Y3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0DQp3aXRoIHRoZSBoY3Bfc2h5IEhl
YWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5IHdpdGggYSAiTGVnYWN5DQpEaXNw
bGF5IiBwYXJ0Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFtcGxlDQot
LTU4Mg0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rp
bmc6IDdiaXQNCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0PSJ1cy1h
c2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNCjxodG1sPjxoZWFkPjx0
aXRsZT48L3RpdGxlPjwvaGVhZD48Ym9keT4NCjxkaXYgY2xhc3M9ImhlYWRlci1w
cm90ZWN0aW9uLWxlZ2FjeS1kaXNwbGF5Ij4NCjxwcmU+DQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeQ0KRnJvbTogQWxpY2Ug
Jmx0O2FsaWNlQHNtaW1lLmV4YW1wbGUmZ3Q7DQpUbzogQm9iICZsdDtib2JAc21p
bWUuZXhhbXBsZSZndDsNCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTM6MDIg
LTA1MDANCjwvcHJlPg0KPC9kaXY+PHA+VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNp
```

Z25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5PC9iPg0KbWVzc2FnZS48L3A+
DQo8cD5UaGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3Nh
Z2UgdXNpbmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRh
LiAgVGhlIHBheWxvYWQgaXMgYQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3Nh
Z2Ugd2l0aCBhbiBpbmxpbmUgaW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2Vz
IHRoZSBIZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSB0aGUgZHJhZnQNCndp
dGggdGhlIGhjcF9zaHkgSGVhZGVyIENvbmZpZGVudGlhbGl0eSBQb2xpY3kgd2l0
aCBhICJMZWdhY3kNCkRpc3BsYXkiIHBhcnQuPC9wPg0KPHA+PHR0Pi0tIDxicj5B
bGljZTxicj5jZUBzbWltZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRt
bD4NCi0tPkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpD
b250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiBiYXNlNjQNCkNvbnRlbnQtRGlzcG9z
aXRpb246IGlubGluZQ0KDQppVkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFB
VUNBWUFBQUNOaVIwTkFBQUFjRWxFUVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBS
dzIwZHFwYmZBUlFFak95d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZL
d2taDQpzZ3J6ZmNxVk1wTDJqbzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2lo
QWY1WUpydzd2anYwWldSV00vdWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpS
VTVFcmtKZ2dnPT0NCg0KLS1jZDUtLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0R
OZdKzkJUh6HuPTQGirQwDQYJKoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5Mjcw
NjU0MThaMDsxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYD
VQQDEw5BbGljZSBMb3ZlbGFjZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAJqVKfqLwaLjj+gBUCfkacKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg
9r1mAfIDlB/wlbdmadXPmrszyidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07
k0sV+UdSNRFxrfKeoQEFXgOaGdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74
zFCWp2f1ZkuE4A6l41koaZXCN5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY
9VfVfcrv9w43GG8FtpSX+TWzB2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r
8A4SSwIBaVv4wPxAf1iPsIVKarUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcG
A1UdIAQQMA4wDAYKYIZIAWUDAgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5l
eGFtcGxlMBMGA1UdJQQMMAoGCCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNV
HQ4EFgQUolNB1UQ8gCkVfAEj8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfx
CShlNhpnHGh29FkwDQYJKoZIhvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRG
zJdYA+R9eBAuDLsatbtKtl4FzkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5
AQ/hgxLvLir3hEUV2Z3MRsMtjH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5U
zpEYPLror2X4P5uXxaP0LIZRzWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGn
UZROSvSYkGiWDp1JhqXwfDz8A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19o
WZD6YrzSWHUz1F00juyuOfQsqm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgw
ggPPMIICt6ADAgECAhM3QQV57XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUA
MFUxDTALBgNVBAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhT
YW1wbGUgTEFNUFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEy
MDA2NTQxOFoYDzIwNTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYD
VQQLEwhMQU1QUyBXRzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l
078oullsk4ASvSwjsCNo7sHUa4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6
uFh1mVpXmFxSpUByQ+950MFz/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEO
ls/gkUP2GxzymsO2kaYWTut3SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBl
fkgKN5wXVgkWFfiOucfCn+IQsaqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4Ku
ElnAtJ7BtZcsl7dUy9u9COgEykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8w

```
gawwDAYDVR0TAQH/BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0R
BBcwFYETYWxpY2VAc21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAO
BgNVHQ8BAf8EBAMCBsAwHQYDVR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8G
A1UdIwQYMBaAFJEwjnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IB
AQBziaI2p86poGkjd/4KkkOHG25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAo
cCn5zbzhW/JVdYn30UxfyrZlRAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoT
WgAkoqENt1sRxlcvb7HVX524bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2z
L3HR+M9CDr4Opq2JCkzP0Qhp7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF
07rNmT0TzPCVzUAuBlr+JJtzOKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSr
JNtjh+AqJ5QfH+0e7NSzNnEmMYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRG
MREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBD
ZXJ0aWZpY2F0aW9uIEF1dGhvcml0eQITN0EFee11f0Kpolw69PhqzpqP1zALBglg
hkgBZQMEAgGgaTAYBgkqhkiG9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJ
BTEPFw0yMTAyMjAxNzEzMDJaMC8GCSqGSIb3DQEJBDEiBCBllHSf7b+HyaqXmEwT
DQLFcyd845Y683fln5KaB6NJmjANBgkqhkiG9w0BAQEFAASCAQCRRSDM+MtNb5av
W1U6o2LxrDXrrIy7lb8Vw1D3gHSgEaeZ3ZvZ6OefQPh4OkHNy/oescj+rKZzcLHB
s3RZ9Tnybr7p3kawIEFv1DW3aiyXQ49gQyPHn2Nwi6hK7Gn5d7rjSFuzprWYACg7
hAVWBd4/prAE1mNMR4DOOXoPYZn+ggJb/oaagcbdEy3WrznO2n6TW6Eb7bBoUT4t
IrZRWxPrdP30T7N1eHMmCDNGSXt/fC9rgcRLz+cj+1czfU1Gf+qIxg05HyrVMrkL
+XiCEoOck2+pbpz5WFPcmnRXLgH2FMlSNWU5RwbRu5YZejoKBiUZNlUmlA08d5JV
U3Zqnl/G
```

C.3.12.2. S/MIME Signed and Encrypted Over a Complex Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-legacy
Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:13:02 -0500
User-Agent: Sample MUA Version 1.0
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:13:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
Content-Type: multipart/mixed; boundary="cd5"; hp="cipher"

--cd5
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="582"
```

```
--582
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/plain; charset="us-ascii";
 hp-legacy-display="1"

Subject: smime-signed-enc-complex-hp-shy-legacy
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:13:02 -0500

This is the
smime-signed-enc-complex-hp-shy-legacy
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.

--
Alice
alice@smime.example
--582
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit
Content-Type: text/html; charset="us-ascii";
 hp-legacy-display="1"

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>
Subject: smime-signed-enc-complex-hp-shy-legacy
From: Alice &lt;alice@smime.example&gt;
To: Bob &lt;bob@smime.example&gt;
Date: Sat, 20 Feb 2021 12:13:02 -0500
</pre>
</div><p>This is the
<b>smime-signed-enc-complex-hp-shy-legacy</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy with a "Legacy
Display" part.</p>
```

```
<p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
--582--

--cd5
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--cd5--
```

C.3.13. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10575 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6820 bytes
    (unwraps to)
    └─┬ multipart/mixed 2345 bytes
      ├─┬ multipart/alternative 1136 bytes
      │ ├─ text/plain 389 bytes
      │ └─ text/html 484 bytes
      └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-baseline-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:15:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
```

References: <smime-signed-enc-complex-hp-baseline@example>

MIIefAYJKoZIhvcNAQcDoIIebTCCHmkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAB4+rUywYwd5++VSpboCoB0ZnRSxJI2onFBv
klMu5xi3XKYXOMBoxnRCzqXrG5U56fnqNGN61fytQNYOuPTYzb8PE4x22E1DGTGl
+PreSLEb/poN0c9k4Of72wBi31tN9e6cNJI45aulpg7lsyfqR2Hh1sNUkO+/qeBv
C4+6xvR1zudZARFPFBVbSg5Y78mHBc6Eyeu9Dprv3sMIej/t2WLkfzsyZQB3ip6d
y7r4Hrl4nTn3NWf1T5PiLU7Md0iAXmXk4+5ZMVHguq/YAQ1X24Nqloih4RJb4+tB
JKvZuwldG48r7Xh3N4sDuefzNJyZruC6T6bL6oKIydOxbftbBKAwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAoDxdIdVEOaRiQQ80GO/7+zdr
XaL2a/LqIOQgeDC7+NarHKxIPGromx5GGs/0A7Hc1WmUUAEl26/3yULmY1RIQ7FR
QbfUzddUUlt7nSm3k4J9dVENgfhpqIjZYp4xqsmJNYYbBH0+GL85BMw8MpB3ndvE
d7pzGCHWYtN/7mPYmf1vJmfC25u3kkmkcuFWafKBCfai6fSe85UQg2G5Y/Q44tNb
B5Q9N3QbFysX+u5etKwnPd08rEL76BflCBhTu6gOaO3HodL/A5jGu8kg9CXqkSwW
vJ+tVggRQTU/Z7hxav2kDa0weKsCdOhSCPbKl4e9E+l6bc2QLg6GnIu2Eu+bYjCC
G04GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEMIDwGtky+IO9HP6uP4Udg6Aghsg
v/eTch+9+5zUIxYIGGJHR0R2nyggJcHXvA8SU2XqzstdG3b7AzrDoIRcKjqiCVSF
4iojFAqAw0A0rFecSokWgHtqL3DAw4BTlIc/alh7n4IuENIEpdX8wIE3X4xd9np1
Vic3K4eq3Er3WoHNssA8gazrU2Xinftqt15S6sCy5pSK7PN1kxWUUBp14lWRMFRG
iWr6IfyVm9By2whh80v7p/bRqC+4rwmIqQU3SuWzMj8oyrrmAlt+A3zEPRwwjj5p
hRAUVeAZwFZN7BVNtqGN34LFdlsLs0YXWXWkrhFF48nL97yxufY6eJt5j/I+L46k
2gufwjkVM8JNQ2LeIdJgBfJDny/zXG0Uim4OOm1G4VrwfoLRDgbidVGWYShiyYd1
azu5pTjhnK+o0tn/SQ0y6wmSwUtHry5zAAI7oiMoAfQOvYRHZ0iE0fMUw45dW7jH
COFSIO6nh9ieAUPodc+Br1o+ICvD2I1VGXIEtUk3/nC2iXcaMxvAUNVN7f6YqM4H
0+ABTX3JUYvw0GvPWegMRZUax478CqIW6I29A8hbJE2/nA3YEv+TiRggBFKfJKS9
9CgLD09e0mD88+NZRW8Xh1UfGHg538KK6mZT6NooBdT+Q6TghMDsxWHfZGTMpacZ
HVQ0IPvC143eODBQ/dhI5ijA0teab/EPV1uevc8ezHKJymBMX+VJnBf7D/IPygjd
c42YtLuW7Gon/rWkhJiDNwJ/YUkUUSnRI3JKGqfuxQ5Q5nIfrQFziRKTHEvL3Xir
74jR+Oj5HuLVRhYV+uA3+DD8dwe8EGu+HPDfmzGkAWGWaLtrojPlyrzcEs12jPMq
Q4dpFTfEJsKV2vj0MkoK6pSmPYAcJsaRKyVykZwILOZ5O46E/wYZ+JV+bB7vgn91
7u+6ocEJbeNzloIkpkD56vDPEzNTDs9zGOZdA4q2FM31ITK/fdgtznQuu1/0FY0f
5O7fhnUIIfFGkEro0Fm1Cq4FjljsJIQF8zeIn623dFfW5E5wicuLXBWbx+lVlcI+
854RcFUrAjK8C0xUlJH3tK/DK3Pee0QVi20wbcdYWBYQ9mGA2kOaJO0c4Cd9fg9V
i1VoqxwW2RO3SBAilYBmZOQEaoyOTLjvr2TCK1LQQFv/rCi+Mv41ggF/9KAGOaFA
8b2hoYDWP2MIZBbZMlp+SVENRVmjdV5ok+NW/nFlC/eD75BH5AZyzkatfE4S1oXj
Qlyle+fGzD3ia0xuzOi++PsdU/7SRXefnJog1hpKormrLE4WACamfLVCFPiEepPM
OYCiy+2Yie+jRTEiGw5gSP6GLH3Q8QDPX7Ycd7bDTt7Kv1rJ9/u6nM3N72qfU0sO
KwDQf/b85KgbM5Dl1UWBG/oWmTSicq5rfKRknyJIUulfk13QxmYW1yk3ZSPSlA6x
opMhoGLOk+BJsmWWVPYuZb7X+UbpmaqPAX9jhezzpGo56Z/4o6lK+ydGs2IBMR4b
BXGozhRp+tTw+FV5NeZn7BbjgupRrMkybLP3ihAiMPpKBjl1+ZWV79SnwQmsRrmV
iGeLd9rH4A/Wp4Le8M88ZbCursTbGMZ7AcTZved4GdNFi5tAzieyUfuOgeQePKSR
GiJ8cObCYK23tDzBM4czpxtoT1hayHIgeRrKzE8Ve6K6fd56Ycaw/AdnB+orIpc8
ZC7yDKC9omlIYhs+v4iYpzSeAllZ1EMY/PUcAKMGpjj32fvdZD1mfO+5GuXSis4q
mpr8giCDhPCs5INWBFyFVAy4dXJSszOnfptphOBM+DXgU0opZzi46nRyDK4rH1XX

eAJj5Xn4vA8rMoiRZkzTBanMuDCMH7eBftzV6tE1LwJvGpsOtTsluYmY9CK/g6bG
AXNi3DZF6r4PYsSvhA4DvODVhu4ZyYuavo7KBwp+79oz9/oR+aWoQ4yyPH66tOQ6
v+PdlZ6j/KmLFDdZkGND0+4xJqrf6L2MIe3K+GFfuCW+QB9zu+prW627gFnL8EeA
M8EDJI7IYoCqcc5pjTejeOEyVTOjhxaTtbqKkYtvidDxQUYvlxVBzGClv/BuOhGi
8HntDWHPTHFfDvKeWJ44vAMATWzWtlEoAyMtpAWboN9CYv19V5GfwSdQdYEQTC8v
VAXvf2ucI7RFQI28Uv8g1IHdh+oHNq9QsY+d2ItswzJKRhbUU1GX9oXrR5snKTHJ
ZG/loE0tOzgmXX8AEmu7onPtAhF0jrnJ68EACVQpc4vWcJ8x2FyFwfUQTmcbqFPc
YUIDyZLJ1oV3eXPCSTYBc0LCFlkaaz8XXSLOEwBBcmvu3X5enPi3ac8LdPH7vjEr
ZvbbQHNgzvX/QubBGpA3gYb0sKMv7tZtoQ84ZLvPisqoNwzETQRRwljoomekk3Cp
gSLSy8xqc4Ip5Auf15Bu3VMp1J2XtFphfSIao2FYXkliiATRVCfV8LsKWWyfOYZy
owJrYBtJ+S0kRK8X1Lc9EYpBTJ+evNXjHO2t0S6B4j2y6VFePVplzEXWn377tZzu
su3AhwlQ98rkaZYHxCTS2klFlePjwJLUFmL4qly6jBBdGjMMxZWsgn/MMACJBYWH
qbhCvcxfl3D6AhED40/DnN57yh1nJDj6nVg8tq2KOIocom75nXoOEOmM7kSZuwIS
dr4HhRk2ZlzyPX3rrcX85VMGUjPaiI4/E3l0fWi0mk4ZRAih0fM3IfMFe0Wdw2O+
9umTwAvIYggG6ZqEiJz8uKpZk+0pqxXkaZlY0h203KHg3s1BKcJbfZOPPZ6tfex1
0Bs7B4K3z9swIct1uqoVF7rHjZ0VOINkLT38ixkrkk7/JGPwXyuwVBZP1JWJRtUu
0hDZUMXK+B3tD8W1M0Lq8tx0MSBPf3BIP8ttWSYUlc7IQYGRs52PoMNApWw80Vty
mjDwKZ/rS86T2wujRG3AB0hRIQcyMXi42dWsDSHIdzjexOILddgDbSMJiW2Vneg/
OEZ90WUxSi99ewLiB8Wjlh59942xIootNhKujfbFYgtUAbli43mXXqOzpsc5VbVw
7c5HK50g6C5TQDG0aNYBqutP3d7df8abe1rtsZBcG2mfh+Pxh0LtsZrTziourUtE
b3xnh2EkOpudGTuOCjAkyGHIbMPhkXpJWoHojj66F8iToH8jL1eTheBnWl/NWQ3O
U/1jquVs6a0GbMImg5/vxIIW/qnozyDfrwsmFSfIhs0cNyJ6pUSeNMYRVUEtoK6n
63DX9EQ0Bm/rKZhaznxHrH4u0b7amC8uXKHEK39JZaKg0gUNpjWXbVkJxBlNtORg
LoBZzt4u0JNoNl3zdDM+2/+JNP0Gq90SO3SkAY31InkSjSB98OBJY6V+f+02nPdS
QoB+DFXtAk5EV9DYcJRFI1wCLCIhGMcy5n0lPrjucaUPwfbFd3JDkk7AzNtBpQQ0
W/BXtyvT6GFvWnc2P8cnKrXvGcb6YvN+i7mh9JbIC9rIl8x+iM6oXE9c7Xxz1l/8
R2VatyR3S7v2gj5X2hbqz1xgZHuX+ZaXm6muozmspyM2tNMolYpvpX/kmHN/RPzN
vza7XzHXcZdqNWwHKub8Tl/ZIJeA12MMKDRpERDndaR4j0iyqZTMU8qCrtPhmmI6
A51LjLkN6Vy09AWmAEl35H+OtDOkwqE3E6DHgS8znl4oBfY+2+NtFdQmCKYF/EKr
s8NGezoAtPxq0Swh/crfgmfk3oOhv9FGM119qUU0LAMy9nUKv0Nsci+70cBR2Sus
WPPZJDJW12F8z+oATPT5+XjEsGzm1AcWSVf4PG1tlSmBPn7RWmSAE74T1Eu0EvfX
4Vv84/BLcTo31H/caIT+SInxeDAON2aFx+gNRteIo+MMQeHNU1C+iHZnZs6ye1Vy
ySJ7X2HijnisxBMkM0l5zJN75KdDpQrZt0c9/ko++AGIpYcSLzsyxL5PuQTAXWGA
1ioCI7A3icYsSly7SLUZQXAFMcV6xVXL4zx4ACohEFgydA9s7MNnuYg/DC71qtHJ
iWtODQK2cnP7rptU4R9u8524AwrZbTpvaJeaXzZ5gB57ziN9JFTNicUWf88UkJcc
Zjk1HxtdmtpP4kqiT8MEJQEY8Y4Q0Trn45GazsZnfZZxXxK2EC0w/Mj7/RJ7mCPu
SEOYDfAu2PtDh1jW1JjJv6AeqosoSpPuuvRZt8gBE38oKiHlRgkKRHdjEyVsg0yj
eD7qVk7DzYz+sZhRQyiGZY+p1A/hItQknAFbLiSB6X0ZCIml/+n0/lB7hkDSaT7X
wYTKdpA1bCgB1/9z8WAUwojaqu2wCDBG5wvKZsfeViSloxVgxezysvJCVFiHdgn8
8AuYmkph9MrjRvM6eq1bDZWQ0Pxb0kV15obEKTLk7tFbudaoEmYI0sGbQ0LWGRCD
DEu6sftmbXKQCTvy3HjXuZbgSt89VZIFJVu112qU4XxYPWC/vasCJ+atAgQk5Cn+
CD7i9psfPE9ENOnMdxCDu6GHkIYkYpY54dpKeRMKizr8vKrMr04DM+VON5/BgePv
AtgIXxQuQjlchz9z2/AEJsgLnd/61jv5BtJt1FB/mMfmZqRxi4ezRnK9tSiMLLDV
Y6Zj4qmSZxryosNvkUiq3X6ic0rCqlc4z17cQN5lVKJ9k+mb6MDpDUXsub11FnJb
V1waMVWvpPBZyDmrTB/Rtiinzg1p6kNuoS92Di7yGNpZUQOjxf75wdXLm9cWVtDM
9xlsBIPiTtIzyW+x+iYIBuFQLth0g1evYXmUZ4BV90hM3ysKH467v7VcdIhpJgrF
KepFhg+942rWXAgAe1aFEhq5bBgUgydqyJ+N5IIZUunphdodrNgSWI7RHQJfWktX
yi+BbcsWYWYxvouW3UIAr24OFpW7/cMPoRw8w6tPvQ8PCvVfkeG8Xxg/WxiVtpuS

CIetAqBBW4MI7C0icv9lTizUM81hCrcUOdcqtPdNUOXQziGqa/CICFHX/4sOMP0K
UMbP5Q1Y840283qajxk7sVEas4PiDaA1feIn3BhMwkaPXfleRSlvcO779SRhc2Pm
yBuc5UbfgSaZQ0gL/WsZUYLk6VAt4bbO62rntIn9dZTacjRl3uPQtuNQ4brG6IM6
08sfFERdIwRFVxSyT+chE23cMgdCszZ2EwpkDbld0ntdKtKd52FGEgvkfT3gYuDV
XyZc/17Iu9r6kD2M4/dn/W2I9vmBszc+NhXhA/fE2+X6pZgCyTFmbkH25Q3nDDjz
UcbjAmvMEGVI90Kv1kp6+qIdkUCkAAjigA1p4X44JSYDRjSovIreP8CawufuA+9G
vJ+5AyFnexRk4yCGa+IE5Rt5uTctcHXb6ZQKel61k6WLZlLfJ1wrzUObjpcEgNS3
PJ07n6QkxiBpqwnc89mAJOOrSAYxGe13vHpT48kX6CHdqV+LDr+21MNlBMlXBGXI
qRt6X5dG7zfhNCoGQICAd3yj8kGW99VhBBc2QZvK7EUVJF7LAqbfzS2EnZ5G4al9
Zq15tnQkcJzuNOvwaUkQAuGFri5e2LRJILklwskqJP/aMUaXU9XLff+n/ld4Gzp6
m+fgDU6mmkhWasYJtjR2UTdtu2VB1EoIOirhohnUyfyaFbqOkEka+pl6+5kr7ds9
fAbTJNdVjyC0cML77YWqBndfS4k/vs8DteMnwgE8VTZFc4FHBfRLD6rUzxLKkLr6
6tFOWbpHlXnmo6oLswnQBucyLUcZXDZ2PKjSlHbpn3o6FXSdUPTy0qt+g/a7N8q/
QC15Fs77G9kc+dLpETXCUX80/HO87v/74ACcFenSeGAWTwK3gszbmeyvyzqo8MZ6
8xZxoPbf2kglMS8Bbn50DDgU9lG/5Vst70U5RvzoBiHShBOQLNTuYn5dZCaJtW3p
U5StAaVlCoBbdvkCH6U9lGuSoEV+fpplZN/U5vY2PntEhEiUcTwTIHTeeJmpXAHY
KrwT/daJNS3hA1EXu4ZQIx+98lEehhkEqZuXhm+F6AZWCe/NilIAf9YdYrI7pXxO
Ec8jn9roFOSa2X7kDWJ3UrBjzUM7fmU4ypPi6vHlHF4RD6t+IOmAPmkNiMddOxCg
DpEVW9CjMCcZI0W4s+bpjIjwWM9j/TSyNrMp6EUr3QChgghCdVvN3P5WVjtDGZhU
KNWz+s0pB7zMEj8MVeu5RzO/E0J9JXyELJkMviqCRfAmqJ4OekZatX4ZJNYIdav6
C3qVaiBcumVHoQNMAAQy2LkdV6yDzPchMc6umzCeeyufkGs4RmWFaVietjuE76nX
fGfsVjcg0Cm+5BzYvCKmN/xEEYtMjyElByLzwcDvX/nedsZV2pyuggYZqjcC/qYC
1sHSBNjgVWQinYDEbtebj6I4i/0/0eRv4vfcdE7r8mFm5Ukx4JP9MJFKaNQPWDZ2
cyXZsH8/i4+/u+P99onw1y31qdpcU7Xtzo2UKpdNla4GjlfOij7i+Tuf057/13WA
XQBcvABU0H9l0zDNiCioY+A0+qHOWgS95Qgzqfl+wwEZFTC5r1V2yqO7eePrWO/M
Zy0HdPVUNmEavV9CZ2Cv8KQ+atL1uLkw24jNHYf2Fn1Mndb2+iSX9lqP2FfaHXbh
XSzsMcvxj55iA1mlBAFWoHR2yhJUJS+UtB38VxlbyWlrmUtZup61i9wFo89trRx2
S/xfeR8pdtg23ZutvETVfjFmNNG7w8Yx1yKT3gZo/eG0slrY7hR/WA2nARc55fAB
ELxGuZJp2H87J1noU/4L64IGHSNS5kzyStSvoihAg8a2bmV2j9FDBW2yUMdqUiXO
opb2fcM0J0F0SECNmz4n/EDzKlZjJmw8daMbElRVZ2Fz6EoUzmmYQG0BLeeFz37l
Ei0bjuKJAlaUpBfosaw/f+Ft/PUYlpJ5hXPFv8qJ+bpmHF2ACNPyrmYDJ0lTzvMs
Q0zDJUZsMSENb24FCR6eMLMBgA+Uh2ix7FafPTqx1p7B80F/f3royH0NgIHzkm38
SYvwLs6MYKlioM7+wMU8qDOYweh1IgR6oBDqaeC8lrFHai7c6h67QgV2qDlajIyO
ejoTbnWuRDmTrRdINTRpne3SQoKalSzUfARcbuWoVC5cmxdL+wlYT3PM1mWZ94cW
XNhGFb6qcwBtK5PWxxwIj6RxrwEK2Z/+EfWHHiqtHT8Ft73gILqMYMce0ve+8Adx
g4JBn/pKvTaEt+n0/cUJlN1zk9Cpf19ug8y798vMD4vQJ8Iv9xk+zaNZ4SrRVvZC
jbiEXAVuwkGzIRobUDC4gE/PnnPB6hbhJM3dSbHhf+LaZfR2lh3f4anQbunn/sDh
ohLXkzDz9K+9RN2P0uS+0M1IHnBqX7vHlSUXpw3s0l8JVEF8gigXF5GV7F/EXWlM
2LEvrVjXI3OlVHSbhPogCD+98smaAnIUuBQ7Tr+0nSIMKZ4Bct8jyx3C1dlZk31x
X4VrEMLatemExIVkIqk7VC9a+U8zV5vpyJO1SDJo9Bm/mbxi0M7DwSbaxJrOURPI
gFJveIetLrwTNeq0auBcuGXjyQVdNQtLIXydBGTzg6Rj9W0/yeHQYZh8IUlQB4It
TBTniPTYpfUiVe6acfDDKeESd+S6SH9ZNaXnZBTqxpJHeVUBtFnplZagjlZiKP9M
0CRAycswHBfIT9BGIr4odnvOk9aWifBHDqjGJ4XGaiKSQZ0xuZRZdEPyoRg9FsAA
mlyMF+JdANy9hGdbStDS3ok2tKiRPzArphUass9P30Mrp+hphehljDw58vQxyIj2
rTBdv9G4A8gE37hn1A9wo1mW0E0K2nLl/CVPNZDlavLTWcx/RCLUgTtgTvQsERVa
CktsA9Fd6jUK2bqZIcvS4lRXRHyWtLRQD/WbNR6iGFq3ou6iKSWiOAuwmMgfcnsT
yREWaTY3gs1eIHCRMU1qfxz6WecCM2DpgEQVL0cZBDJNB6d2MsDjkcGCrsi9hPda
vPDNKMsxAAfkeUT4nQ1FbkGFN19wfMvHzZdj3t2nv28ORyarOMR7JdZy8uH9ZC2x

```
MBUUpa8dcLqfCsIwfMqHSmHwoE7avo4B+j9gaFbONyUrpS9XivPaR4C/VdpvmEx4
uPCQcON3hnxts4H0Bbnxr567VRLH9M2lh95uURXg2QroDNXBKibYNLEXrGnsuR6e
G1+GPxXVk5LB3QavktPU9UUnCTU/yh7OJUUJC7LAIcOkuQfG8W/cVWa92dXoGFIc
sePH1GM5AmG3EkaeXItR5gT2gG6S2J6WfarVJSkvK2DL962V5btA9qFvu85hxjC+
/XcucUlbcEPixrv0ZfXeKeykOk1NKKiJ3bVnGZpQIql/dT1LxPFF9pEDQMOtucec
cuDbVmh691nt5Wx8Emk09BXRWOsxqgS9Rp0ZnYl9/0CYwJWH178sfRfuZvCG4Lv6
bd1a+A80hEshOhqZxXEZlrSGNSVw7jIN5CIXX0cs62UKsx/+PQQIV8RQZafy2vbz
N7PN501YdbE7nRjIMGMRcs5tibuukn9/HRY4+NsaLik+olW74q1EHp1N0gtRBiYM
wvFTWnTqguogKEWb1RAysycPUuTV8RvnGN95y58c4pnpTwZRFw8rhGnE0VHSTVq8
6796GuKYcExa3RoX2PUU4FDpufq0kfCRlWxvuUM5m2lr73TA2hb6icXhsNJ8OEGa
AfufQi+RH93+6UFTrmWlsxMhRxR2NpWxXNEB/7tkyjpK5jh+oN0f279PapJ3FfLO
AV7phEbm4W0BSBdNJmnzLQipGKzszyTd4XlgaXB2HqxFlWbKWJdAdHkFK8faN4SK
ztxxOBngAlBMdPtxEi4tev7S93SFKoqMwY18vHlLOHi/oFpaWMjJsE4uxdqvtz/x
aeZMmgstD1ZYRykBqGzjm8cMeoQawJ9HF6AkNFPo9+AsgXCuPNhutGZuCv3vAWTg
yXAiMHDuzahSggfr7r2ixkDUxD12/5RSeSDvCkeCWsjBKVpyzoWn2QksAMBoETyN
F2gcjouX2Cp+OkOQV0e8Y6zIOWE/SGUkFkUDRJUSA8gkpfXWDPV8MN6rAMULWUGP
jYcRtabSgnlXKn6VivRiBlGXvp7iOXpsoGtMwof9hUcoo/HYMAvdsd5anaIZU8tA
g+c+8OHky2OJ5mzUWmk1CcBIWO9yyAHsy7ivSVzJtxDuTrQAuuH92MZgyvGnoioM
uaKOwNzrmhAAhBruv0XpMd/RBIu5+e8EM+fIuYwwwYDWIpn9vMbkKiBv4h5PQ8+T
cunAwgNdg0qVFeZ96Gu1sIHttbexEvSADg9fplx7TG+DZgSrDkxhnJ80a0hZhZ2F
CYJJrvEcQn+/ItTftmmV5tpG2r/LCufYFL26h0RXdD8=
```

C.3.13.1. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIITWQYJKoZIhvcNAQcCoIITSjCCE0YCAQExDTALBglghkgBZQMEAgEwggmCBgkq
hkiG9w0BBwGggglzBIIJb01JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtcmVwbHkNCk1lc3NhZ2Ut
SUQ6IDxzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtcmVwbHlA
ZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxlPg0KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZlYiAyMDIx
IDEyOjE1OjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTYVBIFZlcnNpb24g
MS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1i
YXNlbGluZUBleGFtcGxlPg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMt
Y29tcGxleC1ocC1iYXNlbGluZUBleGFtcGxlPg0KSFAtT3V0ZXI6IFN1YmplY3Q6
IFsuLi5dDQpIUC1PdXRlcjogTWVzc2FnZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVu
Yy1jb21wbGV4LWhwLWJhc2VsaW5lLXJlcGx5QGV4YW1wbGU+DQpIUC1PdXRlcjog
RnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjogVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpIUC1PdXRlcjogRGF0ZTogU2F0LCAy
MCBGZWIgMjAyMSAxMjoxNTowMiAtMDUwMA0KSFAtT3V0ZXI6IFVzZXItQWdlbnQ6
IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOg0KIEluLVJlcGx5LVRv
OiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lQGV4YW1wbGU+
```

DQpIUC1PdXRlcjoNCiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLWJhc2VsaW5lQGV4YW1wbGU+DQpDb250ZW50LVR5cGU6IG11bHRpcGFy
dC9taXhlZDsgYm91bmRhcnk9ImIyZiI7IGhwPSJjaXBoZXIiDQoNCi0tYjJmDQpN
SU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvYWx0ZXJu
YXRpdmU7IGJvdW5kYXJ5PSI2ZTgiDQoNCi0tNmU4DQpDb250ZW50LVR5cGU6IHRl
eHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIg0KTUlNRS1WZXJzaW9uOiAxLjAN
CkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCg0KVGhpcyBpcyB0aGUN
CnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1iYXNlbGluZS1yZXBseQ0KbWVz
c2FnZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVk
RGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBt
ZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQg
dXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0
DQp3aXRoIHRoZSBoY3BfYmFzZWxpbmUgSGVhZGVyIENvbmZpZGVudGlhbGl0eSBQ
b2xpY3kuDQoNCi0tIA0KQWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCi0tNmU4
DQpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNjaWkiDQpN
SU1FLVZlcnNpb246IDEuMA0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2Jp
dA0KDQo8aHRtbD48aGVhZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJv
cD5UaGlzIGlzIHRoZQ0KPGI+c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJh
c2VsaW5lLXJlcGx5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD5UaGlzIGIgIEgc2ln
bmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQpl
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMg
YQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVj
dGlvbiBzY2hlbWUgZnJvbSB0aGUgZHJhZnQNCndpdGggdGhlIGhjcF9iYXNlbGlu
ZSBIZWFkZXIgQ29uZmlkZW50aWFsaXR5IFBvbGljeS48L3A+DQo8cD48dHQ+LS0g
PGJyLz5bbGljZTxici8+PC9wPjwvYm9k
eT48L2h0bWw+DQotLTZlOC0tDQoNCi0tYjJmDQpDb250ZW50LVR5cGU6IGltYWdl
L3BuZw0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50
LURpc3Bvc2l0aW9uOiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FB
QUJRQUFBQVVDQVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzcz
OW5PM1RwUncyMGRxcGJmQVJRRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDlj
aWRrRSs2S3drWg0Kc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFm
VFBSaWNpaEFmNVlKcnc3dmp2MFpXUldNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3
QUFBQUJKUlU1RXJrSmdnZz09DQoNCi0tYjJmLS0NCqCCB6YwggPPMIICt6ADAgEC
AhMPLSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMg
UlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIw
NTIwOTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzEXMBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IB
DwAwggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D
9zFCrS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs
165ernT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZu
TtMc1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDH
dZ5qDTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy
6SCf58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/
BAIwADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VA
c21pbWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMC

BSAwHQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEw
jnwHFwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBak
DKU68ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdao
x644DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Na
r2inC0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtl
uLihne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK
49+qYC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vR
hZjVD6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG
9w0BAQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8G
A1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAg
Fw0xOTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVU
RjERMA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIB
IjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTk
fCv4TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DI
Ls7GxVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TC
NO12DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7
ktkNBR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTM
SiPR+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwID
AQABo4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATAB
MB4GA1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYB
BQUHAwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDT
IGZmczAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0B
AQ0FAAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3Bj
JOd64roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIj
So27PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9
cy31wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4P
GHnYxs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+u
CDgNG/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UE
ChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1Q
UyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6a
qdcwCwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkq
hkiG9w0BCQUxDxcNMjEwMjIwMTcxNTAyWjAvBgkqhkiG9w0BCQQxIgQgzz6zrLzs
Pn86IlgrGm7Fheev5QucTU+VJZWxIIrBFk8wDQYJKoZIhvcNAQEBBQAEggEASITl
JnQGy7Cb5U6BdSMX3mnksCOX8mvaxy3o0QqNUbUGhNNPKI0LIWOdjHUL2Eq8+99Y
2+WvVn3ZkAJ7KF/89ja3u4NTiwu30wWsd7DL7t1z8DJBK6JuyaY4xtohUPVa2gL2
1atPowCt0X5RF7lmihqZnDGGUAzjfLpVsFnyIVAL3QG4/vW609d+aeO+ccdwzzUh
lE03h3qpHK9wX5pWBNZCfdmjdXUFacU+fMe1mG9I8A1HMY09zj+rNz3onoIHJWJ2
FBWS2tqK2eW8yCf/LSq9M5k86VbTjPjvjPz8FqupzugC5sUAx2JMUfUOq4A9hW+j
g8PEOcwaEeYOMdSeKw==

C.3.13.2. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
   MIME-Version: 1.0
   Subject: smime-signed-enc-complex-hp-baseline-reply
   Message-ID: <smime-signed-enc-complex-hp-baseline-reply@example>
   From: Alice <alice@smime.example>
   To: Bob <bob@smime.example>
   Date: Sat, 20 Feb 2021 12:15:02 -0500
   User-Agent: Sample MUA Version 1.0
   In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
   References: <smime-signed-enc-complex-hp-baseline@example>
   HP-Outer: Subject: [...]
   HP-Outer: Message-ID:
    <smime-signed-enc-complex-hp-baseline-reply@example>
   HP-Outer: From: Alice <alice@smime.example>
   HP-Outer: To: Bob <bob@smime.example>
   HP-Outer: Date: Sat, 20 Feb 2021 12:15:02 -0500
   HP-Outer: User-Agent: Sample MUA Version 1.0
   HP-Outer:
    In-Reply-To: <smime-signed-enc-complex-hp-baseline@example>
   HP-Outer:
    References: <smime-signed-enc-complex-hp-baseline@example>
   Content-Type: multipart/mixed; boundary="b2f"; hp="cipher"

   --b2f
   MIME-Version: 1.0
   Content-Type: multipart/alternative; boundary="6e8"

   --6e8
   Content-Type: text/plain; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   This is the
   smime-signed-enc-complex-hp-baseline-reply
   message.

   This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_baseline Header Confidentiality Policy.

   --
   Alice
   alice@smime.example
   --6e8
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit
```

```
<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-baseline-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_baseline Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--6e8--

--b2f
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--b2f--
```

C.3.14. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_baseline (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_baseline Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 11205 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 7278 bytes
    (unwraps to)
    └┬ multipart/mixed 2666 bytes
     ├┬ multipart/alternative 1419 bytes
     │ ├─ text/plain 478 bytes
     │ └─ text/html 638 bytes
     └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
References:
 <smime-signed-enc-complex-hp-baseline-legacy@example>

MIIgTAYJKoZIhvcNAQcDoIIgPTCCIDkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGfiAnT52E4dOn3GCoKxpwxZ5jrJBpfmph0+
ue/FmZEv5klqdljABwTObNZZ4JUCbzv6MLOI1Xmn+00SQ8JXpX4WiQhIEOuejfcI
ksFg9SyHfxsqmW5bh9b2VvTC3mXRF9O+4bEkep7dcp60i2X33jw3E2rocPl1cdY1
CKYcOcUiIpf9guS0JPcenBq+OGJHjL7o3HC01fNJPc4XtaPao1xJNAN3UwOTrHNL
RGwkgtyG6Xw1B0U1+Kn/T/rkkUgqqWrw+K7nX5WtPUW1rQgFoUHJUzZx/fXMfeOe
wWrybho46jWISNF+xDiuR1+A4188E/Q7+4RJVIHoJCa3box7MEkwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAcq7+FdWfup7R9o64oTMQaqu2
Zj3DOLonCZ92tFAySyaZY+bCvA6/vLs5Et63c3ETWzFP7HUYnFjBDOTsgrnZAzez
bDsg3XVZGWf2vCYhEDe1RKchq5HlPPEjyg5Pj/HE2p8P0BGidOmsj1nSy23FWM9C
Y+Y3fhXtcV4qB7g7FQMmB4bghxgouiPVE3kt7wCuPw6ekuOWe+GnrmI8qoh7aFdz
ehgq2K1IAO9UXvNGV0r7XIN+w08iVxM6DAELNqZ9dVNZ5fpzOSsIPvGNCZZSrOjU
Lk4+6eyHo/5qLXDFhESGRe0XUe6VSAz3hN4PgOdsyoA02/emgR977VDsavjeVjCC
HR4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEELNpzmwBEJh+gxLdI2Gm1ymAghzw
mLnjPD9k41KZLVG+i7LyAI11h/fYPRxpnRjsm1Z2xWhHKQQmcnVFHf/kyqZDc5fI
Ud3SenoCrxO7gLELALwfH3v065D2ETNIshz/KoujlxswSettcE5LRBDsTeNwRgl7
lxSL1EjagWzAWN3i98C0M2xL679Z1RLVB+a2NjzVhDE/NktouFBQSq5qtlzvCByc
dtBpo9IW0w/COBfm8tuzR+Cs2uanYx751Ku/KDyJfnEl+mDaP65pI5ooKrMcazTX
YLzjwwDi+idhdZxucwuWj977fBe9bQ1R5tnT0jKuch9hTB6KZWAUNANINEA3SISJ
hFIf+bYE48cBaFhSMU+2ccl6qdWFzJeut+F8MESC7xpsZfoeHC3nXXcGEQ+j3UWo
Qtd48yP3mlx7m6Uvd4k2JPaoAu+N3uZhSJLwgePW/J9tMix+VXsiADBZSrV03nnH
Gd8QCyHZKAC8QBefhVaRHcxfFVmtT2Ru20tKZQN7kevlKSPkpFV1u/iJfKFUfYnY
KoPGrWS5HbyD8ap0UGmVHpXjwcmA6anerktkdeOSqohokfQgU9vOGP0DjtNOv+zC
tu96SSm3aEA11wefb1I/9NiAwgfyFdf1bTJEUvfMXERJOCWsfGhyYEQy5LAxq0QM
p5R75Uob2D5CaNof7Uyr0o1zY8aadZ10qQ+NXmFCQx/yG5nrMgv63By+gkgb4bbG
AuamBjdpJ3EGpJ/SMdl9X4vVZOIkqrJ/D0UeFklMMCbsrfRlCaB/OWc5l5wiHxFI
HTXRM8fcq27KCiE//L3OauQkBI3NaP2t2EuBvusEGtCSSBUtb8t2qZxW/PS3OS+b
0Ko/wnrQmoVxC4CqO6ZBozVs/PKZUE/TcWSX9PhRUcaK3236Co1mZVrajlFdcv+D
ktR/Sau12du4SVYez0MKTc0A63BUWuKNHdvI8IJueStL5BBSEWnnjnP7DRj1vvvF
```

```
mEIKebxZzeAcqwhHNbrurjazsQA9GXXQElXm9gWvMg+IM0BH+MEpmUzQis81mb3w
ghPeVB9U4RkGt1OYKcxuR6lQkvXzhfU5ePsVeTzZbWVopx5wNrbb28yyUdG3uobO
MuK1LCeutlRSYJcB4laeQGKEnMhBnxTAlKV2J9aUionWOKcjkPmAL2JfjNcBnUDJ
aUg0UblNss8X7zHhTpinKykEYPinab00YV8g1m3lkt+uam1Msn84u9TSK/a1V35C
qs2jbbqjaVEnV1BMKBk8JZgaQF8YAUPevrPsyFpzY9+Sf9kvJxx7zByV8YRCRBH3
2PSYrChFOog6hNa7dmNpLDix+rZgPiIqAeec4FUzwBJqcnOueHZBYi2k3ExqCX5S
FDwwy0lilHh2DgSl3u5q0ouXZJ3nahivC9JTpJKYpTipEtOD0K9VXExYG2oQ38fH
2J6R8neBfeDWcN2aiBHnDnnTgVMY66QKNYkJM6T9m1pWmjF40Re+cjKO8Y8a91q4
tj55/rPNWPhYrqZqERvda2V0Ia7ywLjPtrQuEbKLVXlts0KDJV6KACps0rTZXmer
Fb3LjKxTZYCDjgGOFIC8TpeGDEC2VTU1gLLN+Tsjx2ZGuCRqrIwzgdyMMwtPL7mQ
ORAK+Ff/HaOuDLGr0oyTpbBGgmKsZx/SEoS3ZL/c4IO29YwhlEyPSlDDMXqVsNE9
8mqbP6um2ZH6l4EzNm8sqPs4Wmxlp4AzNFy3yZPihZe7VVO2hrhPBjOLVVN82gcu
KbnOhhfLTbSvvSdR2/sUbQ9pUJUq8VR85py6OyGUaOEAiEIee7BGy4AjHBGinW3f
8z5qEewOT/Hn9BOHIPY8nNi3k27/RD8bvYXktWoROZ7n4UrkkBmC7ZwELunkp4N3
wzGA/Waff+rcdCl8SwoZQCocwyM9cmu6tcK1bnlVyp4WQVDqqlxakGkXdKcU2tGr
X7d3R/638v5R7ZcTtIscOYvjT/YD/9x9DoR1kqDGHOTP5v9nIyKuRVfvSpsPazBI
2IcZj4d/O42JYIAPKokr09/7DVjn2hODs5RGNWJxcn2gB8ff7MYuMQkn2WpzVcGC
4IQu4k3PpLMPFu4DAbq8qH/XeviqP8nTjURCbtJY2oSOvY02Wy9kAKGjq+JyTt3l
R3KPfydNjc+TckbDx1Ryxr1ZDgIOarfZaZmpWky33LyHfOfS2B3lsix8qQit5/Wj
8EvLPzsZxto31qDNO7AEhQvWD3aVLxfwHcEgrEqXwJBtNx004TfCDCrLR+X2b+iX
U7Va69ojWSmL6xSnXTLTzaJR0QttJ3AmR2gNLsCVH8gqkPuK83N4VyR88pVTutXV
a27zk0tCB0BB3w76cNXNeG2fmM2T7eJHjJlLg9voAgbRM8tva9uT5r6YExK4h0dx
fsNnZuHrWxaObb4AyUGiA/zMHuiLhASTu3Ueru3X/sMGNYxg3nCT1v9epe529TM4
eX66wEY/aPL/Ms4CpSXKfwy2PjU0oOu7JTDgmKc08cQqjC/mxEI25u51QKTAcYhU
dAzow0A8CpEwF1uKtRPaU5BPMoCe/+xdPlxXNSYcHr0yHHZJxrOkC03WJJBGlaEd
MZva54oMQxlLlxZeta2lrF66qMrPfp3uHf2d4I7H2pgDEoLygJBUwqy73jmzMiib
fxozGcbKHdE0VfykiyRgLRZXh7zEsvexyiss7/mhQIkrZkapNiYwzS8KKmcw7OXd
gKxW3dlQG4oa5eK3wYMgAZtpXxeMrx5jrbcYiT3bBatfa/GutvLSJjUog1kK7/MX
E19anA9JKBEFI4cB1jVSapS6oyxWzQ12cSjaVturSNNqlClSdu/nqYx2j2SCkokR
q7LX0Mi0JRyhc7fihBpjkvOQjWO8kfFz/H/EqV5SWabPUwLbMB2ccUQaHlhcofR5
xx5+BSbE/TMywN/ymHFybr+zfCwEaweXE3MxX0bxN2GK4nxSfW7NljEdEq/Piwv5
GnMIdA3OYKOTxXZPYgCSGE+X93aIimDhGySHR7sHtwdt6CfYyvCnU6dclKsFjx7d
nRRjwetZlzkrJ0hGWYEnia5EzHZ3fesqJ2u9JXFBBAUJWNe2nZk5Sj62kzLfsEab
WC5slugY2Ogghb3qkMJW9LJR8H7aU3me+rGR3UeDMqQyTbzUPnd8+pfBupRUNyUg
m9KP5JPBnDX8s0DWhiIQpQiDO9IlUpaRkVqtRQxernB0a5qHTo71q2BmbYoIn8jw
F5b40UAhbC0kvg9AM/5KDLzTSS7/DCFFDRrXUWW4E4kO70qFbahrFmGZmbBcMg7i
x+h7+HlhNRyEQwgEpsYDiCMna7uigdVo0oD1Ik9BXPrEEqiVx32l8d0U3tKrq285
u0EHQTfpG/LD+jeFW0E5pUPF0CfvC6ehmH1JcNoB7xWvf4YEJN8i9jhYxlwECWYR
Clzk9PlhkJvpMv85Du1jQUqHbHg0/w3uZnkP7sj46/z20YWGVKh53uXWqzs+77ea
x7JFKviVo89fALh3rxxrvQu7LVOdqSOnZ8eZtXqabIt2+k15O1DYCyxU32dbjUZL
gfwFdSn/QsNd3v8X+Sg/+95JUU2DihxNPsKZ0Ge1OEznOaxMm8u8Ry7WU38JUKNG
1XrHcgUZ9fqPvJCefZLKT6+H/BPYL5XUn4yxtmx56ejicSdQqmH8qYgc2nn6bN+4
EzsA8Mj0bAfziRD4sNmTd/pWSjWFx39Mhj+dtmNXS6ksXpl3OERv3ivlSfmkp3+z
egRpGurwB0RH/easzdkVSHYgAtmVeD3yvGxVpDVwlG9bz2pb597KK12HErQmJaCK
pqz/Yvac1qE6ZSm0FgNGVMspY9ttLqYUNEPJ+Hu2aCtOxiY9oNsoWFj/kFCZk4jg
I2khWehwOwq9qw5CwODXPhFnPWbsrheTNng60zeNfPkKG5IKIOmHpsg5/CFijV+h
lCYCkiUU9L9Z/ENd3XA31VQWDeRbFqlPIoCQY/8U4mbrH+zmpjPgYKIQ43Lt9UhT
NiwNs3kBcQ9NGy4AtIKjmxqnkcw1UXpFzLLHuPE44yWZ7d30/nv06Lud81tYDnSh
```

WNAG6z4PGMbwJKV4NePEnGi+HDHxpE8mg4YLpmN+Jo7dsRZ9zBtLcWayy7crQEjl
uGwVLKtp2K4ssFSPIMmIQjeTPCVWLZYwuHQxWmt2fhcgG+G4WQmHjjBeqXqftegu
bFX1HioRnjgWhC9f9JG39E4QvzxogsomX+X61UneCu8VOhohqOy8eIyFKI9piFJX
qBk02Yij5ilf0w9EmgAvMO4KgX50ofTC05G3g1r+/NXo5ojmcXR9vbHv3ZZQlAaV
9kntSirAyE3Ug6pBc3F1WRDH8WJ/Ysdd3s8j9BQpTn31hkqwHTadsOzCfKJuoGli
UyMCdcPoxMf7DwpX2LaqDcElgqLUzlzJLNtry56eLmbanGKoTgW5IDz2JTBIdodE
hvZS74pHATmajkAxyjUIGWpZDj81R8B8q09hp0kTUQ1sQpbtnvZaAANo1QcaMaGg
oc6l0/i8g9H++kSdZOSpJD++O15/qSklQXVVyDOS1hNCrwv5MCXD/iAIE2XkMZSv
63TyFubFwN8gK9rARSbWEiuzckuyxviAcP7cm6tsPvfQLnyqzC5is3Vv8GNrFPkX
zXigdLGL8sgQV8haNSY4HjeKBn9JwnqZg/nh5Zq2FRJUtH7kZXu57KLE+8QmV1V9
tniJ1081VjuqoYYsFO+JpjjVVex9gG7t4L+UAzAGiu+LHUHCLp/aU63w8velA6h5
kwt440g/Z5guB866OyhNQKb6yeOdOMtb8mycDA33daQvs6017rDosjKj4U3SJirq
nSsl227PCg26jTeNxBxHMJI6SK9KLPitZKEBgV0g6XYa2pldIC3FAQQ76++APlkl
ruxPv+gdd9lgZh/uFsr2+WswrlRBYyMztQbPEXlg7SWQ+xkRZxwK7+2PBLP/z8yM
sFfFBZhV81hNG0xuBT3r44kMnFxY8GnzR7fHX55Mr3TCV42q9nX2XOdmeHA+Nkci
vSuDOO2wH5f9hHNM1otmghimhbwTS/DP92JqOjwZHQQ9KlwH6AJrZ8YXS5xPRf0u
GBMQSpoF3g6nrvvxLM4T/VXVEarXAp2SsVE1L3EKmmxCujqKdEJ+wxf/AdkdIJll
kpab9Mks5fZLkpWWX2GfTC6j8FnnRWKc/fn+GsjFWaG23O7HYzMt40nxw0JIn3/j
i3xhoYoyoPAZZy6Sio46klwjWfn0XjReWOelgRHRIrVwp0uoq2vS5xoFzWTDla3V
scCei1QcMTvgJkXIDCYG+MZC7TrzNFZf15eOBoXODnT3FQjQcgxNMpiLcuyQ4rj4
hgllV2PjIdkz+MV0rrw3fTX3lVULU0gb1obMog6fUGKabTPgB10rBhjJp2luLyyK
K+siCjlOdEnEgyGoDvYdlaVuDbNhcTUl3kME83+0VoUPFaznTOumnRuVBUxY3scY
lsPe0rHgPu8uhJTbF6/mBHHZwX8EsnrRKCNWWoWdfJ055oyv3NgLSAJMT3ZLoR/l
eUN8f6VEN92ACF9d43j5r6XoeMJJExgi6Lnq+fKdvgbePoOYpN3kdbFQTaqIdeKP
pGMr5lBzW/MGg47EAbwqOd1cMYWCTEjVwhyF8nnfKNcvgVEHcbZ7FNZh2u3vGeqb
zUzDzH7nYtQhI8bJ1TxrS3g0jWnEq0K/HElNtY2uz65q9kbrwOL05hFrtTMsJBBV
L8IUsPy9m4CArNsJ+uZW4rKyw/zZGRmcy87UiCkmsKLUmjzhJSPI6ySxezra1WqW
eXP5mVK1KgLcR4yRpPfw2+DSeMz4wUi80wFR/mf+q+F3Pm0ZxTU6WclYo0Q0bHdL
GD/qNfU21GQRnDo3oob0t2obPVKYVCKNp33/A5KwwAD93bu1Al/vQ6H/zdMwxzwv
aqJog/voP8aVQUHx9demRIpYqj1v8M023AYzDwVbcidIT2tupNt3HIUjVuUCriuK
ZI6i02rSYN2n+YCTjuaSP6+9GzAktEZAeJoS7L2A4TKlCpXUawo1Lyu6WXiC0ipi
124DZg+ibs6BL8nHv1qy12D4yb8NV5qg/xY/gP/YDymLYGJMiUGUGjt33GwZd6Jd
G0CQfDGJekYYWkFyWDzBUuKdh0zHd8ZVd/swhx82bZz7RDrxYBt1IzU3oQwgvxjf
eEHVWX+NcuaMeZuhLKahNApli1mQ+ReY3wfAQey3zg1pYrQEHEGtoYiwDOageAD8
0CcUf6ZqoY3Mpn+qNwX95P09L+GfGK+WLJYyoUp0Mv7IlEDYpdQ28rowkRldB+ba
lt2dPacRH0xTglUXz1JzjvqLOYtPqfF0JQtYFHziTesBJf3tlhQrErV0Qb15fNAH
tspx1xQz5pFHTmCv25HBLeFO4I2Yy1aLmhjREVTs+lxBYFLjb4vV2z1J2ZypXAsg
Ydi9XTH49kXvMSP3Z4CpYzGR06xhEgUC26Rjn87fvFrTCchhRbcQkwxTxu56xQaV
qlBMTCIqKtNCIQwCz8CQey2aPkbLSY8DCwi2Idgy11NUPk1UWjgAYbC1oSdVnXaE
GarLMjmnJm26+ckeTBbMZH34Hw47+6YTirY3/c/cNIvichCMKpamJcKPWWFXpMps
FW27hjKNJ8Wb1Vvay+Rph0CzL54dntxioiPcAxeLA6Lz1l23g7aUygIZFfrb7VNR
Noh9yUrhzsSG3O8HvMyrF+iT0srvD/oSQHz2CasCgN5xz6X6defNayLrKwwIRxam
QNJ6xMFD+5ZHV+E9xaobzlBXY0D/NPYzeTF01UrPpd+o/qB8WZ+qlmR6YiV5KxM8
5CcjvBWhtSxqOmJXpyzhy9Pau8wVe6vGgGFxFeKPDGxQAoSCOW+5xXlg7r6BljZb
Tq2IIwILTcmJ7p7Y0JmJC+LVGClYETX+gt841A7wUMtZB5pgg2NVwS5oj1zOHLc4
GF5RvxsCdM1lG/7c/d8WTPSsIUXjmMo1uaoSPT2licvPYYab7p310GIxgokIpAjx
LDAknzbCgaWRVprPvbXMpGSDrxiW6eKj7/ZAl/GdK9wciOElICwAoDF2Ku8Y4N21
6QdVQ9/z5pXVAzblHBURHDZ+fv/4TlRDEbmNKk8bjcUj9EB4dUF7H7HlMHRUAGMj

```
MNKumY8GdyTqlQ2CLneUpq4YHdkeMU0H/lC20fRqLzGiuQ6+JUZ8lS6dd4fK4zM/
0844Eeq0plCtB3ptpK9+Al4jmX9deiVHs9S5rxkRkQXU7ghUC+Ovg3t8bkq+Xdg/
LCQAtc98/lGTgYoJUHblWZmACYowoQZeMHYofLgogXPJAg5rEsdxRuW1lOUn9GHG
9Q6yG6Qxo7+17jBQHbJk8MVxnKa8Vh1IDHyMS4KAuAJc3kG8xwZsPQHcJX1H+S8o
Me2cTdBNFFNkyKXcY5l4nOK9Leu+tGGsRjOJsI5bek+PKfzOC+U+nUJ238wnNcxe
sIklj4GOuE3AmFEoaqAQM9/UZtBtAIDmcqgzF1bAHtf1bIwMGO/etFmQzB1EgKMd
5EQXHRsWsD97k2QJ5SqzQslJTy6HTGWtMW85RKJPwE8d+Re4uZ+uMYOjm4pHV6hE
lmkzyiqw849RIwj+okEH7amdDS0vHI0U8n+hEJ44vUPpOSV9Zjsg6h95YwHb49rg
fg5FeKQC1KDJ3NfWy3KyjcnvblFAY+4U2tikqVTF6gHuKLl4uRqLe6sRIoHcYPjN
D+2ylKgwRyGtvMSJQ2NzFXb+eIz5F7PrqtUj+KKZ4hyT5qI8GL00/YBuFzQtR3ts
HU7A/aICewOfa0hvgTxok0OWWNPnYQYLcxBo251otY6eqHWacLqb+0rQyCE1irwc
KqEm5uTWwM7OEuUnCc9Rc8P3+78U/zNo42kz8Xmr9QQNA9u09zWKyYCGisSlou0K
eeaaViMiq0iBoqOvCYVxcAPUFLqFa9GlQDKweGeDXcobSI1LAa6F8lVUe16EU+I3
0dcgdsn05ge1tikSoBm635OM2bsXUahKXslzZxlwuZC5gDRyHW9mt8SiRcDBw1/k
+0I2G7Te8u8DDYbrRQay/g0OdWEoqZJ8HRXSgK4heGd9xtYemfvZcSvLDfSGr4Zm
x81Qix6s9LsWhHXx6EEem6xiXEfG/UoUiqToBTg+o0vx/3IR09Gtm5Nr7Kspt/AJ
RCuhq5nMp3tFWtoCpXem6CC4GyTew4wI9U8sv82Hzu9J7IeZuHwqgHvHqUm5if8+
Z86qkKjfuaatH1EHcahU6KvCY2fKTkw4k6ZZ1gb+A+qExuRVXoJ6lOiuzlhkpJhX
4JwV3ri9SjfND3aVDQnBKNdYP0LnVmJdOea+rh1Gj0kIL4IYa3TQoJzK4IEeQt/P
01/wDTLyzmX7BMTP9KLol/iO8ZbeRXefIva6CHVnSNXaJrk3rQ2LVfTJA3qE1Aud
BpJIx9DLYm5cyCD1AJIF4h44TXo1aek5WUFQoJmNM9QdKB1qwrB+oIAhAwT7Zwvr
Hdt99I98G/kyehjuJoJ0RNvJM9LPDgquYCW1jo1sRxv84cYM5/fGdFoDJZo0T35e
E+0WoNjrwQwJv1hdFATH/TVyqFOh2aJ2AXpkpf76h3b1gY9MhzNFVX2uhdMv5nU5
mjYVX6/HLdS5FsjUaDZa9DoYRqBJUv+2W7sPnf3mCvrzyqMP2IAbcSWOnHKovU4S
5JwF698f/nF2zpuAtaAo8CScFO40LNA1WMiOCzhGpaBneeytIUVREtz2zyYMTCSu
h1sP1UFReIei+mAiY12DRVrcVgrgCohoxueJjjtYCBsBv9Vgq1DNohPekjLbC+wd
VsQW0le4xL7OhJTREoW4jhoAmip1dZIp7VLNb5R0yXyKdUK+uRsiccz885vrUSer
ux2LT6mcutD64Y9drHfh1zRh2w0/NW+JqUupsOpUi9uNzMIcZMWrJm+F6ydwLuIS
1FCR121ku9lYhlbFhI9j84JdJAB1XG1l8gi755w/Rh27dxmj3r24iq4wB9Ozlu32
lix5u2oy+nSU/EHwbayAtiLeSm6FVNxzr1AO99xgTDkm8OWxCpSjqznzWffI+uPq
SoqL/FjUUV65GxqmvnN66kGPI9QeX+pmHA9DlsabqWgy2zQKmK5QQfRgOloU+kIG
Aq5U6m0FKBJILTa8gC8h4HbuacHiW9w9wiBFd7Nur6/ZhzZz+CFlyjlolu+SWfbj
M7mpNDtOfifB14SVjHwbupb9mwaToLe44llHrX860x7MTvR7AJZ4e9ATb5ZkOiVA
uzJiLcJbunOsEq4moIHDlPw4xs4U0+6N7qlupHeV1lx9mz392+9RW8/r8nZRkO8g
NBr1VhambZliGNjAF7gS+AoyZdSFHvjyUZ8dx0Tw4qEGvUparsp2MKHqmF0+29Ty
GkOgetOL6bcoW29PkhnodKSscod7sk4C70hJBJ7RrJNlA5YuwrWzokeD3rjEzqlj
dmRN2m9DQnXNeHKsxEsCkgIeLZVsrCxMVONTCrdfQnKnzZDgtoI4EYFfEElN6qQ7
v8LtiJyqtmYSPU3c3xb+zsWtElso+HfHELrwsY8ge485xBwtGTGKZtCcxsKtj97X
gb/4pfvziajCLU/MWnE4fzQXPjXk8NEQRdk+EsgoCOxnTPShAnW+MDN143ndDN+J
+BuTpFVF/duO+Vobv3N+3dH+Qd1qhui+q7R+ojXyp516X0IZCKr6211hAGgI7i+y
Z2RGCHIF3AA3ncH/An0X0RHgQi7ZIoSGDoHR2v0blOXDBNlzRXXiVEUGu1XuBp/o
BDnnXqcLT2Nng2tgdu6XvbIfgdr15/zrwKEAbG3yJa2iGsotgdiu1DgU7lfktlPq
ftTzg2nvDkTGT86AsTQNM2ClARtAmQnul5v/Oo926jCr+471rEXfN6Gm6zkwwoAG
ZyE19pnIaF/p7tczePNgug==
```

C.3.14.1. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIUpgYJKoZIhvcNAQcCoIIUlzCCFJMCAQExDTALBglghkgBZQMEAgEwggrPBgkq
hkiG9w0BBwGgggrABIIKvE1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGdjLXJwbA0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxn
Yy1ycGxAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxl
Pg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZl
YiAyMDIxIDEyOjE2OjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTVVBIFZl
cnNpb24gMS4wDQpJbi1SZXBseS1UbzoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLWJhc2VsaW5lLWxlZ2FjeUBleGFtcGxlPg0KSUmVmZXJlbmNlczoNCiA8
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxlZ2FjeUBleGFt
cGxlPg0KSFAtT3V0ZXI6IFN1YmplY3Q6IFsuLi5dDQpIUC1PdXRlcjogTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5lLWxn
Yy1ycGxAZXhhbXBsZT4NCkhQLU91dGVyOiBGcm9tOiBBbGljZSA8YWxpY2VAc21p
bWUuZXhhbXBsZT4NCkhQLU91dGVyOiBUbzogQm9iIDxib2JAc21pbWUuZXhhbXBs
ZT4NCkhQLU91dGVyOiBEYXRlOiBTYXQsIDIwIEZlYiAyMDIxIDEyOjE2OjAyIC0w
NTAwDQpIUC1PdXRlcjogVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEu
MA0KSFAtT3V0ZXI6IEluLVJlcGx5LVRvOg0KIDxzbWltZS1zaWduZWQtZW5jLWNv
bXBsZXgtaHAtYmFzZWxpbmUtbGVnYWN5QGV4YW1wbGU+DQpIUC1PdXRlcjogUmVm
ZXJlbmNlczoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLWJhc2VsaW5l
LWxlZ2FjeUBleGFtcGxlPg0KQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvbWl4ZWQ7
IGJvdW5kYXJ5PSI2M2MiOyBocD0iY2lwaGVyIg0KDQotLTYzYw0KTUlNRS1WZXJz
aW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZlOyBi
b3VuZGFyeT0iODAyIg0KDQotLTgwMg0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRl
bnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCkNvbnRlbnQtVHlwZTogdGV4dC9w
bGFpbjsgY2hhcnNldD0idXMtYXNjaWkiOw0KIGhwLWxlZ2FjeS1kaXNwbGF5PSIx
Ig0KDQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxp
bmUtbGdjLXJwbA0KDQpUaGlzIGlzIHRoZQ0Kc21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLWJhc2VsaW5lLWxnYy1ycGwNCm1lc3NhZ2UuDQoNClRoaXMgaXMgYSBz
aWduZWQtYW5kLWVuY3J5cHRlZCBTL01JTUUgbWVzc2FnZSB1c2luZyBQS0NTIzcN
CmVudmVsb3BlZERhdGEgYXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBp
cyBhDQptdWx0aXBhcnQvYWx0ZXJuYXRpdmUgbWVzc2FnZSB3aXRoIGFuIGlubGlu
ZSBpbWFnZS9wbmcNCmF0dGFjaG1lbnQuIEl0IHVzZXMgdGhlIEhlYWRlciBQcm90
ZWN0aW9uIHNjaGVtZSBmcm9tIHRoZSBkcmFmdA0Kd2l0aCB0aGUgaGNwX2Jhc2Vs
aW5lIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5IHdpdGggYQ0KIkxlZ2Fj
eSBEaXNwbGF5IiBwYXJ0Lg0KDQotLSANCkFsaWNlDQphbGljZUBzbWltZS5leGFt
cGxlDQotLTgwMg0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRlbnQtVHJhbnNmZXIt
RW5jb2Rpbmc6IDdiaXQNCkNvbnRlbnQtVHlwZTogdGV4dC9odG1sOyBjaGFyc2V0
PSJ1cy1hc2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEiDQoNCjxodG1sPjxo
```

ZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVhZD48Ym9keT4NCjxkaXYgY2xhc3M9Imhl
YWRlci1wcm90ZWN0aW9uLWxlZ2FjeS1kaXNwbGF5Ij4NCjxwcmU+DQpTdWJqZWN0
OiBzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtYmFzZWxpbmUtbGdjLXJwbA0K
PC9wcmU+DQo8L2Rpdj48cD5UaGlzIGlzIHRoZQ0KPGI+c21pbWUtc2lnbmVkLWVu
Yy1jb21wbGV4LWhwLWJhc2VsaW5lLWxnYy1ycGw8L2I+DQptZXNzYWdlLjwvcD4N
CjxwPlRoaXMgaXMgYSBzaWduZWQtYW5kLWVuY3J5cHRlZCBTL01JTUUgbWVzc2Fn
ZSB1c2luZyBQS0NTIzcNCmVudmVsb3BlZERhdGEgYXJvdW5kIHNpZ25lZERhdGEu
ICBUaGUgcGF5bG9hZCBpcyBhDQptdWx0aXBhcnQvYWx0ZXJuYXRpdmUgbWVzc2Fn
ZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcNCmF0dGFjaG1lbnQuIEl0IHVzZXMg
dGhlIEhlYWRlciBQcm90ZWN0aW9uIHNjaGVtZSBmcm9tIHRoZSBkcmFmdA0Kd2l0
aCB0aGUgaGNwX2Jhc2VsaW5lIEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5
IHdpdGggYQ0KIkxlZ2FjeSBEaXNwbGF5IiBwYXJ0LjwvcD4NCjxwPjx0dD4tLSA8
YnI+QWxpY2U8YnI+YWxpY2VAc21pbWUuZXhhbXBsZTwvdHQ+PC9wPjwvYm9keT48
L2h0bWw+DQotLTgwMi0tDQoNCi0tNjNjDQpDb250ZW50LVR5cGU6IGltYWdlL3Bu
Zw0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0DQpDb250ZW50LURp
c3Bvc2l0aW9uOiBpbmxpbmUNCg0KaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJR
QUFBQVVDQVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQ0KTUFnUzczOW5P
M1RwUncyMGRxcGJmQVJRRWpPeXdpd1luQ3RrREtuYmNMazY2c3FsVCt6dDljaWRr
RSs2S3drWg0Kc2dyemZjcVZNcEwyam8wNDQ3Z1lEcGVBcmsrT25KSGtJaEFmVFBS
aWNpaEFmNVlKcnc3dmp2MFpXUldNL3VsaQ0KdmRQZjFRWjJrREQ5eHBwZDh3QUFB
QUJKUlU1RXJrSmdnZz09DQoNCi0tNjNjLS0NCqCCB6YwggPPMIICt6ADAgECAhMP
LSW9ETmXSs5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElF
VEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNB
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIw
OTI3MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEX
MBUGA1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAw
ggEKAoIBAQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D9zFC
rS3i4Pa9ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165e
rnT9O5NLFflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc
1zy++MxQlqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5q
DTII2PVX1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf
58duq/AOEksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIw
ADAXBgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21p
bWUuZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBSAw
HQYDVR0OBBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwH
Fwyn8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBakDKU6
8ro0RsyXWAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdaox644
DsiLOQEP4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Nar2in
C0D+VM6RGDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtluLih
ne0Bp1GUTkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK49+q
YC9faFmQ+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vRhZjV
D6FYMIIDzzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG9w0B
AQ0FADBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UE
AxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0x
OTExMjAwNjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjAN
BgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4
TfA/pdO/KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7G

```
xVwXurhYdZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12
DRVBDpbP4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkN
BR2wZX5ICjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR
+peCrhJZwLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQAB
o4GvMIGsMAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4G
A1UdEQQXMBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUH
AwQwDgYDVR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZm
czAfBgNVHSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0F
AAOCAQEAc4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd6
4roAKHAp+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27
PmhKE1oAJKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31
wbqNsy9x0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnY
xs1FhdO6zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgN
G/D0qyTbY4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UEChME
SUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBS
U0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6aqdcw
CwYJYIZIAWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG
9w0BCQUxDxcNMjEwMjIwMTcxNjAyWjAvBgkqhkiG9w0BCQQxIgQg4f753q+skjOT
bEsl5q6WUySCAbgxotWkN7Ci2/Q7J9cwDQYJKoZIhvcNAQEBBQAEggEAiUGuCHAe
JkzXXnkH3k8yFGtEkkMscuC0JOPwqnxHzILBDYt9udpeParT/drO0VgRKxCQ0mxT
sz0D65erzo+ZXfuXC5+Q4hzqdNkQhC8Vi7H2NL8KLsBrXNLZtG82xco08fTKTWVq
c2HwuAPL0+Yh+fTfqrr5oRnJvPVkTxl97KxTA1YNQh/s+Uuacumnmr/3iuHwjubd
+iesA8wZ9RWsmeg4FGUzaVrTRIHj8p6YQQYJcOomV9GuRbjUzMVTL/fOB0G6Jho1
aq6nGVcsoVTMIrH8nJv54eHQtWtYFBJI855oDbkIS4DxH0wR5121BayRN7MgC6q+
H+cJTAZUD2IF7Q==
```

C.3.14.2. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_baseline (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl
Message-ID:
 <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:16:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
References:
 <smime-signed-enc-complex-hp-baseline-legacy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-baseline-lgc-rpl@example>
HP-Outer: From: Alice <alice@smime.example>
```

```
   HP-Outer: To: Bob <bob@smime.example>
   HP-Outer: Date: Sat, 20 Feb 2021 12:16:02 -0500
   HP-Outer: User-Agent: Sample MUA Version 1.0
   HP-Outer: In-Reply-To:
    <smime-signed-enc-complex-hp-baseline-legacy@example>
   HP-Outer: References:
    <smime-signed-enc-complex-hp-baseline-legacy@example>
   Content-Type: multipart/mixed; boundary="63c"; hp="cipher"

   --63c
   MIME-Version: 1.0
   Content-Type: multipart/alternative; boundary="802"

   --802
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit
   Content-Type: text/plain; charset="us-ascii";
    hp-legacy-display="1"

   Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl

   This is the
   smime-signed-enc-complex-hp-baseline-lgc-rpl
   message.

   This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_baseline Header Confidentiality Policy with a
   "Legacy Display" part.

   --
   Alice
   alice@smime.example
   --802
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit
   Content-Type: text/html; charset="us-ascii";
    hp-legacy-display="1"

   <html><head><title></title></head><body>
   <div class="header-protection-legacy-display">
   <pre>
   Subject: smime-signed-enc-complex-hp-baseline-lgc-rpl
   </pre>
   </div><p>This is the
   <b>smime-signed-enc-complex-hp-baseline-lgc-rpl</b>
```

```
   message.</p>
   <p>This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_baseline Header Confidentiality Policy with a
   "Legacy Display" part.</p>
   <p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
   --802--

   --63c
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --63c--
```

C.3.15. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_shy

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 10445 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 6716 bytes
    (unwraps to)
    └─┬ multipart/mixed 2273 bytes
      ├─┬ multipart/alternative 1116 bytes
      │ ├─ text/plain 379 bytes
      │ └─ text/html 474 bytes
      └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:18:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
References: <smime-signed-enc-complex-hp-shy@example>

MIIeHAYJKoZIhvcNAQcDoIIeDTCCHgkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAHlYUDAZJtrARL+kRtiQU4vNChzIMY4Kq+ga
tvbsejCyWpPOJ6bCjx7IuyFyTQzpi/rkcBdyphDz/sEzyF68mAtFvGBHhV3wi0Bw
V4+TCpXHio01a1fDbWQTmIRhNoT0CwkEq2AWzMerjlPk1YGzRWQ2F8v5conRtN3l
guvkXr3vyaD2wbq6UYIw/x16vTfEmqFVnRMSsdWdqjVrrPHTTVytUI5uBhKq7f1C
dWt7nVOqTglW8WKB0qgABKT6E7PqafUzXMBu1EmjFhJyNP4rrQYnY97iVbPnUyyz
SUUb5pLZ0aa/opENPk5rhCQnb4eEnbGS9lu/dE+6y/I9/l7eGFowggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAh+lzMZeSWj2T8iddrFSZOoV1
VYyCijzcJJEp4Mfq3Ta/ln6Z8wAvgJAuFaph1mMGKX1iZIN48te6SmQ82IyBqvkp
m76opxs26OnNZ1sVvwhTIWzQjNUY4sxTF5UDTqKuLAcrOBPTtVvgsJtMi4rWDbW2
MbzSy+mxyEWlDkDZ0/2BXgEVXNmBgJ5qUUMF+31WixM9Y+iN9kF6194V4TbBQ9U4
fksuKQliK+eOXqaZibATxgn8B4arubpnHFw0bjna2bMkHmQs/eT3VEI1RSF4Qg3p
FvDzXC/jHqrhbtnQkR/zY8bpNDFEiBv3e+myGaL4CsnUOMubx5tkhP4IzWXwRzCC
Gu4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEBjNxqRyzAx39GzHbZO4CwOAghrA
KwtFLWZ1Im0uhZJ/SZ9TDEQXGF8Bt5WnyCp3PC8m2ygxoui8y0XLvH/X353IQzHv
ituNJd5CN8m6RWSHym7NGYwifFciv/usZk1/pvp+jVzvFW/GAaea3oyksAYJz4o+
y5IG/TFykybUNyDKEtJ3kMS5D07rbDgGJn7qoK/7rEbTsUf1NSIEdVkfM8SEHKOi
WdwV8uOJ59d4mx11uOBU7+VOVFbo+YVPBHuJYJz4U6Gp48Tu3IdAJQS+PPmY6IEX
+3rE1+jcf0KXxs7PRjZ684uwteMkekMEehxNSQg2HJw5W9hTtPI/qSdCfx1egfR1
+Lcj+sLi4fPXK8cdo2Kc9qGiRci4PRSLxsNCRX+Pk+YrhE1/L1x1Q+O6GmVR7XYc
fU/SOPL2LO4jFToHu27NF1lT7s4diVsWXl0Mn5umgo+cOBNGdAM6Thh50GuygOlQ
xI0VvwTbhNE6Cm4g2okhIYOj/Ko6SludZXlhCCAxsnG+80b8If9CjwVkb1dv8DqJ
81NPoiSaJj5RCbfNy1RE20jLjkAKzancfCXIzuBuReQaUnVkAHOh6Aj4ixx1awrX
F8hJm+i+WDrnGhkb0zsgR5n9zlIagCfiS6JWZ+N/lYeoeTuoS3dNPEw6wUXmC5h0
oXpJHD9URuOScbrQLF5Kx34B1Ppk/WVRJLxbSy72sm+7wEHOC+Ft200KofzJvZ2N
Vu5f18qGjklYSmJl7/jNVR6t1G4bN5wNIxZbdVeKWDvpv+iCFXbBlhSu1M3x9Dqj
zfzfTa02JlpHZhtxNywOa0OLFDQsbLyVYWJlAKG7mq34m4jKSKWINnbkaeMo0xEN
l5QxwLXbgrE8oeYifgeEsdV6ep7jyGaLFOqU5qXh5PowHiXAIWQO6FI2VVJwmjST
xmcm8iX6sGUffC+8C5Oli2T9whpkoj2RUx4udm2e29TAwHgCIOuwwKGIws3Wusu3
fqhYuzHCPCXqpqsfuJvt6l2KUqhAdrdPOYQNMbef3Pyh95qvHCtln/pNIwDjJHRC
w+BjdZcDIv1XOrAYid6OxFxJL5vjS9/NLG+TD+G3Th7a+TOItnK7RHjff+CSMfi9
68ismududaCBb1okq1yWJiQLxSJ9ozQnwC2Ic933DjXnFkw6PIgade8pNM6TM96X
```

```
   NmN77vF0uKCmMoC5MRGk7FY2h1iQ/w85AZyUL17BRcUL8JH8zyaTMAZAP6Q5ejK/
   XM01usJFBJiD6xVtMeqz5Efl8st6J2bcC8FEg22OEQELere/FkTw69i5XZGBZNEa
   nXy0zF3wQUujqz/XHH/x33AEvjUfbkdJRyqPQMn0poM5NplvS7GVaii+TqdCgdOu
   T3ROu8TIa6tsoWHMk7txFQnAVVOMij/F97vJQZa2ts3WK72I6S8zMpkx1kWxwzhq
   Ov7ksP7t7lfrNHHFLSc3GqzcNwejgstoY4sS0JEuInkqCqAX+tC0wVmLGa8IfhjL
   mYhFxSUazeWwcG/Q9na0ynI5X3z/ccLaUYuI590SmGjYawS5QjDj23s68OlSEba/
   aNF6/7Y9JidaDJBXqFABRXlrrCqZ5l0OwvWnuuPX8daVas0P3b+5Y7YHZkG+6tEo
   x9BhJ1ZpZbMpK7SxMTIZxEhSq3jjsHAuISceOP7FNWvnrrQKulD3eV3ywqrXeI5W
   8rEukobJQgZrkOPPpHw2diFf1bk7YSfWFNk2iD1x0o+5Bsy5XrEUyrACIKzKn8cT
   4jUMw/G7hBQJdrUlcsMtb65lEGP5RSjnzNFOksBYM0+Uh96xPf5FuF6B8IOhPrtv
   HoDsypNnLNPLxc2I/RjjIjR2rC2vkJRwcnG/x2F8JztPwRrSQhgKkopaGkTLY89h
   Dd9u98WAepIr9Wj8DumN3a1fcrsDcDOL//TuSepd9juMwKkTthvXa6fRcjJ2oxNC
   EZLtwLh5wkfF7IdtNVGig2W02ykfDcCBq0TBdcTXTEJNjeGDUhAXFRwYB9rmm4nk
   HkxXKyH2sK3JiUcEGREIfARSJfxAGU4oP328378006QvIoHGHgIP3DnsBMKsOJkU
   2KbBAmT8T4X61x2Me76idmwJPsP+hnE4rPw9bKdn5u9eYlU0F25VoZgln18qJq1b
   C6brgQTszKSHlgvy81ug/wV3PCpz6L80xW5c5J7ig+OWwb2tzfLMO4F3Tvssqp7I
   MA8JFsHSF3pgSuEGenTZxBpR6eTo/VSIEI2rPrYKik1D4MxNzuU10ukL9FCYkWb/
   Lcorm6OhJOPtcvYp1iJJx3MRtndalHNw1lMdVXEbJErpKxhSW/pgaRrCdX/I2prO
   pZMthLKOwl73HAWYeVvGU3scA8mI002KGGFCGJvp4IbbQ4nf0f3M6hcHqsum6cRe
   LgB5e02U1nA5pKR5iWAiMkmXWUTfzCZuYAOaBznTvA7zHNNf0BkQWKgieZjyckVb
   8YaObWSsr98oha6hUOPCfdBtajXL2JrphGXtBc1DVLLf4VTgy+clVYZAXDdiD9Ov
   KGrXftO3xo7cU2TIcFFq/ZbjWJud8Aj+s6jacBjjYoLuNBiNyWMVINjDviHA34rZ
   XSEV5J50nuQtfUP8257z4UCqwk+ABJRW97tMxO1Lo3sCOi+Pyh+c2CdxvUFOt29i
   okI9N5cc2aatwNHg3mHgkEhViDuHXF1v+WFFwjqB1tIY+amUDZsSnTAjXuJ88tAk
   iuptLA07DzBa1Z1CunbQwddIgryiKrzw1T7b5CBaqpugg6V49pNNkXEtv0MIxRO3
   QVaxfFns/ft4dXxKEBmWdj5AMekWDCG699IIAtuM7AYh59g/qRnpkZSSBluUG2zS
   wvQi1iUhK6U0Rf9O4+cWfCIvZuL/FUAToUq892VsVrzZObeyLtqxGAM3yfO5jPpZ
   yStYhYt1HWtX7v7jd6Ni98dNq+3gmfpq9z779aTxIckL9myqTNURGjrNyXf9lmco
   qauyW8MagYn7U/Bwtax0h5qpjLqcmOPUGo/TmPmL6MN+znzxRLBsakvDNED4tARq
   2QYkoR8HLKvbp8q8XBtf/I/23S1qEnqqprnotd0oRgaJUw8Z/QyVmwC3oxVlVQYV
   c4391fZLwnVbky6v54ynmtjIf9HLNCl3fIA3p8DF1mzGsZidD4WS9WCIUOx/lRqT
   hu1M9VMtKoO1sCJ2u2cmF3aYxTFbFH4j92zXv9ugW1EpY75AgyklIjExyIYTUQdq
   PVLPsSG8HXnuoupDb21hx8WjIJCLz5hprxKvZ5UimjsAHb2AOcpIyhx8pfiPohDu
   QL11dDHlRckYPBBm8cAsIP3NAKbOcIk66q+4xMPqxEoD6qXI0yUW22dju42PTT8+
   MgpMRf7IOjlJ+cLoE9/QUcXCTxHOAbIQv7O8dLdfRY7H+Ssci6BS40G+SYpcGDTa
   OTJluDN69HueqqfA4iCCJm0Et5AQ5wyCx492pwxNyeUdRxs0PMfiDAyuaAxQuLww
   25u6R8adQG1x1+d0sotRg96VBNNGw0T6Tx4CFtu58CIWOEtd9m+rRoyKM7VodxSs
   E0Wdga6CW13JOOlcm72S5BRJeBkhDQ446suFtiqjMJhPhS8nctY8esx4wEd7VhF9
   MPmwaxlm54LjkSJQ59oXtQxiw+yQbep6uR4AaE2SMktz0TzuPtmILlHb8njC8GCM
   7bDvosP+ja8FjF+hAw3Cnw47itF+ZmVGxsWmmt+RkiQo54+4uZ3Xi3IZm2/AM0FY
   5TDElYiMK3KWai28NAnThHbl7mrKrJ3Y4LzImYW7sVK6Lim/lQq2QOwTFYs9LYBn
   fRoFT0NuVtteN3eMa+ERIKCVBdunP6c6ufF4OZL/ltKGP0gko29f1EIl3R9VH0jY
   Rvq5pa79y5WkihPUngA2rmZz3IpREvN6wE4c0rix54QBklaz1yW2LMVYXnI2Q0x3
   ZZgC0hz0xjYqY/YeloXR5pPz24CJAbrMSCqAhtohYDmkTJUv/ov5YKvE8IbDvUVu
   fI29aQ7vh504eAKG9HVK8nNV2GvuM/+32LP6alvX+yIUKRr6BLyt7H6lw76E1BDk
   pgxMmU1EpPaSo3BTI8eALDTBNLyGOK98kZqXemnrYbVAJgMS2hUfeyZim8tFf5Ws
   BMKOP14SoK0Emn4PJXV8A/2XMsYpTZz9nWGX25HKaXhaAIZGaB8D0Askil37VhmK
   LGe7dEqg/CHIS0ydVCOCqFOdsIYVqpCzpO2XpbToS+kNoY9T430bUwIq7rdDRIWx
```

```
   PUkgE8AIP0k8uqI6wCeF4giwUOjhjLj4K+ein293xEwKasXD+o7HNcyvluFt3g8F
   s0eezk958peq4R2Jm4KySsuOsPfeq8YXpbdwpZjXRkK2sNQLiKLmBsrTr5OtJoQX
   Paaut5ZMi63Pln8eWMfIFJ1/7lmDPYeTGOzrbyQXg+l111HKgsuBkrlN5iZuuCvk
   sNgGhW26zDpWf2IXxOnAdby/+6ZvCh2PzTO94n9y5yo0W0UfoUK3RxHfleEcsdHq
   3X2/utJZhmM1W3HPxyW8ClpDxkXKnTHArjRVmu3zCcUbeEJEGc/c9pmyzx0NEnlO
   2yfUuM7UYk0sLCcMqY+8UNtOeY373e9RYx/JtRSnYzRQTOI5UdSGdug8fBMc1wkX
   dsKLO/SP/xXo3J3ArIPesF+j8hSJItarYc1RTpcSHuqTZ+QbfXB0fqXIV9KJietb
   3ufjGwvYIRv6fQ81rICQW6TeCRvLM8cX5PtPiEt1rQ7lc9BKgpqgfxt57nsd5b4w
   T/nZ7mM/ks2m6NO9KxZ2H9QYSCCo77MbQCbxdVxhRS4aDUec1gkTQHLSdJDnpRSf
   nO6JxmqSBp90tJ+LDHS50G0Rtlv23GQ1yrL3nWnL9S6s8ohFGlokNl3tgWYQe8Ek
   YwZiyGw9Dz61JQYO6QWKWYkqfblJZqlmoZPxDJY42PqXz5gczGTyvorOXkapWfVz
   l5OJeNPNQ7dZVqECSUh3dqJ6LxEPYTy703my4BPIJLt+ImT6bhFDieig7cf9oxqR
   ZXeSphW6lKYyz3yFpQ+51E6/ebZtejvIdxn3YC65IogPRgdNmrx8AWuzQR/SR5/6
   oiO2YjKc7BwCaZVTcGXHIOYbzplraACMCrrgz94XvbaPZ3WX7AbJZmxekAqMdQR0
   i/OxyiojevnNhr1hfBTCagGJr3UiTKnQzYFBplNphHq9Je45v78N8A5ZjZQIeThg
   pAPu9ZujQIeGQxWKWfsWIAKEmVUFiQ+7WDBf8GOFCRZLqUmitSNP72q5r6Ao5QoI
   OKjIpF+QB1lhqQK69Q+Td/Q/Qsxl3W4OE5p+1qZNhJDgrYneZBxwNy3BU6GXQoCI
   gxiAonb/XB33G463hDEui/MbuVvsM0thgFgvzko6wIIIcqrXYbjKsubVKeCWMs2/
   O9XDeJeZjc2psmuUiOLR4OU+7mlE9YhRmITxkztlL8jJigSL1kmyTMz9EXHndIXd
   7KZZzML0gdy7z3KaPQyPO2huJXjHlM5+Dd/+FI29S9uMLAQrXphJEsKHpnEtK6D3
   H/5rYHV+2qWYEjI0cPnf8RzYkK0H/UI53zISf/sFC3zbbMNBC3+SPH2K73EjpWaz
   zqkYDSWy4pfEn1+maXEaUbbgZsCEE7Jktj2TS44HvtL61UiRnbcPbwEZbn6PMKre
   9vBpBrLJDpmIsbc6dHMnSG16+b/Z72orc1933yBuq98dZltlm7V4R0AqWHrcH5Rx
   oXn5UpvZoqlWU0ounqRQ/DPnsPTPV/6fsQFu++RfrzkossP8Ukiy5VhIQK3LUf3J
   PX+htDHqZg810yoPqj2Sr3tTeYqFeIefaJ3cJhp7YPICxJetCXGssGnOTtl/b+KK
   ZHpaLdtDehkX2p/2+fhXV1a3QQ7vGXyK5oHJ3+FmGatoLqpVL0eRjRJTlTZA3Tq+
   33y6gb8svU7v+CkDQXU3qg6u80LULvTilXhfJNStVwCsyTnY+K9meirGTmdvd1t8
   08oCjTN4FOJpaXrfvHWdR+4anTnvEsCUsFOECQ3a/SrJbHP4zCozgNba8utPIf8n
   P4DDlFKeaSvHr4KHS4hsuC3o4HSbFv0usr+aWZjsgKb0yhPKn0EwiurwbIS+CNiJ
   Pw5ae7VSytlPmC+WfDyRqiflGFJHBTigwEdDTnuKsrYn/MsZGrpUgx0fHFMYBv/k
   Avh3IBP3ky1D+leP/RxkXwvOiyxkFsAF4ewm7zq/Qkp5CYG38+vPuf+iF7fH0aOL
   kk7GonZ69KvKBL5YJXr1oWqs/SQ2SJ8Yc/VvjOaDb/JxkvRXlID0ymvfLWl9K4js
   syVaVsjn43hAP0rHW9atEYnvjU/3qyWSoq50Jxkrm/pgLwzTWol7t2V16uwnY97b
   XVu2/2L/R/VXaLZwTOAqedQ2Xow0pn4qwpFCkvmT0Kci+Zxv5M3A9csSXjciW34Z
   Uk7b16JYaT7Bug6zPtFFco4u2n6AWOr4cBY4uNYb/PKNG5C/4gg+LkuqffrfhHb6
   OdThNppZ+F2KgexYHFaKbt7woVfAnQQvEETgDPlPiqcRp2mmhAzN8r2Ia2Cr0iSf
   5fhLHnZVA3QSkMIyedXfHdFMO25ibApSM89IiEcwpNo71F+APthXCU/9C4fBCYim
   C6N6ORb8T6m16C2rdHGfndZl9pkPfTQtNkTsWE8fP6LwV0V2w/I5h5hWre6Qpqrg
   jjDuIMamfTNiV8RKVtXmXTzHa9cdUnqOWczpnzz+8nLB5vOqh6McrUquSSqxMhMY
   ZeVK5hMssM/OkwcqMFCxCjZtAOidAVYkuPdQLR8Qw7Vw99BHFSV9fI/NCB0LXIPA
   NC3nJELTq21ZI+/EHpIKrz3zDU+oV5ipm1wrFWEGcjSzbxA9+1vvU5Ra9P4tVOxQ
   FfwQ6mojU02Sy4p1vQoaRhDLAN8DPHHFC5AU6TNMxka26OUC9sOuPIRIVFcdpqbX
   QvnEIhLNT+uGt8DKhi3sb/T4GKUlcxCM+QLi8I+9aOsdHyiWGDM4xb3LPrwPhOU/
   yHzOQSM0xwkCRai/WEroFSEP9weogqUq7uIrQBmwFkBQUneQV4KesfkD5H+vzZWb
   opx56gTQRaACZpLCTn0jdIK/Iieeo8xy4h0AAs/nV3s5Qb2f9e15f6EnYfSiWd9X
   dHfN+0txgDbqpUjRumoym0YjuNFwdTxnz8C+YCqkT90f9nzX7+bIz+Bq4CynvAE7
   W5Mk6JRIIRcCwwwX2WSMX7RDVYRg5F+gxFFkxknOZS8UFbAvR/jkwVjjPEUS1FIm
   71EhZW7vLo30aGku7kNiitTeW2qRHD1wZq+aoPG835iQLwgdH62tF/0tRUv/qtNG
```

```
   Jox77mnuq1iW+I1FKvEibrNH1CDipCdE0D1+EXe4iAOUx/OOjKV4ONKy5eDk/t55
   dzB+JpeHlAs2AUBbQeDwKo65R6sO08JC1PbiTXVskuvjmFS/8uzkDGc/JehezRN/
   ZHg4TI47xzVwKABMS3F7nPYWZTKy+jwzdPmueCuDZsktDzlRbgIdDR3dNg87iNTf
   03XfznIaTKplEqoxRMM9Q0LjmzNoDZtPOnWg4awzg/7aNB7BjN1IfXlKV7H5Od3n
   RNx7rnVEFAX57JMTFAJcK+Uo4ibci2dMNqM5cpAX9LPBmsynfSxaTzhPWEWpPQwY
   SCGCmiVvJFG/TbSCumjkIGBXPsJpPCJhx4d4hC1trjq96VjYkV09N20PO5JKlRo0
   az4SI8kqj7Axa5UffXCpSSfbn8ehp78IxsxMG7tBZ0AEFVJV3679zZj2NVdhFNb8
   CkmHo3ya6bdZ/NJdSy77Cd9Vt0jy912g4X3/s0ausdDOZoRbTFTU1VKupLDo9pQb
   C69iMim2eRGg7g7wsh9YQbe8O9hwryUEtDeeeIPhbE5gEk8xjP2t101kmpk4ViRW
   FKaTu/IKsh87trtQE89KCTppUDCEy6N5HEirPnW9vEJo4qRQZ2ApsUpnVYD4kR9t
   sME+PuecHiRhqh+dEo9EHHdrhyu53d9fCcGhbBfNWy4Sf3nCnhO5hzzUw3fcpW9p
   7GkKlO+yWcpxc1fOrvuq0OAnQihtlCQ7NydQ54x3varOZSLZ6dopsxXnjGSlfawI
   GUKl06Cv9Gd8G6ZsMr4bhjyD2prNnJpOcadX1r+LEkfX44Xv3EHge3J9enOR+fMZ
   tVQriToOEMB5mfEtOP07rwfDCiGXkAZPCukMC22y7Yksqib8o512oWcbx5l+FVFO
   tfmy+c375n2x+wth+SPY/LarQUDs0lV/v+NC6u71TjyMhqkWEGDbxtDqO+hrUkqG
   B95VNgIGFmdvV3+IlD13Hx/rAf/eMfadJ5F7HlwOjdXbnEQsYXkwtx6UOturVohH
   lUFqqjdsECXP1o4QFiiO+a+WGFNEy1KafnBYBbVpIouu8g3SGtHKrFAPxH7i4uFb
   nCGXYM1O6HBdQkF5IHeVH/Sh3iDPnK8ilfSUXIbo2QiFnuuvb280VD1hDWys4q1Y
   82bQdIQOz/YQkDNmUoM09ZQEtRzGxGqqyDrKtoeGNuItavI/oQFs+n5f/p+B7ebP
   +Dq4AptNdZliJTVrkKKw0buQJMrcUvWKKxkUC9/N5DeNVV7yVuyVBUOk1Q9Zub8X
   SNFkFDZ4I+CfQDrN9YedY+lAMjcmiYIDn9s2RmYnGgAVlYweN7y8hE36sNAxDUKq
   AEgC8bJrTAy7axaqj2m8c/F1nXzmKBn1+Q4zSW8oeNjvfSpfS5ZeljHnyHrZrUN5
   fVyet/3gok33Qqh58j2kXSVgWJrtbsIk1x5Zu2Q+QeUmMykA2ltAe//NbcRm5NzW
   fdAyOP3IIvpwp6wOrtDxyBeDDmPS6Jkthp/3A9CmD7jewnt2D3f9OG1jlZI1nvvi
   VxqKkC+yHGxYKC1kdvZnkoVPS5sGA3STRxzWgfzZOrnvyNjKneokJY2CMA89A8wm
   cdAbA8WTxoLo7ObjelYiyPgB5BWUqWvRbrVUYS6lrgLToUIfVSS/beNyjwwmjHgR
   C3a2iQQ74kYyMr1iBj9K0cUeyVSBHOMvwG5Xv0Phovz6waVZdSWOcxjDslz+Ghg/
   c74x37hFQSAiIUt9ZzrE569QNP6wcGe/S0MxL5MG6bqu5BH8MGrBeQ0IPRCwXFwI
   +Hvwh/mIF5Uc0hssRDYNn9YxYA0jCLsjpxjMcDJCMUA=
```

C.3.15.1. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_shy, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIITEAYJKoZIhvcNAQcCoIITATCCEv0CAQExDTALBglghkgBZQMEAgEwggk5Bgkq
hkiG9w0BBwGgggkqBIIJJk1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LXJlcGx5DQpNZXNzYWdlLUlEOiA8
c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1yZXBseUBleGFtcGxlPg0K
RnJvbTogQWxpY2UgPGFsaWNlQHNtaW1lLmV4YW1wbGU+DQpUbzogQm9iIDxib2JA
c21pbWUuZXhhbXBsZT4NCkRhdGU6IFNhdCwgMjAgRmViIDIwMjEgMTI6MTg6MDIg
LTA1MDANClVzZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkluLVJl
cGx5LVRvOiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeUBleGFtcGxl
Pg0KUmVmZXJlbmNlczogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHlA
```

```
ZXhhbXBsZT4NCkhQLU91dGVyOiBTdWJqZWN0OiBbLi4uXQ0KSFAtT3V0ZXI6DQog
TWVzc2FnZS1JRDogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktcmVw
bHlAZXhhbXBsZT4NCkhQLU91dGVyOiBGcm9tOiBhbGljZUBzbWltZS5leGFtcGxl
DQpIUC1PdXRlcjogVG86IGJvYkBzbWltZS5leGFtcGxlDQpIUC1PdXRlcjogRGF0
ZTogU2F0LCAyMCBGZWIgMjAyMSAxNzoxODowMiArMDAwMA0KSFAtT3V0ZXI6IFVz
ZXItQWdlbnQ6IFNhbXBsZSBNVUEgVmVyc2lvbiAxLjANCkhQLU91dGVyOiBJbi1S
ZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHlAZXhhbXBs
ZT4NCkhQLU91dGVyOiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLXNoeUBleGFtcGxlPg0KQ29udGVudC1UeXBlOiBtdWx0aXBhcnQvbWl4
ZWQ7IGJvdW5kYXJ5PSI0NmYiOyBocD0iY2lwaGVyIg0KDQotLTQ2Zg0KTUlNRS1W
ZXJzaW9uOiAxLjANCkNvbnRlbnQtVHlwZTogbXVsdGlwYXJ0L2FsdGVybmF0aXZl
OyBib3VuZGFyeT0iZmE1Ig0KDQotLWZhNQ0KQ29udGVudC1UeXBlOiB0ZXh0L3Bs
YWluOyBjaGFyc2V0PSJ1cy1hc2NpaSINCk1JTUUtVmVyc2lvbjogMS4wDQpDb250
ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQoNClRoaXMgaXMgdGhlDQpzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LXJlcGx5DQptZXNzYWdlLg0KDQpU
aGlzIGlzIGEgc2lnbmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNp
bmcgUEtDUyM3DQplbnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhl
IHBheWxvYWQgaXMgYQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0
aCBhbiBpbmxpbmUgaW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBI
ZWFkZXIgUHJvdGVjdGlvbiBzY2hlbWUgZnJvbSB0aGUgZHJhZnQNCndpdGggdGhl
IGhjcF9zaHkgSGVhZGVyIENvbmZpZGVudGlhbGl0eSBQb2xpY3kuDQoNCi0tIA0K
QWxpY2UNCmFsaWNlQHNtaW1lLmV4YW1wbGUNCi0tZmE1DQpDb250ZW50LVR5cGU6
IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNjaWkiDQpNSU1FLVZlcnNpb246IDEu
MA0KQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogN2JpdA0KDQo8aHRtbD48aGVh
ZD48dGl0bGU+PC90aXRsZT48L2hlYWQ+PGJvZHk+DQo8cD5UaGlzIGlzIHRoZQ0K
PGI+c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1yZXBseTwvYj4NCm1l
c3NhZ2UuPC9wPg0KPHA+VGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMv
TUlNRSBtZXNzYWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQg
c2lnbmVkRGF0YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5h
dGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVu
dC4gSXQgdXNlcyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGhl
IGRyYWZ0DQp3aXRoIHRoZSBoY3Bfc2h5IEhlYWRlciBDb25maWRlbnRpYWxpdHkg
UG9saWN5LjwvcD4NCjxwPjx0dD4tLSA8YnIvPkFsaWNlPGJyLz5hbGljZUBzbWlt
ZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tZmE1LS0NCg0KLS00
NmYNCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOiBiYXNlNjQNCkNvbnRlbnQtRGlzcG9zaXRpb246IGlubGluZQ0KDQpp
VkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFBQUFj
RWxFUVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95d2l3
WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1wTDJq
bzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00v
dWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0KLS00
NmYtLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
```

yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElfVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzE4MDJa
MC8GCSqGSIb3DQEJBDEiBCD0vcxZnCjxaOpfz5cIo9Maa0SVODPCXLJlV2Wbq4Z6
7zANBgkqhkiG9w0BAQEFAASCAQB3m6q708hB5tmuz6jzSJ+nCR7C0BRbfKypEnSP
k2tdLaOAJWrHqljSd4klEJWy3x2SvLL9q+rSbmIWpK34PWVL1E7gbbJIBjfpoIUo
+YMSIkhKFaKfUgulEi0zQG/HgnMENl6CDXa5ZrbW53SEpNpYgchUcqpg6Z0yOB07
oH7YOqF2111RRSzsjNMMDAm/1LvOFBR+nUERAhHvq1dpGpNuvbtAh4itWLLbDLlR
gIvrihHbqaUhf4VDQNg4MWjdHGATgPHNAb4hpfaxHxGEv+NYB/65VQWKGKMZujqk
aLH9nVThiAlEOyirAA7VlmvlUQgBem0pjh6ixnwK9HfPb7pG

C.3.15.2. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_shy, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-reply
Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:18:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
References: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: Subject: [...]
HP-Outer:
 Message-ID: <smime-signed-enc-complex-hp-shy-reply@example>
HP-Outer: From: alice@smime.example
HP-Outer: To: bob@smime.example
HP-Outer: Date: Sat, 20 Feb 2021 17:18:02 +0000
HP-Outer: User-Agent: Sample MUA Version 1.0
HP-Outer: In-Reply-To: <smime-signed-enc-complex-hp-shy@example>
HP-Outer: References: <smime-signed-enc-complex-hp-shy@example>
Content-Type: multipart/mixed; boundary="46f"; hp="cipher"

--46f
MIME-Version: 1.0
Content-Type: multipart/alternative; boundary="fa5"

--fa5
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

This is the
smime-signed-enc-complex-hp-shy-reply
message.

This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.

--
Alice
alice@smime.example
--fa5
```

```
Content-Type: text/html; charset="us-ascii"
MIME-Version: 1.0
Content-Transfer-Encoding: 7bit

<html><head><title></title></head><body>
<p>This is the
<b>smime-signed-enc-complex-hp-shy-reply</b>
message.</p>
<p>This is a signed-and-encrypted S/MIME message using PKCS#7
envelopedData around signedData.  The payload is a
multipart/alternative message with an inline image/png
attachment. It uses the Header Protection scheme from the draft
with the hcp_shy Header Confidentiality Policy.</p>
<p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
--fa5--

--46f
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--46f--
```

C.3.16. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_shy (+ Legacy Display)

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the Header Protection scheme from the draft with the hcp_shy Header Confidentiality Policy with a "Legacy Display" part.

It has the following structure:

```
└─ application/pkcs7-mime [smime.p7m] 11505 bytes
  (decrypts to)
  └─ application/pkcs7-mime [smime.p7m] 7508 bytes
    (unwraps to)
    └┬ multipart/mixed 2832 bytes
     ├┬ multipart/alternative 1621 bytes
     │ ├─ text/plain 576 bytes
     │ └─ text/html 748 bytes
     └─ image/png inline 236 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-signed-enc-complex-hp-shy-legacy-reply@example>
From: alice@smime.example
To: bob@smime.example
Date: Sat, 20 Feb 2021 17:19:02 +0000
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
References: <smime-signed-enc-complex-hp-shy-legacy@example>

MIIhLAYJKoZIhvcNAQcDoIIhHTCCIRkCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAGlAuaN5i488nW0BLsFYGGzv05Z7lYU/2JcF
bCWNgMWKZXJg15jwdzYH+xrTDHMk3Lm3+zgK9UoV+SCIBH2canLBrEgBk7KeqP6C
XSZ5q9yxGyZ+CqJ8oMsjvhezu/F/WROolCP/ALvzwu3TMlC7WGX2VId+dkYbJlqh
84usiISToli4K5GBGP5TwCt40qFNq0oiCh3PMUyZQO2RxCqvW031j8J7ASKxA4gl
ilSjC4Qs5kf+TEUc+iylX8DQJu5t2CMmvtaBShCBOkxnqQlQC78JQxojZ+xEP182
HHqi3Mqd45z2mRl2GuJaMnlW/OhaUolY7AgDOTGDIY+8QeyiFJEwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEADR9K8p6a0/i4HviQ9Tt9Pb7R
NtG9AajTJ6rALd1mRmDlpwQjKLduufYKBCxxB60LkiTUXGPddtruirSbEsjOa3cs
ueHgTUPxC8z7Jpmjk0ab3pgilymcCB3ajskxKFNC+kssejHIc/fE8KoJO89fYMjv
J8BPk6giYB+FCfz9FEDGXxWjU4OQdmYRQlhRBHmaF7CIpCyjo2VnJJllp7STKfAe
nKbbEbBOsFfw3U2F2AfEmobmNixtNCaNFbdMQLV/k1+oGuAkggZC0+N+sSfAZ5DV
ZQvdd5ex5lNjMhSVh1qp152LcGbtQhP3qOhWaqDYjmDlP6nWP5/PrFgQjOcZBjCC
Hf4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEFzxfgxbmalkU7vL68qwqfyAgh3Q
LvLr/03CJmjSYS/t5iURfgrocyJrvZk3RW3i14gxNLDFElcTKR1fCuUGnaV9irYB
A4FUWy0QR8NUPbEihtDXlDuhfIR9bzGO5am3GdoNJWbNPEcC9Vta7QlDWjfzxNF8
NJw6q/SlZ1mAQCHq8p5dtBsRWsOH7gokScgyB7oOXBHnOmQ0ObUbJ9WcIbA8FNCg
tJDPxBTI8kDqduwhStetZwl0HrXspvSojb6+siJIFcah2p/hFc0Wxf0h1sz754wm
13q0t2BGGWippElLS9Xysuof+zbmwwA57FkJp53n0PsnKqhvKEo0ZyEMPkKu5z9p
XN40X/3PwrBxo4HoHut/N3HNwyJs7tb71/8AbmrTltAAHUhDYc1dCpza8wF4wGnC
kFxFVOE+3rTKIZdTmNdywyoBpobY8KSLheKrpaRGaeBv6QnFavph/1w4sdlEPGVa
CXNn35GjtB5bAE5dMkxbrEiaDi3DupuQFSxhNWzBPLVILWxBnjgDWaUhfVRSx5OX
MzU/GSefZ6lC4eynr9KG3F2EiRm12yNj/ORlZTm3dbfUxSp+mRO262nkj1UMcyLe
3eTwxK5yKH8pMNOuQOpEB6CGJY19I5zryFtdNb5BaPNSGznwkgMnX4qPEG18UXlq
yKfz/hjcLXYyYbM4ey/xh3uDRWXPXAtMnJpXDyvfDMSK/DaFI2eN02fdZ1Hnr7xD
MRAKrFGR0NDirjjxjYVGHkUeBCn9H+zz6bl0HdcNM132QtZHsYhIe6PSvmybZ/oF
R2uqR2uEJIFtoPAA+0F5hj26RBAoLeJhGddyvXfNp0X0Nun8FwzpsjN6nPwoyPN0
hedCV1Oi5XCuH6J6ShJD1etim8A7dxKduX6lp4ts/SHKN2wvnP95zZExvy9L3b9a
m/eWq28vri4i3MLcPbswFWkjBkgZ1DPuwwmv4c+6NeWyZSJMMK6ftZDuAKUfHwVR
```

VS+PHx4kT9vwg2KSzJKkbt9IaYDUrNbGsPJbZftigBS0z267GG2mYSjasSxv+uUX
bLkgoHEixJuUbg/Jvsncnby7JwJErgDnLN7S2ZGLyAaetyWBDWbZYFy0SQX0WrfZ
hEzgZ/F7oLfAqD9P5O+I2OSxl8tHVHCnRrAXaMUl7I1EArminSw+G8QTSoV8Hd0L
EwwpYKZMmaXf87+KApqYTYK+fv31eI7qaBB+8Hxia26eg9xMa/eI256J8MGPAPTu
3cwKCTDAG70GChrSIKZQJCNBZnbIq2gYWAyF2+BEVqsmy3mXXNcAuPxwbC4UUJQJ
lttVXZJpDrHqOrg17ew2WzvNTnVdPwvQLxSJsZpA1Yx7xnHKX3+U+MzLXfUkKg2E
LQ2O3o2OY0oaf7POL7yg9X0A/qiOsz7QaNQQTaG49M5G/GIXy5YifzbteZIa62RQ
GsCJfD8pibMs/rylNOkXpCXNwc5+gVJeb/9pAz+ZaAH3Bh8iHKtS13elDmudMcfw
/CnZiD9e3fmFuYZHAMQT4PwfRCz6VczxsJhNYTURJ6wiqybSoDXgXkHrx1jq7ZA5
LJmpXcSxAowigMM7bs0eQSzDCesSCFrT4AdsT02645pVS6nZex0P4MB0X7TPcB6x
6kelmj53tpG5zYlBon1A0tWz9rNPGU2AGrOuAMgotaol+q8Nq3r5bamJ7idQSUzt
Ow/vujhPnKU5Wt5XXBDaXl1+H5cfawdkDh8M+eaI1nGNQRhCI8+JNcRcLLMiZHDl
rcvkx38pksBWlEejze9y64GN0iA01tCdGTmIorxDjIJToeSOmqeDHTIiqFH2qsVA
O/zuWRE+3AnXrwivGePaCq9pO+ir4D/S8oZG0DJ6gQ29apgUJR/AxEd2w3g9vGC7
pnIp81vjZord15aGzSuM81+uk/By4PQ3kZm3Ot6vh0+/bSZK0VVo4Ow+wPfOna4F
Bj0AJi3s4oFwNLNq2qybjuEtS5ufImm5c9iAO+kIyXOMsLLJA3WJph0Ct+0dE73Z
89362hoH+JiDLp9jvsuECvaUIWSs5Y815GXrmtVbk4bgvNLX1X8619BjlPkMbMJj
eYSt/uDoOYth5VSJo1IdQGXznCXARz6QBX/UdoEqMNzAM7VOHOK2J6VpvN+WHxLW
hrIx6w3nEsfeikCm8s9sDkbrgJwmHT/WQDzfFArAkuRXNczJlEO1evLcz0YKnk/E
/IaFSs2dobuDDUXklmbxXYOW2Vk+VMt+svjEwCYLXpPOhqhufN1HIUqG9D//4RiB
/jrJOy8ci5fn2vM+czragUNNAusuCI9RnPgSyPHLwMyAXLZo3kWFtB68OKO9cT6Z
k1temLL7OOk0VBU4411Sc7S568kYXByU60JZtbdwnChId0YTszQ5cq5P/3tnlCbw
1HFc3yvlW2CLOB3wNmxo2jOmd48R2kmzV6Mc/C+P0VxIW0hh/gcVqt854WiQxVw6
aODr69oj59olH/bPa5wVICKO+3CrucfQWLi3eRNtGnQ2N23eZWFeayDZ+U63SDyw
Iubr9tRIwZNu2kvf2eHTLoLswoTF87SSbcHbzwpeLEbp250HodTkfL0KIAxcZMe/
zspTEUaOBysL/0z59X3Sk7lei4qpAP9uOGyvqK9iQw0N+G75v8VPWGwYDTsmAnb7
x/qZOpX3MS17i8f9rI75jYUpmU5l+HbOrPw6cywnvGKcjN+ElyE+VY1Eud/PL1hj
Q24GE8nC7EQnmKFuNXz0guDek/a7SMWgcp/VoPMd/1cI2Vr9Wwlhcf/FULqGROuC
ANeBlaUgZvDIWXqdimYAFjFBvx+pYlghcAyzymoKnK9wjW1xeyscr7vN8GKARjCC
WLMIhuX3AK2FQUcWpzjuAhQhleY1AbV0FKTk1pXLbfA526KxUDY9uEV+8M5iRpv6
uz4X01Pk7bwTSNkwGIRWT8SSbWA1VbGARsUinhFinhKmkvdc/CKDtPTdchkmcGEA
D+bIpuWKMhQdAnSCoi5XmcN+5q8PH7Ivw6iz6WHGjiQNoqYadiTr+AZu98uRnU0H
vbYXr63tBK60XIjPFcuHMnk8x6aQpUYAWYuaN+EvVvtecStf340tuPg0XWdh9ghG
/MfFiQMLOn4gT+vq6PZPlriCHU4Q97qmdwThrQQsr7kY0zcEF4zOuDxNAccK2UNT
Va1j0a/Ucn25l2UtMW+QSiz9IryWBhBAllqFdYOsgqYPMBnZx1fQ+DpNwmQ7E8XA
HES6WKGMZNZOJnpu443BPGHUnJk4SyrDKQwL2EfK5tsc0BoAGrGhKdSkdlAB9Z7/
rIfi5efz9HKv8rnHd2vxzXmdB6Lc3eKNC7ICNE5U9ow/Yd90aMBrIdK9f5imw3Uk
CL27LkV1x8aieahJTwwAVVBRZz27FgkmB1x2R42mj99zWZtecrSkGx8wj4/qscqq
39wi/tD8tR4iyqzoP8TDNP2YVmkFnSVSOYXeEMSrazTbdOi/sxKqTtx5sZQi9f/J
7K99QYOGkJmhjiCl5H/tA7kLD5HPC0fgPDB5m0lp31siMDij46r4ORahUjpPdtPk
IgtxhWdiJ+hn63rm6WFzoWRlfm/k9yxSsegOpYoCKgi24ZOH/84rtVOXfcMKz+in
+8mkwRVl7bQ7hKkNs9JwnQD37xx5HCw150wNivynBIGlP5ISsr2aRo+eids223FE
9R2TVNXtJp2Nmg6Y+LKbMdCUwaZ7w3vWT3sQmG0rn2nwb1ShnHvQ2Nlw7hAAEbqd
/I3dFrvVPxqm+Q60NVjXrACtIlfcTM+LSUc9MCXjgaxXlTMyiWgmO9m6UnEGtvWi
LGImq/0CHgW6YCT9bwLnPfkz2L1vk2p78gTUqlH77iXt8THE1WjBIB/GJl5LGInF
vI1lsLQMkK355Ztg5wk5FhD47k/EFzQWKfyn6+V1u3hfwG0Q5+FRwgYRS5nfA32T
XxFQIdL57tSXzSrQcDxIe6r2buKOW4glaHWF5kmbK8gchyes4fmvE+pL90s44SUK
ZqBkW3kjaGogZActlWZkq+0QcRYnti5KRyk7jzKT/9f1LLB4qdcrPwyotGKJWip5

pyiLwkxMgWxhociW9/3u1gPwu/K4w42zJQUtX3N5l7TvmPhfDU7L3ognCJeaZvbE
wEJ9KYb8JimYySr+IOrOQ12YVvm/Wq0ZCL9qb2E+Hbxxb9+1FvBt1WGp2zYnBVaY
RSuxr+TFu1IQtMgDjPD0glGiV8sCGXD1rSc4m6p8pSFlIrXNBEF26cianPaJV1DF
YSqqcopBNfM4zEIreRpp0Nhce6wKW7nhcxpwTnSrB+SZA8pjizoOxjSDllaX/wGr
ZDAEflXBwiC6cp9gWivHY2pA1d3LO9joVjfIfx5QxBc3vyYmJ1ATgoQIX6aLJq+/
Uh2hFTw//9lprqgpkKSdr/3TLKbXDlyY5ysVFKl7OAFUhbaLs6MbVrXaRHG34AOu
wTv2tsbFcq3qkqCrx7rf8mZXIyGEzbIhQ++I1jEVSzwz2E9ruH4jr3lM5d9uus6C
VMysVTCbLnwGKefk1Hh2OvSvF902US1PmbcwBFeoYy8XWdt+xHK8aIcbbj6xxBA4
tvBIsfAqCcKYovXdNtWO9Ex00eAIa77NUmLaRPCYWsmgGJ5NlYgNyP0yrsxz/6Xc
2lTcTotmEqMjWCRMdWvQnGUSWY0Qe/DsjtXrVcPjSCBdxZ8DWjCYI8mmmyo4lu1X
PSCMXwqcQDbGcvNHqzxy0eT72ZhL319aD7ealbqZ5got87H1fURQ/mkp/LRZyeu/
b9gAIL5UAQ+E+1NgQdY/meuOawNp3q0Wpkgl0bqglYdEUm77vGO+DlDTQ3ruxeb/
IdBiVypb7YlJcNx5/O3bf5JUyLpipeiwzXTeRH5vbzBKkmBsLFkwRW9H+AtI/DV1
OqhGyLon8JkPNO/1WC6c2ftQ2Kp73tT+dsQIObSrrkSXQ9nUaaPbStepczhPptwS
x4zxF8gsc68dZ0OsyjpcwiJaIm6gWseeB1bPW59IlinNHFhxq6lmt37n7a+VQCpC
oNvnfjGaVwoBW2SGX+Qsu6LQ/7ZBXbAn/ZfPABJOinn7xycBCArV1NAIr/CgrzUK
H3AhI+7f8UnG1JrOnMaJuIccp8LVzYlFIEleTOBLcKRK/5ye6dTR0OsX/bWLJiZr
wFLUpA1SH4KxPWQGFe1x+LCuXBIo6Q0q3STUkkgD07afCs6xaEZH9as/9jP2jpGO
ZLiV5Ii8/zZ22vHIt9EjjfvjPNDEgo9++RTw1cOJasWvgUAJcWhRwRzgTeXm8luk
IXnX/Q2HHCQthgIYTdPvJ81uH9TXfuKiT7kDnmbjXGhaPE4uUtV5mokuF65d2ZRy
nRYQTt7jEZ2Ve7+6h+AZi3KGW3xVvMibv2isGGI+tAUefrVAC1bKnRnj/3skzRz7
JyFIsOSEH51W6GiapYVwhwIya6Jbq2fCBY5c/0sEvjljQU845P6KjLfCUJ1UdOR7
aNp6L6piJ9V4b2vbVXeCmzVXAkphV1pkiz3H/KyMy/7HU77ROsrzWc1XPupAV9gA
4CaEAlOqx5VRgSpko0jQa+UJ6hvC8kOwhBx+Qq1D/GLAc5kL8nNdkLZfIyO/yLmh
+khKI9TEEEup5BJwGNw/DxZg+mnMG0wJdeT/y9oKqqBajQHgk2xRPyvEGjyi1zrq
HDgjY6YMalTwhxFNUSv8JoHbKU0WYjNDds1APqFbJq6EMs8HgVryDJjQT9ijrEE+
tWb+T1kPWxSWKR3sU6mXhVHqJVzcHMJbKj0kohDdb/LaNzD0SQr5RH/4uH3G57B/
n8PhgNNrkQ1snGmqw2JLfSRXpvdL2GA3ne7azpYRgELMs1FSfh5tTrFrWtc2dsvH
bxxPxQY7dBCC6qw02kTNHubYBuR0Dau4SNBivvFAVaqRpQ15OdeTPm8G5vEukpFc
Uxh8OcALRVOb5P3KjyIdCrDK3+i6Z7/dHKo+MeSbrKPdZtVWWPteUnB6pDt3GN1o
WLrJ2KIV7u2Y6NseJyV3G89BPUthwgY+WDKheo6vnNf284JZxfIqviIZIyrZcQWA
EhW5/b4KymtMHaB54A4MnhYrqqGQm918bgPJvQOW+cd2uEGe5Dli+Z2BxyHDhCT0
SPOgJLUPATJR4shHRpoduH3RWhTOe89s89LTnIRAjr+m17r10sTYbXxLwswUzQ6l
I5VXww6/HTp5Je2G1xtgLvOKYypTIFzxiPwjLn3rqfYJNQWcLQ8c9jWoviy3JSOb
xtwrY/fJ0mDceBFbUtgm/Gbeg5yXmN9EkOgRcdV7FWNGHziHIUQa1knXdEhWDLuu
0hqFcTUlRYMeoZCpnyEt75c8rmwmnVVGhb3FyLrUO9vVeyPvPuB0AiwK9dECvcz/
US+HkNoJSUdLC2/QVV2cJtJIb82c2AM1CaeMoTTjXMK9KyZOeWhBCYNULsR6FzeL
1GQwfJWcdiEEIbrvc/tkYHDnksSgDXxb14E5D2PWmkogtNAs+Uu0WLcz9AhhG9Zr
2YTTj1JA1vQ9Xq6XB/7cOqAXZx5dYqAJM1j7v0Ndget6bUUZluAEJzN5Q4xiK4Hk
BTJb/oSj1Ul2hMMsuQNeHVQYJQmlUpP43Nod6FdGlDsDSY/ZqMh7i6x4vqwjMjEw
LlGdpjgOrqB7RzBwFHzeP84vles38HBgnEIdnBQvQUEOoIMAHPrBNu4LJJgpQ47r
3C0F7J/1+d1otCFcfCmWmrwSrT2cSFVEmndEK39/TU5vSlKdm3Xtn6FtXA9iYNXt
5f3UGBNuuLfzp2n9A9pLTY2h57Hw2nJTZ1gZI9pA8H3akoSokGacL5ztXOONYHBx
4aC0uNNDPXzXCGlzTUjCKJyh+MhFSuFPjwRZNRgMintvJJlCs88A7x05v1B/+aEn
rz0eSyJoGa6AP1NJOfE7MzSL3bTzd/pi9fH4m3GuiOe1/v9O7GPoEmdJ8b3LhIKi
awgN4ugc4+SNuoNFOU1Z8fxejeMkGBot+3Kbuzbyq2i2qRIf6/O7owwFlA4urfEo
m/SvXwC+0069AqUVQfl3Bre/gnf9DweYOBGis4bKuWxcug4xYict9010eDU/8xeg
dfO59nBd+CMbqR8yAFu6buJB0E64sSJwWYVp4XWM+HRXSbJKrPqpb18Z2hzFCVN7

Hq1YNQGkGV1bn6z1uO08kY0gXY83qI2lfWtbX7Rf+sj1OuWdt6mkcq3Di0DamZNP
Kk9syvk6QndtHmHrivnXjWdMp6cjVnS8szBxBqiDKbvZHOrhfIIlBd/jIm3QbjXY
tPOooqqmIScHkWo+c5aSy7YUEXHNZO3DXWlyjAwYIf95gA752fPfaP7axmg7qFN/
d+KhAN5F+p5y+MYJYJmzEydWWuTNrAHjJXo1I+m6PKWm1Fpm5gUhrEyX6WFPxkga
IaF+Z36LenDmePleJ8YinC9FIzWaO04BC2Qc/K1JpCVWuHHQj9nfuc40lB6Q3O2D
A6HxBeE5vXHOFp6KWwDhucGSWeM/TILI/uiWH4lkvJVu6t+pGgOQl7+JHSDfPmgJ
oA3MVWdK5wPYekh6KtM2nLfpO8Coj+s7xXffq1haCcjnw3/qcQK84FcQrYKBX6Ve
4lM+bYTzvjfBY/TCDb9UoKuYsRdg1tPk3ACFaVso1nsHh4WM3ID5NyVBzwISn7D5
78Scp6oFZQ+5Bil8dSTfLhkCWN9DYP6TT4aqGUZlWYInbK5yMAIKMLN5heMjCziy
zvEsbjog9tCqiwSXLVz6CnqfB4swJe2rIiPi2dhR88Z825L5Fb/p6AUH/j/OkYrJ
9BITo8qSY0rz7Hac+WE+oPhL/BCcilVxZrDsGHhybup6qdJa1kjDaIadrJbe2Y/L
UoxPQomUoVzjPLyQ0IZFVx1CynBuJVtQzfGQ6HUaBApFWs3e19PlVikQOGiI7gad
aDAQrzR4zW1t7Wwfp1d8a9dNizwmmEn9VuycjLL7vFZ1Md1f3hJNFYFUS8dcS2ke
BHo6mMYE8zqEQ/MbSOTNFP7np1j0x/elqbF227CWL4bdUCPD5F7fM01lR6uvJeKh
xgWLeGNi+dtYAJ+x4Q8/Zp/zxq+djBlAuVa3pJWUENoE9qMOupvxIPTdihzWrEcE
y2tl6eO53d65H8FrvJBQ9zr7D0B742IDzXsCo+jx5tiR714DrGMQteXTrz+1NFMQ
NObzn4rCCFe//mcSlt8puhMhbe5wcvjA4bEpmghBjo0cOgegHkhPOPfFRRF1VD+T
Z8PAarUtXl7PM+mEZc+xQti3mNuDaPHGcbUWk3OXfX8ct4Na0TE4XaTEHKI6NaxR
7e6349X2JkULYoi7bFg2c1NZXDut+mnhtYYrPjdXbssljfZs/RBufDo2nWTHp01G
SYmlhr4N/TOrKfapzi91WUVltoGo+U5VyhXyt97KDcj0yEaCe3z3nNVhUAJGj2Dm
8ak/NmE+dShqxWOf7isCMr84lmUtQ/s/Qh3RUgKSf6qNoVZ2+pWhaXK+NuhKMnIq
MAF/NspdJ8r5uNhklb9O3MmzKuW26z3LgiVBfzkYecY57mre+iBo0zpioLBGk/pw
j1bXvQ/9Uo9frPPQQyHD/5M594sPZ+lu43ItvIoz0+SDcE9LlGQeO9KXaGC8R8Py
fx13oQ9IRbZ3BJngc4E9taY1KNWnj2rZY3GOtjfAVPXR2N6ARgFBWc0GIIcGJNc9
HIlw0rDaE8SHK0x4u6p67bY1R4qkpD5ejPHRUOQelIQ2I5oFJWwCqYYI5MeQ+DBx
oV0jfLysKAC14Vmc29pOxFh2tYJK/axLgSTCCP9a0bX2yS7gOonrmGyNm7qWJBXU
74ClITuOpPhbd7QZfekBjuwt+D9SkhEOJ6Ij8lf/pv+JzUgjkpe+lOxvHnfkIJqZ
IFbpokdcFUevEKWfHJQY08FYIlfHf91HQ/Lrb6MebrkW7bY1VKEROEANj3mlSQNX
GypZBRrCPJoDxRUHDyfH2t5GDzDv9eakpIuBm/fm9NSPgPkIvXbJkBqWrD+WjMNB
aRzi6C/HcQj9+eFVr9DfTBAJ90gkws0Fl/EmUMmTrBQzVj49MDbO7TyPntK1NYsz
csPeXy86g4+xbW0IAar2rXiJjVbcTZuPFCR/NtcRXwe+Gdw4MyPfcM8Y6Wa/ByQ0
3XbZdfwy69MuYnKJ5Ie22McGBEa3nODlpc23UeyDyxlf9jgsaktT1qIb+bFDE0YR
7aVZoyTzGZTWmw2Ae4rDQOW/SPq11roZ8vQxPeVnXVy4KJD/2JK5/sCXuRzXk4kX
0SVyOm0MeLNf+NWPIe4deeGaQAwtU2jQvnmuJkXHWcGAunwa4GW25ETxccqekt6y
k3PBKBeZejvoxsrteoYeOWHbPcvthlUkJfp2I9emnhTjELsqqvbEaS8DZ3nPbNnD
p8ug5WoUp9plX6gfl93Cj6I81B0KhtKzaiLXVRq9orNlacOyYieOKQhk+dpzIBDe
BqXB22FC225jWrKnwYzOVWFTyZfziarDDS+RjVjcWCDO/6OKsdl1d0zbp0VkXkEu
qix/0NgrilfwOZ4waYTLOu9ihN9KVHIgHOFn9q0BU9OngirE14bkuSu4KvIMmtyT
3eZo3Nm+bwWzJzlo4yogzlTgH0SGnxyoibzOXzMqFgLkVbWvqTnw9UZASvoLAyrS
SFctnufOoPlH9JrL+mfoU83prsRDMmOqudzyi5/xWh4IvamvvQsq5+3xsQr1duA+
W/HeZ8jx5hgO5UfexS5hAcgNs4Wz2NVCCl9fProSuYh9Caoz2PwlK87c/MliEqWc
jZ5oSk0+zwLXTp3xpv4MHwDzHwqV6Sdg+cOUtl6wlZp0vJVxPD5tljBU9EW2vjfF
Iq19LN50RLPQ7RpfCtJAIYUAuYGz0mwd66Q71d39Wx56wHA9TqQBTzNqI0CK6/mX
sRZKrMvLBTdHKk4Capu6ehFJgUt3Oifib6DWV6v5HUG14Dt4z8Bj9a3R66NBLWlR
K+2PoBYdd942K9XlMGBn3LJl4ALdvIcPBWj3GF+uGyuVe7wBlSx9CflX2WSI5YSg
UDSpg+5kGBqjvtMlI8+4lfWZWKxub8YY4IMzkQxJcbvfqIwwjrevtIArQbtPlZDG
q5zPmbmEot+ceJepsSmSeiEXJoDQJgbl6ZodjzNaAzLdOcGZI+qvi9m1S95VDfVG
qrLl6hDxECQwnHKXwGrH6Qt4lftSzDHOnWKRERbiAgu9JPEuek4MY4C3u6dteyC+

C.3.16.1. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"

MIIVUAYJKoZIhvcNAQcCoIIVQTCCFT0CAQExDTALBglghkgBZQMEAgEwggt5Bgkq
hkiG9w0BBwGgggtqBIILZk1JTUUtVmVyc2lvbjogMS4wDQpTdWJqZWN0OiBzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KTWVzc2Fn
ZS1JRDoNCiA8c21pbWUtc2lnbmVkLWVuYy1jb21wbGV4LWhwLXNoeS1sZWdhY3kt
cmVwbHlAZXhhbXBsZT4NCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5leGFtcGxl
Pg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQsIDIwIEZl
YiAyMDIxIDEyOjE5OjAyIC0wNTAwDQpVc2VyLUFnZW50OiBTVVBIFZlcnNpb24g
cnNpb24gMS4wDQpJbi1SZXBseS1UbzogPHNtaW1lLXNpZ25lZC1lbmMtY29tcGxl
eC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+DQpTdWJqZWN0OiBbLi4uXQ0KSFAtT3V0ZXI6IE1lc3NhZ2UtSUQ6DQogPHNtaW1l
LXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5LXJlcGx5QGV4YW1wbGU+
DQpIUC1PdXRlcjogRnJvbTogYWxpY2VAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6
IFRvOiBib2JAc21pbWUuZXhhbXBsZQ0KSFAtT3V0ZXI6IERhdGU6IFNhdCwgMjAg
RmViIDIwMjEgMTc6MTk6MDIgKzAwMDANCkhQLU91dGVyOiBVc2VyLUFnZW50OiBT
YW1wbGUgTVVBIFZlcnNpb24gMS4wDQpIUC1PdXRlcjoNCiBJbi1SZXBseS1Ubzog
PHNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHktbGVnYWN5QGV4YW1wbGU+
DQpIUC1PdXRlcjoNCiBSZWZlcmVuY2VzOiA8c21pbWUtc2lnbmVkLWVuYy1jb21w
bGV4LWhwLXNoeS1sZWdhY3lAZXhhbXBsZT4NCkNvbnRlbnQtVHlwZTogbXVsdGlw
YXJ0L21peGVkOyBib3VuZGFyeT0iZDM3IjsgaHA9ImNpcGhlciINCg0KLS1kMzcN
Ck1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6IG11bHRpcGFydC9hbHRl
cm5hdGl2ZTsgYm91bmRhcnk9ImQzZSINCg0KLS1kM2UNCk1JTUUtVmVyc2lvbjog
MS4wDQpDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0DQpDb250ZW50LVR5
cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIjsNCiBocC1sZWdhY3kt
ZGlzcGxheT0iMSINCg0KU3ViamVjdDogc21pbWUtc2lnbmVkLWVuYy1jb21wbGV4
LWhwLXNoeS1sZWdhY3ktcmVwbHkNCkZyb206IEFsaWNlIDxhbGljZUBzbWltZS5l
eGFtcGxlPg0KVG86IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+DQpEYXRlOiBTYXQs
IDIwIEZlYiAyMDIxIDEyOjE5OjAyIC0wNTAwDQoNClRoaXMgaXMgdGhlDQpzbWlt
ZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxlZ2FjeS1yZXBseQ0KbWVzc2Fn
ZS4NCg0KVGhpcyBpcyBhIHNpZ25lZC1hbmQtZW5jcnlwdGVkIFMvTUlNRSBtZXNz
YWdlIHVzaW5nIFBLQ1MjNw0KZW52ZWxvcGVkRGF0YSBhcm91bmQgc2lnbmVkRGF0
YS4gIFRoZSBwYXlsb2FkIGlzIGENCm11bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNz
YWdlIHdpdGggYW4gaW5saW5lIGltYWdlL3BuZw0KYXR0YWNobWVudC4gSXQgdXNl
cyB0aGUgSGVhZGVyIFByb3RlY3Rpb24gc2NoZW1lIGZyb20gdGhlIGRyYWZ0DQp3
aXRoIHRoZSBoY3Bfc2h5IEhlYWRlciBDb25maWRlbnRpYWxpdHkgUG9saWN5IHdp
dGggYSAiTGVnYWN5DQpEaXNwbGF5IiBwYXJ0Lg0KDQotLSANCkFsaWNlIDxhbGlj
ZUBzbWltZS5leGFtcGxlDQotLQ0KTUlNRS1WZXJzaW9uOiAxLjANCkNvbnRl
bnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdiaXQNCkNvbnRlbnQtVHlwZTogdGV4dC9o
dG1sOyBjaGFyc2V0PSJ1cy1hc2NpaSI7DQogaHAtbGVnYWN5LWRpc3BsYXk9IjEi
```

DQoNCjxodG1sPjxoZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVhZD48Ym9keT4NCjxk
aXYgY2xhc3M9ImhlYWRlci1wcm90ZWN0aW9uLWxlZ2FjeS1kaXNwbGF5Ij4NCjxw
cmU+DQpTdWJqZWN0OiBzbWltZS1zaWduZWQtZW5jLWNvbXBsZXgtaHAtc2h5LWxl
Z2FjeS1yZXBseQ0KRnJvbTogQWxpY2UgJmx0O2FsaWNlQHNtaW1lLmV4YW1wbGUm
Z3Q7DQpUbzogQm9iICZsdDtib2JAc21pbWUuZXhhbXBsZSZndDsNCkRhdGU6IFNh
dCwgMjAgRmViIDIwMjEgMTI6MTk6MDIgLTA1MDANCjwvcHJlPg0KPC9kaXY+PHA+
VGhpcyBpcyB0aGUNCjxiPnNtaW1lLXNpZ25lZC1lbmMtY29tcGxleC1ocC1zaHkt
bGVnYWN5LXJlcGx5PC9iPg0KbWVzc2FnZS48L3A+DQo8cD50aGlzIGlzIEEgc2ln
bmVkLWFuZC1lbmNyeXB0ZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3DQpl
bnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWREYXRhLiAgVGhlIHBheWxvYWQgaXMg
YQ0KbXVsdGlwYXJ0L2FsdGVybmF0aXZlIG1lc3NhZ2Ugd2l0aCBhbiBpbmxpbmUg
aW1hZ2UvcG5nDQphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBIZWFkZXIgUHJvdGVj
dGlvbiBzY2hlbWUgZnJvbSB0aGUgZHJhZnQNCndpdGggdGhlIGhjcF9zaHkgSGVh
ZGVyIENvbmZpZGVudGlhbGl0eSBQb2xpY3kgd2l0aCBhICJMZWdhY3kNCkRpc3Bs
YXkiIHBhcnQuPC9wPg0KPHA+PHR0PiDxicj5BbGljZTxicj5hbGljZUBzbWlt
ZS5leGFtcGxlPC90dD48L3A+PC9ib2R5PjwvaHRtbD4NCi0tZDNlLS0NCg0KLS1k
MzcNCkNvbnRlbnQtVHlwZTogaW1hZ2UvcG5nDQpDb250ZW50LVRyYW5zZmVyLUVu
Y29kaW5nOiBiYXNlNjQNCkNvbnRlbnQtRGlzcG9zaXRpb246IGlubGluZQ0KDQpp
VkJPUncwS0dnb0FBQUFOU1VoRVVnQUFBQlFBQUFBVUNBWUFBQUNOaVIwTkFBQUFj
RWxFUVZSNDJ1VlRPeGJBDQpNQWdTNzM5bk8zVHBSdzIwZHFwYmZBUlFFak95d2l3
WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtFKzZLd2taDQpzZ3J6ZmNxVk1wTDJq
bzA0NDdnWURwZUFyaytPbkpIa0loQWZUUFJpY2loQWY1WUpydzd2anYwWldSV00v
dWxpDQp2ZFBmMVFaMmtERDl4cHBkOHdBQUFBQkpSVTVFcmtKZ2dnPT0NCg0KLS1k
MzctLQ0KoIIHpjCCA88wggK3oAMCAQICEw8tJb0ROZdKzkJUh6HuPTQGirQwDQYJ
KoZIhvcNAQENBQAwVTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cx
MTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3Jp
dHkwIBcNMTkxMTIwMDY1NDE4WhgPMjA1MjA5MjcwNjU0MThaMDsxDTALBgNVBAoT
BElFVEYxETAPBgNVBAsTCExBTVBTIFdHMRcwFQYDVQQDEw5BbGljZSBMb3ZlbGFj
ZTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJqVKfqLwaLjj+gBUCfk
acKTg8cc2OtJ9ZSed6U3jUoiZVpMLcP3MUKtLeLg9r1mAfIDlB/wlbdmadXPmrsz
yidmbuZmOpB5voVQfiLYYy3iOx7YOqzXrl6udP07k0sV+UdSNRFxrfKeoQEFXgOa
Gdmnx4OG/e3p1fIKM0dPzZLoOAJF5m5O0xzXPL74zFCWp2f1ZkuE4A6l41koaZXC
N5XL7wWTLMLeNf9Byb5ksKqUuqEHAMd1nmoNMgjY9VfVfcrv9w43GG8FtpSX+TWz
B2zNS2OF+XIVnzRG5DeoULq8v88Z5bLpIJ/nx26r8A4SSwIBaVv4wPxAf1iPsIVK
arUCAwEAAaOBrzCBrDAMBgNVHRMBAf8EAjAAMBcGA1UdIAQQMA4wDAYKYIZIAWUD
AgEwATAeBgNVHREEFzAVgRNhbGljZUBzbWltZS5leGFtcGxlMBMGA1UdJQQMMAoG
CCsGAQUFBwMEMA4GA1UdDwEB/wQEAwIFIDAdBgNVHQ4EFgQUolNB1UQ8gCkVfAEj
8OeOr83zdw8wHwYDVR0jBBgwFoAUkTCOfAcXDKfxCShlNhpnHGh29FkwDQYJKoZI
hvcNAQENBQADggEBAIFJeKCcsTKcFqQMpTryujRGzJdYA+R9eBAuDLsatbtKtl4F
zkgRyOg31/+Cw7H8e30iLrPIFlWN1qjHrjgOyIs5AQ/hgxLvLir3hEUV2Z3MRsMt
jH2x9SG91PEM046gfPnc9gMGHjMTg1qvaKcLQP5UzpEYPLror2X4P5uXxaP0LIZR
zWmkw1RF7FOD7PfB5v94M5274XYxW2W4uKGd7QGnUZROSvSYkGiWDp1JhqXwfDz8
A0enITGXnoEkAFvvjiCqh64P1hIeMorj36pgL19oWZD6YrzSWHUz1F00juyuOfQs
qm6hvrDTqNpHNZ015fOURza1SkCvi9GFmNUPoVgwggPPMIICt6ADAgECAhM3QQV5
7XV/QqmiXDr0+GrOmqnXMA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYx
ETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENl
cnRpZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3
MDY1NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUG

```
A1UEAxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQC09InoWDgWPk2af0+StijSNOR8K/hN8D+l078oullsk4ASvSwjsCNo7sHU
a4xQUl5JO6VqY18LANwORjrc9BaX4MguzsbFXBe6uFh1mVpXmFxSpUByQ+950MFz
/evPgP96wV+z4TtAwW2Z34rTiz4DxMI07XYNFUEOls/gkUP2GxzymsO2kaYWTut3
SryCqeHEFbZFkB4urMk4xrIJC3CzWruS2Q0FHbBlfkgKN5wXVgkWFfiOucfCn+IQ
saqpo1d3f9jSkbtAV5w3vzfog8919MxKI9H6l4KuElnAtJ7BtZcsl7dUy9u9COgE
ykRiVokFQgqQ7XNDU+r3SeOWwks7AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAX
BgNVHSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUu
ZXhhbXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFLv2zLItHQYSHJeuKWqQENMgZmZzMB8GA1UdIwQYMBaAFJEwjnwHFwyn
8QkoZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQBziaI2p86poGkjd/4KkkOH
G25nY/0eNARD6/oF0/sYonX2doizcGMk53riugAocCn5zbzhW/JVdYn30UxfyrZl
RAzEf7GHqgB/NyjOad3pdpVYeDh4ciNKjbs+aEoTWgAkoqENt1sRxlcvb7HVX524
bKZa1oPTUNlm6QpivtqDIdqGJdGf8L1zLfXBuo2zL3HR+M9CDr4Opq2JCkzP0Qhp
7poIccGE6I9Tsg+RrOA9iCQsPn1+Tg8YedjGzUWF07rNmT0TzPCVzUAuBlr+JJtz
OKypyQ3eoZ6EPazXqMyHAVcsm0GI364IOA0b8PSrJNtjh+AqJ5QfH+0e7NSzNnEm
MYICADCCAfwCAQEwbDBVMQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBX
RzExMC8GA1UEAxMoU2FtcGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhv
cml0eQITN0EFee11f0Kpolw69Phqzpqp1zALBglghkgBZQMEAgGgaTAYBgkqhkiG
9w0BCQMxCwYJKoZIhvcNAQcBMBwGCSqGSIb3DQEJBTEPFw0yMTAyMjAxNzE5MDJa
MC8GCSqGSIb3DQEJBDEiBCDmeJ6lsrSkjN4AZBIkFqDsd0GBqHEAIhAZzSPkodWm
CTANBgkqhkiG9w0BAQEFAASCAQA8+6A0jm2WrDdfvFYh0OQ4Rpy+6ofiRnx5jI8I
a0iD6U77+KS/1W9c4rm5Sk2ElE7gZb/XL5D7l9X5aoiuF6KgyPrzNCL4G3Zz9zLY
1l+7Cc+VsR8HcY9mgI5U34bmT1xZCHk3V+hTSUn+zE2XV5khxX0E5OxGzkrSz39Y
TReERGZGPPXorUIc/MPPKVNE0uhlVUY3WVp9oECnYOBnZ8Ed91rzJWH9hbvUq+jx
22s5mbPGSi5napgEIr/vv66CuCSBK9oqUG4/dyd/hvLVgtZ3knoxn8VPXUgf8Yw6
my5/oStqcO3Q9Sd176LsZ4Otgc4kG789qHAlTax4HGqU3bAi
```

C.3.16.2. S/MIME Signed and Encrypted Reply Over a Complex Message, Header Protection With hcp_shy (+ Legacy Display), Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Subject: smime-signed-enc-complex-hp-shy-legacy-reply
Message-ID:
 <smime-signed-enc-complex-hp-shy-legacy-reply@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:19:02 -0500
User-Agent: Sample MUA Version 1.0
In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
References: <smime-signed-enc-complex-hp-shy-legacy@example>
HP-Outer: Subject: [...]
HP-Outer: Message-ID:
 <smime-signed-enc-complex-hp-shy-legacy-reply@example>
HP-Outer: From: alice@smime.example
```

```
   HP-Outer: To: bob@smime.example
   HP-Outer: Date: Sat, 20 Feb 2021 17:19:02 +0000
   HP-Outer: User-Agent: Sample MUA Version 1.0
   HP-Outer:
    In-Reply-To: <smime-signed-enc-complex-hp-shy-legacy@example>
   HP-Outer:
    References: <smime-signed-enc-complex-hp-shy-legacy@example>
   Content-Type: multipart/mixed; boundary="d37"; hp="cipher"

   --d37
   MIME-Version: 1.0
   Content-Type: multipart/alternative; boundary="d3e"

   --d3e
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit
   Content-Type: text/plain; charset="us-ascii";
    hp-legacy-display="1"

   Subject: smime-signed-enc-complex-hp-shy-legacy-reply
   From: Alice <alice@smime.example>
   To: Bob <bob@smime.example>
   Date: Sat, 20 Feb 2021 12:19:02 -0500

   This is the
   smime-signed-enc-complex-hp-shy-legacy-reply
   message.

   This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_shy Header Confidentiality Policy with a "Legacy
   Display" part.

   --
   Alice
   alice@smime.example
   --d3e
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit
   Content-Type: text/html; charset="us-ascii";
    hp-legacy-display="1"

   <html><head><title></title></head><body>
   <div class="header-protection-legacy-display">
   <pre>
   Subject: smime-signed-enc-complex-hp-shy-legacy-reply
```

```
   From: Alice &lt;alice@smime.example&gt;
   To: Bob &lt;bob@smime.example&gt;
   Date: Sat, 20 Feb 2021 12:19:02 -0500
   </pre>
   </div><p>This is the
   <b>smime-signed-enc-complex-hp-shy-legacy-reply</b>
   message.</p>
   <p>This is a signed-and-encrypted S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the Header Protection scheme from the draft
   with the hcp_shy Header Confidentiality Policy with a "Legacy
   Display" part.</p>
   <p><tt>-- <br>Alice<br>alice@smime.example</tt></p></body></html>
   --d3e--

   --d37
   Content-Type: image/png
   Content-Transfer-Encoding: base64
   Content-Disposition: inline

   iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
   MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
   sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
   vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

   --d37--
```

C.3.17. S/MIME Signed and Encrypted Over a Complex Message, Legacy RFC 8551 Header Protection With hcp_baseline

This is a signed-and-encrypted S/MIME message using PKCS#7 envelopedData around signedData. The payload is a multipart/alternative message with an inline image/png attachment. It uses the legacy RFC 8551 header protection (RFC8551HP) scheme with the hcp_baseline Header Confidentiality Policy.

It has the following structure:

```
   └─┬ application/pkcs7-mime [smime.p7m] 9580 bytes
     (decrypts to)
     └─┬ application/pkcs7-mime [smime.p7m] 6082 bytes
       (unwraps to)
       └─┬ message/rfc822 1876 bytes
         └─┬ multipart/mixed 1828 bytes
           ├─┬ multipart/alternative 1166 bytes
           │ ├── text/plain 392 bytes
           │ └── text/html 490 bytes
           └── image/png inline 232 bytes
```

Its contents are:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
Subject: [...]
Message-ID:
 <smime-enc-signed-complex-rfc8551hp-baseline@example>
From: Alice <alice@smime.example>
To: Bob <bob@smime.example>
Date: Sat, 20 Feb 2021 12:28:02 -0500
User-Agent: Sample MUA Version 1.0

MIIbnAYJKoZIhvcNAQcDoIIbjTCCG4kCAQAxggMQMIIBhAIBADBsMFUxDTALBgNV
BAoTBElFVEYxETAPBgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFN
UFMgUlNBIENlcnRpZmljYXRpb24gQXV0aG9yaXR5AhMPLSW9ETmXSs5CVIeh7j00
Boq0MA0GCSqGSIb3DQEBAQUABIIBAIGTjqXl+E6A5sPoSiC4rgKQPp/Sq9KlmiYZ
kHuhai6C1kyLR/I+dsQNtJb+T6nUMs6u0C8lHLFMolShXNbmU0UFxbzTjBmz6qdb
gqzLeYdkT+l+EuFrsgQ8XtDNqIZHHo6u0c4lZWxdJ1kBGaatjQjzo7qA4fG1uQ/A
NDPZHozuhLE5/Q2+0CTbAawvfXDmA+Ss+Sh5vVxtw7evOxNoRPzypAvcc/gLCly9
C5RJDy2ctavux6LmC89561I25uUHhgSxCaVT8lxhUMxvgCeN0nWBDp1n68Xy836V
d2LKSiEq0INfA4O0OrsujxP5WJaJm4xh+eSUQcCpPcJEGBMuWaUwggGEAgEAMGww
VTENMAsGA1UEChMESUVURjERMA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNh
bXBsZSBMQU1QUyBSU0EgQ2VydGlmaWNhdGlvbiBBdXRob3JpdHkCEzB8R0APhiY6
HGLS64MvlsDXhpQwDQYJKoZIhvcNAQEBBQAEggEAMVD52+ksD3N5L7ElKbclg44f
WmBMTTsrUeL+q+sqHAzPNf+7x2Yitv9X4QjctucZQNo09s41d7WiaV6TtMvCExcM
Vi+bu0jPHiei2WxtASZ9arH0W2+aB46Iw7UTbrwl3EXSAN5IXFIyeQTl4mjte2Rd
Mxp3o0z42WOzsfAh+3mr6bNvoSiS2WUbvwP36VfWir1GT1wf2Wdv8a0iCcSE0jIE
5oKEenck4jNNxXe3i30L3x3FR51piNpxcxo60iuJcyNpBnzjZ6FLzPDKyqPLzhDg
mBMG4XyMsNeL8fq5Yjjuuz7xtUKQi8lEih5G1MeeLCy7IyPR1vzraIe42CNpwzCC
GG4GCSqGSIb3DQEHATAdBglghkgBZQMEAQIEEFNM7bcQDJtZl9ZLfi1Ni2aAghhA
nYiY1WB73GOhddIjiceKCfuPfWFmUwC3zkyxz5Qgh/O7UYL2YXPH/+W2xZnSl1U5
eHN3eLqCmsRC2bRfPApVda/ZW7J2GCEHYORRg44m1k7bLrQACA5PDn3T5cYT+syq
evYnIqK0tAcqo7cphQZ/n/uwdvkPWvkn8dQe0H8RTw+CsMPo9SezKr3hyJTENhre
Tswyoow5httSgHf1vSv51dKJMuKAGvXW7AaAImuNh6rtknzXS+VzUNVh0FvzgLUA
36SzeFdJ1NTrpM04p/Du00S9saLdxF0O1TMLaungoLMZgM60ZCCLi3z4CFuQyIlt
UB2viRGOfJhkePgWaoty6eLvllTXKCXb10ehMU7f8VowVwRWm62h0/SYvPBuGuXJ
```

```
   7GEVYHlrp4aXR2KQbeMoyxxY5hUGKWzDg4zJc1r80IAZXc64s7SR01x5BVinXhSE
   w4VGQ7Qv3CpolKQeuyQ14XK7/nzlkYWdXLFefuU528gHy42Xt+FaKR6ZElFURPdr
   0IIWN+Gdr28bpQomhbmhm71Srz7q3IIG3wXEh/qrxWf0yzSrrJluLcCAh9dyWM3e
   vfuneXrnxTr9Tf1GW/rNygZoHMvrjpSRIrzEAqqCzt/Vs1+ds0TBHn5fs9E2poIW
   9bXm54ucpXavu5ZafpHUReTrXLMGPJ+IkyGGVrACwAsIDYm/aPSM4HA41DzHtkY8
   q/HRYWR6So7rlYEo74bY2e+TyOJhSApZ87b2I1JMkHUZeB3aAPswZeMdZoA0HF+K
   HK2zXm1havuDecCc59q+DP4ROnfMbAU2ACTxvh+dJzX9GdifCUeh9NXn73fb8f50
   7k3GRbg3TgoUDJmfbU8wxeHtx7DvaylbaRLAW8CT0fyedJFGl7qhL3izlhHp9Jjs
   SzZpzlLCP/Yv/O6zNuP0RsR0WuaqYdK3qppgIoGta5Z+ZcHxLAhlrxr/mF1qxDoP
   sFhG/UoPSLT/lyzYN4pbBqC/QRuC3gr0MMKHpBm7G6gJppBW74se9w4IwIBmlnO2
   f8T2FgobF7Z3ne1LRpLCDcaQhFvCyN1IRu9PJH5Kcc0hGYqIAH7t6JPRfcImNbtS
   W8Y5bcZ0/1S5kY/Q9NpeAiUDVNdt0qdYEOtcNSpPhi9TrtqULD5EpGJscO5Gmkcn
   ATDL5nzJdLB7XvRQKi+FeWIzUzlr+IH7ik37WGkjZwwt+ClY1kAjgX39poUJTf+7
   r/gaI0pg/vz88lqZk6vgRQmIRwBv2GvLEfvMz0Ohf9vAwzYxbc3uj64/5aXJbsxr
   PxpatoiRJu+pF1nh6bPK+THYTnej2tlG1zLWuEvxZvHnUqlWNh4cRsuwm6Cf0H/2
   kv0HY4Rcnjiz13aPMIU/zjg0rkfmPfZfofyPJfNsiXC1h8Cty0HKZC/nWlLg0pJg
   hm+FbvUIrvhPhMKMJgY3nOqF6eEkwqnZpWzQxp8wcaVNsP10GoBG3Lef1MbSnsIh
   rUx6OyXXdpxaIgRWJQpXkSd59z5VTIyEbJj8iil/GEqqXs0WMGOnlRE+o9sR21Za
   +m65T7hsq0U776EWjZwcrb44rn/sW+mg+8+leuXL4UNADrm64qXvCcIkHrTpPRML
   k/W71PtYybEx8eZRkEG3tIWog3HV8w+WRKS1smFYvFxw66eU9cFDnKoYJAQi7USq
   fdkW/QLuXUJuGvpKGGWm8IJgOezbGPkbiYw+BTMJKExgXStAhAhhVFP3m/47AUx9
   bGiRMGgEBvprT9Iu7mydHOjUO//qRm6fUXOYJ5Xm8OUjk/wI/wOCdtO66tw/d9L4
   n2skZbRlMEdSja62427CHLCedZAWyyTaCdkj3QiC/vfj74okv+U7SsDyUWxnSK0p
   pMZESdV8qUpPRjT9Eh6BSD4B3SrGDuhSEdNuW60Qb2Yab0ZjWaurJeGqVn23A+tR
   u92mwIBB4K/9w9LGv6NXRVoLuSZ7wxcERmM9aXg4f6UjPKijbPzADnPrahqsZ4hb
   TpbxZkU/U6KmNmO/l9M5KZjfRMO87dIA8K8e40eJoqGeCyTezC8SzuKy6w26bLQQ
   TonyUBgbpnRzPg3dx6A6Qfr+H7E1XXDTTWcoY9FCGPuYkkmjYgjRW/7phcASXgHz
   76+C15RI/CdZh5q2hCZE7L9dqHO3sX/12pyR/DCoGDNlO0x/u9xqBo6mxR3LTYf3
   RP6TVLKnT70ynXDmYjaJMaMWj/+EKsip70TxZanpHeh74lO+YWpvKL5PQtxvSko+
   EohJTUaPjxG6EJj4K7Xu4aq9UqW7c0fyYM1oOabQaB9ZY1K3aQdRwvY2D7//bCo9
   56J84DhlKfp1MkakehPJFY3FvParM9kRYxf7CnhVdQX2UkAi5xasZRK020ksUr0k
   sOM1TvefRZbgaffX+DhtvvbUvFlit7PVwjc5Q0c5YiLELlgSqTpKKnO+IL0u0X3H
   pZmms25AZqtY8VZEtjuFv5XoZK/HtF646ipe0yawWi1JoNGSw50CVz5zy9YtcfPI
   Gz56LodAyQVl7CHSZCRE9tTlyyFxsZzyfK+AqgcahrdT7sc83lpd3PiwAjUL0VCg
   8EFNHILF3VT9+DsjGZJbqvoITgB51p0i4cdXgS3/yaZ0aESnZBAnEBUXtQQL9wqP
   l8UcDog+kvMK37AYeqGgoseh6ZvJXd5hIMj6WesXUTOQy6IGzZciDAPeNUdMmW0U
   NivI9SL8uxbSXG8NB9Q63xHj6J8WjNaNzWZPEr/qylfzQaP7uywTKXr4cVTVYwKG
   TZGZt1OZnymvwWoH7LhJ5qS1pPqe/4gNijCcngBmRpeG0qDHOSFJ//3Lncg94gnJ
   N8f9Y8zUkulrO2LHsTuzz0I2YCZsP42ZgL66H3uy7MkvgYYFO3IHrSim/evQqS/Z
   WKpHRCO2Cof8hta9pZQsR6WBWCxCUSEbgcBskZVg2iApVXVDgDyYPHIt0KSUef1S
   QKsXXlCT7IR4g//0MRP2RyKcrYiIkz09auKYex7CNyQYZfqeeMKUuKw5gXjMZS/p
   jV2Enoo1UG2kzAYFL2mRzdbaxeoqXVvbgErM4c7WKkomfoGIP6Kk4mOWwcEvPozJ
   pNxUOCPIUBoRcXMuoZp0u0bvU30EBRX+gJWYqRi9p1dnc9EXzm1MHX7Ui6xT6ZCv
   DF7YhBWV2GvGC+YKR5IJpXEPO0l5PEnGi3cNV9htahhtQWK8DiYjR4BOtHQ0mZRL
   NGWRyDbV60ac7pvl/wPwCEEfySu2dT4hvFIEn17B2oLKxowoJsEzOeOF+C23xR9n
   HfMNe/Fd2JtxJ6WJfpYmG/hvdYY5FNt4VlNpK/guwMbjbYfuRbHhCb5AG0gbxiIx
   bszWSIv/af5aFhQWh7eXZcSZoJ3PZIK2z6r9ALFaGy69Qiswbgop4VGs89kjBrZQ
   42+eD859Xw2zr8YRuskKIrAdl1jB2txZQYZQkHhzMjagEgc6scYEgikMTRyMDY2T
```

```
   PgJtyLi11Vec6ZQ29/go9N/rIYDmYx1wN/eBM7SqvQqkhE6AerBhiGetmllgRn8i
   BbCgc8ClQUbVQ45XQzE3mhm5UnAbJWofEdHJabShy1hoMfuFQFXd4b4okMUFOw9H
   hTi3daOLjmqgo47E1OHalXt4MItAhLXP9+GrhVE5vYN1h/cVRA94K8MlL+5HzT1f
   l8Rgls8gLVKV1D+BlXFw7JfS04vAtfv62ttuEinRUicte2rMKi4RKa0m7FYGiD36
   QleGa9W69kkJOxpykFAR6qX/UE0TVydER4+6f4/43Pu53DQs3HqoKsW65q1xb3vX
   zci638qUL4lu2LjmxWmeBm8vRyhY84QR95qI/RHoYWIXNSEXggcX2Evvow+cOrc6
   s3C3KjD08EyT7CKtqOyApOHcWhFI3gLvgJf7kd4hvZ3IsgZ0TPpNhPoOLw7OwWtX
   qX3akv8xPBPQ2DfUSuoJyhoMQFLx3zVL2Bl7wm5Q+TqcjM6R56MGfvBGuMmbEIQ4
   Wm4NY7I8LPN58UeKJ3A2pxhRXG/s/q8PMZUJeXL5QtYBonMFNnISS11T2cP8bB/G
   LYTC3q8aejWKSg+mX15sovgxDGFFR/Ru2y/Rlx2Mk76tJPr+8nbCYVnNFfdlZEkc
   htdwLlm1ocXvtb4bjKyMkd9LqH3bDfBAapQquQ+6FG3wTedEsEvPOxvg3byYYXb/
   E/nvvKhX5Dp90jNkhlGhGfDmoJwJCXutvvd+tnhIFFlarvqfo6zFCQXetwFgBEgg
   SYXUugaiovw5r09/7fJs4+9Lwr8phsH1tNibweWGmh9o3GM8tGgxfhaOtikRWx3y
   MpKecxe9RWUufrUwScDYpTI7sjnqHAjm3qT4YCTnX0QsYeE14yXUo+fTU5WA4evq
   xzNcaHo+61Y+/rgB6TFYIQg1tRINAp86EB930uKbJN6xga2QjICTZlvzF9aperRF
   Tcmqws2kESiyvxZBGbVhqGSPn7fBknlbAA8MLHhBQVhiA7h28biGv5gOnhipApDo
   lRDxJh1q37N0fLOxQXDzuqUt44MMY9CqFZxeRDTcq/dGHztoKum6NHHZTbA9ugnT
   ZzcFrtK3yor5ahbjcsWO+44cq52TSRBZy4yGL14+oMD1TbePqRyKdpuUxNeaZmex
   80fBFBDN1p095LRb85tOtLzXDALvhshpuWVn+sH8uC6clrJ/x+LRP6idSiTDlglE
   +yRzeG3YXa2LtLbE+PjDmFla9cOeO89nNGvqYKoqjDYFdnAgX99stX2gJ5pZKuzn
   k8lGBnH1/ytiRKMlNOVQSROQuRniUnlM7UjAuvDt4WhpOyo6d4n5EG03IrAs/0ms
   0fd5KwaQV2kM7gLVWC8EDFFPAQtLjVXnbqrJHnpnzb8+3Umdc7bbtTHrHdvbOgXW
   Qi2IOPME+CC4pY7QVjLdW7EUHtWzu577RVyjCgKnh4qVtPSqnDk0lfogprqO8Oos
   9UUNreV+Ie06Mk54JjGsw4yeKYTYl0zEuxZ2X1ec6ah5pDdofAln5uOwAMBVBodL
   q388bcdVtmLWKd0TEc+3Jx+fGCUQfQJq18lpzx6gPm1h/61QXF9R5JPc1fiA7gJ7
   hpSLRkiQrXZ7tvpxRAFdK9xp/hyKfo8SBPYGZAKvt7H8Wv3akP3hPBhDsKdTg2yL
   kZciqnm8fa+A8QM6fjHXF9CQ7kAKL5Kyzrn+hQ8gndovU5hKCmLOOPRKC488lXGX
   sHqQMP/36DGjEGXyGmmlCIDWiuIfHxQ9vaDZB9c5muWYbI00anAUBiPsuQYDOvap
   vyxeONavr53nofOv/AlrMUBiEaJcokDU9LjdqqbmO2DBwhqL7Qkju+fvgl8+jOtB
   8BuGWtTHFpvXY0wQARIfEonj4qM4PM/TmZYggqaWkSgqCfcMKa0LoIEHLe3k927w
   TKnKuorWmjdSm0PzWzekxVuEvwmMPWCkL/MRhDkbgm1tCrc58UsgdznEy2K15c/W
   BPc9dhuzhyAP30tgN8NiPjANFymRYlZ1XRibTFrWbGZ4JkUr7rjLAJVhMb3a7TBB
   16Bl226lYu2cfbEpJNr/yTvG67xEB8dGA0etD85ZaKGCtvTN4K13SsCEvkNydf7L
   GjzW7UvGHnYQoPZ7c+rLLAvmQpLsbsvZDIidYvq7GjO5C+N3K/Kz1VL7RQOabErj
   I+xB1lC/D+LOUjFsZiphJjI57P6wAL3euP9Y6Ytr+SJQmndw6Nkq3t8l2S0FWMVz
   zLeAvJ4SaRHy0ERQ/nrfGTIx2GmTZUvrsrn9KUtBn7dPLmyKqzl3zYf55nLNA+Gc
   LheU12GH5K4Qja3qKEnpz0KpDXuEFyxA7iFvcKEqJm2f3fEJ2KfSDeNdNDFf642m
   oX3Z7y3dls4iKds83wjOPORCo8j9ro03GxSCjmlgTHnR5sM1bYrye6oh0pw3SjyB
   8FAKn+qdH4Z/ndk/K/UqZ8MyDJAXuSQu6rHaEv9zz2K6HfyLqX83obnFYE3WNHzY
   TFFLKqw31A5ZRtCUTN0D6LfZ0ikwrgB+pWzfzGvRbghK+sGKweMEFF2Cbn0z3A3g
   bvC3sG6/rxBFZ/iU3Yd6hBiRMjqUUojsl9zSowRlkbUIRXZteaDnhz5qwcmPt3rO
   iod4Z2QmnW8mJM0OT8uX0MBIFwCjKRgqKHfjeTnT1NCpxOH5+6DJrj0mEPhfOB1o
   nHKJor6EOMU4zsDAZHCcepPyvRfLTp7TvUf0D5RBkqNf6JfGoPTLQ6JClQnMOPzS
   SlFAodd2Qng3q5fQh9tiaohZdyf2hN+lb9bvac1LUblSZM6mS/JenvA/+NVVoqdh
   3IEAepXOHv6B0PxN7V/R4JtTgVIJTWbC3TyLdseAii+Y3yEFFKIUABGGd2mSpJNV
   mPze3fiKmsfj+O5kcKb7q+EB0/CDSU+upSFmRSq2YbyM+P5/1faoUz2Nny+ee5Z7
   0YVfMt6jhWqZgvpdTaVzbKiQ/aCQmmRnxEwRQ8fhbtXrnzdebHK7sFuqn5mtsfgR
   jL/s+D5nQLkc+VtpslqaOXFAFz+iGLFuA2FDuwIkECu4qoMsE0EP+gbcQlEbjAx2
```

oR82st4KgqDeBga/3GTqx5TN0nbn584ujZ+VAYy0UZjShlH+4NJY1GMRHlA1b3kA
hWtP//PnkX1aZFVGWAHhiPIneG/ZCtRGUWqWUMn9DRd5BNMS7S/xl17KIF9lFbLS
6b5f5R5J/wjdwCC8mH0CCNXrdWRID3vqVEyBvH4usBoA8v64+ttQIUSttweBoG6W
Al2Qorxi8wZGqZ6qLp4glATHp2Ni1Aq90kP2cBfUNkP5GLdBD61O2qoBLtUuRliA
T25cdgz1JOtHrFsKJ4t04Udb8PWSr5DuFINhjcDP/wMthFRhCrLSipJsOEzreASD
C1fuEYbwD2or7UiWaZC37ERT10VC+kyNS2j/bxNubKpXWgOH0TWT0LdXjCj3OsDN
llhPugAjgZOpx8f+wyaucDExq6ubMcMtE4QLng7ivqw7vJFs51FIigskVPRnB0ro
k6rPrEMP/zgVSEBt0ULp2CG0RdUnPCLTlGR/B9F3WRfjHhowbnYANAZU1LgR/doC
qEkgjxVKfThjV+Xf9BWU6sBAVvq/I8O5hdZEn6ALRDrSnusIwmfVTdkbl6uSQD1p
MZjuGe+TkSpUY2CUIVucmmV6HCVJm4H+J3U9bsmQOWeCtR1kDKLaquuqYCjJk1NB
vJOaDR/0NJizyCpC4seGJ8gPRKV4VDvcH3jCjNOXFc9sS3YQdJWS13NpYoZkBymg
CR6Gf4WX5Mt8yhWPBP2ZYCF9yj6B30SVd8UU/01/v3z3kH8gtni7rwq9YX5+SOx4
h5FKsYkYFbt+Llh9BEaHvYF7ENwT3IS6tIs+A5g06By7O8pPoEKrZclMYAOpZste
nKrOIJNLjUNtHyJFI5K6o98GGJ3REHJ3i83rfkWO31G5SVgYqk72m7j/dlJ28x68
A2iqgtcaZJgzgAKYQDz7Lyvbd5lYaEU0yt+CjhsJjS6JmTab23D5iovFfoD+AmpX
5GKRKIHv1JF6ok8wQp9dKYDNmocg4m+oqIngVoioLn1N0A370i8yhC1qmFXpEwox
saxFq/hBWHKmxJlCxEFBF/AYw8M9ibOwOJA5r0U4Lg/+3UiUKRimbX6X8R+FS3c3
5Eqs0RH1VDzTvu4aaIb5OfVZCjX/L9xT4ezXZqbR7JSGryHZr/CNH+8AtfTXEC4U
xAmFAXgfuNc18ZkVtSLPjJ418cSe+VOlQ3WH2Os2N3PP6UqR7hlgymJeisV80C0N
kuu0AYauvHf6mDPhbsvdtTLQUY9cQ991c1XFB3NZwZa1GL9BtYpLU9xsd4k+qyzI
5zW1UEG0B265+FhYBMz12KRvjfTMegaMCqo3WKG0p/HfdGRFXzYScZCDKe/n7pDW
45+PhVyrxqQpsdyxTHb0qetjbYM/OlydenM47tvb9D+UIpRjYLmk3RCMKfbAd6nE
ctVLhUHswCMx4lnVRdIXuIc4yQrquAVPvlfzBVIxDeemkf2kmrA1P5aYZniflr7i
SRG+XntvfKyyKqr09A605hOz8GyDSOIDRq5SykbeuUZd2MkhMHiqn3pkgWxfFADH
rptkhjQytcY4j8Znqg8O70da9J4G4sbILV5OgKaTt/7okM+rQ8ikzR9UJsAAgewn
DrnutsyrGrSmz7wIFkexxWnM6NZYMcJpdy0KXuctfBWIQs+ZyYrsd4pH3MP/hc+1
t2W57Gm57dXBh0lqxDnaGFGVBlYioWj/v1s0EoaVUM+XCYEsRKge45drULGh0qAZ
sG1/1VBptLyt3UY3jh1tUw==

C.3.17.1. S/MIME Signed and Encrypted Over a Complex Message, Legacy RFC 8551 Header Protection With hcp_baseline, Decrypted

The S/MIME enveloped-data layer unwraps to this signed-data part:

```
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="signed-data"
```

MIIRQAYJKoZIhvcNAQcCoIIRMTCCES0CAQExDTALBglghkgBZQMEAgEwggdpBgkq
hkiG9w0BBwGgggdaBIIHVk1JTUUtVmVyc2lvbjogMS4wDQpDb250ZW50LVR5cGU6
IG1lc3NhZ2UvcmZjODIyDQoNCk1JTUUtVmVyc2lvbjogMS4wCkNvbnRlbnQtVHlw
ZTogbXVsdGlwYXJ0L21peGVkOyBib3VuZGFyeT0iMjY2IgpTdWJqZWN0OiBzbWlt
ZS1lbmMtc2lnbmVkLWNvbXBsZXgtcmZjODU1MWhwLWJhc2VsaW5lCk1lc3NhZ2Ut
SUQ6CiA8c21pbWUtZW5jLXNpZ25lZC1jb21wbGV4LXJmYzg1NTFocC1iYXNlbGlu
ZUBleGFtcGxlPgpGcm9tOiBBbGljZSA8YWxpY2VAc21pbWUuZXhhbXBsZT4KVG86
IEJvYiA8Ym9iQHNtaW1lLmV4YW1wbGU+CkRhdGU6IFNhdCwgMjAgRmViIDIwMjEg
MTI6Mjg6MDIgLTA1MDAKVXNlci1BZ2VudDogU2FtcGxlIE1VQSBWZXJzaW9uIDEu
MAoKLS0yNjYKTUlNRS1WZXJzaW9uOiAxLjAKQ29udGVudC1UeXBlOiBtdWx0aXBh

```
cnQvYWx0ZXJuYXRpdmU7IGJvdW5kYXJ5PSJkYjYiCgotLWRiNgpDb250ZW50LVR5
cGU6IHRleHQvcGxhaW47IGNoYXJzZXQ9InVzLWFzY2lpIgpNSU1FLVZlcnNpb246
IDEuMApDb250ZW50LVRyYW5zZmVyLUVuY29kaW5nOiA3Yml0CgpUaGlzIGlzIHRo
ZQpzbWltZS1lbmMtc2lnbmVkLWNvbXBsZXgtcmZjODU1MWhwLWJhc2VsaW5lCm1l
c3NhZ2UuCgpUaGlzIGlzIGFuIGVuY3J5cHRlZCBhbmQgc2lnbmVkIFMvTUlNRSBt
ZXNzYWdlIHVzaW5nIFBLQ1MjNwplbnZlbG9wZWREYXRhIGFyb3VuZCBzaWduZWRE
YXRhLiAgVGhlIHBheWxvYWQgaXMgYQptdWx0aXBhcnQvYWx0ZXJuYXRpdmUgbWVz
c2FnZSB3aXRoIGFuIGlubGluZSBpbWFnZS9wbmcKYXR0YWNobWVudC4gSXQgdXNl
cyB0aGUgbGVnYWN5IFJGQyA4NTUxIGhlYWRlciBwcm90ZWN0aW9uCihSRkM4NTUx
SFApIHNjaGVtZSB3aXRoIHRoZSBoY3BfYmFzZWxpbmUgSGVhZGVyIENvbmZpZGVu
dGlhbGl0eQpQb2xpY3kuCgotLSAKQWxpY2UKYWxpY2VAc21pbWUuZXhhbXBsZQot
LWRiNgpDb250ZW50LVR5cGU6IHRleHQvaHRtbDsgY2hhcnNldD0idXMtYXNjaWki
Ck1JTUUtVmVyc2lvbjogMS4wCkNvbnRlbnQtVHJhbnNmZXItRW5jb2Rpbmc6IDdi
aXQKCjxodG1sPjxoZWFkPjx0aXRsZT48L3RpdGxlPjwvaGVhZD48Ym9keT4KPHA+
VGhpcyBpcyB0aGUKPGI+c21pbWUtZW5jLXNpZ25lZC1jb21wbGV4LXJmYzg1NTFo
cC1iYXNlbGluZTwvYj4KbWVzc2FnZS48L3A+CjxwPlRoaXMgaXMgYW4gZW5jcnlw
dGVkIGFuZCBzaWduZWQgUy9NSU1FIG1lc3NhZ2UgdXNpbmcgUEtDUyM3CmVudmVs
b3BlZERhdGEgYXJvdW5kIHNpZ25lZERhdGEuICBUaGUgcGF5bG9hZCBpcyBhCm11
bHRpcGFydC9hbHRlcm5hdGl2ZSBtZXNzYWdlIHdpdGggYW4gaW5saW5lIGltYWdl
L3BuZwphdHRhY2htZW50LiBJdCB1c2VzIHRoZSBsZWdhY3kgUkZDIDg1NTEgaGVh
ZGVyIHByb3RlY3Rpb24KKFJGQzg1NTFIUCkgc2NoZW1lIHdpdGggdGhlIGhjcF9i
YXNlbGluZSBIZWFkZXIgQ29uZmlkZW50aWFsaXR5ClBvbGljeS48L3A+CjxwPjx0
dD4tLSA8YnIvPkFsaWNlPGJyLz5hbGljZUBzbWltZS5leGFtcGxlPC90dD48L3A+
PC9ib2R5PjwvaHRtbD4KLS1kYjYtLQoKLS0yNjYKQ29udGVudC1UeXBlOiBpbWFn
ZS9wbmcKQ29udGVudC1UcmFuc2Zlci1FbmNvZGluZzogYmFzZTY0CkNvbnRlbnQt
RGlzcG9zaXRpb246IGlubGluZQoKaVZCT1J3MEtHZ29BQUFBTlNVaEVVZ0FBQUJR
QUFBQVVDQVlBQUFDTmlSME5BQUFBY0VsRVFWUjQydVZUT3hiQQpNQWdTNzM5bk8z
VHBSdzIwZHFwYmZBUlFFak95d2l3WW5DdGtES25iY0xrNjZzcWxUK3p0OWNpZGtF
KzZLd2taCnNncnpmY3FWTXBXTXBvMDQ0N2dZRHBlQXJrK09uSkhrSWhBZlRQUmlj
aWhBZjVZZnJJZ3JREQ5eHBwZDh3QUFBQUJK
UlU1RXJrSmdnZz09CgotLTI2Ni0tCqCCB6YwggPPMIICt6ADAgECAhMPLSW9ETmX
Ss5CVIeh7j00Boq0MA0GCSqGSIb3DQEBDQUAMFUxDTALBgNVBAoTBElFVEYxETAP
BgNVBAsTCExBTVBTIFdHMTEwLwYDVQQDEyhTYW1wbGUgTEFNUFMgUlNBIENlcnRp
ZmljYXRpb24gQXV0aG9yaXR5MCAXDTE5MTEyMDA2NTQxOFoYDzIwNTIwOTI3MDY1
NDE4WjA7MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzEXMBUGA1UE
AxMOQWxpY2UgTG92ZWxhY2UwggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIB
AQCalSn6i8Gi44/oAVAn5GnCk4PHHNjrSfWUnnelN41KImVaTC3D9zFCrS3i4Pa9
ZgHyA5Qf8JW3ZmnVz5q7M8onZm7mZjqQeb6FUH4i2GMt4jse2Dqs165ernT9O5NL
FflHUjURca3ynqEBBV4DmhnZp8eDhv3t6dXyCjNHT82S6DgCReZuTtMc1zy++MxQ
lqdn9WZLhOAOpeNZKGmVwjeVy+8FkyzC3jX/Qcm+ZLCqlLqhBwDHdZ5qDTII2PVX
1X3K7/cONxhvBbaUl/k1swdszUtjhflyFZ80RuQ3qFC6vL/PGeWy6SCf58duq/AO
EksCAWlb+MD8QH9Yj7CFSmq1AgMBAAGjga8wgawwDAYDVR0TAQH/BAIwADAXBgNV
HSAEEDAOMAwGCmCGSAFlAwIBMAEwHgYDVR0RBBcwFYETYWxpY2VAc21pbWUuZXhh
bXBsZTATBgNVHSUEDDAKBggrBgEFBQcDBDAOBgNVHQ8BAf8EBAMCBSAwHQYDVR0O
BBYEFKJTQdVEPIApFXwBI/Dnjq/N83cPMB8GA1UdIwQYMBaAFJEwjnwHFwyn8Qko
ZTYaZxxodvRZMA0GCSqGSIb3DQEBDQUAA4IBAQCBSXignLEynBakDKU68ro0RsyX
WAPkfXgQLgy7GrW7SrZeBc5IEcjoN9f/gsOx/Ht9Ii6zyBZVjdaox644DsiLOQEP
4YMS7y4q94RFFdmdzEbDLYx9sfUhvdTxDNOOoHz53PYDBh4zE4Nar2inC0D+VM6R
```

GDy66K9l+D+bl8Wj9CyGUc1ppMNURexTg+z3web/eDOdu+F2MVtluLihne0Bp1GU
Tkr0mJBolg6dSYal8Hw8/ANHpyExl56BJABb744gqoeuD9YSHjKK49+qYC9faFmQ
+mK80lh1M9RdNI7srjn0LKpuob6w06jaRzWdNeXzlEc2tUpAr4vRhZjVD6FYMIID
zzCCAregAwIBAgITN0EFee11f0Kpolw69Phqzpqp1zANBgkqhkiG9w0BAQ0FADBV
MQ0wCwYDVQQKEwRJRVRGMREwDwYDVQQLEwhMQU1QUyBXRzExMC8GA1UEAxMoU2Ft
cGxlIExBTVBTIFJTQSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAgFw0xOTExMjAw
NjU0MThaGA8yMDUyMDkyNzA2NTQxOFowOzENMAsGA1UEChMESUVURjERMA8GA1UE
CxMITEFNUFMgV0cxFzAVBgNVBAMTDkFsaWNlIExvdmVsYWNlMIIBIjANBgkqhkiG
9w0BAQEFAAOCAQ8AMIIBCgKCAQEAtPSJ6Fg4Fj5Nmn9PkrYo0jTkfCv4TfA/pdO/
KLpZbJOAEr0sI7AjaO7B1GuMUFJeSTulamNfCwDcDkY63PQWl+DILs7GxVwXurhY
dZlaV5hcUqVAckPvedDBc/3rz4D/esFfs+E7QMFtmd+K04s+A8TCNO12DRVBDpbP
4JFD9hsc8prDtpGmFk7rd0q8gqnhxBW2RZAeLqzJOMayCQtws1q7ktkNBR2wZX5I
CjecF1YJFhX4jrnHwp/iELGqqaNXd3/Y0pG7QFecN7836IPPdfTMSiPR+peCrhJZ
wLSewbWXLJe3VMvbvQjoBMpEYlaJBUIKkO1zQ1Pq90njlsJLOwIDAQABo4GvMIGs
MAwGA1UdEwEB/wQCMAAwFwYDVR0gBBAwDjAMBgpghkgBZQMCATABMB4GA1UdEQQX
MBWBE2FsaWNlQHNtaW1lLmV4YW1wbGUwEwYDVR0lBAwwCgYIKwYBBQUHAwQwDgYD
VR0PAQH/BAQDAgbAMB0GA1UdDgQWBBS79syyLR0GEhyXrilqkBDTIGZmczAfBgNV
HSMEGDAWgBSRMI58BxcMp/EJKGU2GmccaHb0WTANBgkqhkiG9w0BAQ0FAAOCAQEA
c4miNqfOqaBpI3f+CpJDhxtuZ2P9HjQEQ+v6BdP7GKJ19naIs3BjJOd64roAKHAp
+c284VvyVXWJ99FMX8q2ZUQMxH+xh6oAfzcozmnd6XaVWHg4eHIjSo27PmhKE1oA
JKKhDbdbEcZXL2+x1V+duGymWtaD01DZZukKYr7agyHahiXRn/C9cy31wbqNsy9x
0fjPQg6+DqatiQpMz9EIae6aCHHBhOiPU7IPkazgPYgkLD59fk4PGHnYxs1FhdO6
zZk9E8zwlc1ALgZa/iSbczisqckN3qGehD2s16jMhwFXLJtBiN+uCDgNG/D0qyTb
Y4fgKieUHx/tHuzUszZxJjGCAgAwggH8AgEBMGwwVTENMAsGA1UEChMESUVURjER
MA8GA1UECxMITEFNUFMgV0cxMTAvBgNVBAMTKFNhbXBsZSBMQU1QUyBSU0EgQ2Vy
dGlmaWNhdGlvbiBBdXRob3JpdHkCEzdBBXntdX9CqaJcOvT4as6aqdcwCwYJYIZI
AWUDBAIBoGkwGAYJKoZIhvcNAQkDMQsGCSqGSIb3DQEHATAcBgkqhkiG9w0BCQUx
DxcNMjEwMjIwMTcyODAyWjAvBgkqhkiG9w0BCQQxIgQgzbXAB7rXfNs26yYOHvuE
D4KQ9RzsSF5fL55lZZY7AjgwDQYJKoZIhvcNAQEBBQAEggEAAs1y7DQLS7S+Vh2b
Ju5W9UwkHp6lUk/F7mJE80FRc8K6z8pcSn4xTrlCaLgL7azQ0o/iNQEh2EVJqdy6
huwwtlaeiPa2gXwIHCKcLGhA2bW3/R+sEsJZi7FryqTakOZ9eXcYRXoPWv6ncf+I
eA7jlQX3Z4Ln5pP9p+Uw7H1oroH2Y4e0yAqIMtYXnS+GKALTtbxTa1p2Y9dsHQLS
2cXbfUsU2zc5bstgKXZyTkjuKJ8ivbYJ2ttk79AOMosWkDBmgzKTTS/0HptfO9SD
mX58BvQt6GHQZ4TR2NVDvq3z+/CAlzsR5xmNH1C+uDH99ORoy3w6CHmv4aTTmRM9
S+uZXg==

C.3.17.2. S/MIME Signed and Encrypted Over a Complex Message, Legacy RFC 8551 Header Protection With hcp_baseline, Decrypted and Unwrapped

The inner signed-data layer unwraps to:

```
MIME-Version: 1.0
Content-Type: message/rfc822

MIME-Version: 1.0
Content-Type: multipart/mixed; boundary="266"
Subject: smime-enc-signed-complex-rfc8551hp-baseline
```

```
   Message-ID:
    <smime-enc-signed-complex-rfc8551hp-baseline@example>
   From: Alice <alice@smime.example>
   To: Bob <bob@smime.example>
   Date: Sat, 20 Feb 2021 12:28:02 -0500
   User-Agent: Sample MUA Version 1.0

   --266
   MIME-Version: 1.0
   Content-Type: multipart/alternative; boundary="db6"

   --db6
   Content-Type: text/plain; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   This is the
   smime-enc-signed-complex-rfc8551hp-baseline
   message.

   This is an encrypted and signed S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the legacy RFC 8551 header protection
   (RFC8551HP) scheme with the hcp_baseline Header Confidentiality
   Policy.

   --
   Alice
   alice@smime.example
   --db6
   Content-Type: text/html; charset="us-ascii"
   MIME-Version: 1.0
   Content-Transfer-Encoding: 7bit

   <html><head><title></title></head><body>
   <p>This is the
   <b>smime-enc-signed-complex-rfc8551hp-baseline</b>
   message.</p>
   <p>This is an encrypted and signed S/MIME message using PKCS#7
   envelopedData around signedData.  The payload is a
   multipart/alternative message with an inline image/png
   attachment. It uses the legacy RFC 8551 header protection
   (RFC8551HP) scheme with the hcp_baseline Header Confidentiality
   Policy.</p>
   <p><tt>-- <br/>Alice<br/>alice@smime.example</tt></p></body></html>
   --db6--
```

```
--266
Content-Type: image/png
Content-Transfer-Encoding: base64
Content-Disposition: inline

iVBORw0KGgoAAAANSUhEUgAAABQAAAAUCAYAAACNiR0NAAAAcElEQVR42uVTOxbA
MAgS739nO3TpRw20dqpbfARQEjOywiwYnCtkDKnbcLk66sqlT+zt9cidkE+6KwkZ
sgrzfcqVMpL2jo0447gYDpeArk+OnJHkIhAfTPRicihAf5YJrw7vjv0ZWRWM/uli
vdPf1QZ2kDD9xppd8wAAAABJRU5ErkJggg==

--266--
```

Appendix D. Composition Examples

This section offers step-by-step examples of message composition.

D.1. New message composition

A typical MUA composition interface offers the user a place to indicate the message recipients, the subject, and the body. Consider a composition window filled out by the user like so:

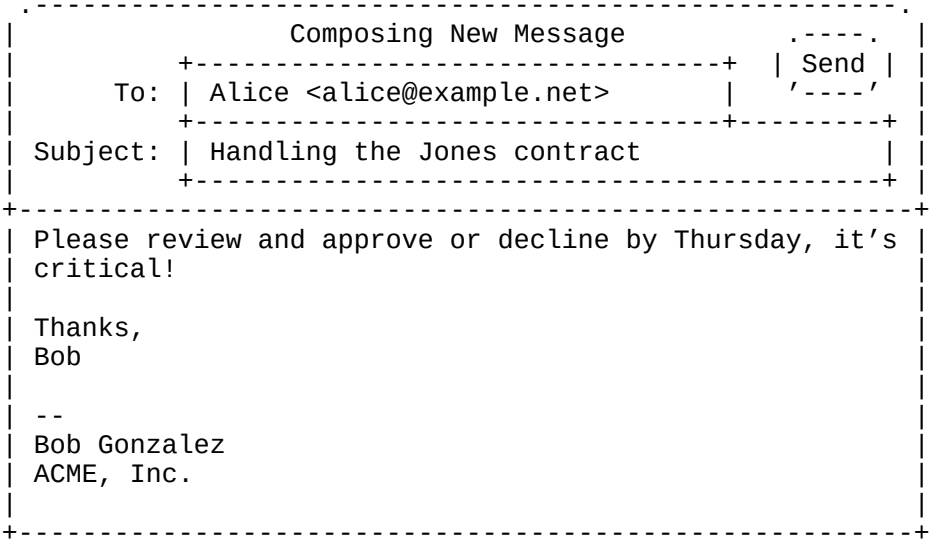

Figure 1: Example Message Composition Interface

When Bob clicks "Send", his MUA generates values for Message-ID, From, and Date Header Fields, and converts the message body into the appropriate format.

D.1.1. Unprotected message

The resulting message would look something like this if it was sent without cryptographic protections:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0

Please review and approve or decline by Thursday, it’s critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

D.1.2. Encrypted with hcp_baseline and Legacy Display

Now consider the message to be generated if it is to be cryptographically signed and encrypted, using HCP hcp_baseline, and the legacy variable is set.

For each Header Field, Bob’s MUA passes its name and value through hcp_baseline. This returns the same value for every Header Field, except that:

hcp_baseline("Subject", "Handling the Jones contract") yields "[...]".

D.1.2.1. Cryptographic Payload

The Cryptographic Payload that will be signed and then encrypted is very similar to the unprotected message in Appendix D.1.1. Note the addition of:

* The hp="cipher" parameter for the Content-Type
* The appropriate HP-Outer Header Field for Subject
* The hp-legacy-display="1" parameter for the Content-Type

* The Legacy Display Element (the simple pseudo-header and its trailing newline) in the Main Body Part.

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: Handling the Jones contract
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:08:43 -0500
HP-Outer: From: Bob <bob@example.net>
HP-Outer: To: Alice <alice@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <20230111T210843Z.1234@lhp.example>

Subject: Handling the Jones contract

Please review and approve or decline by Thursday, it’s critical!

Thanks,
Bob

--
Bob Gonzalez
ACME, Inc.
```

D.1.2.2. External Header Section

The Cryptographic Payload from Appendix D.1.2.1 is then wrapped in the appropriate Cryptographic Layers. For this example, using S/MIME, it is wrapped in an application/pkcs7-mime; smime-type="signed-data" layer, which is in turn wrapped in an application/pkcs7-mime; smime-type="enveloped-data" layer.

Then an external Header Section is applied to the outer MIME object, which looks like this:

```
Date: Wed, 11 Jan 2023 16:08:43 -0500
From: Bob <bob@example.net>
To: Alice <alice@example.net>
Subject: [...]
Message-ID: <20230111T210843Z.1234@lhp.example>
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
MIME-Version: 1.0
```

Note that the Subject Header Field has been obscured appropriately by hcp_baseline. The output of the CMS enveloping operation is base64-encoded and forms the body of the message.

D.2. Composing a Reply

Next we consider a typical MUA reply interface, where we see Alice replying to Bob's message from Appendix D.1.

When Alice clicks "Reply" to Bob's signed-and-encrypted message with Header Protection, she might see something like this:

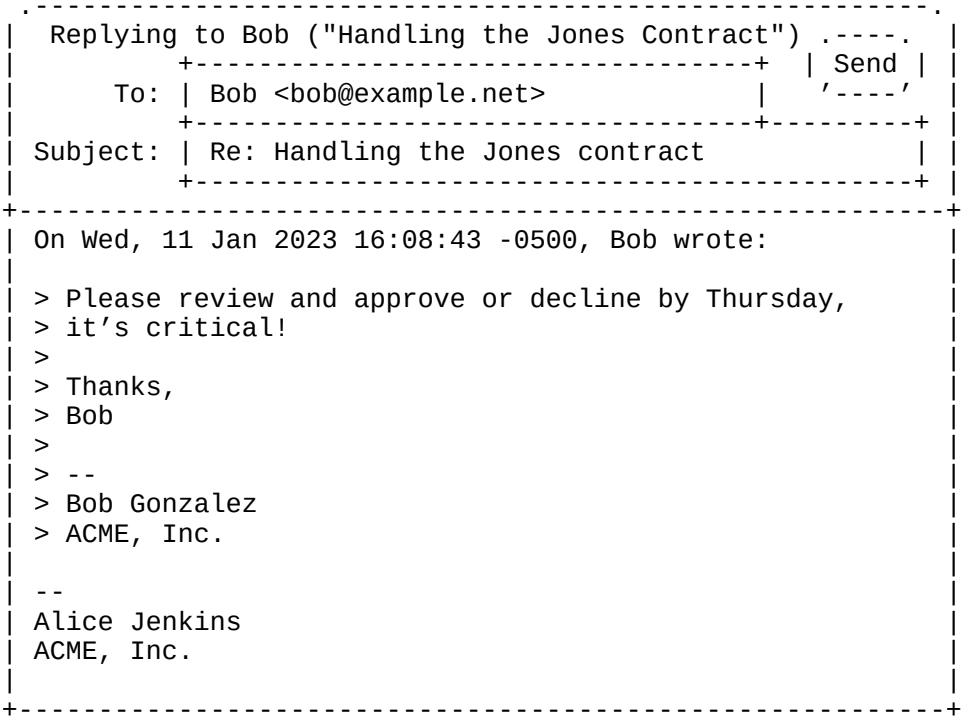

Figure 2: Example Message Reply Interface (unedited)

Note that because Alice's MUA is aware of Header Protection, it knows what the correct Subject header is, even though it was obscured. It also knows to avoid including the Legacy Display Element in the quoted/attributed text that it includes in the draft reply.

Once Alice has edited the reply message, it might look something like this:

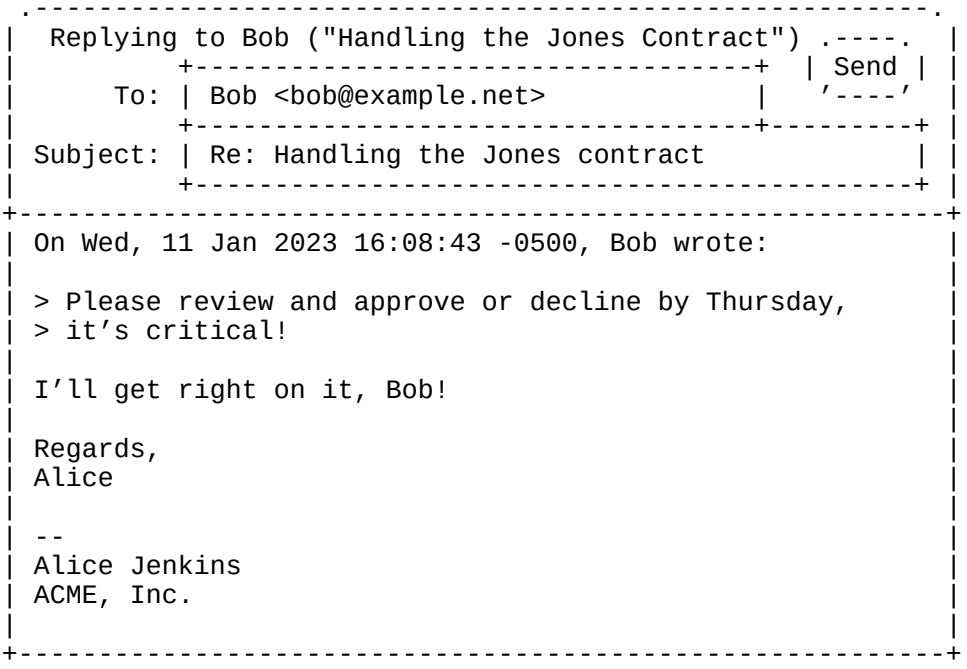

Figure 3: Example Message Reply Interface (edited)

When Alice clicks "Send", the MUA generates values for Message-ID, From, and Date Header Fields, populates the In-Reply-To, and References Header Fields, and also converts the reply body into the appropriate format.

D.2.1. Unprotected message

The resulting message would look something like this if it were to be sent without any cryptographic protections:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: Handling the Jones contract
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"
MIME-Version: 1.0

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it's critical!

I'll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.
```

Of course, this would leak not only the contents of Alice's message, but also the contents of Bob's initial message, as well as the Subject Header Field! So Alice's MUA won't do that; it is going to create a signed-and-encrypted message to submit to the network.

D.2.2. Encrypted with hcp_no_confidentiality and Legacy Display

This example assumes that Alice's MUA uses hcp_no_confidentiality, not hcp_baseline. That is, by default, it does not obscure or remove any Header Fields, even when encrypting.

However, it follows the guidance in Section 6.1, and will make use of the HP-Outer field in the Cryptographic Payload of Bob's original message (Appendix D.1.2.1) to determine what to obscure.

When crafting the Cryptographic Payload, its baseline HCP (hcp_no_confidentiality) leaves each field untouched. To uphold the confidentiality of the sender's values when replying, the MUA executes the following steps (for brevity only Subject and Message-ID/In-Reply-To are shown):

* Extract the referenced header fields (see Section 4.2):

  - refouter contains:

        - Date: Wed, 11 Jan 2023 16:08:43 -0500
        - From: Bob <bob@example.net>
        - To: Alice <alice@example.net>
        - Subject: [...]
        - Message-ID: <20230111T210843Z.1234@lhp.example>
      - refprotected contains:
        - Date: Wed, 11 Jan 2023 16:08:43 -0500
        - From: Bob <bob@example.net>
        - To: Alice <alice@example.net>
        - Subject: Handling the Jones contract
        - Message-ID: <20230111T210843Z.1234@lhp.example>
  * Apply the response function:
    - respond(refouter) contains:
      - From: Alice <alice@example.net>
      - To: Bob <bob@example.net>
      - Subject: Re: [...]
      - In-Reply-To: <20230111T210843Z.1234@lhp.example>
      - References: <20230111T210843Z.1234@lhp.example>
    - respond(refprotected) contains:
      - From: Alice <alice@example.net>
      - To: Bob <bob@example.net>
      - Subject: Re: Handling the Jones contract
      - In-Reply-To: <20230111T210843Z.1234@lhp.example>
      - References: <20230111T210843Z.1234@lhp.example>

* Compute the ephemeral response_hcp (see Section 6.1):

  - Note that all headers except Subject are the same.

  - confmap contains only ("Subject", "Re: Handling the Jones contract") -> "Re: [...]"

Thus all Header Fields that were signed are passed through untouched. The reply's Subject is obscured as Subject: Re: [...] if and only if the user does not edit the subject line from that initially proposed by the MUA's reply interface. If the user edits the subject line, e.g., to Subject: Re: Handling the Jones contract ASAP, the response_hcp will _not_ obscure it, and instead pass it through in the clear.

For stronger header confidentiality, the replying MUA should use a reasonable HCP (not hcp_no_confidentiality). Also recall that the local HCP is applied first, and that response_hcp is only applied to what is left unchanged by the local HCP.

D.2.2.1. Cryptographic Payload

Consequently, the Cryptographic Payload for Alice's reply looks like this:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: Handling the Jones contract
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
MIME-Version: 1.0
HP-Outer: Date: Wed, 11 Jan 2023 16:48:22 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: Re: [...]
HP-Outer: Message-ID: <20230111T214822Z.5678@lhp.example>
HP-Outer: In-Reply-To: <20230111T210843Z.1234@lhp.example>
HP-Outer: References: <20230111T210843Z.1234@lhp.example>

Subject: Re: Handling the Jones contract

On Wed, 11 Jan 2023 16:08:43 -0500, Bob wrote:

> Please review and approve or decline by Thursday,
> it’s critical!

I’ll get right on it, Bob!

Regards,
Alice

--
Alice Jenkins
ACME, Inc.
```

Note the following features:

* the hp="cipher" parameter to Content-Type

* the appropriate HP-Outer Header Field for Subject,

* the hp-legacy-display="1" parameter for the Content-Type

* the Legacy Display Element (the simple pseudo-header and its trailing newline) in the Main Body Part.

D.2.2.2. External Header Section

The Cryptographic Payload from Appendix D.2.2.1 is then wrapped in the appropriate Cryptographic Layers. For this example, using S/MIME, it is wrapped in an application/pkcs7-mime; smime-type="signed-data" layer, which is in turn wrapped in an application/pkcs7-mime; smime-type="enveloped-data" layer.

Then an external Header Section is applied to the outer MIME object, which looks like this:

```
Date: Wed, 11 Jan 2023 16:48:22 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Re: [...]
Message-ID: <20230111T214822Z.5678@lhp.example>
In-Reply-To: <20230111T210843Z.1234@lhp.example>
References: <20230111T210843Z.1234@lhp.example>
Content-Transfer-Encoding: base64
Content-Type: application/pkcs7-mime; name="smime.p7m";
 smime-type="enveloped-data"
MIME-Version: 1.0
```

Note that the Subject Header Field has been obscured appropriately even though hcp_no_confidentiality would not have touched it by default. The output of the CMS enveloping operation is base64-encoded and forms the body of the message.

Appendix E. Rendering Examples

This section offers example Cryptographic Payloads (the content within the Cryptographic Envelope) that contain Legacy Display Elements.

E.1. Example text/plain Cryptographic Payload with Legacy Display Elements

Here is a simple one-part Cryptographic Payload (Header Section and body) of a message that includes Legacy Display Elements:

```
Date: Fri, 21 Jan 2022 20:40:48 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Dinner plans
Message-ID: <text-plain-legacy-display@lhp.example>
MIME-Version: 1.0
Content-Type: text/plain; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
HP-Outer: Date: Fri, 21 Jan 2022 20:40:48 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <text-plain-legacy-display@lhp.example>

Subject: Dinner plans

Let’s meet at Rama’s Roti Shop at 8pm and go to the park
from there.

A compatible MUA will recognize the hp-legacy-display="1" parameter
and render the body of the message as:

Let’s meet at Rama’s Roti Shop at 8pm and go to the park
from there.

A legacy decryption-capable MUA that is unaware of this mechanism
will ignore the hp-legacy-display="1" parameter and instead render
the body including the Legacy Display Elements:

Subject: Dinner plans

Let’s meet at Rama’s Roti Shop at 8pm and go to the park
from there.
```

E.2. Example text/html Cryptographic Payload with Legacy Display Elements

Here is a modern one-part Cryptographic Payload (Header Section and body) of a message that includes Legacy Display Elements:

```
Date: Fri, 21 Jan 2022 20:40:48 -0500
From: Alice <alice@example.net>
To: Bob <bob@example.net>
Subject: Dinner plans
Message-ID: <text-html-legacy-display@lhp.example>
MIME-Version: 1.0
Content-Type: text/html; charset="us-ascii"; hp-legacy-display="1";
 hp="cipher"
HP-Outer: Date: Fri, 21 Jan 2022 20:40:48 -0500
HP-Outer: From: Alice <alice@example.net>
HP-Outer: To: Bob <bob@example.net>
HP-Outer: Subject: [...]
HP-Outer: Message-ID: <text-html-legacy-display@lhp.example>

<html><head><title></title></head><body>
<div class="header-protection-legacy-display">
<pre>Subject: Dinner plans</pre>
</div>
<p>
Let’s meet at Rama’s Roti Shop at 8pm and go to the park
from there.
</p>
</body>
</html>
```

A compatible MUA will recognize the hp-legacy-display="1" parameter and mask out the Legacy Display div, rendering the body of the message as a simple paragraph:

Let’s meet at Rama’s Roti Shop at 8pm and go to the park from there.

A legacy decryption-capable MUA that is unaware of this mechanism will ignore the hp-legacy-display="1" parameter and instead render the body including the Legacy Display Elements:

Subject: Dinner plans

Let’s meet at Rama’s Roti Shop at 8pm and go to the park from there.

Appendix F. Other Header Protection Schemes

Other Header Protection schemes have been proposed in the past. However, those typically have drawbacks such as sparse implementation, known problems with legacy interoperability (in particular with rendering), lack of clear signalling of sender intent, and/or incomplete cryptographic protections. This section lists such schemes known at the time of the publication of this document out of historical interest.

F.1. Original RFC 8551 Header Protection

S/MIME [RFC8551] (as well as its predecessors [RFC5751] and [RFC3851]) defined a form of cryptographic Header Protection that has never reached wide adoption, and has significant drawbacks compared to the mechanism in this draft. See Section 1.1.1 for more discussion of the differences and Section 4.10 for guidance on how to handle such a message.

F.2. Pretty Easy Privacy (pEp)

The pEp (pretty Easy privacy) [I-D.pep-general] project specifies two different MIME schemes that include Header Protection for Signed-and-Encrypted e-mail messages in [I-D.pep-email]: One scheme -- referred as pEp Email Format 1 (PEF-1) -- is generated towards MUAs not known to be pEp-capable, while the other scheme -- referred as PEF-2 -- is used between MUAs discovered to be compatible with pEp. Signed-only messages are not recommended in pEp.

Although the PEF-2 scheme is only meant to be used between PEF-2 compatible MUAs, PEF-2 messages may end up at MUAs unaware of PEF-2 (in which case they typically render badly). This is due to signalling mechanism limitations.

As the PEF-2 scheme is an enhanced variant of the RFC8551HP scheme (with an additional MIME Layer), it is similar to the RFC8551HP scheme (see Section 4.10). The basic PEF-2 MIME structure looks as follows:

```
A └┬multipart/encrypted [Outer Message]
B  ├─application/pgp-encrypted
C  └─application/octet-stream inline [Cryptographic Payload]
D    (decrypts to)
E   └┬multipart/mixed
F    ├─text/plain
G    ├┬message/rfc822
H    │└─[Inner Message]
I    └─application/pgp-keys
```

The MIME structure at part H contains the Inner Message to be rendered to the user.

It is possible for a normal MUA to accidentally produce a message that happens to have the same MIME structure as used for PEF-2 messages. Therefore, a PEF-2 message cannot be identified by MIME structure alone.

The lack of a mechanism comparable to HP-Outer (see Section 2.2) makes it impossible for the recipient of a PEF-2 message to safely determine which Header Fields are confidential or not, while forwarding or replying to a message (see Section 6).

Note: As this document is not normative for PEF-2 messages, it does not provide any guidance for handling them. Please see [I-D.pep-email] for more guidance.

F.3. "draft-autocrypt" Protected Headers

[I-D.autocrypt-lamps-protected-headers] describes a scheme similar to the Header Protection scheme specified in this document. However, instead of adding Legacy Display Elements to existing MIME parts (see Section 5.2.2), "draft-autocrypt" injects a new MIME element "Legacy Display Part", thus modifying the MIME structure of the Cryptographic Payload. These modified Cryptographic Payloads cause significant rendering problems on some common Legacy MUAs.

The lack of a mechanism comparable to hp="cipher" and hp="clear" (see Section 2.1.1) means the recipient of an encrypted "draft-autocrypt" message cannot be cryptographically certain whether the sender intended for the message to be confidential or not. The lack of a mechanism comparable to HP-Outer (see Section 2.2) makes it impossible for the recipient of an encrypted "draft-autocrypt" to safely determine which Header Fields are confidential or not, while forwarding or replying to a message (see Section 6).

Appendix G. Document Changelog

[[RFC Editor: This section is to be removed before publication]]

* draft-ietf-lamps-header-protection-25
  - Address editorial clarifications from IESG review
  - Update acknowledgements
* draft-ietf-lamps-header-protection-24

  - Deal with From spoofing risk: when inner and outer From differ with no valid signature, render outer From and warn

  - Add test vectors to show historical 8551HP variants

  - clarify PEF-2 and draft-autocrypt commentary

* draft-ietf-lamps-header-protection-23

  - normalize on "signed-and-encrypted" across the document

  - replace hcp_strong with hcp_shy

  - Remove "Wrapped Message" scheme

  - Rename "Injected Headers" to "Header Protection"

  - Add guidance about From Header Field spoofing risk

  - offer guidance on handling RFC8551HP messages when received

* draft-ietf-lamps-header-protection-22

  - Reorganize document for better readability.

  - Add more details about problems with draft-autocrypt.

  - Rename hcp_minimal to hcp_baseline: in addition to obscuring Subject, it now removes other Informational Header Fields Comments and Keywords.

  - Add an example message up front for easier explainability.

  - Unwrap sample message test vectors.

  - Name pseudocode algorithms, number steps.

  - Reply guidance also applies to forwarded messages.

  - hcp_strong: stop rewriting Message-Id.

* draft-ietf-lamps-header-protection-21

  - HP-Outer mechanism replaces HP-Removed and HP-Obscured. This enables the recipient to easily calculate the sender’s actions around header confidentiality.

  - Replace Content-Type parameter protected-headers= with hp= and hp-scheme=. The presence of hp= indicates that the sender used Header Protection according to this document, and the value indicates whether the sender tried to encrypt and sign the message or just sign it. hp-scheme="wrapped" advises the recipient that they should look for the protected Header Fields in subtly different place.

  - Provide a clear algorithm for reasonably safe handling of confidential headers during Reply and Forward operations.

  - Do not register the example HCP hcp_hide_cc, rename to hcp_example_hide_cc

  - Rename hcp_null to hcp_no_confidentiality

  - Provide a clear algorithm for the recipient to compute the protection state of each Header Field.

* draft-ietf-lamps-header-protection-20

  - clarify IANA guidance about registration policy and designated expert review

  - emphasize that Content-Type parameter hp-legacy-display=1 belongs on all main body parts with a legacy display element

  - clean up/normalize pseudocode variable names and text (no algorithm changes)

* draft-ietf-lamps-header-protection-19

  - improve text, capitalize defined terms, fix typos

  - Clean up from AD review:

  - updates RFC 8551 explicitly

  - add "Legacy Signed Message" and "Ordinary User" explicitly to terms

  - tighten up SHOULDs/MUSTs for conformant MUAs

  - expand references to other relevant Security Considerations

  - drop nudge about non-existent Content-Type Parameters registry

  - clarify IANA notes to align with table columns

  - explicitly request HCP registry

  - add references to other header protections schemes, but move all of them to appendix

* draft-ietf-lamps-header-protection-18

  - only allow US-ASCII as modified output of HCP, adjusted ABNF to match

* draft-ietf-lamps-header-protection-17

  - More edits from WGLC:

  - clean up definition of "Header Field"

  - note leakage of encrypted recipient hints

  - clarify explanation of LDE generation

  - clarify how some obscured headers might not actually be private

* draft-ietf-lamps-header-protection-16

  - correct variable names in message composition algorithms

  - make text more readable

* draft-ietf-lamps-header-protection-15

  - include clarifications, typos, etc from comments received during WGLC

* draft-ietf-lamps-header-protection-14

  - provide section references for draft-ietf-lamps-e2e-mail-guidance

  - encouarge a future IANA named HCP registry if HCP development takes off

* draft-ietf-lamps-header-protection-13

  - Retitle from "Header Protection for S/MIME" to "Header Protection for Cryptographically Protected E-mail"

* draft-ietf-lamps-header-protection-12

  - MUST produce HP-Obscured and HP-Removed when generating encrypted messages with non-null HCP
  - Wrapped Message: move from forwarded=no to protected-headers=wrapped
  - Wrapped Message: recommend Content-Disposition: inline

* draft-ietf-lamps-header-protection-11
  - Remove most of the Bcc text (transferred general discussion to e2e-mail-guidance)
  - Fix bug in algorithm for generating HP-Obscured and HP-Removed
  - More detail about handling Reply messages
  - Considerations around handling risky Legacy Display Elements
  - Narrative descriptions of some worked examples
  - Describe potential leaks to recipients
  - Clarify debugging/troubleshooting UX affordances

* draft-ietf-lamps-header-protection-10
  - Clarify that HCP doesn’t apply to Structural Header Fields
  - Drop out-of-date "Open Issues" section
  - Brief commentary on UI of messages with intermediate/mixed protections
  - Deprecation prospects for messages without protected headers
  - Describe generating replies to encrypted messages with stronger HCP

* draft-ietf-lamps-header-protection-09
  - clarify terminology
  - add privacy and security considerations
  - clarify HCP examples and baselines
  - recommend hcp_minimal as default HCP

  - add HP-Obscured and HP-Removed (avoids reasoning about differences between outside and inside the Cryptographic Envelope)
  - regenerated test vectors

* draft-ietf-lamps-header-protection-08
  - MUST compose injected headers, MAY compose wrapped messages
  - MUST parse both schemes
  - cleanup and restructure document

* draft-ietf-lamps-header-protection-07
  - move from legacy display MIME part to legacy display elements within main body part

* draft-ietf-lamps-header-protection-06
  - document observed problems with legacy MUAs
  - avoid duplicated outer Message-IDs in hcp_strong test vectors

* draft-ietf-lamps-header-protection-05
  - fix multipart/signed wrapped test vectors

* draft-ietf-lamps-header-protection-04
  - add test vectors
  - add "problems with Injected Messages" subsection

* draft-ietf-lamps-header-protection-03
  - dkg takes over from Bernie as primary author
  - Add Usability section
  - describe two distinct formats "Wrapped Message" and "Injected Headers"
  - Introduce Header Confidentiality Policy model
  - Overhaul message composition guidance

- Simplify document creation workflow, move public face to gitlab

* draft-ietf-lamps-header-protection-02

- editorial changes / improve language

* draft-ietf-lamps-header-protection-01

- Add DKG as co-author

- Partial Rewrite of Abstract and Introduction [HB/AM/DKG]

- Adding definitions for Cryptographic Layer, Cryptographic Payload, and Cryptographic Envelope (reference to [I-D.ietf-lamps-e2e-mail-guidance]) [DKG]

- Enhanced MITM Definition to include Machine- / Meddler-in-the-middle [HB]

- Relaxed definition of Original message, which may not be of type "message/rfc822" [HB]

- Move "memory hole" option to the Appendix (on request by Chair to only maintain one option in the specification) [HB]

- Updated Scope of Protection Levels according to WG discussion during IETF-108 [HB]

- Obfuscation recommendation only for Subject and Message-Id and distinguish between Encrypted and Unencrypted Messages [HB]

- Removed (commented out) Header Field Flow Figure (it appeared to be confusing as is was) [HB]

* draft-ietf-lamps-header-protection-00

- Initial version (text partially taken over from draft-ietf-lamps-header-protection-requirements

Index

H

Authors' Addresses

Daniel Kahn Gillmor
American Civil Liberties Union
125 Broad St.
New York, NY, 10004
United States of America
Email: dkg@fifthhorseman.net

Bernie Hoeneisen
pEp Project
Oberer Graben 4
CH- 8400 Winterthur
Switzerland
Email: bernie@ietf.hoeneisen.ch
URI: https://pep-project.org/

Alexey Melnikov
Isode Ltd
14 Castle Mews
Hampton, Middlesex
TW12 2NP
United Kingdom
Email: alexey.melnikov@isode.com