

Limited Additional Mechanisms for PKIX and SMIME  
Internet-Draft  
Intended status: Standards Track  
Expires: 6 April 2026

J. Mandel  
AKAYLA  
R. Housley  
Vigil Security  
S. Turner  
sn3rd  
3 October 2025

PKCS #8 Private-Key Information Content Types  
draft-ietf-lamps-pkcs8-prikeyinfo-contenttypes-04

## Abstract

This document defines PKCS #8 content types for use with PrivateKeyInfo and EncryptedPrivateKeyInfo as specified in RFC 5958.

## 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://github.com/lamps-wg/pkcs8-PriKeyInfoCt>. Status information for this document may be found at <https://datatracker.ietf.org/doc/draft-ietf-lamps-pkcs8-prikeyinfo-contenttypes/>.

Discussion of this document takes place on the Limited Additional Mechanisms for PKIX and SMIME 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://github.com/lamps-wg/pkcs8-PriKeyInfoCt>.

## Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at <https://datatracker.ietf.org/drafts/current/>.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 6 April 2026.

## Copyright Notice

Copyright (c) 2025 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (<https://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Revised BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Revised BSD License.

## Table of Contents

1. Introduction . . . . .	2
2. Private-Key Information Content Types . . . . .	2
3. ASN.1 Module . . . . .	3
4. Security Considerations . . . . .	5
5. IANA Considerations . . . . .	5
6. References . . . . .	5
6.1. Normative References . . . . .	5
6.2. Informative References . . . . .	6
Acknowledgments . . . . .	6
Authors' Addresses . . . . .	6

## 1. Introduction

The syntax for private-key information was originally described in [RFC5208], and the syntax was later revised by [RFC5958] to include the AsymmetricKeyPackage content type that supports multiple PrivateKeyInfos. This document defines PKCS #8 content types for use with one PrivateKeyInfo and EncryptedPrivateKeyInfo. These content type assignments are needed for PrivateKeyInfo and EncryptedPrivateKeyInfo to be carried in the Cryptographic Message Syntax (CMS) [RFC5652].

Note: A very long time ago, media types for PrivateKeyInfo and EncryptedPrivateKeyInfo were assigned as application/pkcs8 and application/pkcs8-encrypted, respectively.

## 2. Private-Key Information Content Types

This section defines a content type for private-key information and encrypted private-key information.

The PrivateKeyInfo content type is identified by the following object identifier:

```
id-ct-privateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
  member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
  smime(16) ct(1) TBD1 }
```

The EncryptedPrivateKeyInfo content type is identified by the following object identifier:

```
id-ct-encrPrivateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
  member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
  smime(16) ct(1) TBD2 }
```

### 3. ASN.1 Module

The ASN.1 module [X680][X690] in this section builds upon the modules in [RFC5911].

```
<CODE BEGINS>
PrivateKeyInfoContentTypes
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) smime(16) modules(0) id-mod-pkcs8ContentType(TBD0) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL

IMPORTS

CONTENT-TYPE
FROM CryptographicMessageSyntax-2009 -- in [RFC5911]
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) smime(16) modules(0) id-mod-cms-2004-02(41) }

PrivateKeyInfo, EncryptedPrivateKeyInfo
FROM AsymmetricKeyPackageModuleV1 -- in [RFC5958]
{ iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1)
  pkcs-9(9) smime(16) modules(0)
  id-mod-asymmetricKeyPkgV1(50) } ;

PrivateKeyInfoContentTypes CONTENT-TYPE ::= {
  ct-privateKeyInfo | ct-encrPrivateKeyInfo,
  ... -- Expect additional content types -- }

ct-privateKeyInfo CONTENT-TYPE ::= { PrivateKeyInfo
  IDENTIFIED BY id-ct-privateKeyInfo }

id-ct-privateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
  member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
  smime(16) ct(1) TBD1 }

ct-encrPrivateKeyInfo CONTENT-TYPE ::= { EncryptedPrivateKeyInfo
  IDENTIFIED BY id-ct-encrPrivateKeyInfo }

id-ct-encrPrivateKeyInfo OBJECT IDENTIFIER ::= { iso(1)
  member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-9(9)
  smime(16) ct(1) TBD2 }

END
<CODE ENDS>
```

The security considerations in [RFC5958] apply here.

For the private key info content types defined in section Section 2, IANA is requested to assign an object identifier (OID) for each of the content types. The OIDs for the content types should be allocated in the "SMI Security for S/MIME CMS Content Type" registry (1.2.840.113549.1.9.16.1) [IANA-CMS-CTS], and the description should be set to id-ct-privateKeyInfo (TBD1) and id-ct-encrPrivateKeyInfo (TBD2).

For the ASN.1 Module in Section 3, IANA is requested to assign an object identifier (OID) for the module identifier. The OID for the module should be allocated in the "SMI Security for S/MIME Module Identifier" registry (1.2.840.113549.1.9.16.0) [IANA-SMIME-MODS], and the Description for the new OID should be set to "id-mod-pkcs8ContentType".

IANA is also requested to update the application/cms entry in the "Media Types" registry to add [ RFC-to-be ] to the list of RFCs where Inner Content Types (ICTs) are defined in the "Optional parameters" and the "Interoperability considerations" sections.

IANA is also requested to update the application/cms entry in the "Media Types" registry to add the following values to the "innerContent" list:

- ```
* privateKeyInfo
* encrPrivateKeyInfo
```

And, to update the following row in the application/cms entry's "Security considerations" section:

|               |                                            |
|---------------|--------------------------------------------|
| RFC           | CMS Protecting Content Type and Algorithms |
| [ RFC-to-be ] | privateKeyInfo and encrPrivateKeyInfo      |

Table 1

## 6.1. Normative References

- [RFC5652] Housley, R., "Cryptographic Message Syntax (CMS)", STD 70, RFC 5652, DOI 10.17487/RFC5652, September 2009, <<https://www.rfc-editor.org/rfc/rfc5652>>.
- [RFC5911] Hoffman, P. and J. Schaad, "New ASN.1 Modules for Cryptographic Message Syntax (CMS) and S/MIME", RFC 5911, DOI 10.17487/RFC5911, June 2010, <<https://www.rfc-editor.org/rfc/rfc5911>>.
- [RFC5958] Turner, S., "Asymmetric Key Packages", RFC 5958, DOI 10.17487/RFC5958, August 2010, <<https://www.rfc-editor.org/rfc/rfc5958>>.
- [X680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <<https://www.itu.int/rec/T-REC-X.680>>.
- [X690] ITU-T, "Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1-2021, February 2021, <<https://www.itu.int/rec/T-REC-X.690>>.

## 6.2. Informative References

- [IANA-CMS-CTS] "SMI Security for S/MIME CMS Content Type", n.d., <<https://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#security-smime-1>>.
- [IANA-SMIME-MODS] "SMI Security for S/MIME Module Identifier", n.d., <<https://www.iana.org/assignments/smi-numbers/smi-numbers.xhtml#security-smime-0>>.
- [RFC5208] Kaliski, B., "Public-Key Cryptography Standards (PKCS) #8: Private-Key Information Syntax Specification Version 1.2", RFC 5208, DOI 10.17487/RFC5208, May 2008, <<https://www.rfc-editor.org/rfc/rfc5208>>.

## Acknowledgments

Thanks to John Gray, Deb Cooley, Mohamed Boucadair, Orie Steele, and テ詠ic Vyncke for reviewing the document and providing comments.

## Authors' Addresses

Joe Mandel  
AKAYLA, Inc.  
Email: joe@akayla.com

Russ Housley  
Vigil Security, LLC  
Email: housley@vigilsec.com

Sean Turner  
sn3rd  
Email: sean@sn3rd.com