Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 21 November 2026

M. Ounsworth
Cryptic Forest
H. Tschofenig
Siemens
H. Birkholz
Fraunhofer SIT
M. Wiseman

N. Smith
20 May 2026

Use of Remote Attestation with Certification Signing Requests
draft-ietf-lamps-csr-attestation-27

Abstract

Certification Authorities (CAs) issuing certificates to Public Key Infrastructure (PKI) end entities may require a certificate signing request (CSR) to include additional verifiable information to confirm policy compliance. For example, a CA may require an end entity to demonstrate that the private key corresponding to a CSR's public key is secured by a hardware security module (HSM), is not exportable, etc. The process of generating, transmitting, and verifying additional information required by the CA is called remote attestation. While work is currently underway to standardize various aspects of remote attestation, a variety of proprietary mechanisms have been in use for years, particularly regarding protection of private keys.

This specification defines ASN.1 structures which may carry attestation data for PKCS#10 and Certificate Request Message Format (CRMF) messages. Both standardized and proprietary attestation formats are supported by this specification.

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://lamps-wg.github.io/csr-attestation/draft-ietf-lamps-csr-attestation.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-ietf-lamps-csr-attestation/.

Source for this draft and an issue tracker can be found at https://github.com/lamps-wg/csr-attestation.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

Certification Authorities (CAs) issuing certificates to PKI end entities may require a certificate signing request (CSR) include verifiable attestations that contain claims regarding the platform used by the end entity to generate the key pair for which a certificate is sought and also contains claims of attributes of the key pair with respect to its protection, use and extractability. At the time of writing, the most pressing example of the need for remote attestation in certificate enrollment is the Code-Signing Baseline Requirements (CSBR) document maintained by the CA/Browser Forum [CSBR]. The [CSBR] requires compliant CAs to "ensure that a Subscriber's Private Key is generated, stored, and used in a secure environment that has controls to prevent theft or misuse". This requirement is a natural fit to enforce via remote attestation.

This specification defines an attribute and an extension that allow for conveyance of verifiable attestations in several Certificate Signing Request (CSR) formats, including PKCS#10 [RFC2986] or Certificate Request Message Format (CRMF) [RFC4211] messages. Given several standard and proprietary remote attestation technologies are in use, this specification is intended to be as technology-agnostic as is feasible with respect to implemented and future remote attestation technologies. This aligns with the fact that a CA may wish to provide support for a variety of types of devices but cannot dictate what format a device uses to represent attestations. However, if a certificate requester does not include the number and types of attestations required by the CA, it is unlikely the requester will receive the requested certificate.

While CSRs are defined using Abstract Syntax Notation One (ASN.1), attestations may be defined using any data description language, i.e., ASN.1 or Concise Data Description Language (CDDL), or represented using any type of encoding, including Distinguished Encoding Rules (DER), Concise Binary Object Representation (CBOR), JavaScript Object Notation (JSON). This specification RECOMMENDS that attestations that are not encoded using the Basic Encoding Rules (BER) or Distinguished Encoding Rules (DER) be wrapped in an ASN.1 OCTET STRING.

2. Relationship to the IETF RATS Working Group

As noted, attestation-related technologies have existed for many years, albeit with no standard format and no standard means of conveying attestation statements to a CA. This draft addresses the latter, and is equally applicable to standard and proprietary attestation formats. The IETF Remote Attestation Procedures (RATS) working group is addressing the former. In [RFC9334], RATS defined vocabulary, architecture, and usage patterns related to the practice of generating and verifying attestations.

In its simplest topological model, attestations are generated by the certificate requester and verified by the CA/RA. Section 5 of [RFC9334] defines topological patterns that are more complex, including the background check model and the passport model. This document may be applied to instantiating any of these topological models for CSR processing, provided the required security requirements specific to the context of certificate issuance are satisfied.

Section 4.2 of [RFC9334] defines several roles that originate, forward or process attestation statements (also see Section 1.2 of [RFC9683]): the Attester; Endorser; Relying Party; and Verifier. Attestation statements, such as Evidence, may be directed to an entity taking at least one of these roles, including to an CA/RA acting as a Verifier. An CA/RA may also forward attestation statements to a Verifier for appraisal. Each attestation statements may contain one or more claims, including claims that may be required by an RA or CA. Attestation statements transmitted by these parties are defined in Section 8 of [RFC9334] as the "conceptual messages" Evidence, Endorsement, and Attestation Results. The structure defined in this specification may be used by any of the roles that originate attestation statements, and is equally applicable to these three conceptual messages.

3. Conventions and Definitions

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.

This document re-uses the terms defined in [RFC9334] related to remote attestation. Readers of this document are assumed to be familiar with the following terms defined in [RFC9334]: Evidence, Endorsement, Claim, Attestation Result (AR), Attester, Relying Party, and Verifier. Per [RFC9334], the CA/RA is the Relying Party with respect to remote attestation. This use of the term "relying party" differs from the traditional PKIX use of the term. This specification uses CA/RA to refer to an [RFC9334] Relying Party, which may or may not include an integrated Verifier.

The term "Certification Request" message is defined in [RFC2986]. Specifications, such as [RFC7030], later introduced the term "Certificate Signing Request (CSR)" to refer to the Certification Request message. While the term "Certification Request" would have been correct, the mistake was unnoticed. In the meanwhile CSR is an abbreviation used beyond PKCS#10. Hence, it is equally applicable to other protocols that use a different syntax and even a different encoding, in particular this document also considers messages in the Certificate Request Message Format (CRMF) [RFC4211] to be "CSRs". In this document, the terms "CSR" and Certificate Request message are used interchangeably.

The term "hardware security module (HSM)" is used generically to refer to the combination of hardware and software designed to protect keys from unauthorized access. Other commonly used terms include Secure Element, Trusted Platform Module, and Trusted Execution Environment.

Since this document combines terminology from two domains, Remote Attestation (RATS) and X.509 PKI, it follows a naming convention to avoid ambiguity. RATS terminology is written in uppercase (e.g., Verifier), while X.509/PKI terminology is written in lowercase (e.g., certification authority (CA)). This distinction clarifies terms that exist in both domains; for instance, a Verifier refers to the RATS entity that processes Evidence, whereas a verifier refers to the PKI entity that validates certificates. This convention is distinct from camel-case identifiers like "AttestationStatement", which denote ASN.1 types.

4. Conveying Attestations in CSRs

The focus of this specification is the conveyance of attestations to a CA/RA as part of a CSR. The following sub-sections define formats to support this conveyance, an optional mechanism to limit support to specific attestation types at the ASN.1 level, and bindings to the attribute and extension mechanisms used in certificate managment protocols.

4.1. AttestationStatement and AttestationBundle

The AttestationStatement structure (as shown in Figure 1) facilitates the representation of Evidence, Endorsements, and Attestation Results generated by an Attester, Endorser, or Verifier for processing by a Verifier or Relying Party, such as verification by a CA/RA.

* The type field is an OBJECT IDENTIFIER that identifies the format of the stmt field.

* The stmt field contains the attestation for processing, constrained by the type field. Formats that are not defined using ASN.1 MUST define an ASN.1 wrapper for use with the AttestationStatement structure. For example, a CBOR-encoded format may be defined as an OCTET STRING for AttestationStatement purposes, where the contents of the OCTET STRING are the CBOR-encoded data.

```
ATTESTATION-STATEMENT ::= TYPE-IDENTIFIER

AttestationStatement ::= SEQUENCE {
   type   ATTESTATION-STATEMENT.&id({AttestationStatementSet}),
   stmt   ATTESTATION-STATEMENT.&Type({AttestationStatementSet}{@type})
}
```

Figure 1: Definition of AttestationStatement

In some cases, a CA may require CSRs to include a variety of claims, which may require the cooperation of more than one Attester. Similarly, a CA/RA may outsource verification of claims from different Attesters to a single Verifier. The AttestationBundle structure, Figure 2, facilitates the representation of one or more AttestationStatement structures along with an OPTIONAL collection of certificates that may be useful for certification path building and validation to verify each AttestationStatement. AttestationBundle is the structure included in a CSR attribute or extension.

```
AttestationBundle ::= SEQUENCE {
   attestations SEQUENCE SIZE (1..MAX) OF AttestationStatement,
   certs SEQUENCE SIZE (1..MAX) OF LimitedCertChoices OPTIONAL,
}
```

Figure 2: Definition of AttestationBundle

At least one element in the attestations field SHOULD contain an attestation that is cryptographically bound to the public key that is the subject of the CSR containing the AttestationBundle.

The CertificateChoices structure defined in [RFC6268], and reproduced below along with OtherCertificateFormat, allows for carrying certificates in the default X.509 [RFC5280] format, or in other non-X.509 certificate formats. CertificateChoices MUST only contain certificate or other. In this context, CertificateChoices MUST NOT contain extendedCertificate, v1AttrCert, or v2AttrCert. Note that for non-ASN.1 certificate formats, the CertificateChoices MUST contain other with an OTHER-CERT-FMT.Type of OCTET STRING and data consistent with OTHER-CERT-FMT.id. LimitedCertChoices is defined to limit the available options to certificate and other.

```
CertificateChoices ::= CHOICE {
  certificate Certificate,
  extendedCertificate [0] IMPLICIT ExtendedCertificate,
       -- Obsolete
  ...,
  [[3: v1AttrCert [1] IMPLICIT AttributeCertificateV1]],
       -- Obsolete
  [[4: v2AttrCert [2] IMPLICIT AttributeCertificateV2]],
  [[5: other      [3] IMPLICIT OtherCertificateFormat]] }

OTHER-CERT-FMT ::= TYPE-IDENTIFIER

OtherCertificateFormat ::= SEQUENCE {
  otherCertFormat OTHER-CERT-FMT.
          &id({SupportedCertFormats}),
  otherCert       OTHER-CERT-FMT.
          &Type({SupportedCertFormats}{@otherCertFormat})}

LimitedCertChoices ::=
   CertificateChoices
       (WITH COMPONENTS {certificate, other})
```

The certs field contains a set of certificates that may be used to validate an AttestationStatement contained in attestations. For each AttestationStatement, the set of certificates SHOULD contain the certificate that contains the public key needed to directly validate

the AttestationStatement, unless the signing key is expected to be known to the Verifier or is embedded within the AttestationStatement. Additional certificates MAY be provided, for example, to chain the attestation key back to a trust anchor. No specific order of the certificates in certs should be expected because certificates contained in certs may be needed to validate different AttestationStatement instances.

This specification places no restriction on mixing certificate types within the certs field. For example a non-X.509 attestation signer certificate MAY chain to a trust anchor via a chain of X.509 certificates. It is up to the Attester and its Verifier to agree on supported certificate formats.

4.2. AttestationStatementSet

```
AttestationStatementSet ATTESTATION-STATEMENT ::= {
   ... -- None defined in this document --
}
```

Figure 3: Definition of AttestationStatementSet

The expression illustrated in Figure 3 maps ASN.1 Types for attestation statements to the OIDs that identify them. These mappings are used to construct or parse AttestationStatement objects that appear in an AttestationBundle. Attestation statements are typically defined in other IETF standards, in standards produced by other standards bodies, or as vendor proprietary formats along with corresponding OIDs that identify them. AttestationStatementSet is left unconstrained in this document. However, implementers MAY populate it with the formats that they wish to support.

4.3. CSR Attribute and Extension

By definition, attributes within a PKCS#10 CSR are typed as ATTRIBUTE and within a CRMF CSR are typed as EXTENSION.

```
id-aa-attestation OBJECT IDENTIFIER ::= { id-aa 59 }

-- For PKCS#10
attr-attestations ATTRIBUTE ::= {
  TYPE AttestationBundle
  COUNTS MAX 1
  IDENTIFIED BY id-aa-attestation
}

-- For CRMF
ext-attestations EXTENSION ::= {
  SYNTAX AttestationBundle
  IDENTIFIED BY id-aa-attestation
}
```

Figure 4: Definitions of CSR attribute and extension

The Extension variant illustrated in Figure 4 is intended only for use within CRMF CSRs and is NOT RECOMMENDED to be used within X.509 certificates due to the privacy implications of publishing information about the end entity’s hardware environment.

Multiple different types of AttestationStatement(s) may be included within a single top-level AttestationBundle. Note that this document does not require the AttestationBundle.attestations field to contain only one AttestationStatement of a given type. For example, if a given type is a "wrapper" type containing the conceptual message wrapper (CMW) structure [I-D.ietf-rats-msg-wrap], multiple copies of a CMW-typed AttestationStatement may be included.

Per [RFC5280] no more than one instance of a given type of Extension may be carried within an Extensions structure, so an Extensions structure MUST contain no more than one Extension of type id-aa-attestation.

PKCS#10 uses the legacy structures Attributes and Attribute rather than the later defined SingleAttribute and AttributeSet structures - all of which are defined against the ATTRIBUTE ASN.1 CLASS. The ATTRIBUTE CLASS has a COUNTS MAX n clause which can be used to limit the copies of ATTRIBUTE related structures. For the purposes of this document the COUNTS MAX 1 clause in the attr-attestation shall be taken to mean the following:

* An Attributes structure carried within a PKCS#10 CSR MUST contain no more than one Attribute of type id-aa-attestation.

* An Attribute of type id-aa-attestation MUST contain exactly one copy of an AttestationBundle.

When multiple Verifiers support the same attestation-format OID, ambiguity can arise in routing attestations to the appropriate Verifier. Resolving that ambiguity is outside the scope of this document and must be defined by the attestation-format specification, particularly for opaque (wrapper) formats. Two pragmatic approaches are recommended: (1) assign distinct OIDs for different verifier or verification types even when the underlying format structure is identical, or (2) encapsulate the opaque attestation object in a wrapper that carries an explicit hint. Implementations should adopt one of these approaches and attestation-format specifications should mandate the precise mechanism for nonce selection and routing of attestations.

5. IANA Considerations

IANA is requested to allocate a value from the "SMI Security for PKIX Module Identifier" registry for the included ASN.1 module, and to allocate a value from "SMI Security for S/MIME Attributes" to identify an attribute defined within.

5.1. Module Registration - SMI Security for PKIX Module Identifier

IANA is asked to register the following within the registry id-mod SMI Security for PKIX Module Identifier (1.3.6.1.5.5.7.0).

* Decimal: IANA Assigned - *Replace TBDMOD*

* Description: CSR-ATTESTATION-2025 - id-mod-pkix-attest-01

* References: This Document

5.2. Object Identifier Registrations - SMI Security for S/MIME Attributes

IANA is asked to register the following within the registry id-aa SMI Security for S/MIME Attributes (1.2.840.113549.1.9.16.2).

* Attestation Statement

* Decimal: IANA Assigned - Note: .59 has already been early-allocated as "id-aa-evidence" referencing this document, so the request is to change the name of this entry to "id-aa-attestation" and leave the allocation of .59 as-is.

* Description: id-aa-attestation

* References: This Document

6. Security Considerations

This document defines a structure to convey attestations as additional information in CSRs, as well as an attribute to convey that structure in the Certification Request Message defined in {[RFC2986]} and an extension to convey that structure in the Certificate Request Message Format defined in {[RFC4211]}. The CA/RA that receives the CSR may choose to verify the attestation(s) to determine if an issuance policy is met, or which of a suite of policies is satisfied. The CA/RA is also free to discard the additional information without processing.

A CA which accepts or requires attestation(s) SHOULD document its requirements with its Certification Practice Statement(s).

The remainder of this section identifies security considerations that apply when the CA/RA chooses to verify the attestation as part of the evaluation of a CSR.

6.1. Binding Attestations to the CSR's Public Key

Regardless of the topological model, the CA/RA is ultimately responsible for validating the binding between the public key and the attestation(s) in the CSR. For CAs issuing in conformance with the CA/Browser Forum's Code Signing Baseline Requirements, this means verifying the attestation of HSM generation and protection is cryptographically bound to the public key in the CSR.

Multiple attestations from multiple sources, as envisioned in [RFC9334], can introduce additional complications as shown in the following example.

For example, a CA may have an issuance policy that requires key generation in an HSM on a company-owned platform in a known good state. The CSR might contain three AttestationStatements originated by three different attesters:

1. that a key pair was generated in an HSM;

2. that a particular platform is company-owned; and

3. that a particular platform was in a known good state (e.g, up to date on patches, etc.).

While each of these attestations may be independently correct, the CA/RA is responsible for confirming the attestations apply in concert to the public key in the CSR. That is, the CA/RA must analyze the attestations to ensure that:

1. the attestation of HSM generation by AttestationStatement 1 applies to the public key in the CSR;

2. the attestation of company ownership by AttestationStatement 2 applies to the platform that contains the HSM; and

3. the attestation that a platform was in a known good state by AttestationStatement 3 applies to the platform that contains the HSM.

6.2. Freshness

To avoid replay attacks, the CA/RA may choose to ignore attestations that are stale, or whose freshness cannot be determined. Mechanisms to address freshness and their application to the RATS topological models are discussed in [RFC9334]. Other mechanisms for determining freshness may be used as the CA/RA deems appropriate. When CSRs are embedded within certificate management protocols such as EST [RFC7030] or CMP [RFC4210], these protocols can supply the Attester with a nonce. Further details are specified in [I-D.ietf-lamps-attestation-freshness].

6.3. Relationship of Attestations and Certificate Extensions

Attestations are intended as additional information in the issuance process, and may include sensitive information about the platform, such as hardware details or patch levels, or device ownership. It is NOT RECOMMENDED for a CA to copy attestations into the published certificate. CAs that choose to republish attestations in certificates SHOULD review the contents and delete any sensitive information.

6.4. Additional Security Considerations

In addition to the security considerations listed here, implementers should be familiar with the security considerations of the specifications on which this specification depends: PKCS#10 [RFC2986], CRMF [RFC4211], as well as general security concepts relating to remote attestation; many of these concepts are discussed in Section 6 of [RFC9334], Section 7 of [RFC9334], Section 9 of [RFC9334], Section 11 of [RFC9334], and Section 12 of [RFC9334]. Implementers should also be aware of any security considerations relating to the specific attestation formats being carried within the CSR.

7. References

7.1. Normative References

[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>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/rfc/rfc2986>.

[RFC4211] Schaad, J., "Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)", RFC 4211, DOI 10.17487/RFC4211, September 2005, <https://www.rfc-editor.org/rfc/rfc4211>.

[RFC5280] Cooper, D., Santesson, S., Farrell, S., Boeyen, S., Housley, R., and W. Polk, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", RFC 5280, DOI 10.17487/RFC5280, May 2008, <https://www.rfc-editor.org/rfc/rfc5280>.

[RFC5912] Hoffman, P. and J. Schaad, "New ASN.1 Modules for the Public Key Infrastructure Using X.509 (PKIX)", RFC 5912, DOI 10.17487/RFC5912, June 2010, <https://www.rfc-editor.org/rfc/rfc5912>.

[RFC6268] Schaad, J. and S. Turner, "Additional New ASN.1 Modules for the Cryptographic Message Syntax (CMS) and the Public Key Infrastructure Using X.509 (PKIX)", RFC 6268, DOI 10.17487/RFC6268, July 2011, <https://www.rfc-editor.org/rfc/rfc6268>.

[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>.

[RFC9334] Birkholz, H., Thaler, D., Richardson, M., Smith, N., and W. Pan, "Remote ATtestation procedureS (RATS) Architecture", RFC 9334, DOI 10.17487/RFC9334, January 2023, <https://www.rfc-editor.org/rfc/rfc9334>.

7.2. Informative References

[CSBR] CA/Browser Forum, "Baseline Requirements for Code-Signing Certificates, v.3.7", February 2024, <https://cabforum.org/uploads/Baseline-Requirements-for-the-Issuance-and-Management-of-Code-Signing.v3.7.pdf>.

[I-D.ietf-lamps-attestation-freshness]
Tschofenig, H., Brockhaus, H., Mandel, J., and S. Turner, "Nonce-based Freshness for Remote Attestation in Certificate Signing Requests (CSRs) for the Certification Management Protocol (CMP), for Enrollment over Secure Transport (EST), and for Certificate Management over CMS (CMC)", Work in Progress, Internet-Draft, draft-ietf-lamps-attestation-freshness-06, 20 April 2026, <https://datatracker.ietf.org/doc/html/draft-ietf-lamps-attestation-freshness-06>.

[I-D.ietf-rats-msg-wrap]
Birkholz, H., Smith, N., Fossati, T., Tschofenig, H., and D. Glaze, "RATS Conceptual Messages Wrapper (CMW)", Work in Progress, Internet-Draft, draft-ietf-rats-msg-wrap-23, 11 December 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-msg-wrap-23>.

[RFC4210] Adams, C., Farrell, S., Kause, T., and T. Mononen, "Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)", RFC 4210, DOI 10.17487/RFC4210, September 2005, <https://www.rfc-editor.org/rfc/rfc4210>.

[RFC7030] Pritikin, M., Ed., Yee, P., Ed., and D. Harkins, Ed., "Enrollment over Secure Transport", RFC 7030, DOI 10.17487/RFC7030, October 2013, <https://www.rfc-editor.org/rfc/rfc7030>.

[RFC9683] Fedorkow, G. C., Ed., Voit, E., and J. Fitzgerald-McKay, "Remote Integrity Verification of Network Devices Containing Trusted Platform Modules", RFC 9683, DOI 10.17487/RFC9683, December 2024, <https://www.rfc-editor.org/rfc/rfc9683>.

[SampleData]
"CSR Attestation Sample Data", n.d., <https://github.com/lamps-wg/csr-attestation-examples>.

Appendix A. Examples

Examples and sample data will be collected in the "CSR Attestation Sample Data" GitHub repository [SampleData].

Appendix B. ASN.1 Module

```
CSR-ATTESTATION-2025
  { iso(1) identified-organization(3) dod(6) internet(1) security(5)
  mechanisms(5) pkix(7) id-mod(0) id-mod-pkix-attest-01(TBDMOD) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

EXPORTS ALL;

IMPORTS

CertificateChoices
  FROM CryptographicMessageSyntax-2010 -- from [RFC6268]
    { iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs-9(9) smime(16) modules(0) id-mod-cms-2009(58) }

EXTENSION, ATTRIBUTE
  FROM PKIX-CommonTypes-2009 -- from [RFC5912]
    { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-pkixCommon-02(57) }

id-aa
  FROM SecureMimeMessageV3dot1-2009
    { iso(1) member-body(2) us(840) rsadsi(113549)
    pkcs(1) pkcs-9(9) smime(16) modules(0) msg-v3dot1-02(39) }
  ;

ATTESTATION-STATEMENT ::= TYPE-IDENTIFIER

AttestationStatementSet ATTESTATION-STATEMENT ::= {
   ... -- None defined in this document --
}

AttestationStatement ::= SEQUENCE {
   type   ATTESTATION-STATEMENT.&id({AttestationStatementSet}),
   stmt   ATTESTATION-STATEMENT.&Type(
              {AttestationStatementSet}{@type})
}

-- Arc for Attestation types
id-aa-attestation OBJECT IDENTIFIER ::= { id-aa 59 }

-- For PKCS#10 (Attestation)
attr-attestation ATTRIBUTE ::= {
  TYPE AttestationBundle
  COUNTS MAX 1
  IDENTIFIED BY id-aa-attestation
}
```

```
   -- For CRMF (Attestation)
   ext-attestation EXTENSION ::= {
     SYNTAX AttestationBundle
     IDENTIFIED BY id-aa-attestation
   }

   -- Allow either X.509 or OTHER-CERT certificates
   LimitedCertChoices ::=
       CertificateChoices
          (WITH COMPONENTS {certificate, other})

   AttestationBundle ::= SEQUENCE {
      attestations SEQUENCE SIZE (1..MAX) OF AttestationStatement,
      certs SEQUENCE SIZE (1..MAX) OF LimitedCertChoices OPTIONAL
   }

   END
```

Appendix C. Acknowledgments

This specification is the work of a design team created by the chairs of the LAMPS working group. We would like to specifically thank Mike StJohns for writing initial version of this draft and for his substantial work on the final version. The following persons, in no specific order, contributed to the work directly, participated in design team meetings, or provided review of the document.

Richard Kettlewell, Chris Trufan, Bruno Couillard, Jean-Pierre Fiset, Sander Temme, Jethro Beekman, Zsolt Rzsahegyi, Ferenc Pet, Mike Agrenius Kushner, Tomas Gustavsson, Dieter Bong, Christopher Meyer, Carl Wallace, Michael Richardson, Tomofumi Okubo, Olivier Couillard, John Gray, Eric Amador, Giri Mandyam, Darren Johnson, Herman Slatman, Tiru Reddy, James Hagborg, A.J. Stein, John Kemp, Daniel Migault and Russ Housley.

Additionally, we would like to thank Andreas Kretschmer, Hendrik Brockhaus, David von Oheimb, Corey Bonnell, and Thomas Fossati for their feedback based on implementation experience.

Close to the end of the specification development process, the working group chairs, Russ Housley and Tim Hollebeek, reached out to Steve Hanna, Tim Polk, and Carl Wallace to help improve the document and resolve contentious issues. Their contributions substantially impacted the final outcome of the document.

Authors' Addresses

Mike Ounsworth
Cryptic Forest Software
Sioux Lookout, Ontario
Canada
Email: mike@ounsworth.ca

Hannes Tschofenig
Siemens
Germany
Email: Hannes.Tschofenig@gmx.net

Henk Birkholz
Fraunhofer SIT
Rheinstrasse 75
64295 Darmstadt
Germany
Email: henk.birkholz@sit.fraunhofer.de

Monty Wiseman
United States
Email: mwiseman@computer.org

Ned Smith
United States
Email: ned.smith.ietf@gmail.com