Workgroup:
Limited Additional Mechanisms for PKIX and
SMIME
Internet-Draft:
draft-wallace-lamps-key-attestation-ext-01
Published: 10 August 2022
Intended Status: Standards Track
Expires: 11 February 2023
Authors: C. Wallace S. Turner
Red Hound sn3rd

Key Attestation Extension for Certificate Management Protocols

Abstract

Certification Authorities (CAs) issue certificates for public keys conveyed to the CA via a certificate management message or protocol. In some cases, a CA may wish to tailor certificate contents based on whether the corresponding private key is secured by hardware in non-exportable form. This document describes extensions that may be included in any of several widely used certificate management protocols to convey attestations about the private key to the CA to support this determination.

About This Document

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

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-wallace-lamps-key-attestation-ext/.

Discussion of this document takes place on the spasm 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/.

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 11 February 2023.

Table of Contents

1. Introduction
2. Conventions and Definitions
3. Key Attestation Attribute or Extension
   3.1. Usage in PKCS #10 requests
   3.2. Usage in CRMF requests
4. Security Considerations
5. IANA Considerations
   5.1. Key attestation extension object identifier
   5.2. Key attestation extension ASN.1 module object identifier
   5.3. Attestation statement formats
      5.3.1. WebAuthn Attestation Statement Format Identifiers for Certificate Request Protocols
      5.3.2. WebAuthn Extension Identifiers for Certificate Request Protocols
6. ASN.1 Module
7. References
   7.1. Normative References
   7.2. Informative References
Acknowledgments
Authors' Addresses

1. Introduction

Many different certificate management protocols exist, including:

*PKCS #10 [RFC2986]

*Simple Certificate Enrolment Protocol (SCEP) [RFC8894]

*Certificate Management over CMS (CMC) [RFC5272]

*Certificate Management Protocol (CMP) [RFC4210]

*Certificate Request Management Format (CRMF) [RFC4211]

*Enrollment over Secure Transport (EST) [RFC7030]

*Automatic Certificate Management Environment (ACME) [RFC8555]

Each of these specifications defines extensibility mechanisms to customize requests sent to a Certification Authority (CA), Registration Authority (RA), or certificate management server. This document addresses the first six specifications in the above list, as all can be customized using attributes or extensions. [RFC8555] is somewhat different and is addressed by [I-D.draft-bweeks-acme-device-attest].

Many operating system and device vendors offer functionality enabling a device to generate a cryptographic attestation that can be used to establish the provenance of a key:

*Android Key Attestation

*Trusted Platform Module

*Apple Key Attestation

*Yubico PIV Attestation

[WebAuthn] defines an "API enabling the creation and use of strong, attested, scoped, public key-based credentials by web applications, for the purpose of strongly authenticating users." In support of this goal, it defines a model and corresponding formats to support attestation functionality. Section 6.5 of [WebAuthn] describes the general attestation structure and section 8 defines some specific attestation formats. Similar to [I-D.draft-bweeks-acme-device-attest], this specification uses the attestation object definition from [WebAuthn] as a means of supporting a variety of attestation formats, which are defined in the IANA registry that was established by [RFC8809]; see [WebAuthnReg].

This document defines a structure, KeyAttestation, that can be used to convey a [WebAuthn] attestation statement as an attribute or extension when using the protocols listed above.

2. 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.

3. Key Attestation Attribute or Extension

A key attestation attribute or extension **MAY** be included in certificate request messages to convey an attestation statement for the private key corresponding to the public key contained in the request. The attribute definition and the certificate extension definition are exactly the same, and they are identified by the same object identifier.

```
ext-keyAttestation EXTENSION ::= {
  SYNTAX KeyAttestation IDENTIFIED BY id-pe-keyAttestation }

attr-keyAttestation ATTRIBUTE ::= {
  SYNTAX KeyAttestation IDENTIFIED BY id-pe-keyAttestation }

id-pe-keyAttestation OBJECT IDENTIFIER ::=  { id-pe TBD }

KeyAttestation ::= OCTET STRING
```

The KeyAttestation conveys an attestation statement as defined in [WebAuthn] encoded as an OCTET STRING.

While the format of an attestation statement varies, all attestation statement formats conveyed via a keyAttestation extension **MUST** include the public key that is the subject of the corresponding certificate management request. Certificate request messages that contain a key attestation that does not include a public key or that contain a public key that does not match the public key in the certificate request **SHOULD** be rejected with no certificate issued, however, a CA **MAY** elect to issue a certificate as if the request did not contain a key attestation per local policy.

Some attestation statement formats support the use of challenge password or nonce values. While the means of conveying challenge password value or a nonce value to certificate request clients is outside the scope of this document, each of SCEP [RFC8894], CMC [RFC5272], CMP [RFC4210] and EST [RFC7030] define means for conveying nonce values to certificate request clients. In some cases, challenge password or nonce values may be conveyed outside of a certificate management protocol. For example, SCEP payloads in Apple's Over-the-Air Profile Delivery and Configuration specification [OTA] deliver challenge passwords in an XML-formatted set of instructions.

Similarly, use and verification of a nonce value relative to an attestation statement is outside the scope of this document. Verification procedures for currently defined attestation statement

formats can be found in Section 8 of [WebAuthn]. Certificate request messages that contain a key attestation that cannot be validated, including processing any nonce or challenge password values, **SHOULD** be rejected with no certificate issued, however, a CA **MAY** elect to issue a certificate as if the request did not contain a key attestation per local policy.

3.1. Usage in PKCS #10 requests

The PKCS #10 structure may be used directly or in SCEP, CMC, CMP or EST contexts. Where PKCS #10 is used, the public key in the attestation statement **MUST** match the public key in the CertificationRequestInfo.subjectPKInfo field and the keyAttestation attribute **MUST** appear in the CertificationRequestInfo.attributes field.

3.2. Usage in CRMF requests

The CRMF structure may be used in CMC, CMP or EST. Where CRMF is used, the public key in the attestation statement **MUST** match the public key in the CertTemplate.publicKey field and the keyAttestation extension **MUST** appear in the CertTemplate.extensions field.

4. Security Considerations

See Section 13 of [WebAuthn] for additional security considerations related to attestation statement formats, including certificate revocation.

CAs, RAs and certificate management servers will need a set of trust anchors to validate attestation statements that may originate from any number of sources. Where possible, a dedicated trust anchor and issuing CA should be used when verifying a given type of attestation statement. Where a trust anchor or issuing CA are shared for mulitple sources of attestation statements, including constraints in attestation signer certificates or attestation certificates is recommended. [COTS] and [fido-metadata] define structures for conveying trust anchors that may be used for verifying attestations such that constraints are implied or are explicitly stated. Expression and validation of constraints imposed on trust anchors, CAs or attestation signers is beyond the scope of this specification.

Key attestation statements may include a variety of information in addition to the public key being attested. While not described in this document, CAs, RAs and certificate management servers are free to use any policy when evaluating this information. This evaluation can result in rejection of a certificate request that features a verifiable key attestation for the public key contained in the

request. For example, an attestation statement may indicate use of an unacceptable firmware version.

5. IANA Considerations

5.1. Key attestation extension object identifier

An object identifier from the id-pe arc defined in [RFC7299] should be assigned for id-pe-keyAttestation.

5.2. Key attestation extension ASN.1 module object identifier

An object identifier from the id-mod arc defined in [RFC7299] should be assigned for id-mod-keyAttestation.

5.3. Attestation statement formats

Section 2.1 of [RFC8809] describes registration of new attestation statement format types used when authenticating users via [WebAuthn]. This specification reuses the same format, but, because the context for use is different, a different registry is required. This section defines IANA registries for W3C Web Authentication (WebAuthn) attestation statement format identifiers and extension identifiers used in the context of a certificate request. This specification establishes two registries:

* the "WebAuthn Attestation Statement Format Identifiers for Certificate Request Protocols" registry

* the "WebAuthn Extension Identifiers for Certificate Request Protocols" registry

Any additional processes established by the expert(s) after the publication of this document will be recorded on the registry web page at the discretion of the expert(s), who may differ from the experts associated with the registry established by [RFC8809].

NOTE: these two registries are shared with [I-D.draft-bweeks-acme-device-attest], which features similar registry establishment language. The registries need be created only one time. Delete these sections if registry is already in place.

5.3.1. WebAuthn Attestation Statement Format Identifiers for Certificate Request Protocols

WebAuthn attestation statement format identifiers are strings whose semantic, syntactic, and string-matching criteria are specified in the "Attestation Statement Format Identifiers" (https://www.w3.org/TR/2019/REC-webauthn-1-20190304/#sctn-attstn-fmt-ids) section of

[WebAuthn], along with the concepts of attestation and attestation statement formats.

Registered attestation statement format identifiers are those that have been added to the registry by following the procedure in Section 5.3.1.1.

Each attestation statement format identifier added to this registry **MUST** be unique amongst the set of registered attestation statement format identifiers.

Registered attestation statement format identifiers **MUST** be a maximum of 32 octets in length and **MUST** consist only of printable ASCII [RFC20] characters, excluding backslash and double quote, i.e., VCHAR as defined in [RFC5234] but without %x22 and %x5c. Attestation statement format identifiers are case sensitive and may not match other registered identifiers in a case-insensitive manner unless the designated experts determine that there is a compelling reason to allow an exception.

5.3.1.1. Registering Attestation Statement Format Identifiers

WebAuthn attestation statement format identifiers are registered using the Specification Required policy (see Section 4.6 of [RFC8126]).

The "WebAuthn Attestation Statement Format Identifiers for Certificate Request Protocols" registry is located at https://www.iana.org/assignments/webauthn_for_certreq. Registration requests can be made by following the instructions located there or by sending an email to the webauthn-for-certreq-reg-review@ietf.org mailing list.

Registration requests consist of at least the following information:

- WebAuthn Attestation Statement Format Identifier:
  - An identifier meeting the requirements given in Section 5.3.1.
- Description:
  - A relatively short description of the attestation format.
- Specification Document(s):
  - Reference to the document or documents that specify the attestation statement format.

*Change Controller:

  -For Standards Track RFCs, list "IETF". For others, give the name of the responsible party. Other details (e.g., postal address, email address, home page URI) may also be included.

*Notes:

  -[optional]

Registrations **MUST** reference a freely available, stable specification, e.g., as described in Section 4.6 of [RFC8126]. This specification **MUST** include security and privacy considerations relevant to the attestation statement format.

Note that WebAuthn attestation statement format identifiers can be registered by third parties (including the expert(s) themselves), if the expert(s) determines that an unregistered attestation statement format is widely deployed and not likely to be registered in a timely manner otherwise. Such registrations still are subject to the requirements defined, including the need to reference a specification.

5.3.1.2. Registration Request Processing

As noted in Section 5.3.1.1, WebAuthn attestation statement format identifiers are registered using the Specification Required policy.

The expert(s) will clearly identify any issues that cause a registration to be refused, such as an incompletely specified attestation format.

When a request is approved, the expert(s) will inform IANA, and the registration will be processed. The IESG is the arbiter of any objection.

5.3.1.3. Initial Values in the WebAuthn Attestation Statement Format Identifiers for Certificate Request Protocols Registry

The initial values for the "WebAuthn Attestation Statement Format Identifiers for Certificate Request Protocols" registry have been populated with the values listed in the "WebAuthn Attestation Statement Format Identifier Registrations" (https://www.w3.org/TR/2019/REC-webauthn-1-20190304/#sctn-att-fmt-reg) section of [WebAuthn]. Also, the Change Controller entry for each of those registrations is:

*Change Controller:

  -W3C Web Authentication Working Group (public-webauthn@w3.org)

5.3.2. WebAuthn Extension Identifiers for Certificate Request Protocols

WebAuthn extension identifiers are strings whose semantic, syntactic, and string-matching criteria are specified in the "Extension Identifiers" (https://www.w3.org/TR/2019/REC-webauthn-1-20190304/#sctn-extension-id) section of [WebAuthn].

Registered extension identifiers are those that have been added to the registry by following the procedure in Section 5.3.2.1.

Each extension identifier added to this registry **MUST** be unique amongst the set of registered extension identifiers.

Registered extension identifiers **MUST** be a maximum of 32 octets in length and **MUST** consist only of printable ASCII characters, excluding backslash and double quote, i.e., VCHAR as defined in [RFC5234] but without %x22 and %x5c. Extension identifiers are case sensitive and may not match other registered identifiers in a case-insensitive manner unless the designated experts determine that there is a compelling reason to allow an exception.

5.3.2.1. Registering Extension Identifiers

WebAuthn extension identifiers are registered using the Specification Required policy (see Section 4.6 of [RFC8126]).

The "WebAuthn Extension Identifiers" registry is located at https://www.iana.org/assignments/webauthn. Registration requests can be made by following the instructions located there or by sending an email to the webauthn-for-certreq-reg-review@ietf.org mailing list.

Registration requests consist of at least the following information:

- *WebAuthn Extension Identifier:
  - -An identifier meeting the requirements given in Section 5.3.2.
- *Description:
  - -A relatively short description of the extension.
- *Specification Document(s):
  - -Reference to the document or documents that specify the extension.

*Change Controller:

  -For Standards Track RFCs, list "IETF". For others, give the name of the responsible party. Other details (e.g., postal address, email address, home page URI) may also be included.

*Notes:

  -[optional]

Registrations **MUST** reference a freely available, stable specification, e.g., as described in Section 4.6 of [RFC8126]. This specification **MUST** include security and privacy considerations relevant to the extension.

Note that WebAuthn extensions can be registered by third parties (including the expert(s) themselves), if the expert(s) determines that an unregistered extension is widely deployed and not likely to be registered in a timely manner otherwise. Such registrations still are subject to the requirements defined, including the need to reference a specification.

5.3.2.2. Registration Request Processing

As noted in Section 5.3.2.1, WebAuthn extension identifiers are registered using the Specification Required policy.

The expert(s) will clearly identify any issues that cause a registration to be refused, such as an incompletely specified extension.

When a request is approved, the expert(s) will inform IANA, and the registration will be processed. The IESG is the arbiter of any objection.

5.3.2.3. Initial Values in the WebAuthn Extension Identifiers Registry

The initial values for the "WebAuthn Extension Identifiers" registry have been populated with the values listed in the "WebAuthn Extension Identifier Registrations" https://www.w3.org/TR/2019/REC-webauthn-1-20190304/#sctn-extensions-reg section of [WebAuthn]. Also, the Change Controller entry for each of those registrations is:

*Change Controller:

  -W3C Web Authentication Working Group (public-webauthn@w3.org)

6. ASN.1 Module

The following ASN.1 module makes use of the conventions from [RFC5912].

```
KeyAttestationExtn-2022
  { iso(1) identified-organization(3) dod(6)
    internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-keyAttestation(TBD2) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS

  id-pe
  FROM PKIX1Explicit-2009 -- from [RFC5912]
    { iso(1) identified-organization(3) dod(6) internet(1) security(5)
      mechanisms(5) pkix(7) id-mod(0) id-mod-pkix1-explicit-02(51) }

  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) }
  ;

-- EXPORT ALL --

ext-keyAttestation EXTENSION ::= {
  SYNTAX KeyAttestation IDENTIFIED BY id-pe-keyAttestation }

attr-keyAttestation ATTRIBUTE ::= {
  TYPE KeyAttestation IDENTIFIED BY id-pe-keyAttestation }

id-pe-keyAttestation OBJECT IDENTIFIER ::=  { id-pe TBD }

KeyAttestation ::= OCTET STRING

END
```

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>.

[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>.

[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>.

[RFC5272] Schaad, J. and M. Myers, "Certificate Management over CMS (CMC)", RFC 5272, DOI 10.17487/RFC5272, June 2008, <https://www.rfc-editor.org/rfc/rfc5272>.

[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>.

[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>.

[RFC7299] Housley, R., "Object Identifier Registry for the PKIX Working Group", RFC 7299, DOI 10.17487/RFC7299, July 2014, <https://www.rfc-editor.org/rfc/rfc7299>.

[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>.

[RFC8809] Hodges, J., Mandyam, G., and M. Jones, "Registries for Web Authentication (WebAuthn)", RFC 8809, DOI 10.17487/RFC8809, August 2020, <https://www.rfc-editor.org/rfc/rfc8809>.

[RFC8894] Gutmann, P., "Simple Certificate Enrolment Protocol", RFC 8894, DOI 10.17487/RFC8894, September 2020, <https://www.rfc-editor.org/rfc/rfc8894>.

[WebAuthn]
Hodges, J., Jones, J., Jones, M. B., Kumar, A., and E. Lundberg, "Web Authentication: An API for accessing Public Key Credentials Level 2", April 2021, <https://www.w3.org/TR/webauthn-2/>.

7.2. Informative References

[COTS] Wallace, C. and R. Housley, "Concise TA Stores (CoTS)", June 2022.

[fido-metadata] FIDO Alliance, "FIDO Metadata Statement", May 2021, <https://fidoalliance.org/specs/mds/fido-metadata-statement-v3.0-ps-20210518.html>.

[I-D.draft-bweeks-acme-device-attest]
Weeks, B., "Automated Certificate Management Environment (ACME) Device Attestation Extension", Work in Progress, Internet-Draft, draft-bweeks-acme-device-attest-01, 7 August 2022, <https://datatracker.ietf.org/doc/html/draft-bweeks-acme-device-attest-01>.

[OTA] Apple, "Over-the-Air Profile Delivery and Configuration", April 2018, <https://developer.apple.com/library/archive/documentation/NetworkingInternet/Conceptual/iPhoneOTAConfiguration/Introduction/Introduction.html>.

[RFC8555] Barnes, R., Hoffman-Andrews, J., McCarney, D., and J. Kasten, "Automatic Certificate Management Environment (ACME)", RFC 8555, DOI 10.17487/RFC8555, March 2019, <https://www.rfc-editor.org/rfc/rfc8555>.

[WebAuthnReg] IANA, "WebAuthn Attestation Statement Format Identifiers", <https://www.iana.org/assignments/webauthn/webauthn.xhtml>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Carl Wallace
Red Hound Software

Email: carl@redhoundsoftware.com

Sean Turner
sn3rd

Email: sean@sn3rd.com