Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 23 April 2026

J.-P. Fiset
Crypto4A
M. Ounsworth
Entrust
H. Tschofenig
H-BRS
M. Wiseman

20 October 2025

Extended Key Usage (EKU) for X.509 Certificates associated with Attestation Keys
draft-jpfiset-lamps-attestationkey-eku-01

Abstract

As described in RFC5280, key usages are specified in X.509 certificates using the certificate extensions "Key Usage" and "Extended Key Usage". This document defines an Extended Key Usage (EKU) relating to keys that are dedicated to the purpose of signing attestation evidence as introduced in RFC9334.

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 23 April 2026.

Copyright Notice

Table of Contents

1. Introduction

Attesters, as defined in Remote Attestation Procedures (RATS) in [RFC9334], can use cryptographic private keys to identify the origin of the evidence and protect its integrity. Those private keys are referred to as Attestation Keys.

Attestation Keys can be endorsed by a Certification Authority (CA) by issuing X.509 certificates (see [RFC5280]). Those certificates SHOULD include an extended key usage to indicate that the associated key is dedicated to the purpose of attesting evidence. This allows recipients of signed evidence to trust that the associated key is controlled according to the constraints specified in this document.

2. Terminology

Much of the terms used in this specification are borrowed from RATS ([RFC9334]). Readers of this specification should review the RATS architecture and its terminology to put in context the text presented in this specification.

Attestation Key : A key under the control of the Attester and reserved for the purpose of signing evidence.

3. Extended Key Usage for Attestation Key

This specification defines the KeyPurposeId id-kp-attestationKey. This KeyPurposeId is reserved for Attestation Keys.

The term "signing evidence" refers to performing a digital signature using an Attestation Key over content that includes claims and measurements about the target environment (see [RFC9334]).

An Attestation Key must be associated with the "digital signing" key usage, as any other keys used to performed digital signature. No other key usage should be assigned to an Attestation Key.

Furthermore, an Attestation Key MUST adhere to the following constraints:

* An Attestation Key SHOULD be used by an Attester only to digitally sign evidence that the Attester can observe in the target environment. The Attester SHOULD NOT use the Attestation Key for any other purpose (dedication).

* An Attestation Key MUST NOT be controlled by any entity other than the associated Attester. This constraint is to ensure that other entity can not impersonate the Attester (non-repudiation).

3.1. Including the EKU for Attestation Key in Certificates

When the EKU id-kp-attestationKey is included in a X.509, other considerations should be taken:

* The X.509 extension "key usage" MUST be set to "digital signature". In other words, the value of the associated field includes the bit "digitalSignature" set. Other key usages MUST NOT be set.

* The X.509 extension "extended key usage" SHOULD NOT include usage other than the one defined in this document (id-kp-attestationKey). If other extended key usages are provided, they MUST be compatible with constraints outlined in this specification.

When the extended key usage id-kp-attestationKey is added to the X.509 EKU extension, it is not necessary to mark this extension as critical. This is to foster interoperability between systems that are not aware of this extended key usage. Systems that consume the evidence signed by an attestation key, such as a Verifier, can enforce the presence of this extended key usage through policy.

3.2. Implication for a Certificate Authority

When a Certificate Authority issues a X.509 certificate that includes the extended key usage defined in this specification, certain additional considerations MUST be taken to ensure that the constraints defined in this document are respected.

Issuing a X.509 certificate with the extended key usage id-kp-attestationKey equates to providing an endorsement of the attester as defined in the RATS architecture. Therefore, the procedures and practices employed by a Certificate Authority MUST be augmented to take into account the security considerations relating to the Attestation Key as outlined in the RATS architecture.

In particular, it is not sufficient for a CA to verify that the subject of the certificate, the Attester, has possession of the subject key. It MUST also ensure that the Attester is the only entity that controls the key. This can be accomplished (but not restricted to) by using a key confined to specialized hardware under the control of the Attester.

3.3. Implication for the RATS Verifier

In [RFC9334], the Verifier is the role that consumes the evidence produced by an Attester. As part of the verification process, the Verifier assesses endorsements, among other things. A X.509 certificate containing the EKU id-kp-attestationKey is an endorsement of the Attester by the issuing authorities.

3.4. Implication for Cryptographic Modules

Attestation Keys are instantiated and operated on by cryptographic modules. These modules MUST provide the services required to restrict the use of an Attestation Key to its associated Attester.

The mechanisms used to perform those restrictions are out of scope for this specification.

4. 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.

5. Security Considerations

For attestation evidence to be valuable, coordination between the various roles is required:

* The cryptographic module MUST restrict the use of the Attestation Key to the associated Attester.

* The CA MUST ensure that the Attester is the only entity that controls the Attestation Key which is subject to the issuance of a certificate.

* A Verifier must perform the assessment of the presented evidence using all the procedures required to ascertain as to the origin and validity of the attester.

The risks associated with a failure of this coordination reduces the quality of the trustworthiness of the evidence.

The implications are outlines in the Security Considerations section in RATS ([RFC9334]).

6. IANA Considerations

For the ASN.1 module found in Appendix A, IANA is requested to assign an object identifier for the module identifier (TBD0) with a description of "id-mod-attestation-eku-2025". This should be allocated in the "SMI Security for PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

For the ASN.1 module found in Appendix A, IANA is requested to assign an object identifier for the extended key usage value (XX) with a description of "id-kp-attestationKey". This should be allocated in the "SMI Security for PKIX Extended Key Purpose" registry (1.3.6.1.5.5.7.3).

7. Normative References

[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/info/rfc9334>.

[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/info/rfc5280>.

[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/info/rfc2119>.

[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/info/rfc8174>.

Appendix A. ASN.1 Module

The following module adheres to ASN.1 specifications [X.680] and [X.690]. It defines the OID used for Attestation Key Extended Key Usage.

```
AttestationEKU-2025 { iso(1) identified-organization(3) dod(6) internet(1)
     security(5) mechanisms(5) pkix(7) id-mod(0)
     id-mod-attestation-eku-2025(TBD0) }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS ALL --

-- IMPORTS NOTHING --

-- OID Arc --

id-kp  OBJECT IDENTIFIER  ::= {
  iso(1) identified-organization(3) dod(6) internet(1)
  security(5) mechanisms(5) pkix(7) kp(3) }

-- Attestation Key Extended Key Usage --

id-kp-attestationKey OBJECT IDENTIFIER ::= { id-kp XX }

END
```

Acknowledgments

TODO acknowledge.

Authors' Addresses

Jean-Pierre Fiset
Crypto4A Inc.
1550A Laperriere Ave
Ottawa, Ontario K1Z 7T2
Canada
Email: jp@crypto4a.com

Mike Ounsworth
Entrust Limited
2500 Solandt Road - Suite 100
Ottawa, Ontario K2K 3G5
Canada
Email: mike.ounsworth@entrust.com

Hannes Tschofenig
University of Applied Sciences Bonn-Rhein-Sieg
Germany
Email: Hannes.Tschofenig@gmx.net

Monty Wiseman
United States of America
Email: montywiseman32@gmail.com