Network Working Group
Internet-Draft
Intended status: Standards Track
Expires: 3 September 2026

J.-P. Fiset
Crypto4A
M. Ounsworth
Cryptic Forest
H. Tschofenig
H-BRS
M. Wiseman
2 March 2026

X.509 Certificate Extended Key Usage (EKU) for Attestation Keys
draft-jpfiset-lamps-attestationkey-eku-02

Abstract

X.509 certificates ([RFC5280]) defines the Extended Key Usage (EKU) extension and specifies several key purpose identifiers (KeyPurposeIds) for use with that extension. This document defines a KeyPurposeId for the purpose of signing Evidence to provide remote attestation functions as defined in the RATS Architecture ([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 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

Key purpose identifiers (KeyPurposeId) are added to the Extended Key Usage (EKU) extension of X.509 certificates to express the intent of the certified key. It is used to further define the basic purpose indicated in the key usage (KU) extension.

This specification introduces the KeyPurposeId id-kp-attestationKey for X.509 certificates that endorse Attestation Keys for the purpose of validating Evidence.

Attesters, as defined in RATS [RFC9334], can use cryptographic private keys to identify the origin of generated Evidence and to 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 certified key is dedicated to the purpose of signing Evidence.

Verifiers responsible of validating Evidence generated by an Attester use the CA's endorsement (X.509 certificate) to support the appraisal process.

The KeyPurposeId id-kp-attestationKey allows the Verifier to trust that the associated key is controlled according to the guidance proposed in this specification.

1.1. Example

A Hardware Security Module (HSM) is designed to generate Evidence about itself and cryptographic keys that it hosts. For the purpose of generating Evidence, an Attestation Key is dedicated for this purpose and endorsed by the manufacturing CA.

The Attestation Key is not the only key endorsed by the manufacturing CA as many cryptographic signing keys are necessary to manage a HSM. As a result, there are many X.509 certificates issued to the HSM by the manufacturing CA.

A Verifier responsible of appraising Evidence generated by the HSM must ensure that the Attestation Key was used. Evidence signed by a different key, even if endorsed by the same manufacturing CA, can not be trusted. The key purpose introduced in this specification allows Verifiers to determine during validation if a cryptographic key was intended to be used for signing Evidence.

2. Terminology

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.

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.

Attester: Role defined in [RFC9334] and assigned to entities responsible of generating Evidence.

Evidence: The term Evidence respects the definition offered in [RFC9334]. Evidence is composed of claims and may include information such as configuration data, measurements and telemetry.

RATS: Remote ATtestation procedureS. Refers to a working group

within IETF and all the documents developed under this umbrella of effort. This specification is developed to support concepts developed in RATS but more particularly refers to the RATS Architecture as introduced in [RFC9334].

Verifier: Role defined in [RFC9334] and assigned to entities responsible of appraising the Evidence generated by an Attester.

3. Extended Key Usage for Attestation Keys

This specification defines the KeyPurposeId id-kp-attestationKey. This KeyPurposeId is reserved for endorsement of Attestation Keys. In other words, the intent of the certified key is to be dedicated to the signing of Evidence.

As described in [RFC5280], the EKU extension "MAY, at the option of the certificate issuer, be either critical or non-critical". Selecting to identify the EKU extension as critical might have significant impacts on the overall system performance and this decision is left to the issuing authority.

Also specified in [RFC5280], "[i]f multiple purposes are indicated the application need not recognize all purposes indicated, as long as the intended purpose is present". Since Attestation Keys should be dedicated to the purpose of signing Evidence, this specification RECOMMENDS that EKUs with the KeyPurposeId id-kp-attestationKey not include any other key purpose.

This specification RECOMMENDS that the extension Key Usage (KU) be included for the endorsement of Attestation Keys. Furthermore, if the KU extension is included, it SHOULD be set to "digital signature".

3.1. 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 identified Attester as defined in the RATS Architecture. Therefore, the procedures and practices employed by a Certificate Authority MUST 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.

3.2. Implication for the RATS Verifier

In [RFC9334], the Verifier is the role that appraises the Evidence produced by an Attester. As part of the verification process, the Verifier assesses endorsements. A X.509 certificate containing the EKU id-kp-attestationKey is an endorsement of the Attester by the issuing authority.

A Verifier MAY reject Evidence if the X.509 certificate issued to the signing key does not contain an EKU extension specifying the key purpose id-kp-attestationKey.

A Verifier MAY reject Evidence if the X.509 certificate issued to the signing key contains an EKU extension with a key purpose other than id-kp-attestationKey.

A Verifier SHOULD reject Evidence if the X.509 certificate issued to the signing key contains a KU extension with a basic purpose other than "digital signature".

3.3. Implication for Attesters

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 SHOULD be under the sole control of the Attester identified in the X.509 certificate. This constraint is to ensure that another entity can not impersonate the Attester (non-repudiation).

3.4. Implication for Cryptographic Modules

Attestation Keys are instantiated and operated on by cryptographic modules. These modules MUST provide the services required to accomplish the recommendations proposed in this specification.

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

4. Security Considerations

[RFC5280] introduces security considerations that are applicable to this specification. The EKU purpose id-kp-attestationKey does not introduce additional security risks. On the other hand, the adoption of this extended key purpose mitigates specific cross-protocol attacks in relation to use of Attestation Keys.

The RATS Architecture ([RFC9334]) offers many security considerations that should be reviewed by implementers of this specification.

5. 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).

6. Normative References

[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>.

[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>.

[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
Cryptic Forest Software
Sioux Lookout
Canada

Email: mike@ounsworth.ca

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