LAMPS
Internet-Draft
Intended status: Standards Track
Expires: 28 October 2025

M. Ounsworth
Entrust
M. Wiseman
Beyond Identity
H. Tschofenig
H-BRS
T. Reddy
Nokia
N. Smith
Intel Corporation

26 April 2025

X.509 Certificate Extensions for Attestation Results
draft-ounsworth-lamps-x509-ar-00

Abstract

This document defines extensions for X.509 certificates to include attestation results as part of the certificate's content. The primary use case for these extensions is in the context of Certificate Signing Request (CSR) attestation, where claims about the trustworthiness of an Attester are conveyed to the Certification Authority (CA) as part of the CSR process. These extensions enable the CA to appraise the submitted evidence and embed attestation results into the issued certificate. This allows Relying Parties to evaluate the Attester's trustworthiness consistently and efficiently, supporting scalable policies for verification in environments with diverse attestation technologies.

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 28 October 2025.

Table of Contents

1. Introduction

Attestation mechanisms are increasingly used to verify the trustworthiness of devices and cryptographic keys. These mechanisms provide evidence that a device or key meets specific security criteria before being relied upon by an application. However, relying parties need a standardized way to access and validate these attestation results.

This document introduces the Evidence Claims Certificate Extension, which enables Certification Authorities (CAs) to embed attestation results into issued X.509 certificates. By incorporating attestation results directly into certificates, Relying Parties can assess trustworthiness without requiring additional protocol interactions with external verifiers.

This extension is particularly useful in environments where:

* Devices generate key pairs and request certificates while providing evidence of their security characteristics, such as key storage protection and tamper resistance.
* Certification Authorities evaluate and verify attestation claims before issuing a certificate.
* Relying Parties need a standardized way to verify the security characteristics of a key or the platform managing it, as stated in the certificate, without requiring real-time attestation checks, since these characteristics are relatively static.

While PKIX Key Attestation [I-D.ietf-rats-pkix-key-attestation] defines a mechanism for carrying attestation evidence within a CSR, this document extends that concept to X.509 certificates by defining a Certificate Evidence Claims extension. This extension allows attestation evidence to be embedded directly into an issued certificate, enabling Relying Parties to verify the security characteristics of a key or its platform without requiring access to the original CSR or real-time attestation. Additionally, this document defines the ASN.1 syntax for the Evidence Claims Certificate Extension and specifies how it should be included in X.509 certificates.

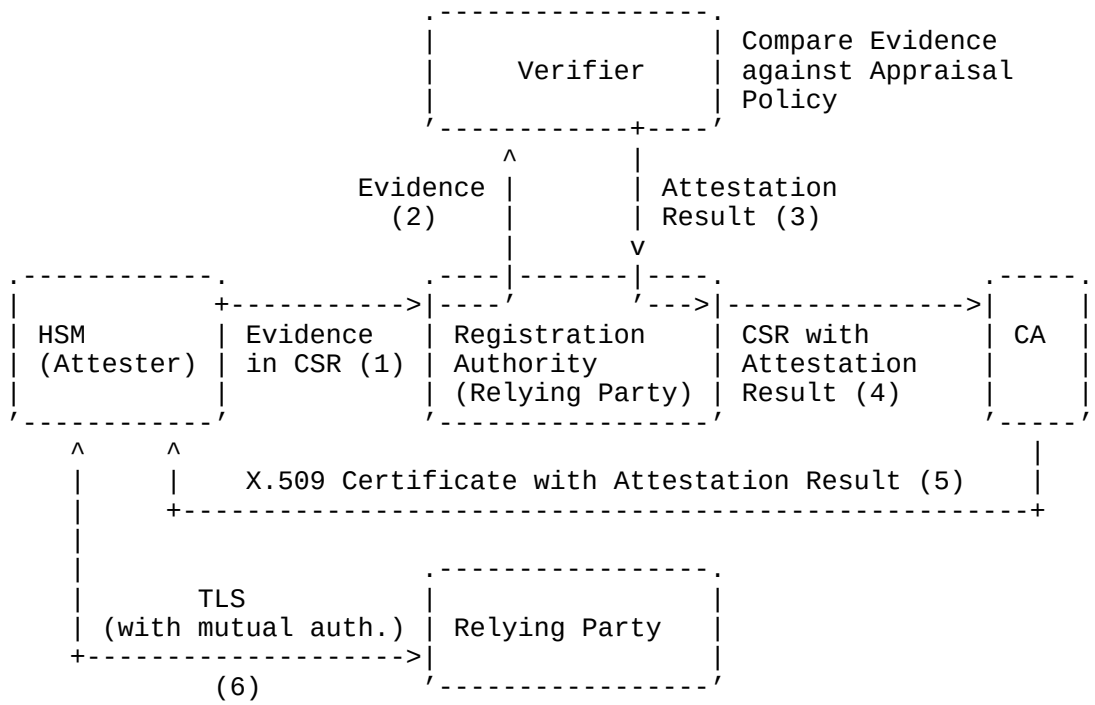

Figure 1: Example Data Flow demonstrating Attested CSR with Background Check Model.

Steps 1 to 4, covering the generation of evidence in a CSR, its verification by a Registration Authority, and the issuance of a CSR with an attestation result, are already specified in [I-D.ietf-rats-pkix-key-attestation].

* Step 5: The CA issues an X.509 certificate embedding the attestation result within the Evidence Claims Certificate Extension.
* Step 6: The Relying Party uses TLS with mutual authentication to verify the certificate and its Evidence Claims, authenticating the Attester.

This ensures that the security characteristics of the key or platform are verifiable without requiring real-time attestation checks.

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. Certificate Extensions

This section specifies the syntax and semantics of the Attestation Result Claims certificate extension, which provides a list of claims associated with the certificate subject appraised by the CA.

The Attestation Result Claims certificate extension MAY be included in public key certificates [RFC5280]. The Attestation Result Claims certificate extension MUST be identified by the following object identifier:

```
id-pe-ar-claims OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-pe(1) 34
}
```

This extension MUST NOT be marked critical.

The Attestation Result Claims extension MUST have the following syntax:

```
AR-Claims ::= SEQUENCE SIZE (1..MAX) OF ReportedEntity
```

The AR-Claims field represents a sequence of attestation result claims (ReportedEntity) included by the CA in the certificate. It MUST contain at least one claim. For privacy reasons, the CA MAY choose to include only a subset of the claims from the Attestation Result it received from a Verifier. The CA may include in their certificate profile a list of verified evidence claims (identified by OID) that MAY be copied from the CSR to the certificate, while any other claims MUST NOT be copied. By removing the signature from the evidence, the CA is asserting that it has verified the Evidence to chain to a root that the CA trusts, but it is not required to disclose in the final certificate what that root is.

See Section 4 for a discussion of privacy concerns related to re-publishing Evidence into a certificate.

The platform entity and key entity are relevant to the Evidence Claims Certificate Extension in the context of attesting to the security properties of a key or the platform that manages it.

3.1. id-pkix-attest-entity-platform (Platform Attestation)

* This attests that the platform hosting the key meets security requirements.
* Useful when the integrity of the system running cryptographic operations is important.
* Example: A certificate extension proving the FIPS level at which the attestor is currently operating in compliance with.

3.2. id-pkix-attest-entity-key (Key Attestation)

* This attests to the security properties of a specific cryptographic key, regardless of the platform.
* Ensures that the key is stored securely and follows cryptographic policies.
* Example: A certificate extension proving that the private key of the certificate is hardware-protected and cannot be exported to a software cryptographic module.

3.3. ASN.1 Module

This section provides an ASN.1 Module for the Evidence Claims certificate extension, and it follows the conventions established in [RFC5912] and [RFC6268].

```
EvidenceClaimsCertExtn
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-evidenceclaims(TBD) }

DEFINITIONS IMPLICIT TAGS ::= BEGIN

IMPORTS
    EXTENSION
    FROM PKIX-CommonTypes-2009 -- RFC 5912
        { iso(1) identified-organization(3) dod(6) internet(1)
          security(5) mechanisms(5) pkix(7) id-mod(0)
          id-mod-pkixCommon-02(57) };

-- Evidence Claims Certificate Extension OID
id-pe-ar-claims OBJECT IDENTIFIER ::= {
    iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-pe(1) 34
}

-- Evidence Claims Certificate Extension
ext-EvidenceClaims EXTENSION ::= {
    SYNTAX AR-Claims
    IDENTIFIED BY id-pe-ar-claims
}

-- Evidence Claims Syntax
AR-Claims ::= SEQUENCE SIZE (1..MAX) OF ReportedEntity

-- Alignment with PkixAttestation structure
ReportedEntity ::= SEQUENCE {
    entityType         OBJECT IDENTIFIER,
    reportedAttributes SEQUENCE SIZE (1..MAX) OF ReportedAttribute
}

ReportedAttribute ::= SEQUENCE {
    attributeType      OBJECT IDENTIFIER,
    value              AttributeValue
}

AttributeValue ::= CHOICE {
    bytes       [0] IMPLICIT OCTET STRING,
    utf8String  [1] IMPLICIT UTF8String,
    bool        [2] IMPLICIT BOOLEAN,
    time        [3] IMPLICIT GeneralizedTime,
    int         [4] IMPLICIT INTEGER,
    oid         [5] IMPLICIT OBJECT IDENTIFIER
}
```

4. Security Considerations

The extension MUST NOT publish in the certificate any privacy-sensitive information that could compromise the end device. What counts as privacy-sensitive will vary by use case. For example:

1. *HSM Usage*: For a hardware security module (HSM) backing a public code-signing service, the model and firmware patch level could be considered sensitive as it could give an attacker an advantage in exploiting known vulnerabilities.
2. *Mobile Devices*: For a certificate issued to an end-user mobile computing device, any unique identifier could be used for tracking.
3. *IoT Devices*: For small IoT devices, knowing hardware and firmware version information could help edge gateways deny access to devices with known vulnerabilities.

The CA MUST have a configurable mechanism to control which information is copied from the provided Evidence into the certificate, for example, via a certificate profile or Certificate Practice Statement (CPS). CA operators should err on the side of caution and exclude unnecessary claims. Avoiding unnecessary claims also mitigates the risk of targeted attacks, where an attacker could exploit knowledge of hardware versions, models, etc.

5. IANA Considerations

For the EvidenceClaims certificate extension in Section 3.3, IANA is requested to assign an object identifier (OID) for the certificate extension. The OID for the certificate extension should be allocated in the "SMI Security for PKIX Certificate Extension" registry (1.3.6.1.5.5.7.1).

For the ASN.1 Module in Section 3.3, 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 PKIX Module Identifier" registry (1.3.6.1.5.5.7.0).

6. References

6.1. Normative References

[I-D.ietf-rats-eat]
Lundblade, L., Mandyam, G., O'Donoghue, J., and C. Wallace, "The Entity Attestation Token (EAT)", Work in Progress, Internet-Draft, draft-ietf-rats-eat-31, 6 September 2024, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-eat-31>.

[I-D.ietf-rats-pkix-key-attestation]
Ounsworth, M., Fiset, J., Tschofenig, H., Birkholz, H., Wiseman, M., and N. Smith, "PKIX Key Attestation", Work in Progress, Internet-Draft, draft-ietf-rats-pkix-key-attestation-00, 3 March 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-rats-pkix-key-attestation-00>.

[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>.

[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>.

[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>.

6.2. Informative References

[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>.

[RFC9344] Asaeda, H., Ooka, A., and X. Shao, "CCNinfo: Discovering Content and Network Information in Content-Centric Networks", RFC 9344, DOI 10.17487/RFC9344, February 2023, <https://www.rfc-editor.org/rfc/rfc9344>.

Acknowledgments

The authors would like to thank ...

Authors' Addresses

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

Monty Wiseman
Beyond Identity
United States of America
Email: monty.wiseman@beyondidentity.com

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

Tirumaleswar Reddy
Nokia
Bangalore
Karnataka
India
Email: kondtir@gmail.com

Ned Smith
Intel Corporation
United States of America
Email: ned.smith@intel.com