Limited Additional Mechanisms for PKIX and SMIME
Internet-Draft
Intended status: Informational
Expires: 19 March 2026

R. Housley
Vigil Security
C. Bonnell
DigiCert
J. Mandel
AKAYLA
T. Okubo
Penguin Securities
15 September 2025

Media Access Control (MAC) Addresses in X.509 Certificates
draft-housley-lamps-macaddress-on-00

Abstract

This document defines a new otherName for inclusion in the X.509 Subject Alternative Name (SAN) extension to carry an IEEE Media Access Control (MAC) address. The new name form makes it possible to bind a layer-2 interface identifier to a public key certificate. This is needed for secure onboarding and key establishment protocols that operate below the network layer, such as IEEE 802.1AE (MACsec).

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://CBonnell.github.io/draft-housley-lamps-macaddress-on/draft-housley-lamps-macaddress-on.html. Status information for this document may be found at https://datatracker.ietf.org/doc/draft-housley-lamps-macaddress-on/.

Discussion of this document takes place on the Limited Additional Mechanisms for PKIX and SMIME 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/.

Source for this draft and an issue tracker can be found at https://github.com/CBonnell/draft-housley-lamps-macaddress-on.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

This Internet-Draft will expire on 19 March 2026.

Copyright Notice

Table of Contents

1. Introduction

IEEE 802.1AE [IEEE802.1AE] provides point-to-point link-layer data confidentiality and integrity ("MACsec"). Deployments that use X.509 certificates for MACsec key establishment frequently need to bind a Media Access Control (MAC) address to a public key when devices lack a stable IP address or operate in media where IP addressing is not yet available. The Subject Alternative Name (SAN) and Issuer Alternative Name (IAN) extensions defined in [RFC5280] allows an X.509 certificate to contain multiple name forms, but no standard name form exists for MAC addresses.

This document defines a new otherName form "MACAddress". The name form carries either a 48-bit IEEE 802 MAC address (EUI-48) or a 64-bit extended identifier (EUI-64) in an OCTET STRING. Additionally, the name form also can convey constraints on EUI-48 or EUI-64 values when included in the Name Constraints extension defined in [RFC5280]. The new name form enables certificate-based authentication at layer 2 and facilitates secure provisioning in Internet-of-Things and automotive networks.

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. MACAddress otherName

The new name form is identified by the object identifier (OID) id-on-MACAddress (TBD1). The name form has variants to convey a EUI-48 as an OCTET STRING comprising of 6 octets, or a EUI-64 as an OCTET STRING comprising of 8 octets. Constraints on EUI-48 and EUI-64 values are conveyed as N-bit bit patterns, where the bit pattern establishes a constraint on the upper N bits of a EUI-48 or EUI-64 value.

The following sub-sections describe how to encode EUI-48 and EUI-64 values and their corresponding constraints.

3.1. Encoding a MACAddress as an alternative name

When the name form is included in a Subject Alternative Name or Issuer Alternate Name extension, the syntax consists of exactly six or eight octets. Values are encoded with the most significant octet encoded first ("big-endian" or "left-to-right" encoding). No text representation is permitted in the certificate, as human-readable forms such as "00-24-98-7B-19-02" or "0024.987B.1902" are used only in management interfaces. When a device natively possesses a 48-bit MAC identifier, the CA MUST encode it using a 6-octet OCTET STRING as the MACAddress value. When the device's factory identifier is a 64-bit EUI-64 or when no canonical 48-bit form exists, the CA MUST encode it using an 8-octet OCTET STRING as the MACAddress value. The macAddress48Constraint and macAddress64Constraint tagged BIT STRING arms of MACAddress MUST NOT be used.

3.2. Encoding a MACAddress constraint

When the name form is included in the Name Constraints extension, the syntax consists of a context-specific, implicitly tagged BIT STRING that specifies a N-bit bit pattern. Bit patterns representing the constraint are encoded with the most significant bit encoded first ("big-endian" or "left-to-right" encoding). Constraints on EUI-48 values MUST be encoded using the macAddress48Constraint arm of MACAddress. Likewise, constraints on EUI-64 values MUST be encoded using the macAddress64Constraint arm of MACAddress. The macAddress OCTET STRING arm of MACAddress MUST NOT be used.

When a constraint is included in the permittedSubtrees field of a Name Constraints extension, certificates containing a MACAddress name form of the specific identifier type (EUI-48 or EUI-64) that are issued by the Certification Authority are trusted only when the upper N bits of the value are binary equal to the pattern. When a constraint is included in the excludedSubtrees field of a Name Constraints extension, certificates containing a MACAddress name form of the specific identifier type (EUI-48 or EUI-64) that are issued by the Certification Authority are trusted only when the upper N bits of the value are not binary equal to the pattern.

3.3. Generation and Validation Rules

A certificate MAY include one or more MACAddress otherName values if and only if the subject device owns (or is expected to own) the corresponding MAC address for the certificate lifetime. MAC addresses SHOULD NOT appear in more than one valid certificate issued by the same Certification Authority (CA) at the same time, unless different layer-2 interfaces share a public key.

A Relying party that matches a presented MAC address to a certificate SHALL perform a byte-for-byte comparison of the OCTET STRING contents. Canonicalization, case folding, or removal of delimiter characters MUST NOT be performed.

Wildcards are not supported.

Self-signed certificates that carry a MACAddress otherName SHOULD include the address of one of the device's physical ports.

3.4. Name Constraints Processing

The MACAddress otherName follows the general rules for otherName constraints in RFC 5280, Section 4.2.1.10. A name constraints extension MAY impose permittedSubtrees and excludedSubtrees on id-on-MACAddress.

A constraint that is represented as a macAddress48Constraint is relevant only to macAddress values that are encoded using 6 octets; such a constraint is ignored for macAddress values that are encoded using 8 octets. Likewise, a constraint that is represented as a macAddress64Constraint is relevant only to macAddress values that are encoded using 8 octets; such a constraint is ignored for macAddress values that are encoded using 6 octets.

To determine if a constraint matches a given name value, the certificate-consuming application performs an exclusive OR (XOR) operation of the N-bit bit pattern of the constraint and the upper N bits of the macAddress OCTET STRING value. If the result of the XOR operation is a bit string consisting of entirely zeros, then the name matches the constraint. Conversely, if the result of the operation is a bit string with at least one bit asserted, then the name does not match the constraint.

The first octet of a MAC address contains two flag bits.

* I/G bit (bit 0) 0 = unicast, 1 = multicast. Multicast prefixes are never OUIs.

* U/L bit (bit 1) 0 = universal (IEEE-assigned), 1 = local.

These flags let the implementations exclude multicast and local prefixes but still cannot prove that a 24-bit value is an IEEE-registered OUI. 36-bit CIDs share the same first 24 bits and enterprises MAY deploy pseudo-OUIs. CAs MUST include only prefixes the subscriber legitimately controls (registered OUI or CID). Before issuing a certificate that contains a MACAddress or a name constraint based on such a prefix, the CA MUST verify that control—for example, by consulting the IEEE registry or reviewing manufacturer documentation.

4. Security Considerations

The binding of a MAC address to a certificate is only as strong as the CA's validation process. CAs MUST verify that the subscriber legitimately controls or owns the asserted MAC address.

Some systems dynamically assign or share MAC addresses. Such practices can undermine the uniqueness and accountability that this name form aims to provide.

Unlike IP addresses, MAC addresses are not typically routed across layer 3 boundaries. Relying parties in different broadcast domains SHOULD NOT assume uniqueness beyond their local network.

4.1. Privacy Considerations

A MAC address can uniquely identify a physical device and by extension, its user. Certificates that embed unchanging MAC addresses facilitate long-term device tracking. Deployments that use the MACAddress name SHOULD consider rotating addresses, using temporary certificates, or employing MAC Address Randomization where feasible.

5. IANA Considerations

IANA is requested to make the following assignments in the "SMI Security for PKIX Module Identifier" (1.3.6.1.5.5.7.0) registry

Decimal	Description	References
TBD0	id-mod-mac-address-other-name-2025	This doc

IANA is requested to make the following assignment in the "SMI Security for PKIX Other Name Forms" (1.3.6.1.5.5.7.8) registry

Decimal	Description	References
TBD1	id-on-MACAddress	THis doc

6. ASN.1 Module

This Appendix contains the ASN.1 Module for the MAC Address; it follows the conventions established by [RFC5912].

```
MACAddressOtherName-2025
  { iso(1) identified-organization(3) dod(6) internet(1)
    security(5) mechanisms(5) pkix(7) id-mod(0)
    id-mod-mac-address-other-name-2025(TBD0) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

IMPORTS
  OTHER-NAME FROM PKIX1Implicit-2009
    { iso(1) identified-organization(3) dod(6) internet(1)
      security(5) mechanisms(5) pkix(7) id-mod(0)
      id-mod-pkix1-implicit-02(59) }

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

-- id-pkix 8 is the otherName arc
id-on  OBJECT IDENTIFIER ::= { id-pkix 8 }

-- OID for this name form
id-on-MACAddress OBJECT IDENTIFIER ::= { id-on TBD1 }

-- Contents of the otherName field
MACAddressOtherNames OTHER-NAME ::= { on-MACAddress, ... }

on-MACAddress OTHER-NAME ::= {
MACAddress IDENTIFIED BY id-on-MACAddress }

MACAddress ::= CHOICE {
  -- 48-bit EUI-48 or 64-bit EUI-64
  macAddress OCTET STRING (SIZE (6 | 8)),
  -- constraint on the upper bits of a 48-bit EUI-48
  macAddress48Constraint [0] BIT STRING (SIZE (1..48)),
  -- constraint on the upper bits of a 64-bit EUI-64
  macAddress64Constraint [1] BIT STRING (SIZE (1..64))
}

END
```

7. MAC Address otherName Examples

The following is a human-readable summary of the Subject Alternative Name extension from a certificate containing a single MACAddress otherName with value 00-24-98-7B-19-02:

```
SEQUENCE {
  otherName [0] {
    OBJECT IDENTIFIER id-on-MACAddress (TBD)
    [0] OCTET STRING '0024987B1902'H
  }
}
```

An EUI-64 example (AC-DE-48-00-11-22-33-44):

```
[0] OCTET STRING 'ACDE480011223344'H
```

8. Normative References

[IEEE802.1AE] IEEE, "IEEE Standard for Local and metropolitan area networks - Media Access Control (MAC) Security", IEEE 802-1ae-2018, DOI 10.1109/IEEESTD.2018.8585421, 21 December 2018, <https://doi.org/10.1109/IEEESTD.2018.8585421>.

[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>.

[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>.

[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>.

[X680] ITU-T, "Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation", ITU-T Recommendation X.680, ISO/IEC 8824-1:2021, February 2021, <https://www.itu.int/rec/T-REC-X.680>.

[X690] ITU-T, "Information technology -- ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER)", ITU-T Recommendation X.690, ISO/IEC 8825-1-2021, February 2021, <https://www.itu.int/rec/T-REC-X.690>.

Acknowledgments

TODO acknowledge.

Authors' Addresses

Russ Housley
Vigil Security, LLC
Email: housley@vigilsec.com

Corey Bonnell
DigiCert, Inc.
Email: corey.bonnell@digicert.com

Joe Mandel
AKAYLA, Inc.
Email: joe@akayla.com

Tomofumi Okubo
Penguin Securities Pte. Ltd.
Email: tomofumi.okubo+ietf@gmail.com