Workgroup: LAMPS Working Group
Internet-Draft:
draft-ietf-lamps-rfc7030-csrattrs-02
Published: 8 April 2023
Intended Status: Standards Track
Expires: 10 October 2023
Authors: M. Richardson, Ed.
Sandelman Software Works
O. Friel
Cisco
D. von Oheimb
Siemens
D. Harkins
The Industrial Lounge

Clarification of RFC7030 CSR Attributes definition

Abstract

The Enrollment over Secure Transport (EST, RFC7030) is ambiguous in its specification of the CSR Attributes Response. This has resulted in implementation challenges and implementor confusion.

This document updates RFC7030 (EST) and clarifies how the CSR Attributes Response can be used by an EST server to specify both CSR attribute OIDs and also CSR attribute values, in particular X.509 extension values, that the server expects the client to include in subsequent CSR request.

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 10 October 2023.

Copyright Notice

Table of Contents

1. Introduction

Enrollment over Secure Transport [RFC7030] (EST) has been used in a wide variety of applications. In particular, [RFC8994] and [RFC8995] describe a way to use it in order to build out an autonomic control plane (ACP) [RFC8368].

The ACP requires that each node be given a very specific subjectAltName. In the ACP specification, the solution was for the EST server to use section 2.6 of [RFC7030] to convey to the EST client the actual subjectAltName that will end up in its certificate.

As a result of some implementation challenges, it came to light that this particular way of using the CSR attributes was not universally agreed upon, and it was suggested that it went contrary to section 2.6.

Section 2.6 says that the CSR attributes "can provide additional descriptive information that the EST server cannot access itself". This is extended to mention also values that the EST server demands to use.

After significant discussion, it has been determined that Section 4.5 of [RFC7030] specification is sufficiently difficult to read and ambiguous to interpret that clarification is needed.

This document motivates the different use cases, and provides additional worked out examples.

Also, section 4.5.2 is extended to clarify the use of the existing ASN.1 syntax. This covers all uses and is fully backward compatible with the existing use.

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.

3. CSR Attributes Handling

3.1. Extensions to RFC 7030 section 2.6.

Replace the second paragraph with the following text:

These attributes can provide additional descriptive information that the EST server cannot access itself, such as the Media Access Control (MAC) address of an interface of the EST client. The EST server can also provide concrete values that it tells the client to include in the CSR, such as a specific X.509 Subject Alternative Name extension. Moreover, these attributes can indicate the kind of enrollment request, such as a specific elliptic curve or a specific hash function that the client is expected to use when generating the CSR.

3.2. Extensions to RFC 7030 section 4.5.2.

The ASN.1 for CSR Attributes as defined in EST section 4.5.2 is as follows:

```
CsrAttrs ::= SEQUENCE SIZE (0..MAX) OF AttrOrOID

AttrOrOID ::= CHOICE (oid OBJECT IDENTIFIER, attribute Attribute }

Attribute { ATTRIBUTE:IOSet } ::= SEQUENCE {
     type   ATTRIBUTE.&id({IOSet}),
     values SET SIZE(1..MAX) OF ATTRIBUTE.&Type({IOSet}{@type}) }
```

This remains unchanged, such that bits-on-the-wire compatibility is maintained.

Key parts that were unclear were which OID to use in the 'type' field and that the 'values' field can contain an entire sequence of X.509 extensions.

The OID to use for such extensions in the 'type' field MUST be extensionRequest, which has the numerical value 1.2.840.113549.1.9.14. There MUST be only one such attribute.

The 'values' field of this attribute MUST contain a set with exactly one element, and this element MUST by of type Extensions, as per Section 4.1 of [RFC5280]:

```
Extensions  ::=  SEQUENCE SIZE (1..MAX) OF Extension

Extension  ::=  SEQUENCE  {
     extnID      OBJECT IDENTIFIER,
     critical    BOOLEAN DEFAULT FALSE,
     extnValue   OCTET STRING
                 -- contains the DER encoding of an ASN.1 value
                 -- corresponding to the extension type identified
                 -- by extnID
     }
```

In each such Extensions sequence, an extnID OID MUST appear at most once.

An Extension comprises of the OID of the specific X.509 extension (extnID), optionally the 'critical' bit, and the extension value (extnValue).

(TODO: Do we want to allow an empty extnValue (which is of type OCTET STRING), which would mean that the client is told to include an X.509 extension of the given type and fill in the concrete value itself?)

With this understanding, the needs of [RFC8994] and [RFC8995] are satisfied with no change to the bits on the wire.

(TODO: Do we want to give the empty list of Extensions a specific meaning, such as, no X.509 extensions should be included in the CSR?)

(TODO: Note that this mechanism does not support telling the client to include in the CSR a specific subject DN, simply because there is no OID for this. I think we should better make this clear, or we have to define such an OID if setting a subject name should be supported.)

4. Co-existence with existing implementations

5. Examples

5.1. RFC8994/ACP subjectAltName with specific otherName and other extensions included

This is a CSR Attributes object with two non-critical basicConstraints and extKeyUsage extensions and a critical X.509 subjectAltName extension that contains both an RFC8994/ACP Subject Alternative Name with a specific otherName and an example Subject Alternative Name value of type dNSName.

```
SEQUENCE {
  SEQUENCE {
    OBJECT IDENTIFIER extensionRequest (1 2 840 113549 1 9 14)
    SET {
      SEQUENCE {
        SEQUENCE {
          OBJECT IDENTIFIER basicConstraints (2 5 29 19)
          OCTET STRING, encapsulates {
            SEQUENCE {}
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER extKeyUsage (2 5 29 37)
          OCTET STRING, encapsulates {
            SEQUENCE {
              OBJECT IDENTIFIER serverAuth (1 3 6 1 5 5 7 3 1)
              }
            }
          }
        SEQUENCE {
          OBJECT IDENTIFIER subjectAltName (2 5 29 17)
          BOOLEAN TRUE
          OCTET STRING, encapsulates {
            SEQUENCE {
              [0] {
                OBJECT IDENTIFIER '1 3 6 1 5 5 7 8 10'
                [0] {
                  IA5String
            'fd89b714f3db00000200000064000000+area51.research'
            '@acp.example.com'
                  }
                }
              [2] 'domain.example'
              }
            }
          }
        }
      }
    }
  }
```

5.2. EST server requires public keys of a specific size

TBD

5.3. EST server requires a public key of a specific algorithm/curve

TBD

5.4. EST server requires a specific extension to be present

TBD

6. Security Considerations

The security considerations from EST [RFC7030] section 6 are unchanged.

6.1. Identity and Privacy Considerations

An EST server may use this mechanism to instruct the EST client about the identities it should include in the CSR it sends as part of enrollment. The client may only be aware of its IDevID Subject, which includes a manufacturer serial number. The EST server can use this mechanism to tell the client to include a specific fully qualified domain name in the CSR in order to complete domain ownership proofs required by the CA. Additionally, the EST server may deem the manufacturer serial number in an IDevID as personally identifiable information, and may want to specify a new random opaque identifier that the pledge should use in its CSR. This may be desirable if the CA and EST server have different operators.

7. IANA Considerations

No requests are made to IANA.

8. Acknowledgements

TODO

9. Changelog

10. References

10.1. 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/info/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/info/rfc5280>.

[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/info/rfc7030>.

[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>.

[RFC8994] Eckert, T., Ed., Behringer, M., Ed., and S. Bjarnason, "An Autonomic Control Plane (ACP)", RFC 8994, DOI 10.17487/RFC8994, May 2021, <https://www.rfc-editor.org/info/rfc8994>.

[RFC8995] Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructure (BRSKI)", RFC 8995, DOI 10.17487/RFC8995, May 2021, <https://www.rfc-editor.org/info/rfc8995>.

10.2. Informative References

[RFC8368] Eckert, T., Ed. and M. Behringer, "Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance (OAM)", RFC 8368, DOI 10.17487/RFC8368, May 2018, <https://www.rfc-editor.org/info/rfc8368>.

Authors' Addresses

Michael Richardson (editor)
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Owen Friel
Cisco

Email: ofriel@cisco.com

Dr. David von Oheimb
Siemens

Email: dev@ddvo.net

Dan Harkins
The Industrial Lounge

Email: dharkins@lounge.org