Workgroup: LAMPS Working Group
Internet-Draft:
draft-richardson-lamps-rfc7030-csrattrs-00
Published: 22 October 2021
Intended Status: Standards Track
Expires: 25 April 2022
Authors: M. Richardson D. Harkins
Sandelman Software Works The Industrial Lounge
D. von Oheimb O. Friel
Siemens Cisco

Clarification of RFC7030 CSR Attributes definition

Abstract

Enrollment over Secure Transport (EST) is ambiguous in specification of the CSR Attributes Response. This has resulted in implementation challenges and implementor confusion. This document updates 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 that the server expects the client to include in its CSR request.

Status of This Memo

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. So, 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 in fact runs contrary to section 2.6, which says that the CSR attributes "provide additional descriptive information that the EST server cannot access itself" (when, in this case, it is the EST server and not the EST client that has access to this information).

In particular, it is not universally agreed that a CSR Attributes response can be used by an EST server to specify both attribute OIDs and attribute values. This document, therefore, updates section 2.6 to define this behavior.

This document also updates section 4.5 to include revised ASN.1 that covers all uses and is backward compatible with the existing use.

Additional examples are provided in an appendix.

2. CSR Attributes Handling

2.1. Current EST Specification

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

```
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}) }
```

That section also states the following:

> the values indicating the particular
> attributes desired to be included in the resulting certificate's
> extensions

This has been interpreted by some implementations as meaning that the CSR Attributes response can only include values for the attribute OIDs that the client should include in its CSR, and cannot include the actual values of those attributes. This is further reinforced by the example:

```
Attribute:  type = extensionRequest (1.2.840.113549.1.9.14)
                   value = macAddress (1.3.6.1.1.1.1.22)
```

This example illustrates that the 'value' specified is an attribute OID, for example the macAddress OID, and not the value of the attribute itself.

There is no clearly documented mechanism with supporting examples that specifies how a CSR Attributes response can include a value for a given attribute such as SubjectAltName.

EST section 4.5.2 also states the following:

> The structure of the CSR Attributes Response SHOULD, to the
> greatest extent possible, reflect the structure of the CSR
> it is requesting.

This statement aligns closely with the goal of this document. Additionally, EST Extensions [RFC8295] Appendix A has an informative appendix that outlines how a full CSR can be included in the CSR Attributes response.

2.2. Updated CSR Attributes Handling

This is option one.

This document defines how a CSR Attributes response is aligned with the PKCS#10 'CertificationRequestInfo' structure. The CSR Attributes response includes a PKCS#10 CSR structure that optionally includes any required values for included attributes. The following formatting rules apply to the CSR Attributes PKCSC#10 'CertificationRequestInfo' structure included in a CSR Attributes response:

*Concrete attribute values may be ommitted. If an attribute OID is included but the attribute value is not included, this indicates to the client that it should include and specify that attribute value.

*Additional attribute OIDs may be included. For example, for requesting the use of challengePassword, or for specifying public-key algorithms.

TODO Rule for multiple attributes. RFC 2986 and 5967 do not describe how handle conflicting attributes. There was a suggestion to not allow more than one instance of an attribute. However, you can have multiple SubjectAltNames...

2.2.1. Subject Handling

There is no defined OID for the 'subject' field. An EST server can specify 'subject' field values in a CSR Attributes response by including all required relative distinguished names as a sequence of OIDs, for example:

```
SEQUENCE {
  OBJECT IDENTIFIER commonName (2 5 4 3)
  UTF8String "example.com"
  }

SEQUENCE {
  OBJECT IDENTIFIER serialNumber (2 5 4 5)
  PrintableString "EXAMPLE123'
  }
```

2.3. Extend CSR structure to allow values:

This is option two.

This would just add a value to the SEQUENCE:

```
     OBJECT challengePassword
     SEQUENCE
       OBJECT subjectAltName
       SET
         OBJECT someACPgoo
     SEQUENCE
       OBJECT id-ecPublicKey
       SET
         OBJECT secp384r1
     OBJECT ecdsa-with-SHA384
```

For example:

```
  0  30: SEQUENCE {
  2  28:   SEQUENCE {
  4   3:     OBJECT IDENTIFIER subjectAltName (2 5 29 17)
  9  21:     SET {
 11  19:       [1] {
 13  17:         UTF8String 'hello@example.com'
       :         }
       :       }
       :     }
       :   }
```

3. Security Considerations

All security considertions from EST [RFC7030] section 6 are applicable.

3.1. 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.

4. IANA Considerations

None.

5. Acknowledgements

TODO

6. Changelog

7. References

7.1. Normative References

[BCP14] 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>.

[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>.

[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>.

7.2. Informative References

[RFC8295] Turner, S., "EST (Enrollment over Secure Transport) Extensions", RFC 8295, DOI 10.17487/RFC8295, January 2018, <https://www.rfc-editor.org/info/rfc8295>.

[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
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Dan Harkins
The Industrial Lounge

Email: dharkins@lounge.org

Dr. David von Oheimb

Siemens

Email: dev@ddvo.net

Owen Friel
Cisco

Email: ofriel@cisco.com