LAMPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: April 26, 2020

M. Richardson
Sandelman Software Works
T. Werner
Siemens
W. Pan
Huawei Technologies
S. Turner
sn3rd

October 24, 2019

Clarification of Enrollment over Secure Transport (EST): transfer encodings and ASN.1
draft-richardson-lamps-rfc7030est-clarify-04

Abstract

This document updates RFC7030: Enrollment over Secure Transport (EST) to resolve some errata that was reported, and which has proven to have interoperability when RFC7030 has been extended.

This document deprecates the specification of "Content-Transfer-Encoding" headers for EST endpoints, providing a way to do this in an upward compatible way. This document additional defines a GRASP discovery mechanism for EST endpoints, and specifies requirements for them.

Finally, this document fixes some syntactical errors in ASN.1 that was presented.

Status of This Memo

Copyright Notice

Table of Contents

1. Introduction

[RFC7030] defines the Enrollment over Secure Transport, or EST protocol.

This specification defines a number of HTTP end points for certificate enrollment and management. The details of the transaction were defined in terms of MIME headers as defined in [RFC2045], rather than in terms of the HTTP protocol as defined in [RFC2616] and [RFC7230].

[RFC2616] and later [RFC7231] Appendix A.5 has text specifically deprecating Content-Transfer-Encoding.

[RFC7030] calls it out this header incorrectly.

[I-D.ietf-anima-bootstrapping-keyinfra] extends [RFC7030], adding new functionality, and interop testing of the protocol has revealed that unusual processing called out in [RFC7030] causes confusion.

EST is currently specified as part of IEC 62351, and is widely used in Government, Utilities and Financial markets today.

Changes to [RFC7030] to bring it inline with typical HTTP processing would change the on-wire protocol in a way that is not backwards compatible. Reports from the field suggest that many implementations do not send the Content-Transfer-Encoding, and many of them ignore it.

This document therefore revises [RFC7030] to reflect the field reality, deprecating the extranous field.

This document deals with errata numbers [errata4384], [errata5107], and [errata5108].

2. Terminology

The abbreviation "CTE" is used to denote the Content-Transfer-Encoding header, and the abbreviation "CTE-base64" is used to denote a request or response whose Content-Transfer-Encoding header contains the value "base64".

3. Requirements Language

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in BCP 14, RFC 2119 [RFC2119] and indicate requirement levels for compliant STuPiD implementations.

4. Changes to EST endpoint processing

The [RFC7030] sections 4.1.3 (CA Certificates Response, /cacerts), 4.3.1/4.3.2 (Full CMC, /fullcmc), 4.4.2 (Server-Side Key Generation, /serverkeygen), and 4.5.2 (CSR Attributes, /csrattrs) specify the use of base64 encoding with a Content-Transfer-Encoding for requests and response.

This document updates [RFC7030] to require the POST request and payload response of all endpoints in to be [RFC4648] section 4 Base64 encoded DER. This format is to be used regardless of whether there

is any Content-Transfer-Encoding header, and any value in that header is to be ignored.

5. Clarification of ASN.1 for Certificate Attribute set.

Section 4.5.2 of [RFC7030] is to be replaced with the following text:

5.1. CSR Attributes Response

If locally configured policy for an authenticated EST client indicates a CSR Attributes Response is to be provided, the server response MUST include an HTTP 200 response code. An HTTP response code of 204 or 404 indicates that a CSR Attributes Response is not available. Regardless of the response code, the EST server and CA MAY reject any subsequent enrollment requests for any reason, e.g., incomplete CSR attributes in the request.

Responses to attribute request messages MUST be encoded as the content-type of "application/csrattrs", and are to be "base64" [RFC2045] encoded. The syntax for application/csrattrs body is as follows:

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

AttrOrOID ::= CHOICE {
  oid        OBJECT IDENTIFIER,
  attribute  Attribute {{AttrSet}} }

AttrSet ATTRIBUTE ::= { AttributesDefinedInRFC7030, ... }
```

An EST server includes zero or more OIDs or attributes [RFC2986] that it requests the client to use in the certification request. The client MUST ignore any OID or attribute it does not recognize. When the server encodes CSR Attributes as an empty SEQUENCE, it means that the server has no specific additional information it desires in a client certification request (this is functionally equivalent to an HTTP response code of 204 or 404).

If the CA requires a particular crypto system or use of a particular signature scheme (e.g., certification of a public key based on a certain elliptic curve, or signing using a certain hash algorithm) it MUST provide that information in the CSR Attribute Response. If an EST server requires the linking of identity and POP information (see Section 3.5), it MUST include the challengePassword OID in the CSR Attributes Response.

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

Requests to use a particular signature scheme (e.g. using a particular hash function) are represented as an OID to be reflected in the SignatureAlgorithm of the CSR. Requests to use a particular crypto system (e.g., certification of a public key based on a certain elliptic curve) are represented as an attribute, to be reflected as the AlgorithmIdentifier of the SubjectPublicKeyInfo, with a type indicating the algorithm and the values indicating the particular parameters specific to the algorithm. Requests for descriptive information from the client are made by an attribute, to be represented as Attributes of the CSR, with a type indicating the [RFC2985] extensionRequest and the values indicating the particular attributes desired to be included in the resulting certificate's extensions.

The sequence is Distinguished Encoding Rules (DER) encoded [X690] and then base64 encoded (Section 4 of [RFC4648]). The resulting text forms the application/csrattr body, without headers.

For example, if a CA requests a client to submit a certification request containing the challengePassword (indicating that linking of identity and POP information is requested; see Section 3.5), an extensionRequest with the Media Access Control (MAC) address ([RFC2307]) of the client, and to use the secp384r1 elliptic curve and to sign with the SHA384 hash function. Then, it takes the following:

```
OID:        challengePassword (1.2.840.113549.1.9.7)

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

Attribute:  type = id-ecPublicKey (1.2.840.10045.2.1)
            value = secp384r1 (1.3.132.0.34)

OID:        ecdsaWithSHA384 (1.2.840.10045.4.3.3)
```

and encodes them into an ASN.1 SEQUENCE to produce: ~~~ 30 41 06 09 2a 86 48 86 f7 0d 01 09 07 30 12 06 07 2a 86 48 ce 3d 02 01 31 07 06 05 2b 81 04 00 22 30 16 06 09 2a 86 48 86 f7 0d 01 09 0e 31 09 06 07 2b 06 01 01 01 01 16 06 08 2a 86 48 ce 3d 04 03 03 ~~~

and then base64 encodes the resulting ASN.1 SEQUENCE to produce:

```
MEEGCSqGSIb3DQEJBzASBgcqhkjOPQIBMQcGBSuBBAAiMBYGCSqGSIb3DQEJDjEJ
BgcrBgEBAQEWBggqhkjOPQQDAw==
```

6. Clarification of error messages for certificate enrollment operations

errata 5108.

7. Privacy Considerations

This document does not disclose any additional identifies to either active or passive observer would see with [RFC7030].

8. Security Considerations

This document clarifies an existing security mechanism. An option is introduced to the security mechanism using an implicit negotiation.

9. IANA Considerations

The ASN.1 module in Appendix A of this doucment makes use of object identifiers (OIDs). This document requests that IANA register an OID in the SMI Security for PKIX Arc in the Module identifiers subarc (1.3.6.1.5.5.7.0) for the ASN.1 module. The OID for the Asymmetric Decryption Key Identifier (1.2.840.113549.1.9.16.2.54) was previously defined in [RFC7030]. IANA is requested to update the "Reference" column for the Asymmetric Decryption Key Identifier attribute to also include a reference to this doducment.

10. Acknowledgements

This work was supported by the Huawei Technologies.

11. References

11.1. Normative References

[I-D.ietf-anima-bootstrapping-keyinfra]
Pritikin, M., Richardson, M., Eckert, T., Behringer, M., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-28 (work in progress), September 2019.

[RFC2045] Freed, N. and N. Borenstein, "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies", RFC 2045, DOI 10.17487/RFC2045, November 1996, <https://www.rfc-editor.org/info/rfc2045>.

[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>.

[RFC2986] Nystrom, M. and B. Kaliski, "PKCS #10: Certification Request Syntax Specification Version 1.7", RFC 2986, DOI 10.17487/RFC2986, November 2000, <https://www.rfc-editor.org/info/rfc2986>.

[RFC4648] Josefsson, S., "The Base16, Base32, and Base64 Data Encodings", RFC 4648, DOI 10.17487/RFC4648, October 2006, <https://www.rfc-editor.org/info/rfc4648>.

[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>.

[X680] ITU-T, "Information technology - Abstract Syntax Notation One.", ISO/IEC 8824-1:2002, 2002.

[X681] ITU-T, "Information technology - Abstract Syntax Notation One: Information Object Specification.", ISO/ IEC 8824-2:2002, 2002.

[X682] ITU-T, "Information technology - Abstract Syntax Notation One: Constraint Specification.", ISO/IEC 8824-2:2002, 2002.

[X683] ITU-T, "Information technology - Abstract Syntax Notation One: Parameterization of ASN.1 Specifications.", ISO/ IEC 8824-2:2002, 2002.

[X690] ITU-T, "Information technology - ASN.1 encoding Rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER).", ISO/IEC 8825-1:2002, 2002.

11.2. Informative References

[errata4384] "EST errata 4384: ASN.1 encoding error", n.d., <https://www.rfc-editor.org/errata/eid4384>.

[errata5107] "EST errata 5107: use Content-Transfer-Encoding", n.d., <https://www.rfc-editor.org/errata/eid5107>.

[errata5108]
"EST errata 5108: use of Content-Type for error message", n.d., <https://www.rfc-editor.org/errata/eid5108>.

[RFC2307] Howard, L., "An Approach for Using LDAP as a Network Information Service", RFC 2307, DOI 10.17487/RFC2307, March 1998, <https://www.rfc-editor.org/info/rfc2307>.

[RFC2616] Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., and T. Berners-Lee, "Hypertext Transfer Protocol -- HTTP/1.1", RFC 2616, DOI 10.17487/RFC2616, June 1999, <https://www.rfc-editor.org/info/rfc2616>.

[RFC2985] Nystrom, M. and B. Kaliski, "PKCS #9: Selected Object Classes and Attribute Types Version 2.0", RFC 2985, DOI 10.17487/RFC2985, November 2000, <https://www.rfc-editor.org/info/rfc2985>.

[RFC7230] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing", RFC 7230, DOI 10.17487/RFC7230, June 2014, <https://www.rfc-editor.org/info/rfc7230>.

[RFC7231] Fielding, R., Ed. and J. Reschke, Ed., "Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content", RFC 7231, DOI 10.17487/RFC7231, June 2014, <https://www.rfc-editor.org/info/rfc7231>.

Appendix A. ASN.1 Module

This annex provides the normative ASN.1 definitions for the structures described in this specification using ASN.1 as defined in [X680] through [X683].

There is no ASN.1 Module in RFC 7030. This module has been created by combining the lines that are contained in the document body.

```
PKIXEST-2019
     { iso(1) identified-organization(3) dod(6)
       internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
       id-mod-est-2019(TBD) }

DEFINITIONS IMPLICIT TAGS ::=
BEGIN

-- EXPORTS ALL --
```

```
IMPORTS

Attribute
FROM CryptographicMessageSyntax-2010  -- [RFC6268]
      { iso(1) member-body(2) us(840) rsadsi(113549)
        pkcs(1) pkcs-9(9) smime(16) modules(0)
         id-mod-cms-2009(58) }

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


-- CSR Attributes

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

AttrOrOID ::= CHOICE {
   oid        OBJECT IDENTIFIER,
   attribute  Attribute {{AttrSet}} }

AttrSet ATTRIBUTE ::= { AttributesDefinedInRFC7030, ... }


-- Asymmetric Decrypt Key Identifier Attribute

AttributesDefinedInRFC7030 ATTRIBUTE ::= { aa-asymmDecryptKeyID, ... }

aa-asymmDecryptKeyID ATTRIBUTE ::=
    { TYPE AsymmetricDecryptKeyIdentifier
      IDENTIFIED BY id-aa-asymmDecryptKeyID }

id-aa-asymmDecryptKeyID OBJECT IDENTIFIER ::= { iso(1) member-body(2)
    us(840) rsadsi(113549) pkcs(1) pkcs9(9) smime(16) aa(2) 54 }

AsymmetricDecryptKeyIdentifier ::= OCTET STRING

END
```

Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Thomas Werner
Siemens

Email: thomas-werner@siemens.com

Wei Pan
Huawei Technologies

Email: william.panwei@huawei.com

Sean Turner
sn3rd

Email: sean@sn3rd.com