LAMPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 20, 2019

M. Richardson
Sandelman Software Works
T. Werner
Siemens
W. Pan
Huawei Technologies
June 18, 2019

Clarification of Enrollment over Secure Transport (EST): transfer encodings and ASN.1
draft-richardson-lamps-rfc7030est-clarify-02

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

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 December 20, 2019.

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-Transsfer-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.

errata 4384.

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

This document does not require any registrations.

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., Behringer, M., Bjarnason, S., and K. Watsen, "Bootstrapping Remote Secure Key Infrastructures (BRSKI)", draft-ietf-anima-bootstrapping-keyinfra-21 (work in progress), June 2019.

[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>.

[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>.

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>.

[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>.

[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>.

[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>.

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