LAMPS Working Group
Internet-Draft
Intended status: Standards Track
Expires: December 19, 2019

M. Richardson
Sandelman Software Works
T. Werner
Siemens

June 17, 2019

Clarification of Enrollment over Secure Transport (EST): transfer encodings and ASN.1
draft-richardson-lamps-rfc7030est-clarify-00

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 19, 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] 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.

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. This document provides a compromise that moves towards the correct behaviour without breaking existing deployments.

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

2. Terminology

This document uses the term "amended server" to refer to an EST server that complies with the changes in this document. The term "legacy EST server" refers to servers that do not support the changes in this document.

The term "BRSKI EST server" refers to an EST server that also supports the mechanisms described in [I-D.ietf-anima-bootstrapping-keyinfra].

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

[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.

Both section 4.1.3 (CA certificate response), and Section 4.5.2, /csrattrs is a GET operation, and will be dealt with below.

For the other three methods, when the client is aware that this is an amended server then it SHOULD send the POST request in binary form (DER-encoded), and omit the Content-Transfer-Encoding header. How the client knows what kind of server it is dealing with is communicating with is detailed in the next section.

An amended server, when it receives a request that has no Content-Transfer-Encoding header, or has a Content-Transfer-Encoding header with the "binary" attribute, MUST respond in the same binary format.

When an amended server receives a request in CTE-base64 form, then it MAY respond in kind. It is reasonable for a server to be configured to ignore or fail requests of this form, either via run-time configuration, or via a compile-time option. A main reason to do this is to avoid a permutation that requires testing in the future when no legacy EST clients are expected to connect.

4.1. Client configuration

[RFC7030] has some significant deployment. The protocol has no version numbers or other ways to indicate that the format of the operations has changed, and as the protocol is driven by a client state machine, the client has to know whether it has to operate in legacy EST server mode.

In certain market verticals it may be well known to client system designers whether or not this is the case. In those cases, the out-of-band configuration mechanism is appropriate.

Clients that start their process using [I-D.ietf-anima-bootstrapping-keyinfra] SHOULD assume that the server supports this amended specification.

Clients that discover an EST server in an ANIMA ACP via GRASP, using the mechanism detailed in Section 7 SHOULD also assume that these servers support this amended specification.

Other users or extensions for [RFC7030] should specify if clients are to assume this amended specification or not.

4.2. Retrieval of certificate attributes

The 4.5.2 (CSR Attributes, /csrattrs) is a GET operation. It occurs at the beginning of a transaction.

TBD how can the client indicate it is willing to accept an un-encoded response?

The 4.1.3 (CA Certificates Response, /cacerts) is also a GET operation, but it occurs after enrollment. The server SHOULD assume that a client that wanted a binary response also wants a binary response here.

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

errata 4384.

6. Clarification of error messages for certificate enrollment operations

errata 5108.

7. Definition of GRASP discovery for updated EST servers

An ANIMA ACP device can discover the location of the nearest EST server using a [I-D.ietf-anima-grasp-api] M_DISCOVERY mechanism.

objective = ["AN_EST", F_DISC, 255]

EST servers discovered in this way MUST support the amended server mechanism described in this document. The response will include a hostname and port number for a nearby EST server that can be used to renew an ACP credential.

8. Privacy Considerations

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

9. Security Considerations

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

10. IANA Considerations

Allocate the name AN_EST from the [I-D.ietf-anima-grasp-api] "GRASP Objective Names Table".

11. Acknowledgements

This work was supported by the Huawei Technologies.

12. References

12.1. 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.

[I-D.ietf-anima-grasp-api]
Carpenter, B., Liu, B., Wang, W., and X. Gong, "Generic Autonomic Signaling Protocol Application Program Interface (GRASP API)", draft-ietf-anima-grasp-api-03 (work in progress), January 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>.

[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>.

12.2. 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>.

Authors' Addresses

Michael Richardson
Sandelman Software Works

Email: mcr+ietf@sandelman.ca

Thomas Werner
Siemens

Email: thomas.werner@siemens.com