draft-richardson-lamps-rfc7030est-clarify-02

Michael Richardson
mcr+ietf@sandelman.ca

Clarifications to RFC7030: Enrollment over Secure Transport

RFC7030: https://www.rfc-editor.org/info/rfc7030

This document profiles certificate enrollment for clients using Certificate Management over CMS (CMC) messages over a secure transport. This profile, called Enrollment over Secure Transport (EST), describes a simple, yet functional, certificate management protocol targeting Public Key Infrastructure (PKI) clients that need to acquire client certificates and associated Certification Authority (CA) certificates. It also supports client-generated public/private key pairs as well as key pairs generated by the CA.

Has four errata against it. An ASN.1 concern, two issues relating to Base64 encoding of payloads, and a typo.

https://datatracker.ietf.org/doc/draft-ietf-anima-bootstrapping-keyinfra/
Is based upon RFC7030, and the base64 situation has caused confusion during interoperability testing (or BRSKI + EST) in the past 8 months.

EST puts MIME over HTTP

- HTTP is binary-clean, and never requires Base64 encoding!
- RFC includes text like:

Thanks to Sean Turner and Alexey Melnikov For realizing Error!

```
The HTTP content-type of "application/pkcs7-mime" is
used.  The Simple PKI Response is sent with a Content-
Transfer-Encoding of "base64" [RFC2045].
```

- The `Content-Transfer-Encoding` header is MIME, and never belongs in HTTP, and was clearly marked as not belonging in a number of RFCs.
  - In practice, no implementations send it.
  - In practice, all implementations base64 all binary objects in EST!

Can it be fixed?

- It appeared that we could use Content-Transfer-Encoding to signal it was base64, and if not present, then move to binary.
  - There is a challenge figuring out if server supports binary for use in the steps that are HTTP POST. If we could figure this out, then server could assume binary was supported if it received binary.
- BUT, Content-Transfer-Encoding is not sent, so we can not move to binary.

Clarifications

- The “Content-Transfer-Encoding” header field MUST never be sent.
- Any “Content-Transfer-Encoding” header fields present MUST be ignored.
- All content defined in RFC7030 remains base64 encoded.
  - Any new content in derivative protocols (e.g. BRSKI) should be binary.

How to progress this?

- It came from PKIX WG, which is not alive.
- It could be processed in LAMPS.
- Or as AD sponsored.
- Or ??

- My preference is LAMPS, because of errata on ASN.1 coding of CSR, which will require review.