EST Extensions

draft-turner-est-extensions

Sean Turner ~ IETF 97 ~ LAMPS

What is EST?

EST => Enrollment over Secure Transport - RFC 7030

Last RFC published by the venerable PKIX WG

(*cough* PKIX is dead long live LAMPS *cough*)

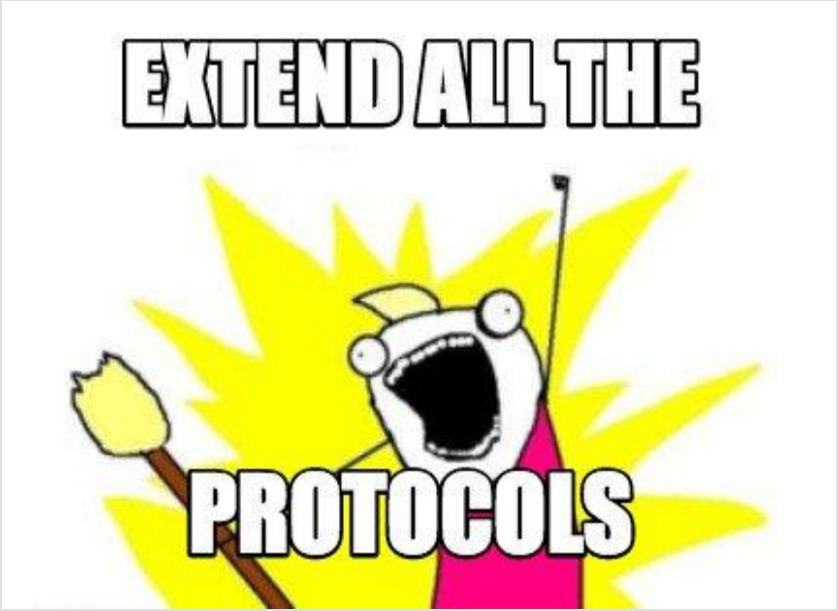
CA certs, PKCS#10/#7s, and CMC over https:

prefix of .well-known/est & path suffix:

/cacerts	/simpleenroll	/simplereenroll
/serverkeygen	/fullCMC	/csrattrs

full e.g.: https://www.example.com/.well-known/est/simpleenroll

What do I want?



Extend /serverkeygen in 3 ways:

1. Encapsulating returned asymmetric keys in additional CMS content types:
    - Was 1) naked (relies on TLS), 2) encrypted data, or 3) enveloped data
    - Want to add encrypted key package (RFC 6032)
2. Returning asymmetric key package receipts and errors (RFC 7191) with POSTs, i.e., add /serverkeygen/return
3. Returning server-generated public key pairs encapsulated in PKCS#12 (RFC 7292).

What new services?

Locate available packages: /pal

Distribute EE certificates: /eecerts

Distribute CRLs & ARL: /crls

Distribute symmetric keys (RFC 6031): /symmetrickeys

Distribute firmware (RFC 4108): /firmware

Distribute TAMP (RFC 5934): /tamp

Return receipts & errors with POSTs:

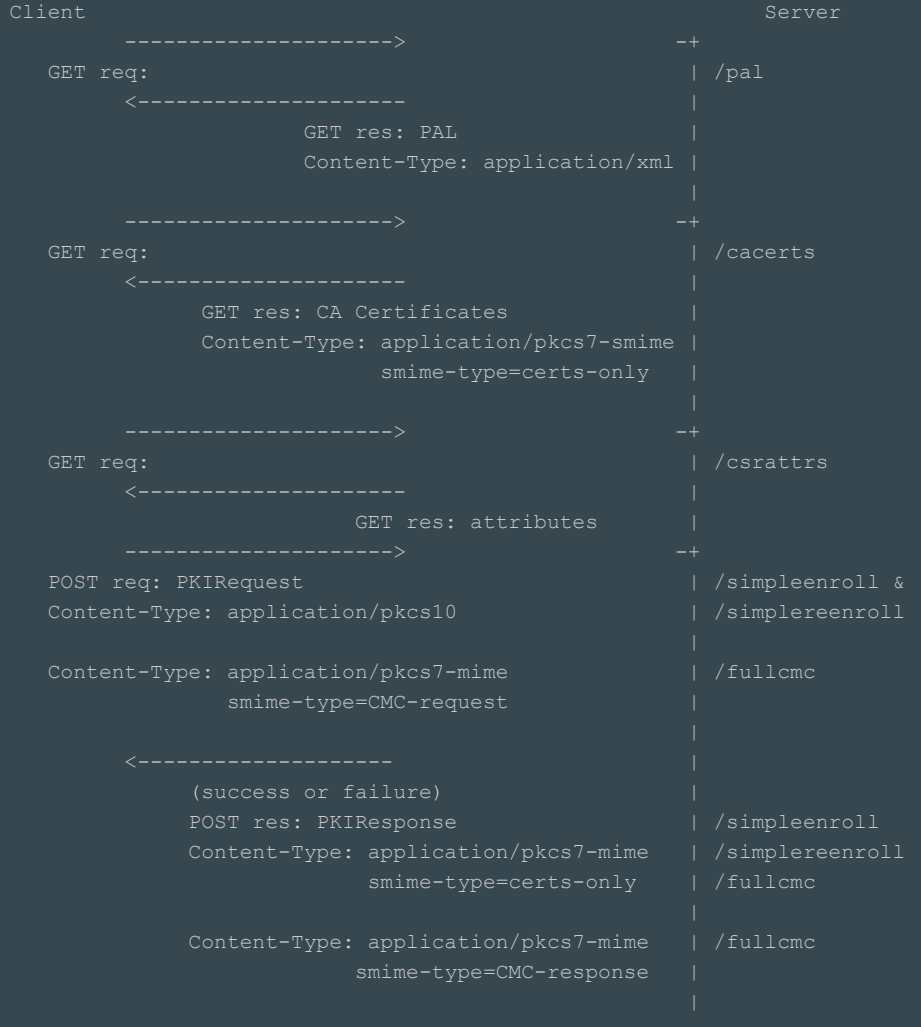
- Sym Keys: /symmetrickeys/return
- Firmware: /firmware/return
- TAMP: /tamp/return

Backup

PAL

```
<pal>
  <message>
    <type>from IANA registry</type>
    <date>YYYY-MM-DDTHH:MM:SSZ</date>
    <size>bytes</size>
    <info>DN, SKI ,URI, or I&SN</info>
  </message>
  <message>
   ...
  </message>
</pal>
```

Package #	Package Description
0000:	Reserved
0001:	Additional PAL value present
0002:	X.509 CA certificate
0003:	X.509 EE certificate
0004:	X.509 ARL
0005:	X.509 CRL
0006:	Start DS certificate enrollment with CSR attribute
0007:	Start DS certificate enrollment
0008:	DS certificate enrollment (success)
0009:	DS certificate enrollment (failure)
0010:	Start DS certificate re-enrollment
0011:	DS certificate re-enrollment (success)
0012:	DS certificate re-enrollment (failure)
...	


Client
Server
GET req:
/pal
GET res: PAL
Content-Type: application/xml
GET req:
/cacerts
GET res: CA Certificates
Content-Type: application/pkcs7-smime
smime-type=certs-only
GET req:
/csrattrs
GET res: attributes
POST req: PKIRequest
Content-Type: application/pkcs10
/simpleenroll &
/simplereenroll
Content-Type: application/pkcs7-mime
smime-type=CMC-request
/fullcmc
(success or failure)
POST res: PKIResponse
/simpleenroll
Content-Type: application/pkcs7-mime
smime-type=certs-only
/simplereenroll
/fullcmc
Content-Type: application/pkcs7-mime
smime-type=CMC-response
/fullcmc


Client
Server
GET req:
/firmware
/tamp
/symmetrickeys
GET res: Firmware, TAMP Query
+ Updates, Symmetric Keys
Content-Type: application/cms
POST res: Firmware Receipts or Errors,
TAMP Response or Confirms or Errors,
Symmetric Key Receipts or Errors,
/firmware/return
/tamp/return
/symmetrickeys/
return
Content-Type: application/cms
POST res: empty
(success or failure)
GET req:
/eecerts
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only