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 ALL THE PROTOCOLS
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>
  <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>
  ...
</pal>

<table>
<thead>
<tr>
<th>Package #</th>
<th>Package Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>0000:</td>
<td>Reserved</td>
</tr>
<tr>
<td>0001:</td>
<td>Additional PAL value present</td>
</tr>
<tr>
<td>0002:</td>
<td>X.509 CA certificate</td>
</tr>
<tr>
<td>0003:</td>
<td>X.509 EE certificate</td>
</tr>
<tr>
<td>0004:</td>
<td>X.509 ARL</td>
</tr>
<tr>
<td>0005:</td>
<td>X.509 CRL</td>
</tr>
<tr>
<td>0006:</td>
<td>Start DS certificate enrollment with CSR attribute</td>
</tr>
<tr>
<td>0007:</td>
<td>Start DS certificate enrollment</td>
</tr>
<tr>
<td>0008:</td>
<td>DS certificate enrollment (success)</td>
</tr>
<tr>
<td>0009:</td>
<td>DS certificate enrollment (failure)</td>
</tr>
<tr>
<td>0010:</td>
<td>Start DS certificate re-enrollment</td>
</tr>
<tr>
<td>0011:</td>
<td>DS certificate re-enrollment (success)</td>
</tr>
<tr>
<td>0012:</td>
<td>DS certificate re-enrollment (failure)</td>
</tr>
<tr>
<td></td>
<td>...</td>
</tr>
</tbody>
</table>
Client -> Server
GET req: /firmware

Server <-+ Client
GET res: Firmware, TAMP Query + Updates, Symmetric Keys
Content-Type: application/cms

Client -> Server
GET req: /tamp

Server <-+ Client
GET res: Firmware Receipts or Errors, TAMP Response or Confirms or Errors, Symmetric Key Receipts or Errors,
Content-Type: application/cms

Client -> Server
GET req: /symmetrickeys

Server <-+ Client
POST res: empty (success or failure)

Client -> Server
GET req: /eecerts

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /pal

Server <-+ Client
GET res: PAL
Content-Type: application/xml

Client -> Server
GET req: /cacerts

Server <-+ Client
GET res: CA Certificates
Content-Type: application/pkcs7-smime
smime-type=certs-only

Client -> Server
GET req: /csrattrs

Server <-+ Client
GET res: attributes

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
GET req: /fullcmc

Server <-+ Client
GET res: Other EE certificates
Content-Type: application/pkcs7-mime
smime-type=certs-only

Client -> Server
POST req: PKIRequest

Server <-+ Client
POST res: PKIResponse
Content-Type: application/pkcs7-mime
smime-type=certs-only