draft-ietf-est-02

Touching on open issues
Continued review & comments appreciated!
v.1

-02 posted

- Please read it
- At least one thread:
  - [pkix] I-D Action: draft-ietf-pkix-est-02.txt

- Feel free to start one if you have questions

/serverKeyGen

- Section 4.6
- For BGPsec RPKI the server provides the key and certificate

- The current text exposes the server generated key to the EST server

Alternative response formats solicited

What about “pkix-cmc-serverkeygeneration”

/CSRAttrs

- Section 4.7
- Informs client of attributes that should be in the request

  macAddress

  Pseudonym

  friendlyName
- Is the format of this response good?

  application/csrattrs

```
csrattrs ::= SEQUENCE SIZE (0..MAX) OF OBJECT IDENTIFIER { }
```

  -or-

  application/pkcs10

Operational Scenario Overviews

- Section 2

To be:

(informative)

Authentication

- Section 3.3.1.1

  Reviews indicate a need for clarification

- Mutual authentication MUST occur prior to enrollment
  - Server is authenticated: set SERVER_AUTH_FLAG
  - Client is authenticated: set CLIENT_AUTH_FLAG

Flag setting

- **Authenticate Server w/ Certificate in TLS layer**
  RFC2818 (HTTP over TLS) Section 3.1w/ a Web TA
  EST specific trust anchor w/ id-kp-cmcRA
  SERVER_AUTH_FLAG
- **Authenticates client w/ Certificate in TLS layer**
  CLIENT_AUTH_FLAG
- **Authenticates client in HTTP layer**
  CLIENT_AUTH_FLAG
- **Cipher suite performing mutual authentication using a shared credential (e.g. PWD, PSK)**
  SERVER_AUTH_FLAG, CLIENT_AUTH_FLAG

Fallback: Distribution of CA certs

- Client MAY request /CAcerts even if SERVER_AUTH_FLAG fails

“but the HTTP content data MUST be accepted manually as described in Section 4.3”

Pinning EST server cert (chain)

- Current draft: Client requests /CAcerts

  Authenticates all subsequent connections to ESTserver using this as an EST specific TA

  – Precludes web CA (alternate) trust anchors for EST server

  or

  – Mandates use of RFC6066 s6 “Trusted CA Indication”.

- Alternative approach:

  /ESTCAcerts

  But this increases certs on client and adds further confusion

Client Security Considerations

- Web TA w/ RFC2818 (HTTP over TLS) s3.1

  All the normal concerns about state of web CA servers

  But a very useful bootstrap.

  RFC6066 s6 “Trusted CA Indication” allows client to use this once and then improve security…

- EST specific trust anchor w/ id-kp-cmcRA

  Prevents a rogue EE from impersonating an EST server and act as a man-in-the middle by downgrading to HTTP authentication methods

“Linking identity Required” error code

- S
- [[EDNOTE: A specific error code (TBD) is returned indicating this additional linkage might be useful. This would be similar to the "WWW-Authenticate response-header" control message. Alternatively simply rejecting the request with an informative text message would work in many use cases.]]

Discussion

- ?

END