draft-ietf-est-03

Touching on open issues

Continued review & comments appreciated!

-03 posted

- Addresses all received -02 comments
- Please read it (only one set of comments received so far – thank you, Steve)
- At least two threads:
  - [pkix] I-D Action: draft-ietf-pkix-est-03.txt
  - [pkix] my comments and edits for EST 03

- Feel free to start another one if you have your own questions and issues

Major Changes in -03

- New explanatory text throughout introductory paragraphs in each section or as appropriate.
- Tried to clarify the intent of the document where previous comments indicated confusing text.
- Added support for “certificate-less” cipher suites in TLS.

Explanatory Text

- Substantially enhanced Section 2 (Operational Scenarios Overview)
- Expanded Figure 3 (list of certificates and their corresponding uses)

Protocol Details

- More detailed explanations for
  - CA certificates distribution (including bootstrap requests)
  - Client certificate requests
  - Server-side key generation requests and responses

Security Considerations

- Wholesale new text here (finally):
  - Downsides to use of HTTP authentication
  - 3rd party TA cautionary measures
  - Certificate-less TLS cipher suite secret protection
  - Certificate-less TLS cipher suite dictionary attack resistance

Appendices

- Added CSR attributes example
- Removed informative appendices on server discovery, external TLS concentrator, and CGI server implementation

Looking Forward

- -04 draft already underway based on Steve Kent's comments
  - New terminology list – simplifies remainder of document by defining otherwise verbose terms
  - Separated certificate and trust anchor lists into separate tables
    - Better differentiation of local and 3rd party TAs
  - Tighter/more consistent RFC 2119 language
    - Particularly important for TLS channel binding
  - Next draft expected by November 26th

Discussion

- Thoughts?
- Slings/arrows?

END