Suite B CMC Profile

http://tools.ietf.org/html/draft-turner-suiteb-cmc-00

IETF 77
Monday, March 22, 2010
Afternoon Session II 1520-1720

Sean Turner
Michael Peck

Summary

- Informational ID
- Requires:
  - Suite B algorithms and curves
  - SignedData as profiled by
    RFC 5008: Suite B S/MIME
  - Template fields set in accordance with
    RFC 5758: Suite B certificate and CRL profile
- Client generated keys

Notables

- Uses Full PKI Requests/Responses
  - CMC Controls: Transaction IDs and Nonces
  - Suite B means use Identity Proof v2 and POP Link Witness V2
- Client's choice to support PKCS#10 or CRMF
- Permits one time use of key establishment key to generate signature for POP. SignedData wrapping request must be signed by signature key.

New Stuff

- Created EKU: id-cmcCA
- Currently CMC requires that the name in the request matches the name in the certificate used to sign the request.
- Want to support client supplied name change in rekeys.
  - Real world scenarios
    - You get married and your name changes. You know what your name is changing to.
    - Devices come already provisioned with certificates.
  - Add SigningCertificateV2 as a control to link the old name to the new name.

Next Steps

- Respond to comments
- Ask for more feedback