Traceable Anonymous Certificates Version 03 Revisions

- David A. Cooper provided extensive comments on the 02 version of the TAC internet draft
- This presentation reviews the changes made in response to David's comments
- For details see
  - SangHwan Park's message of 3/5
  - Stephen Kent's message of 2/18
- 03 version of the I-D will be posted soon. If there is no more list traffic on this I-D, I suggest to proceed WGLC

Major Changes from 02 version

- ❑ Make the Token a CMS ContentInfo object
  - □ Use 'ContentInfo' wrapper to hold the 'Token' instead of using the SignedData CMS construct in a nested fashion
- ❑ Make the ContentType of each message distinct
  - □ Specify a distinct contentType(OID) for each message (Token, TokenandBlindHash,TokenandPartiallySignedCertificateHash)
- ❑ Clarify that the AI uses CRLs (or OCSP) to provide revocation status info to relying parties for TACs
  - □ SCVP is not a viable alternative to OCSP here because it offers a <u>locally managed</u> certificate status verification function

Major Changes from 02 version

- Clarify the Certificate Request formats
  - Subject field MUST be present
  - Delete the optional attribute fields of PKCS#10 and CMC
- Fix inconsistencies
  - Re-submitted Certificate Requests are checked for freshness and duplicates are detected in Step 4 and 6
  - Fix citation errors
- Remove references to DSA-based split signing protocol
  - DSA-based approaches work but require some changes to the protocols between AI and BI
  - DSA support will be incorporated in next version of TAC.

Responses

- Term ‘pseudonymous’ is more appropriate than ‘anonymous’ ?
  - While it is true that a TAC contains a pseudonym as a Subject name, the informal meaning of anonymous and the qualifier “traceable” used in this context makes sense
- Differences from ‘An architecture of Pseudonymous e-commerce’ submitted as paper in 2001
  - The paper just focused on the pseudonymous usage of certificate, not anonymity in the issuance process
  - I-D provides anonymity not only in the issuance processes but also in certificate transactions between AI and BI

Responses

- Reference to DSA based blind signature ?
  - The paper Chapter 4.2 below, in of 2001 Crypto

    http://www.ecc.cmu.edu/~reiter/papers/2001/crypto.pdf
- Threshold based split signing helps in TAC?
  - Use of this technology makes it easier for a system evaluator or auditor to verify that anonymity is preserved in the certificate issuance management processes