Traceable Anonymous Certificate

draft-ietf-pkix-tac-01.txt

IETF-72 at PKIX WG

Park, SangHwan shpark@kisa.or.kr
Stephen Kent kent@bbn.com

KISA Korea Information Security Agency

Overview

- **I-D defines a practical architecture and protocols for offering privacy in X.509 certificate issuance and usages**
  - Architecture separates certificate issuer authorities to secure privacy in X.509 cert issuance and usages
    - One for verifying ownership of private key (Blind Issuer, BI)
    - The other for validating the content of certificate (Anonymous Issuer, AI)
- **The EE certificate issued under this model is called 'Traceable Anonymous Certificate' (TAC)**
- **Intended status : Experimental**

Changes from draft-ietf-pkix-tac-00

- **Added time-out to Token**
  - AI and BI can reject session-level replay attacks and to facilitate garbage collection of AI and BI database
- **Revised Security Consideration Section**
  - It also may be possible to determine the identity of a user via information carried by lower level protocols, or by other, application-specific means. For example IP address or internet browser cache information
- **Changed I-D status ‘Informational’ to ‘Experimental’**

Feature

- **Compatible with Std. X.509 Format**

  ※ Subject Name is pseudonym

- **Compatible with Std. CRMF & PKCS10 Cert Req. Format**

- **Use of Threshold Signature and Blind Signature**

  ※ certificate contents ONLY visible to AI and blind to BI

- **CP/CPS on CA's TAC services**

TAC Issuance (Verifying User's real ID)

User(U)

① U presents his/her Real ID to BI

② BI verifies U's real ID

③ BI create a random Token

※ Token serves two functions; one for verifying whether U be registered or not and the other for later tracing back to U's real ID

③ BI sends a Token to U

※ Token is a random value digitally signed by BI and it is protected with time-out session against replay attacks

Blind Issuer(BI)

KISA Korea Information Security Agency

TAC Issuance (Issue TAC)

User(U)

④ U creates CertReq and sends it to AI

※ Token is carried as attribute in CertRequest Info(PKCS10 or CRMF)

⑤ AI constructs TAC tbsCertificate and blinds the hash of it with its public key

⑥ AI sends blinded hash to BI

⑦ BI signs blinded hash with his partial private key and send it back to AI

⑧ AI un-blinds it with its private key and signs on BI's sign to complete TAC

⑨ AI sends TAC to U

Anonymous Issuer(AI)

KISA Korea Information Security Agency

Mapping TAC to User's real ID

Relying Party (RP)

① RP presents AI the TAC

② AI sends back Token to RP

③ RP sends Token to BI

④ BI sends User ID back to RP

Neither AI nor BI can trace User real ID alone.
(BI Never know of TAC content,
AI Never know of user ID)

Anonymous Issuer(AI)

<DB>
TAC, Token

Blind Issuer(BI)

<DB>
ID, Token

Q & A

- **Any Comments will be welcomed**
- **Thanks for your attention!**