Traceable Anonymous Certificate Protocol

2008. 3. 10

Park, SangHwan(shpark@kisa.or.kr)
Korea Information Security Agency

Backgrounds

- **Today : Internet era**
  - Privacy infringement
    - Ex. SSN, personal profile, trace of transactions
  - Untraceable pseudonym
    - Abuse is another big problem
- **Tomorrow : Ubiquitous computing era**
  - More severe privacy infringement

Backgrounds : PKI

- **Public Key Infrastructure (PKI)**
  - plays an important role in asserting the ownership of public keys
  - Widely deployed in the internet era
- **But, disclose the information about its owner in an authentic manner**

Why simple methods can not work ?

- **If CA issues an X.509 cert with pseudonym**
  - Untraceable
- **If CA issues it but with verifying a real identity**
  - CA can anytime link a pseudonym and a real name
  - CA may be called a big brother
- **If CA issues it but with blind signature**
  - CA can not verify the contents of certificate
  - Maybe untraceable

Our idea

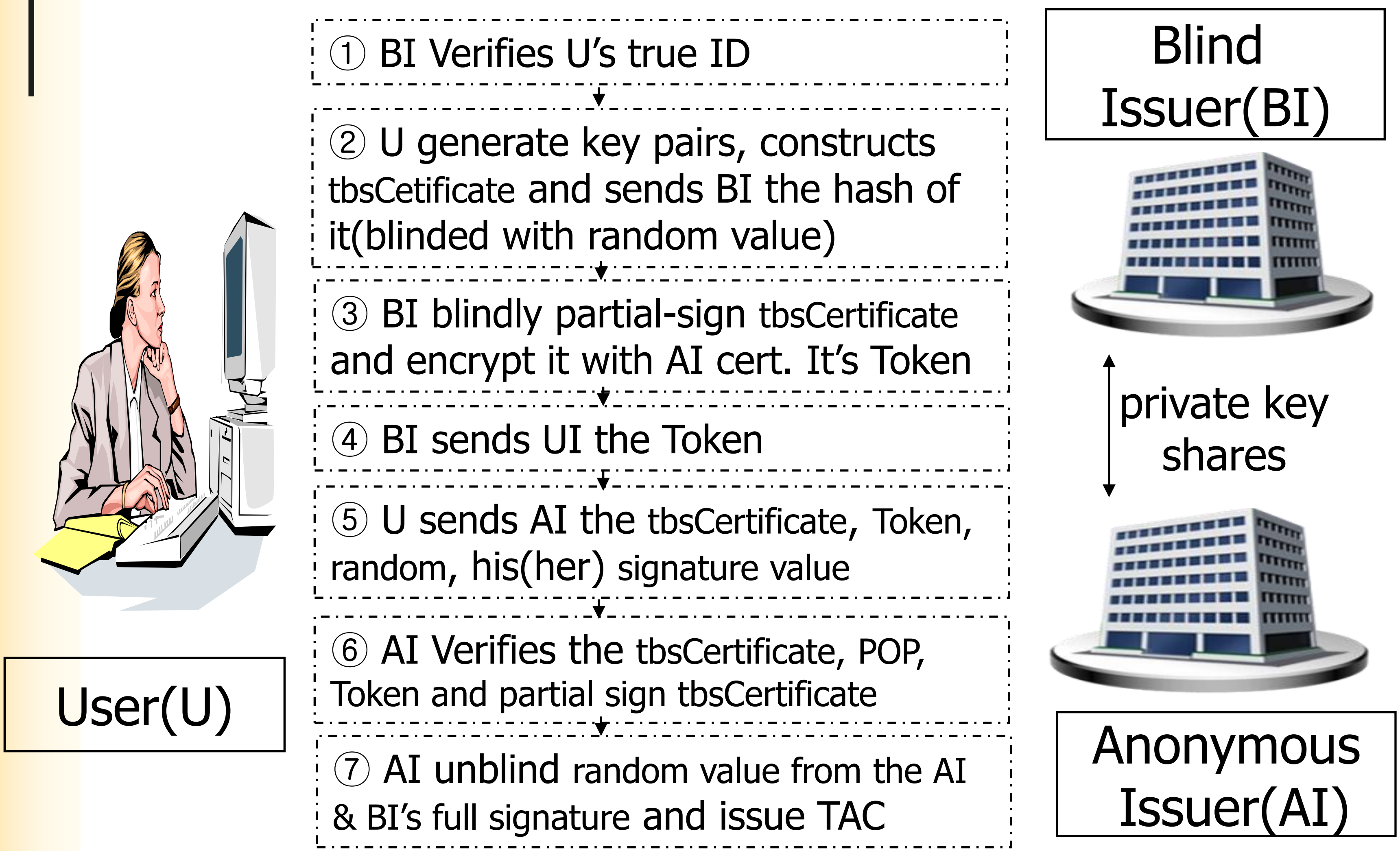
- **Divide issuer more cleverly**
  - 2 CAs(AI & BI) issue cert together, based on threshold scheme
- **Anonymous Issuer (AI)**
  - Verify the contents of pseudonym certificate
  - Can not verify the real identity of user
- **Blind Issuer (BI)**
  - Verify the real identity of user
  - Can not verity the contents of pseudonym certificate

Traceable Anonymous Certificate

- **Profile conform to X.509 cert(RFC3280bis)**
  - One different thing is that Subject Name is set to Pseudonym name

Field	Value
Version	**V3**
Serial Number	**SN(randomly generated)**
Signature Algorithm	**RSA/DSA**
Issuer Name	**AI**
Validity Period	**1yr.(depends)**
Subject Name	**Pseudonym name**
Subject Public Key Info.	**Public key**
Extensions	**Extensions**

Traceable Anonymous Certificate Issuance



① BI Verifies U's true ID

② U generate key pairs, constructs tbsCetificate and sends BI the hash of it(blinded with random value)

③ BI blindly partial-sign tbsCertificate and encrypt it with AI cert. It's Token

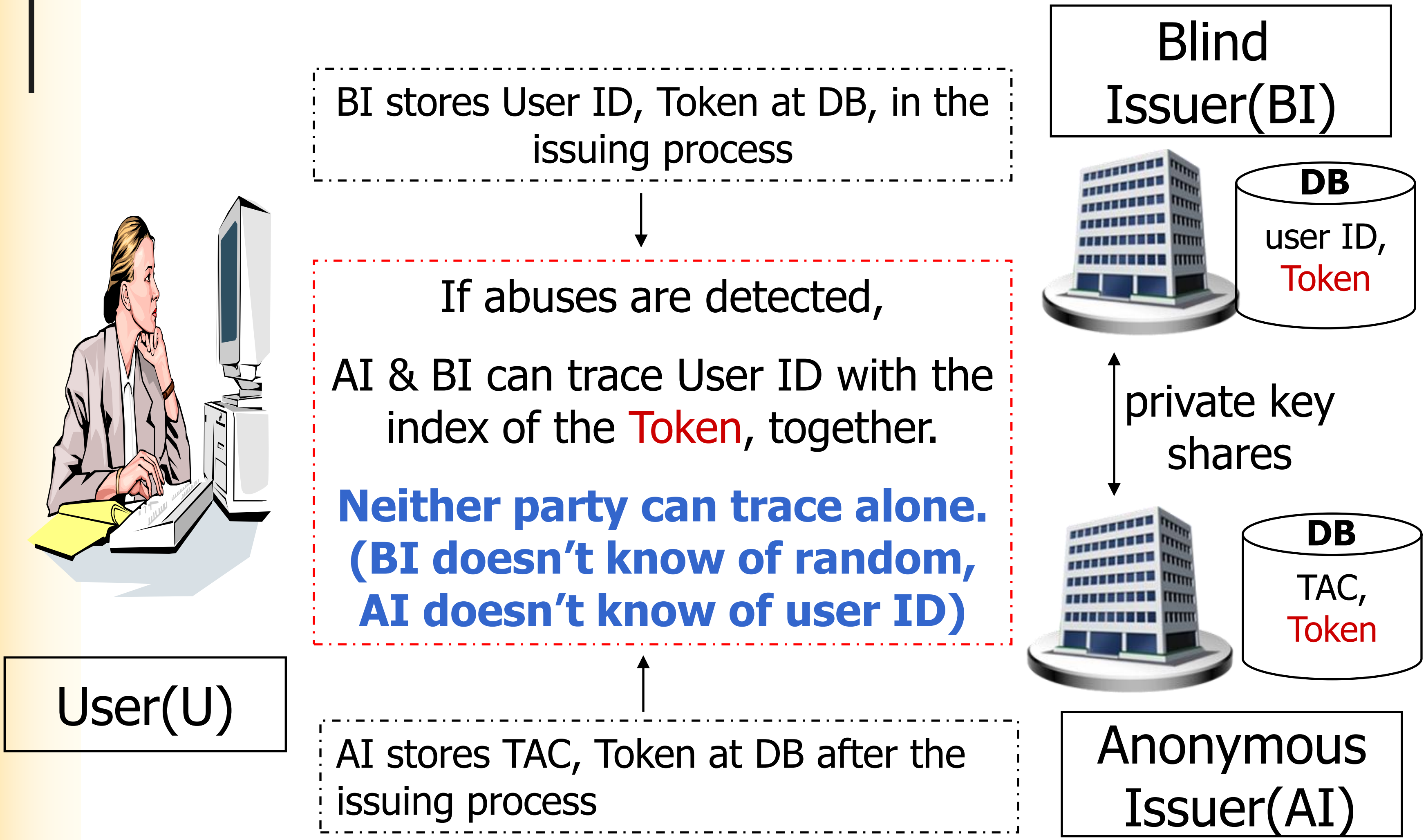
④ BI sends UI the Token

⑤ U sends AI the tbsCertificate, Token, random, his(her) signature value

⑥ AI Verifies the tbsCertificate, POP, Token and partial sign tbsCertificate

⑦ AI unblind random value from the AI & BI's full signature and issue TAC

Mapping TAC to User’s real ID



Blind Issuer(BI)

DB

user ID, Token

BI stores User ID, Token at DB, in the issuing process

If abuses are detected,

AI & BI can trace User ID with the index of the Token, together.

Neither party can trace alone. (BI doesn’t know of random, AI doesn’t know of user ID)

private key shares

User(U)

AI stores TAC, Token at DB after the issuing process

DB

TAC, Token

Anonymous Issuer(AI)

IETF Draft

- **Intended status : Informational**

  ※ Draft will be submitted soon

- **Draft**
  - draft-ietf-park-tacp-00
  - Develop the traceable Anonymous Certificate issuance procedures
  - Develop the Mapping a TAC to a User’s true identity procedures
  - Define the ASN.1 syntax passing between User, BI and AI

Q & A

- **Thanks for your attention!**
- **Looking for co-author, who is interested in our idea.**