

**Group Signatures
with Selective Disclosure
for Privacy Enhanced ID management**

NEC Central Research Labs

Kazue Sako

Jun Furukawa

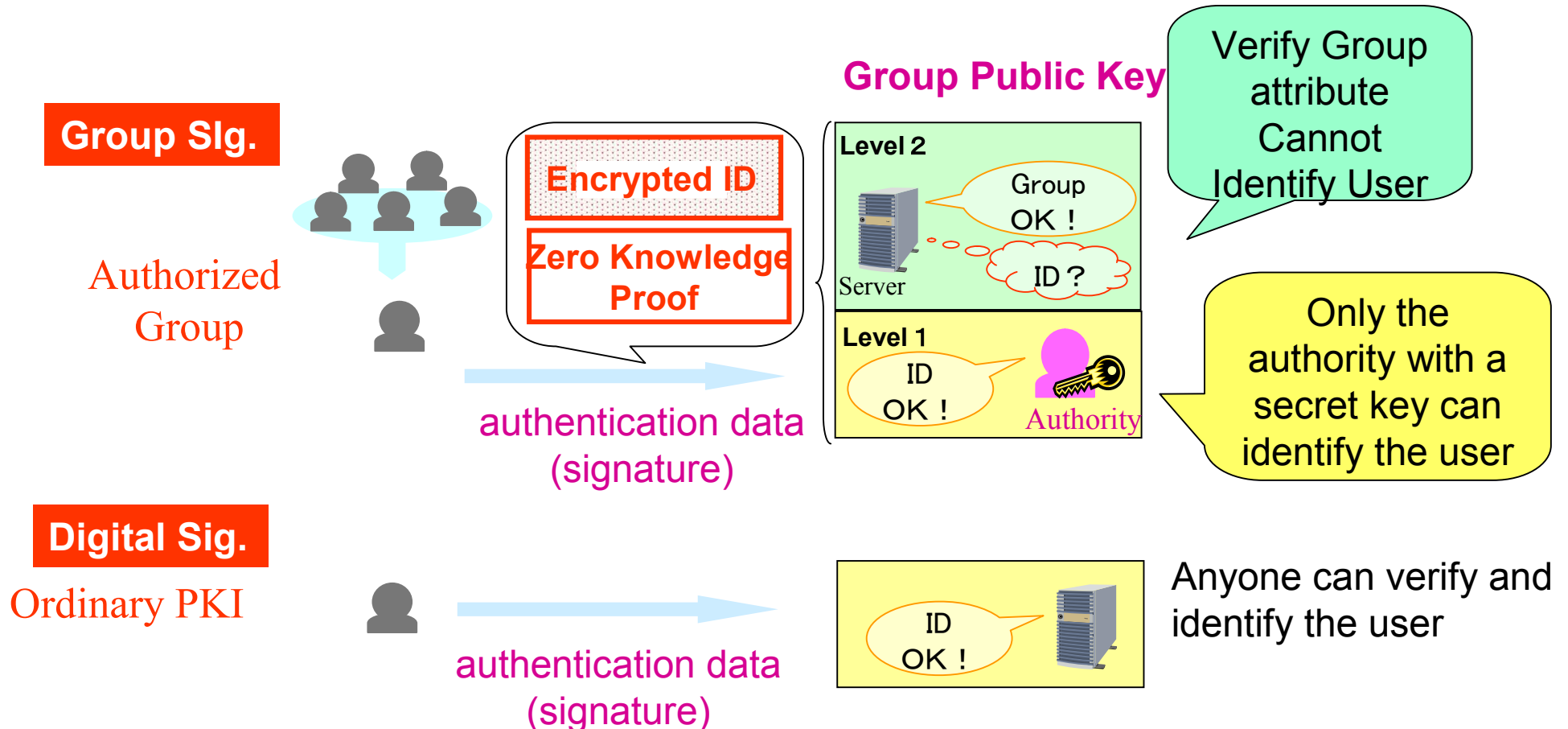
k-sako@ab.jp.nec.com

Self Introduction

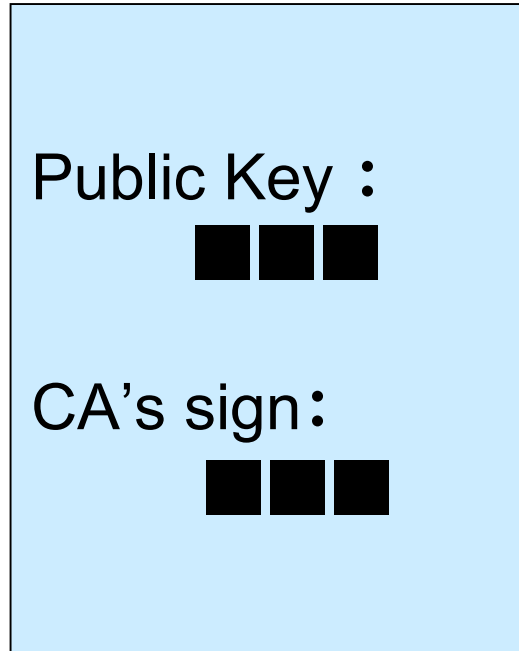
- **Been to many crypto conferences like Crypto, Eurocrypt, FinancialCrypto,... first time to IDTrust**
 - **Worked on implementing remote voting based on MIX-nets, which have been used in a private organization with 20,000 voters for nearly 5 years.**
 - **My belief: Crypto should help build a better system and serve for the future society**
 - **Started discussing the use of Group Signatures at ISO/IEC JTC1 SC27 WG5**
- ...A little discouraged by bad reputation on PKI

Group Signatures

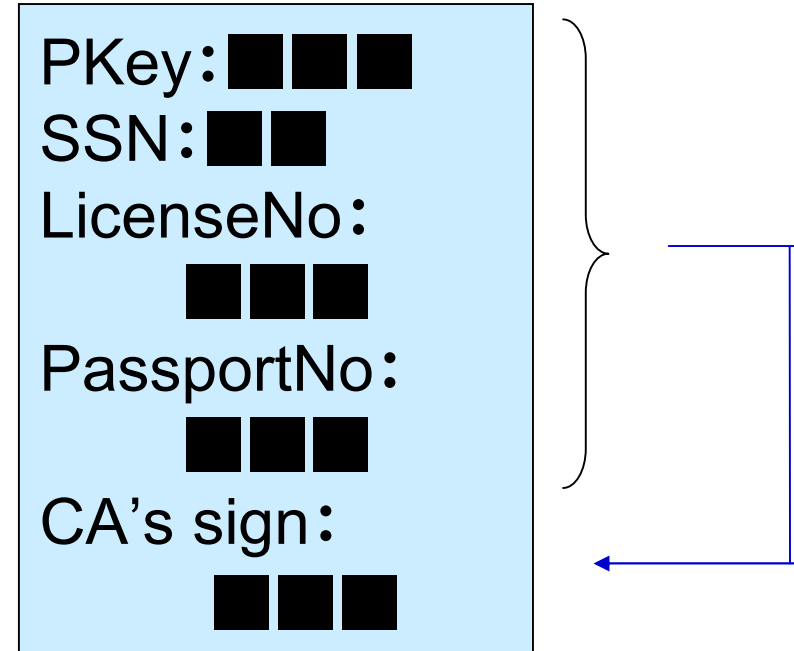
- Generating a single authentication data which provides two levels of verification



Group Signatures



Selective Disclosure Extension



I have a secret key to a public key signed by the CA

My LicenseNo is 12345

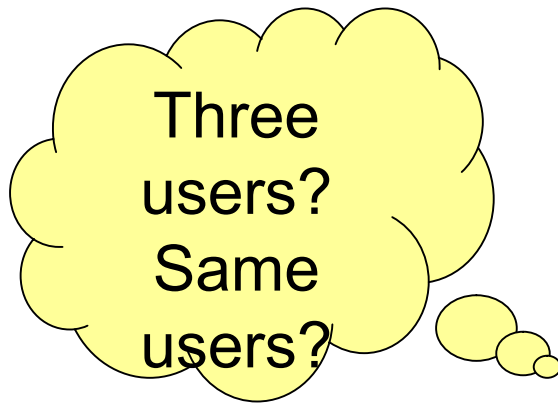
I have a secret key to a valid certificate with Licence No 12345

Merit of Extended Group Signature Scheme

Pkey: ■■■■
SSN: ■■
LicenseID:
12345
PassPortNo:
■■■■
CAsig: ■■■■

Pkey: ■■■■
SSN: 67689
LicenseID:
■■■■
PassportNo:
■■■■
CAsig: ■■■■

Pkey: ■■■■
SSN: ■■
LicenseID:
■■■■
PassportNo:
39305
CAsig: ■■■■



One Signed
Certificate
for each
User

Empowered by Innovation

NEC