

PKI - current and future

Workshop for Japan Germany Information security

Yuichi Suzuki

yuich-suzuki@secom.co.jp

SECOM IS Laboratory

Current Status of PKI in Japan

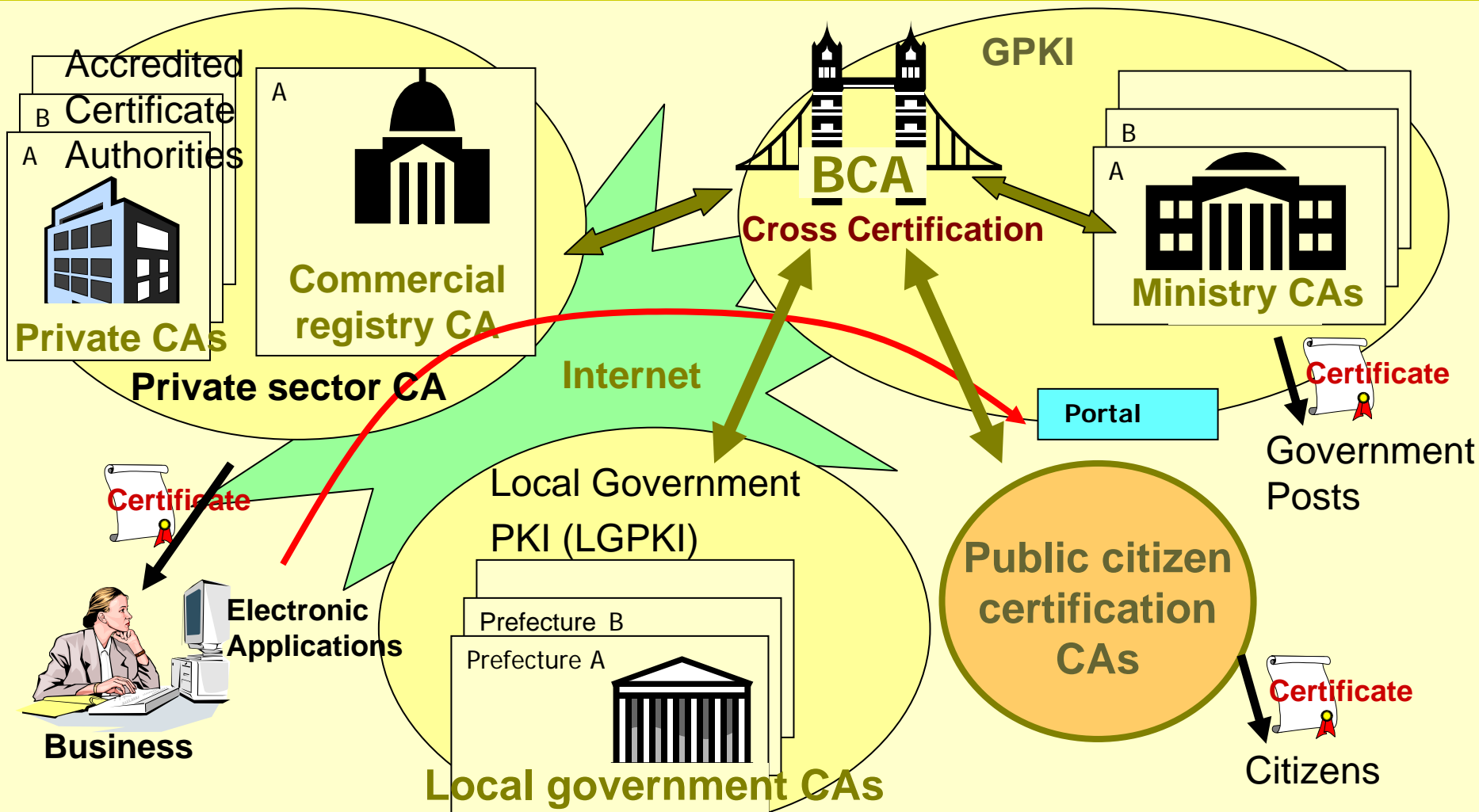
Government PKI

- Government PKI
 - Bridge CA structure
 - All ministry's CAs are cross certified through BCA
 - Private CAs are also cross certified through BCA for private sector business
 - The private CAs must be accredited by electronic signature law
 - Purpose of GPKI
 - B to G, C to G electronic applications with electronic signature for e-Government
 - Electronic bidding
 - Not for enterprise security

Public citizen certification services

- Certificate for citizens issued by local government
 - Started from Jan 2004
 - Linked to the resident register
 - All prefectures have own CA
 - Basic four information on certificate for a resident
 - Name, address, date of birth, sex distinction
 - Certificates and private key in a smart card
- Purpose of citizen certificates
 - C to G (central and local government) electronic applications
 - ex. Tax application, passport issuance, ...
 - Electronic signature on application documents

Government PKI in Japan



Current PKI applications

- Popular PKI applications
 - Web server and client authentication using SSL/TLS
 - VPN for remote access
 - S/MIME for secure e-mail?
- Not so popular
 - Electronic signatures for natural persons in business area
 - e-commerce, e-finance, ...
 - Document encryptions

Standards for PKI

- Basic PKI standards have become matured
- Based on ISO/ITU-T X.509 public key certificate
- IETF PKIX, S/MIME, TLS standards
 - Certificate and CRL profile
 - CP/CPS framework
 - Time stamping
 - S/MIME, CMS
 - TLS ...
- W3C recommendation
 - XML e-signature and encryption
 - XKMS key management
- OASIS Web services security
- ETSI long term signatures

Electronic Signature law

- Japanese electronic signature law
 - effective from 2001
 - Technical neutrality
 - Two mandatory features of electronic signature
 - Identity Authentication
 - Detect alternation
 - Only person who have a secret can sign
 - Accreditation conditions for CA services
 - Certificates issuance for verification of signature
 - Terms for designated examination authority for accredited CA services

e-Document law

- Strong requirements exist to eliminate paper documents and written signature documents
- e-Documents law: Japanese government is preparing
 - Scan paper documents to make e-documents
 - Ex. Tax application, Health Records, ...
 - The e-documents could be original, Ok to destroy the original papers
 - To keep the integrity of scanned data
 - Only the trusted document officers can scan the paper documents
 - He/her must sign digitally on the scanned documents
 - Digital time stamp also required
 - The law will take effect next April
 - Requirement for long term signature validation?

Electronic Signature

- Why electronic signature does not so popularize?
 - High cost for strict certification
 - Difficult to verify signature
 - Lack of killer applications
 - Does not support long term signature verification
 - Influence of US federal electronic signature law?
 - Does not mandate PKI

Time Stamping

- Electronic signature supports
 - **Who** had signed
 - **What** was the target
 - Claimed signing time could not trust
- Time stamping supports
 - **When** the signature was generated
- PKI based Time stamp (RFC 3161)
 - Bind document hash and trusted time by electronic signature of TSA – support contents integrity and creation time
 - Time stamp token has fixed life time
 - It will be desired to use strong key and long validity time

PKI in the future

Will become PKI as real infrastructure?

- To spread PKI
 - Lower cost of certificate
 - Easy to use
 - Legislation support
 - Killer applications
 - These are chicken and egg problem
- More technical support might be needed
 - Long term signature stability
 - e-Authentication and Web service security
 - Combine PKI and PMI
 - Easy verification environment
 - XKMS (X-KISS)
 - Stable cryptographic algorithm
 - Computational to Information theory

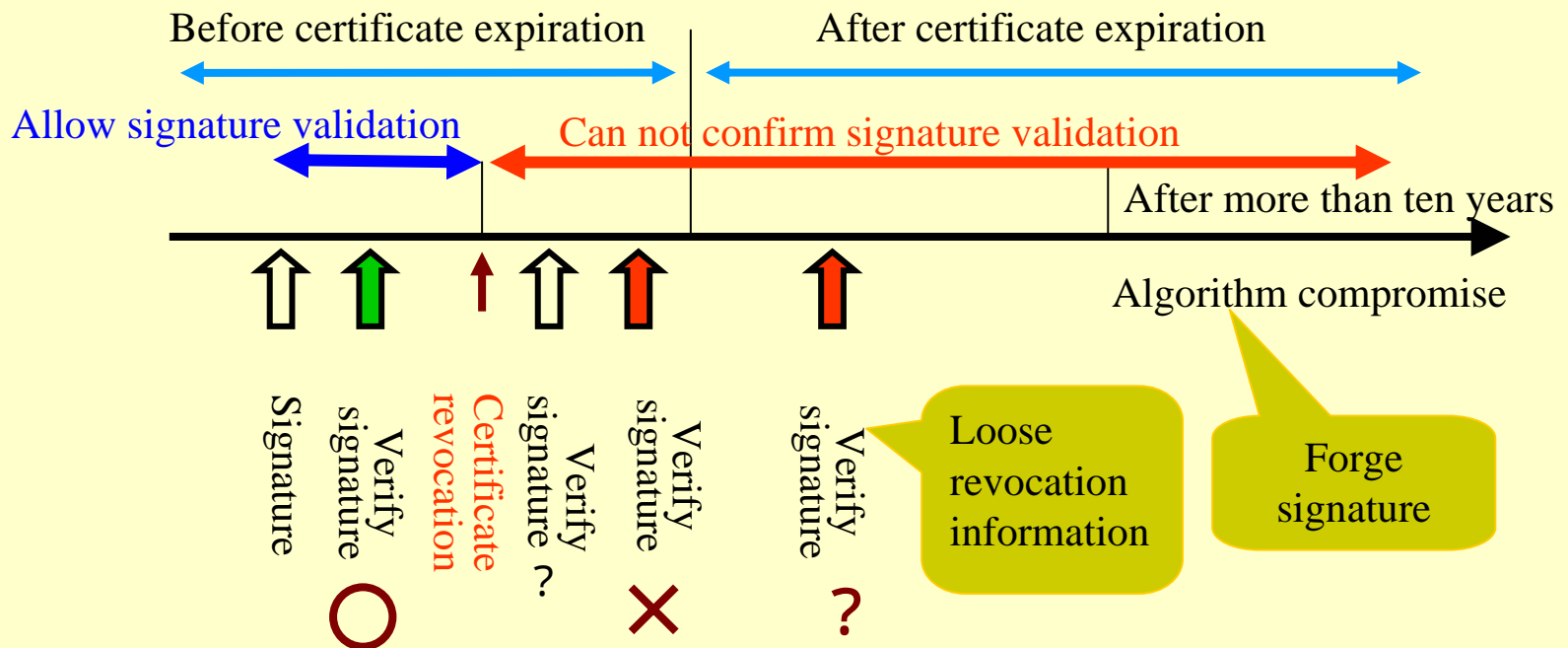
Long term signature

Problem of short certificate validity period

- PKI does work well within certificate validity period
- However, after expiration of certificate
 - No more secure the public key, even if the key does not compromise
 - Should not use the key for verifying the signature
 - Then, digital signature can not verify
- Too short the validity period
 - Usually the period is **one to three** years
 - Many legislations require to keep signature documents over 5 years, 10 years, or more than 30 years

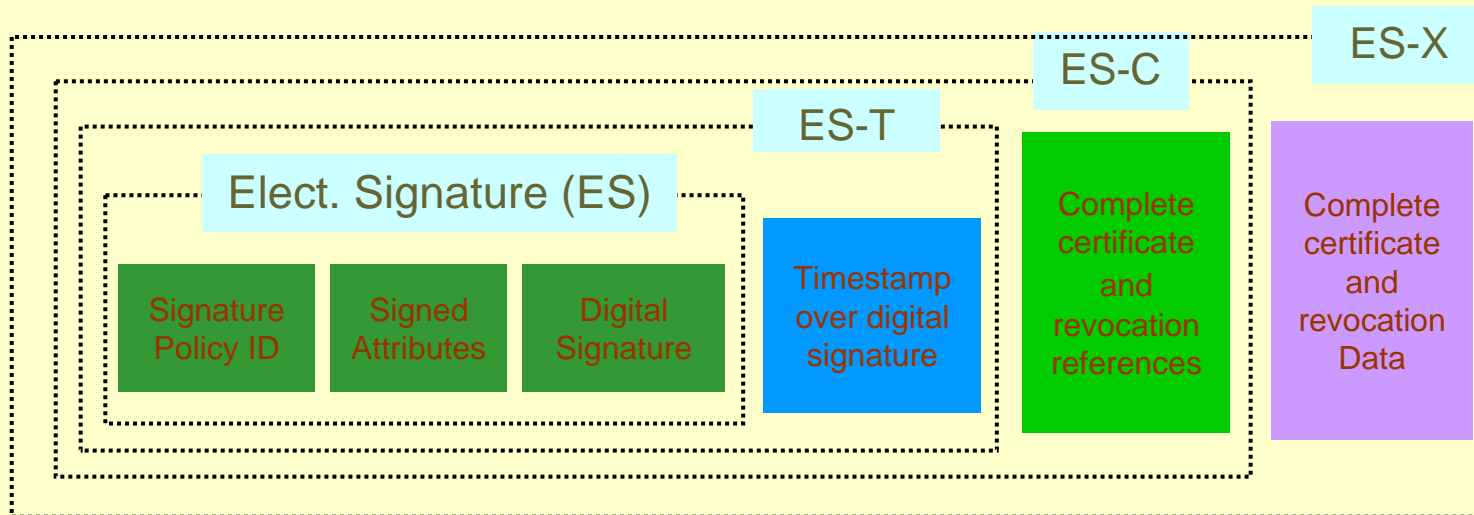
Signature verification

- Usual PKI environment
 - We can not verify the signature after revocation or expiration of the certificate



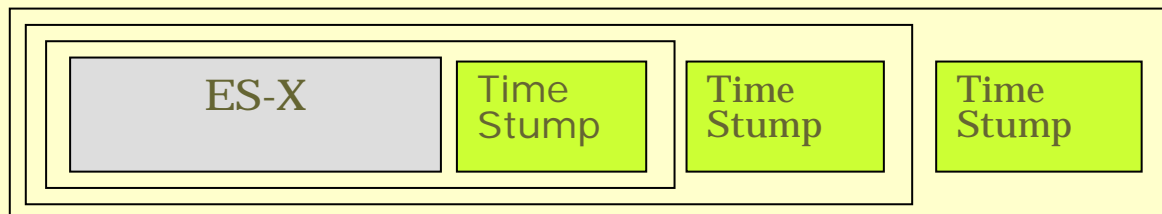
Standard format for long term signature

- Collect all evidences for verification in signature format
 - At the first signature verification
 - Fix signing time – Time stamp on signature value
 - Collect all certificates and revocation information on certification path
- Two standards have been proposed
 - ETSI TS 101 733 (RFC 3126) (ASN.1 extension of CMS Signed Data)
 - ETSI TS 101 903 (W3C Note) XAdES XML signature format extension



Archiving Time Stamp

- Time stamp based on PKI also has fixed life time
 - ex. RFC 3161 time stamp token has digital signature
- Encapsulate by another new strong time stamp
- Archive time stamping before expiration of inner timestamp certificate and/or cryptographic algorithm compromise



e-Authentication and PKI

- Authentication is most important mechanism for cyber space security
 - Secure online services must need authentication
- e-Authentication
 - US government initiative
 - Multiple assurance authentication Level (1 to 4)
 - SAML & Liberty base
 - Identity Federation for privacy protection
 - PKI will play high assurance authentication Level (3, 4)

Web services security

- Web service will emerge in many applications
 - Loosely coupled
 - Platform and language independence
 - Firewall friendly
 - XML and SOAP messaging
- To secure Web services application on the internet
 - SOAP security
 - SAML token
 - Need digital signature security for messaging
 - PKI will play background infrastructure

Combine PKI and PMI

- Will become X.509 Attribute Certificate as PMI?
 - X.509 attribute certificate is too complex to manage
 - It only supports attribute definition and does not support privilege (access) control
- SAML and XACML will work well in online environment
 - Flexible security mechanism including ID-Password to PKI
 - It works in wide domain PMI with Id federation
 - Supports personal information protection
 - Attributes and privileges management might be local

Trusted validation authority XKMS (X-KISS)

- PKI applications have to use many digital signatures
 - Natural persons electronic signatures
 - Message signatures by system
- Verification of certificate and signature
 - Out source verification process from client to trusted verification services for interoperability
 - XKMS (X-KISS) is a good tool for the verification, specially for web services security

Summary

- PKI technologies have been matured
 - Basic Infrastructure has been established
 - However, lack of killer applications
- For near future
 - Long term signature retention is necessary
 - We have to re-verify the signature again to arbitrate the disputes
 - Stable standards are needed for signature verification capability over long term period
 - We have to confirm the stability and usability of these standards
 - e-Authentication and PKI
 - Under clear policy, Id federation can protect personal information
 - PKI supports high assurance security
 - Web services security
 - Many applications will reside on web services
 - PKI will play as security mechanism for web services messaging
 - Trusted validation authority XKMS(X-KISS)
 - Out source validation service from client

Thank You