RTR

We stand for competition and media diversity

The Austrian ROCA case

The lessons we learned

Ulrich Latzenhofer
Austrian Regulatory Authority for Broadcasting and Telecommunications

Agenda

- **Affected services**
  Qualified certificates – Time stamps – Unaffected services
- **Reactive measures**
  Information to public – Qualified certificates – Time stamps
- **Prevention**
  Status of apparently old signatures – General constraints of smart cards
- **Possible improvements**
  Evaluation methodology – Flow of information

Affected services: Qualified certificates

One of currently three qualified Austrian trust service providers (TSPs)

Secure signature creation devices (SSCDs) supported by TSP

- CardOS V5.0 QES, V1.0, based on SLE78CFX*P (M7892 B11)
- CardOS V5.3 QES, V1.0, based on SLE78CFX*P (M7892 B11)

2,048 bit RSA keys generated as signature creation data within SSCDs

Signature validation data in qualified certificates affected by ROCA ☹

Affected services: Time stamps

Austrian TSP providing non-qualified time stamps

TSP's seal creation devices used for sealing time stamps

- CardOS V5.0 QES, V1.0, based on SLE78CFX*P (M7892 B11)

2,048 bit RSA keys generated as seal creation data within seal creation devices

Seal validation data in time-stamping certificates affected by ROCA ☹

Unaffected services

CardOS V5.3 QES, V1.0, also supported as SSCD by other qualified TSPs (since 2014 widely used as “e-card” = Austrian health insurance card), **ACOS EMV-A04V1 & EMV-A05V1** supported as SSCDs by one qualified TSP

- ECDSA used for qualified certificates ☺
- RSA keys for non-qualified certificates generated by hardware security modules (HSMs) and imported into SSCDs ☺

Remote signatures (e.g. “mobile signature”) created by HSMs ☺

Qualified TSPs’ seals in certificates created by HSMs ☺

Reactive measures: Information to public

Customers informed by TSP via e-mail

- Announcement of certificate revocation within five days
- Information regarding retrieval of new certificate free of charge
- Recommendation for renewal of signatures in long-term documents

Information published on TSP's website

- Insecurity of RSA signature creation data generated before
- Serial numbers of affected smart cards (also part of certificate's subject)
- Recommendation for validating signed documents by additional means
- Indication that signature remains valid unless authenticity is disputed

Reactive measures: Qualified certificates (1)

Revocation of affected certificates announced five days in advance

Alternatives

- For users of CardOS V5.3 QES, V1.0: Migration from RSA to ECDSA without necessary change of SSCD
- For users of CardOS V5.0 QES, V1.0: Migration to CardOS V5.3 QES, V1.0

Process of issuing new qualified certificates

- Old (still valid) qualified certificates used for identification

Reactive measures: Qualified certificates (2)

Signatures created before (?)

- Signatures forged after certificate revocation are technically invalid – unless being backdated
- Backdating possible e.g. for XAdES, CAdES and PAdES Baseline Profiles

Level	Trusted time
B (basic level)	☹
T (trusted time for signature existence)	☺
LT (long-term level)	☺
LTA (long-term level with archive time stamps)	☺

Reactive measures: Qualified certificates (3)

TSP's recommendation for renewal of signatures in long-term documents

- Voluntary measure of signatory
- Signatory might take advantage of situation and repudiate signature due to ROCA vulnerability
- Unsatisfactory from relying party's perspective
- Renewal of signatures still the best one can do for existing documents without trusted indication of time

Reactive measures: Time stamps (1)

Options for preventing forgery of future time stamps

- Migration to 3,072 or 3,584 bit RSA keys (still considered secure)
- Import of externally generated RSA keys into TSP's seal creation devices
- Replacement of CardOS V5.0 QES, V1.0, by other seal creation devices

Eventual decision for last option, replacement by certified SSCDs

New time-stamping service demonstrably not affected by ROCA ☺

Old time-stamping service discontinued after going live with new service

Reactive measures: Time stamps (2)

Collection of all time stamps created before in single list sealed by TSP

- Sealed list useful for case of doubt regarding authenticity of time stamp

Renewal of prior time stamps by new service

- Renewed timestamps to be used as needed by customers

Eventual revocation of old time-stamping certificates

Prevention: Status of apparently old signatures

Limited cogency of signatures created before deterioration of security

- Forged signatures easily backdated to time before certificate revocation

Prevention

- Promotion of preservation services
- Promotion of time stamps
- Promotion of advanced signatures complying with T, LT and LTA levels of XAdES, CAdES and PAdES Baseline Profiles
- Promotion of remote signatures including time from trusted source

Prevention: General constraints of smart cards

Constraints of (pseudo-) random number generators in smart cards

- Limited entropy source for generating true random numbers
- Low amount of memory and processing capabilities

Prevention

- Cryptographic keys generated by HSMs and imported into smart cards
  - ✓ Type 2 SSCDs (CWA 14169:2004)
  - ✓ QSCDs with key import (EN 419211-3:2013)
- Remote signatures created by HSMs (e.g. “mobile signature”)

Possible improvements: Evaluation methodology

Cryptographic products not always resistant to new cryptanalytic approaches

Evaluation still necessary

Special care to be taken for evaluation of key generators

- Evaluation of random number generator based on AIS 20 and AIS 31
- Precise method for RSA key generator unclear
- Precise evaluation method for RSA key quality unclear

Improvements of evaluation methodology?

Possible improvements: Flow of information

Disclosure of vulnerability to producer in February 2017, agreement on eight month period before public disclosure

Austrian TSP informed by vendor more than three months later, additional delay of TSP's incident report to SB

Remedies to be found at different levels by different parties – impossible without involving all relevant parties from beginning

Improvements of flow of information for future cases?

RTR

We stand for competition and media diversity

EESTI VABARIIK

Tänan tähelepanu eest ja palju õnne (ilma ROCAta) järgmiseks sajaks aastaks!