Managing SHA-2 migration

Replacing foundations of a PKI

Dr. István Zsolt BERTA
Microsec Ltd.
Contents

- The status of PKI in Hungary
- Changes in regulations on secure cryptographic algorithms
- The way we solved this problem
- Conclusions
The status of PKI in Hungary
Hungarian e-Signature Act

- Act 2001/31 on electronic signatures
- Defines 4 e-signature „trust services”
  - certification services (issuing & maintaining certificates)
  - timestamping
  - provision of signature creation devices / data
  - long-term archiving
- Each service can be provided as a „qualified” service
  - more rigorous supervision
  - financial liability
  - presumed to be provided „well”, the opposite needs to be proven
- Supervisory authority:
  National Media- and Communications Authority
PKI in Hungary

- Notaries, barristers, judicial officers
  - qualified signatures, ~ 20 000 qualified certificates with SSCD cards
  - electronic business registry system
  - judicial officers and financial institutions

- Electronic invoicing
  - advanced electronic signature + qualified timestamp

- Electronic archiving
Interaction of some major Hungarian PKI apps

- barristers
- business registry courts
- financial institutions
- land register
- judicial officers
- notaries
- notarial archives, etc.
- any organization
- e-invoicing
Changes in regulations on secure cryptographic algorithms
Regulations on algorithms for e-signatures

- Electronic signatures are based on cryptographic algorithms
- In Hungary, the National Media- and Communications Authority determines which algorithms can be used for electronic signatures
- It is usually based on ETSI TS 102 176-1 (= the ‘ALGO’ paper)
Change in standards for secure algorithms

- **ETSI TS 102 176-1, v2.0.0, 2007-11:**
  - SHA-1 and RSA with 1024 bit keys are recommended for 1-3 years only
  - a new version will be issued soon (2011 ?)

- **NIST SP 800-57:**
  - RSA with 1024 bit keys is being phased out
  - CAs must not issue such certs after 2011, and these certs must expire before 2013.
  - Microsoft, Mozilla, etc.
This change affects...

- Certificates
- Electronic signatures
- Timestamps
- Certificate Revocation Lists
- OCSP responses
- etc.
Microsec, our company is a...

- Certification Authority
- Timestamping Authority
- Long-term archiving service provider
- Developer of a signature creation application
- System integrator

We feel responsible for the correct PKI operations of a large part of the Hungarian market
Requirements

- Existing PKI applications must not break
- The validity of signatures must not be affected; valid signatures must remain valid and verifiable
- End users must not suffer from this change
The solution we followed
Thus, we needed to make changes

Changes in algorithms:
- RSA: 1024 bits → 2048 bits
- SHA-1 → SHA-256

We modified our...
- CA hierarchy
- Signature creation application
- Timestamping (!)
- Smart cards

Additional issues:
- Relying parties
- Archival of existing signatures
CA hierarchy (1)

- We decided to start a completely new system, new hierarchy, because...
- It makes it easier for end user to differentiate between new and old signatures.
- We decided not to maintain a hierarchy with mixed algorithms
- In the new hierarchy, all
  - RSA keys are at least 2048 bits
  - hash functions are SHA-256
CA hierarchy (2)

- Microsec Root
  - productive CAs
    - TSAs
      - New productive CAs
        - New TSAs
          - End users
Step 1 (2009): Creation of new CA hierarchy

Step 2 (2010): Spreading new CA certs

Step 3 (early 2011): Switch to new CA hierarchy
  - Issue certs from new CA hierarchy only
  - There are still valid certs in the old CA hierarchy

Step 4 (future): Phase out the old hierarchy

Note: Webserver certs are problematic, as there are still a lot of (unpatched) browsers that do not support SHA-256.
Signature creation application (1)

- Most clients use e-Szignó, our own signature creation and verification application
- We were able to deploy e-Szignó updates via an automatic update mechanism
- Not everyone uses our e-Szignó
  - We contacted them via newsletters
  - We provide information on our website
  - They have to update their software too
Signature creation application (2)

Step 1 (2009):
- allow the acceptance of new signatures, certificates, CRLs, timestamps, etc.
- allow the creation of new signatures

Step 2 (early 2011):
- default to creating new signatures

Step 3 (future):
- reject old signatures (if and only if they were created after they had been outlawed)
Timestamping

- Timestamping is CRITICAL:
- An old signature with a new timestamp will remain OK in the future
- We need to urge everyone to use the new TSAs
- Prerequisites:
  - new CA hierarchy and TSAs ready
  - new CA certs distributed
  - signature creation/verification application distributed
Our old SSCD smart cards did not support the new algorithms, but they used a different PIN for signing and encryption supported PIN pad readers.

- We sought new cards with the same properties.
- Two new cards were selected.
- Currently we need to support three cards in parallel.
- All three cards have a different user interface.
Smart Cards (2)

- One PIN for signing and another one for encryption
  - there are but a few SSCD cards like this
  - their software support is more than problematic
  - they are handled differently by various applications
- PIN pad readers
  - not all smart card drivers support all PIN pads
  - they support and handle them differently
  - there are a lot of interoperability problems here
- We decided to develop a common user interface
- In most contracts we pay the cost of new cards
- Deployment of new cards...
Relying party applications

- We were able to update our own applications
- Other major relying parties: we contacted them one-by-one and asked them to
  - accept new algorithms
  - accept new CA certs
  - we provided new smart cards for testing
- This takes a LONG time…
- Currently (2011): Most relying parties already accept the new signatures
Archival of signatures

- New signatures are OK, but…
- Old signatures should be
  - timestamped with new timestamps
  - before old algorithms are outlawed
  - XAdES-A signatures should be used
- Long-term archiving (or information preservation) service should be used
- May 2011: New ETSI standards on information preservation service providers
  - 101 533-1: on requirements for IPSP management
  - 101 533-2: on recommendation for auditors of IPSPs
Conclusions
In a nutshell

1. Create the system for new signatures
2. Prepare verifiers to accept new signatures
3. Wait until most verifiers are prepared
4. Make signers create new signatures by default
5. When old signatures are outlawed, make verifiers reject them
Conclusions

- The migration is mostly done
- Our clients create new signatures
- The new signatures work, relying parties are able to accept them
- End users did not have dramatic experience

- Phasing out old crypto algorithms and introducing new ones instead in a PKI
  - is a HUGE change,
  - it requires a LOT of work and
  - takes a LONG time, it cannot be done quickly
Thank you very much! 😊