Enhancing Trust by Enhancing the Audit Process

Jens Bender

Federal Office for Information Security

NIST CA-WS / 11.04.2013

The BSI – Federal Office for Information Security

- Founded in 1991
- ~ 550 Employees
- IT security provider for the federal government
- Support of the federal states
- Close cooperation with industry, citizens and research community

BSI und PKI

- BSI is architect, operator and user of PKIs
- BSI operates
  - Root CAs for travel documents (passport, ID-card, ...)
  - Root CA for governmental PKI (V-PKI)
  - Several other PKIs
- Responsibilty for requirements for
  - SubCAs of those PKIs
  - Other PKIs used for governmental purposes
- Incident Response: CERT-Bund/Bürger-CERT

What is PKI?

PKI = Certification of identities/attributes

- PKI enables third parties to verify identities/attributes
- PKI does not assign identities/attributes

PKI is Trust

- All parties (have to) trust the root
- The root delegates Trust to SubCAs
- PKI only works if the Trust is justified

Therefore: Loss of Trust is disastrous

CAs need not only to *be* secure,
third parties must be *convinced* that the CA is secure

→ Trustworthiness and Trust ←

Solution?

- „Notaries“ are queried if a certificate is genuine
  - Initial identification of sites by notaries? Are the notaries trustworthy?
- Browser checks if the certificate is the same as before
  - Initial trust in a certificate? Cert. roll-over / several certs for a domain?
- DANE: Certificates stored in the DNS, secured via DNSSEC
  - Is my registry/registrar/zone-signer trustworthy?
- … and more

**Help to detect/mitigate compromises,
but do not solve the basic problem of trust**

„CAs are untrusted, therefore I have to trust others“

Solution!

Only way out:

Trust in <u>all</u> CAs (not only SSL) **must be enhanced/rebuild**

- Transparent security requirements on CAs
  - Better Security leads to higher trustworthiness
- High quality audit as high level assurance
  - Feedback loop of audit enhances security
- Trustworthiness + Assurance → Trust
  - Security + marketing

Requirements and Audit

- Existing requirement/audit-regimes
  - CAB-Forum, Webtrust, ETSI, …
  - Special requirements, e.g. national requirements for qualified signature or governmental CAs

→ Sector specific / focussed on management processes only / focussed on technical requirements only / mixing security and non-security requirements ...

- The Plan: Build a framework consisting of
  - (As far as possible) application-independent CA requirements,
  - Focussing on security
  - Clear requirements what is to be audited in the audit
  - Accreditation of auditors and Certification of CAs

IT Security Standards

- ISO 2700x
  - Security concepts for IT systems
  - Methodology, not specific requirements
- Baseline Protection
  - Specific requirements on normal security level
- Common Criteria
  - Formal security assurance process for components/devices

Needed: System security on high security level with formal process to enhance assurance and compatibility

Therefore ...

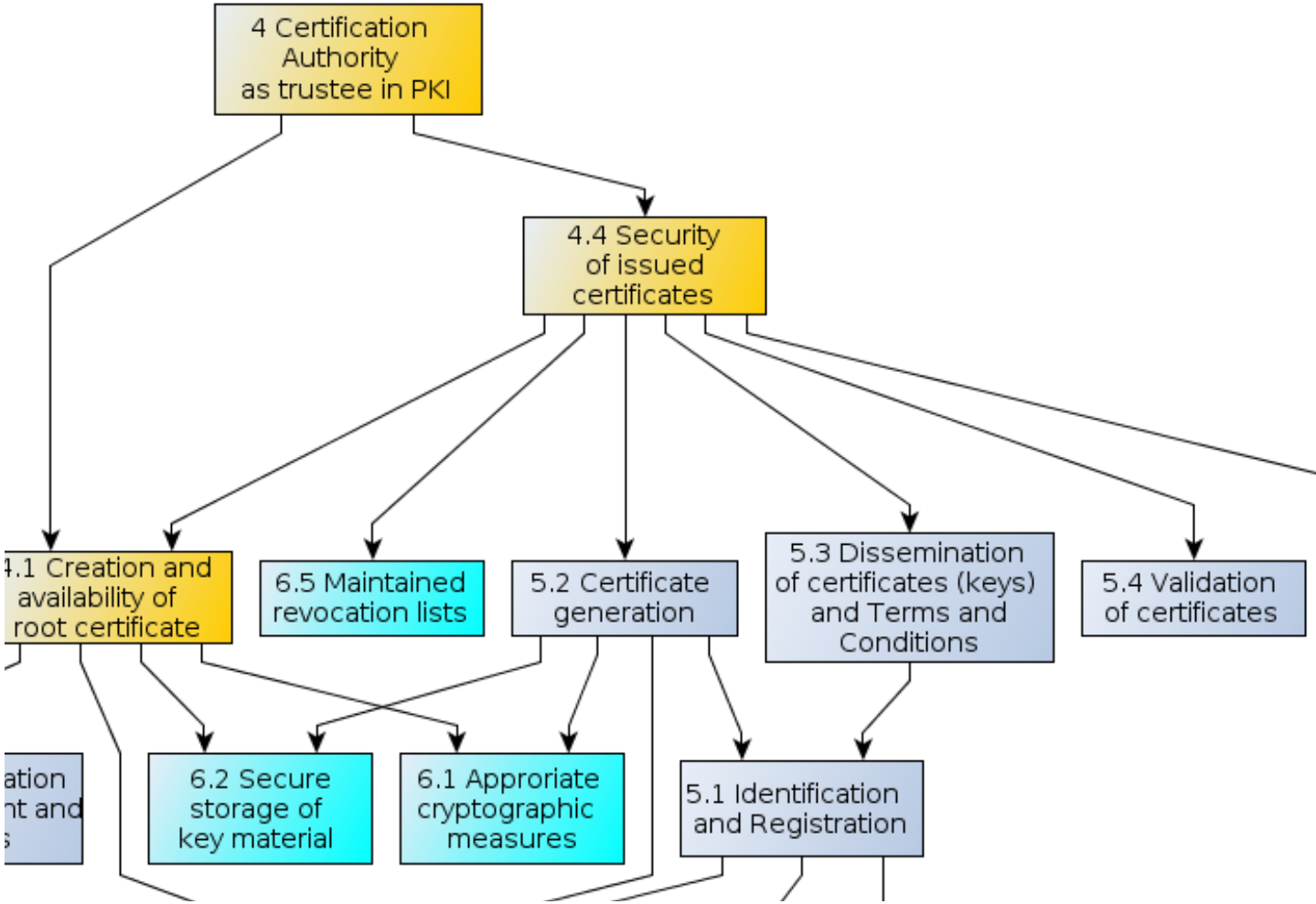
- Formal structure inspired by Common Criteria
  - Security Objectives + Threads → Requirements
  - Mapping of requirements on Security Objectives („rationale“)
  - Formal language to avoid ambiguities
- View on the whole system following ISO 2700x
- Criteria on suitability of requirements
  - Security Objective is actually reached
  - The requirement is necessary to reach objective
  - Technical and commercal feasibility
- Compatible (if possible) to existing frameworks

Structure

→ What is the task of the CA

→ What are the processes required to fulfill the task

→ Technical requirements necessary to have secure processes



Example

Process:

- Creation and availability of root certificate

Depends on Security Objective:

- Secure handling and storage of key material

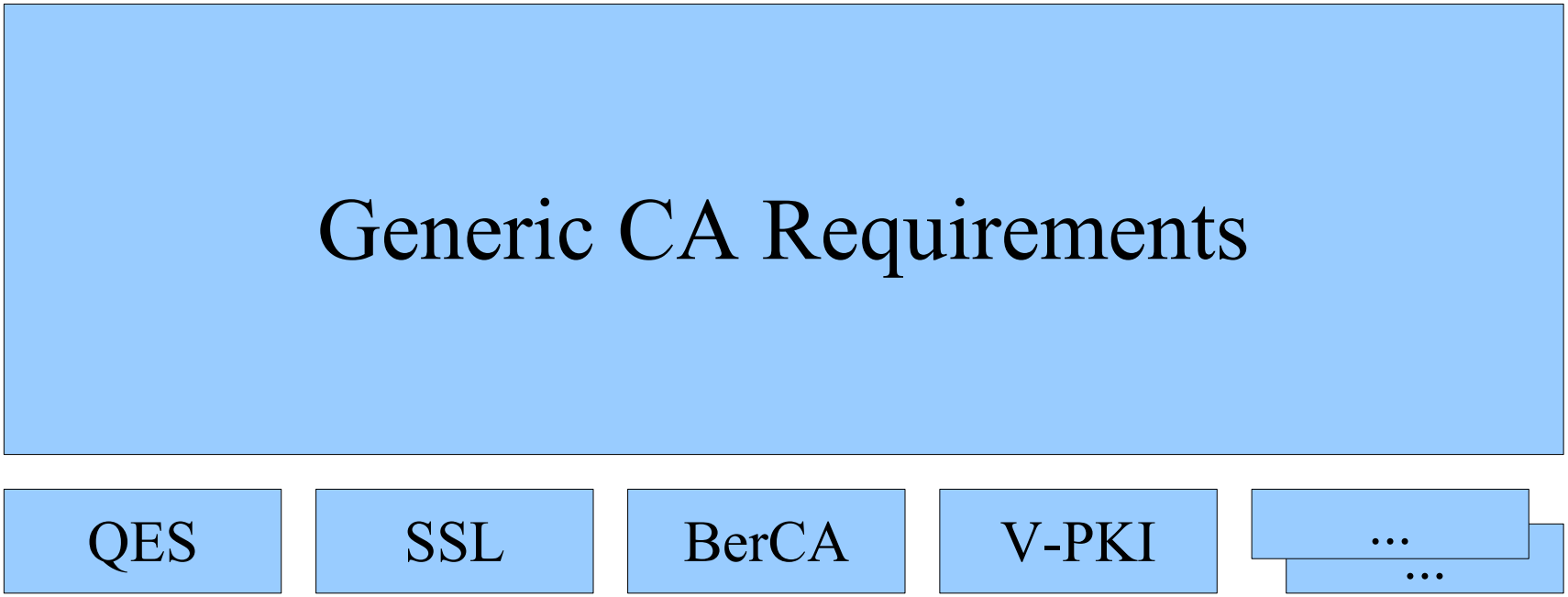
Includes Requirement:

- SecMgmt.Req.2.: The CA private key shall be generated, stored and used in a security device following the standards [selection: *FIPS PUB 140-2, ISO/IEC 15408, other*] with security level [assignment: *level of security product*] or higher ensuring the claimed security features.

Auditor's task:

- Check: CA key is generated and stored in a device …
- Check: Requirements from the Guidance Document are fullfilled
- If 'other' is selected, check rationale for claimed equivalence

Generic and Specific



„80%“ application independent + „20%“ application specific
→ Simplification for CAs by enabling „Base Audit“

Last Words

- Requirements on CAs and on audit
  - Systematic → Verifiably complete coverage of all processes
  - Generic base requirements → Simpler for multi-CA trust center
  - Clear audit criteria → Comparability, reliability, assurance
  - Certification → Criterion for subscribers / relying parties
- Current Status
  - Drafting of requirements underway
  - Commenting by industry to be started soon
  - Audit requirements to be done

Federal Office
for Information Security

Contact

Bundesamt für Sicherheit in der Informationstechnik (BSI)

Jens Bender
Godesberger Allee 185-189
53175 Bonn

Tel: +49 (0)228-9582-5051
Fax: +49 (0)228-99-10-9582-5051

jens.bender@bsi.bund.de
www.bsi.bund.de
www.bsi-fuer-buerger.de