

Legal and Technical Aspects of Qualified Electronic Signatures

6th European Forum on Electronic Signature

Miedzyzdroje, 07-09 June 2006

Jürgen Schwemmer

Section Electronic Signature

Bundesnetzagentur

juergen.schwemmer@BNetzA.de

Definitions according to Article 2 of EU-Directive 1999/93/EC or Section 2 of (german) Electronic Signatures Act:

1. Sec. 2 (1): “**Electronic Signatures**”

- Data in electronic form attached or logically linked to other electronic data, used for authentication

No security (requirements), e.g. scanned/copied manual signature

Definitions, ctd.1:

2. Sec. 2 (2): “ **Advanced Electronic Signatures**”

“electronic signatures” (see above)

+ exclusively assigned to the owner of the signature code

+ enabling identification of the owner

+ sole control of the owner over the means of production possible
(effective protection against unauthorized use)

+ detection of any subsequent alteration of the data signed
possible

No specific requirements for security of organisational processes or of technical components;

No regulations and legal consequences (beside -some MS- evidence)

Definitions, ctd.2:

3. Sec. 2 (3): “**Qualified Electronic Signatures**”

“advanced electronic signatures” (see above)

+ based on qualified certificate valid at the time of the creation of the electronic signature

(for qual. certificate cf. sec 2(7): Certificates issued to natural persons [no company signatures]; meeting the requirements of sec. 7; issued by certification service providers meeting the requirements of the Electronic Signatures Act & Ordinance)

+ produced with secure signature-creation device (smart card...)

Specific requirements for security of organisational processes and of technical components;

Specific legal consequences: E.g. **Equivalence with handwritten signature**, sec. 126 a Civil Code; **Prima facie Evidence**, sec. 371 a Code of Civil Procedure

Definitions, ctd.3:

4. Sec. 2 (3): “**Certification Service Provider**”

(a natural or) legal person

who issues

qualified certificates or qualified time stamps.

5. Sec. 2 (3): “**Secure Signature Creation Device**”

Software or Hardware...

...and that are designed for qualified signatures

The Homonym-Problem of (digital/electronic) Signatures

“Real-World”-Definition:

- **Authentication** tool, Member´s Card, Business Paper (-sheet)
- Banknote, Purse, Credit Card, **Payment** tool
- **Envelope**, Safe, Hideaway
- **Handwritten Signature**, Declaration of Will, Pen

“Electronic-World”-Definition:

- (Digital) Signature
- (Digital) Signature
- **Encryption**
- **Qualified Electronic Signature (QES)**

What is different about Qualified Signatures?

- Validity/**Verification-model** (here and now vs. **now and forever**)
- **Algorithms** (specified **annually** plus if necessary)
- **Hardware compulsory** (non-repudiation, key-holder as attacker !)
- **Long-term verifiability** (at least 5/35 years or “till eternity”)
- **National root** certificate (**by** FNA/BNetzA/**Government**) for accredited certification service providers (only)
- **Quality mark** for accredited certification service providers only

“International Aspects” (EU-Directive Article 7 and/or German Signature Law § 23)

Member States shall ensure that Certificates which are issued as **qualified certificates to the public** by a certification-service-provider (CSP) in a third country are recognized as **legally equivalent** to certificates issued by a CSP within the community **if:**

...

(c) the certificate or the CSP is recognized under a **bilateral or multilateral agreement** between the **Community** and third countries or international organisations.

(What about **Member States** ?)

Enhanced quality through voluntary accreditation

Enhance the level of the certification services to be provided towards the levels of trust, security and quality demanded by the evolving market.

Electronic Signatures Directive, Recital 11

= Secure procedures, archivability, availability, etc



“Voluntary accreditation”

Article 2, paragraph 13 of the Electronic Signatures Directive or Section 15 of the German Electronic Signatures Act

= Permission, setting out rights and obligations for the provision of certification services and granted at the request of the certification service provider concerned by the competent body.

The certification service provider is not entitled to exercise the rights and obligations stemming from the permission until it has received the permission.

Permission

**Competent
body**

Application

Right to operate as accredited provider

EU Directive for Electronic Signatures

Continental European Approach



Prevention through comprehensive pre-implementation checks for

- products,
- technical, administrative and organisational aspects of certification activities, and
- reliability and specialised knowledge of staff.

Anglo-Saxon Approach



Ensuring adequate minimum level of

- **competition** in the market, and
- **liability**.

- Development costs (evaluation of products and security concepts)
- More time-intensive in initial stages



"Teething problem"

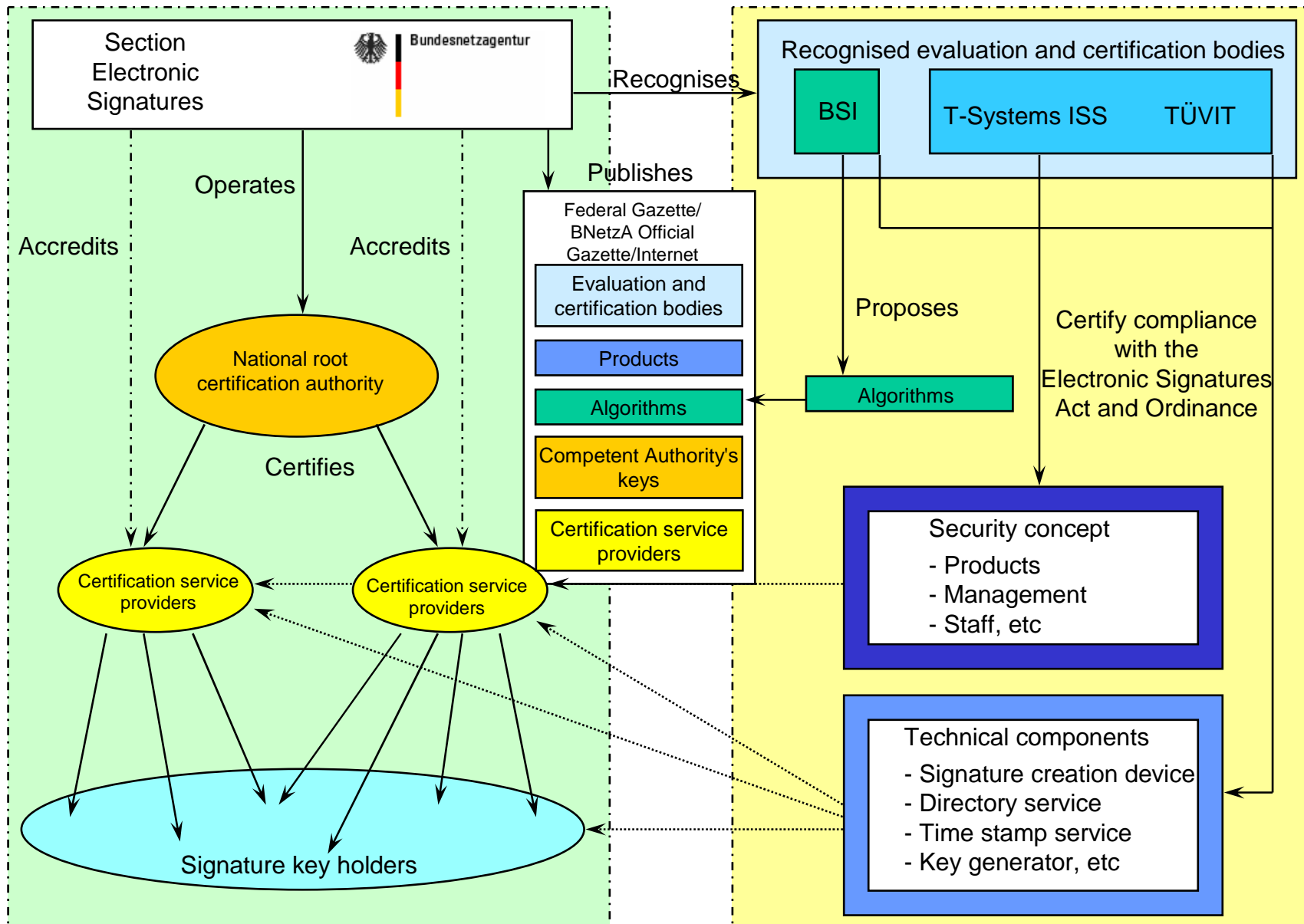
- Liability depends on
- ability and willingness to assume liability in cases of damage, and
 - recognised cases of damage.



Long-term problem

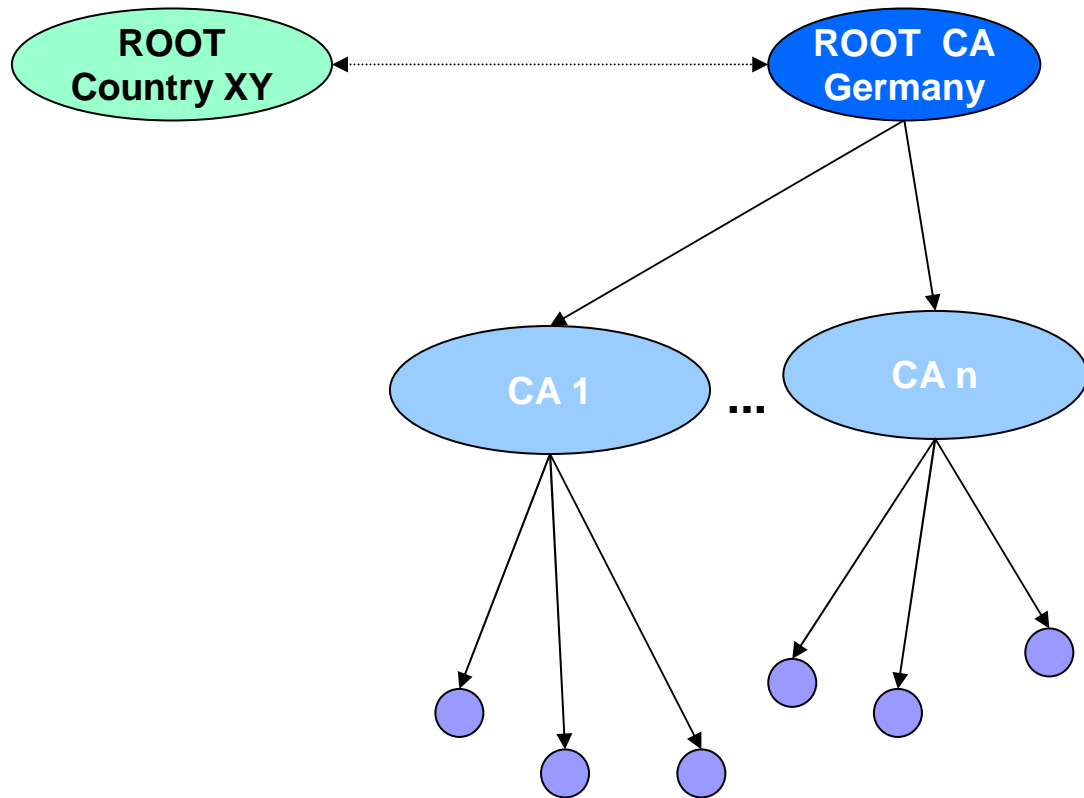
Amendments/Developments in Germany (a.m.o):

- 3rd Law Amending Administrative Proceedings (3. VwVfÄndG) 21.08.2002
- Sec. 14 (3) Value Added Tax Act
- Amendments of the 5th book of the Social Security Code, sec. 291a (Health Card, Health Professional Card)
- Law laying down rules for the communication within legal authorities (“JKomG”)
- First Signature Amendment Act (1. SigÄndG) of 04.01.2005



Implementation

All elements contributing to the **VERIFIABILITY** of **ELECTRONIC SIGNATURES** are termed **CERTIFICATION INFRASTRUCTURE** and include:



National
ROOT CERTIFICATION
AUTHORITY
– State –

issues certificates for

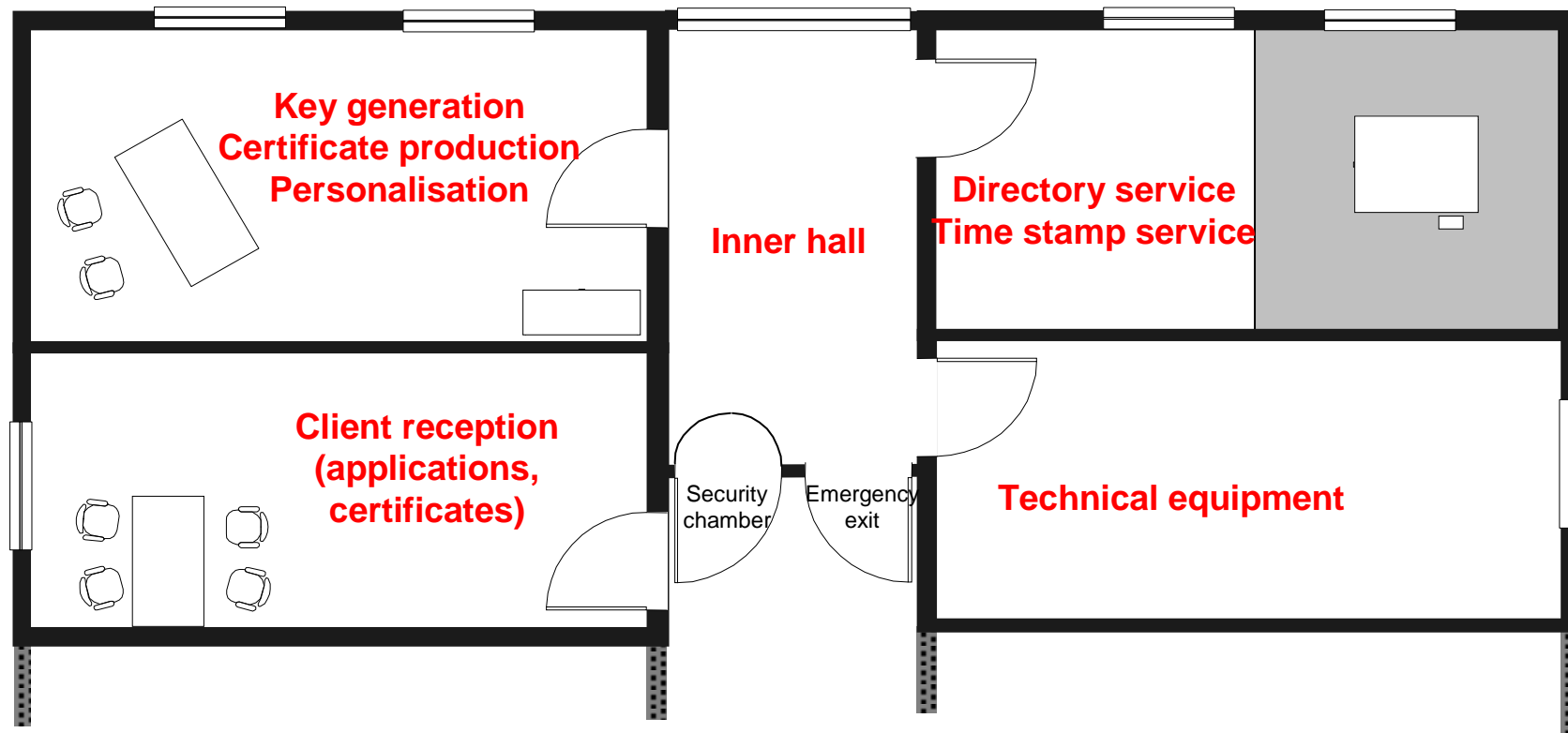
CERTIFICATION SERVICE
PROVIDERS
– Private or state –

issue certificates for

USERS
– Natural persons-
(with/without attributes
and/or pseudonyms)

Implementation

Example layout of a Trust Centre



BNetzA's Tasks

1

Technical operation of the national root certification authority

- Issuance of certificates for accredited certification service providers
- Directory service with certificates available for retrieval and verification 24 hours a day, 7 days a week (www.nrca-ds.de)

Accreditation authority for certification service providers

- Performance of the administrative procedure
- Verification of providers' specialised knowledge and reliability
- Review of certified security concepts
- Publication as required of suitable algorithms (proposed by BSI), certified technical components, etc in the Federal Gazette and on the Internet

BNetzA's Tasks, ctd.1:

2

Supervisory authority

- Regular and prompted checks on accredited certification service providers
- Monitoring compliance with the Signatures Act and Ordinance

Powers of intervention including

- Prohibition of the use of unsuitable components
- Withdrawal of certification for technical components and qualified electronic signature products
- Revocation of certificates
- Prohibition of operation by certification service providers
- Activities in connection with the cessation of operation by certification service providers

BNetzA's Tasks, ctd.2:

Additional tasks

- Recognition of certification bodies for security concepts and technical components
(Accredited Certification Bodies' Working Group – AGAB)
- Supervisory body for "notified" certification service providers
(within the context of qualified certificates)
- Publication of "notified" certification service providers
(<http://www.bnetza.de>)
- Evaluation of Manufacturers' Declarations for Signature Products according to § 17 Sections 3 and 4 (new SigÄndG)

Further Information

Bundesnetzagentur
(für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen)

Referat IS 15 Elektronische Signatur

Jürgen Schwemmer

Canisiusstr. 21, 55122 Mainz

<http://www.bundesnetzagentur.de>

<http://www.nrca-ds.de>

Thank You for Your Attention, Questions ?