

# Trust Levels in Public Key Infrastructures

Anthony Thorn. AT Systems & Services GmbH

28. 3. 2001

FGSec PKI

## Contents

- Factors affecting Trustworthiness of a Certificate, a Signature or an Authentication
- The Problem
- A Vision → Simple Trust Levels
- Questions
- Conclusions

28. 3. 2001

2

FGSec PKI

# A PKI is a Key Management Infrastructure

Key Management is concerned with managing keys during their entire life cycle.

- A PKI must ensure that relying parties know or at least can determine how much trust they can place in a key/certificate and hence a signature.
- A PKI manages Trust.

28. 3. 2001

3

FGSec PKI

# What factors influence the trust level?

*The most important issues can be classified under the following headings:*

- Identification
- Issuing Procedures
- IT Security at Issuer
- Standing of Issuer
- Validation Service
- Usability of Directory
- Scope and Liability
- Independent Review
- Cryptography
- Private Key storage
- Signature Security

28. 3. 2001

4

FGSec PKI

# Identification

Identification is the essence of the CA service !

- Personal appearance with Official ID is the “standard”.
- Test Certificates require no identification.
- Corporate PKIs can leverage pre-existing identification.
- Weak identification may be sufficient.

# Issuing Procedures

Procedures differ widely and may contain subtle vulnerabilities. It is not possible to generalise.

- Certificate request, Key Generation, Identification/Registration, Certification and Issuing must be “bound” together.
- The order in which they take place is a determining factor.

## IT Security at Issuer

- This is a presentation in itself.
- CSPs will not want to publish too much detail.
  - Security management
  - Procedures
  - Technical Security
  - Physical & Environmental Security
  - Personnel security

28. 3. 2001

7

FGSec PKI

## IT Security for CSPs

- Roles
- Segregation of Duties
- Accountability
- Records & Retention Periods
- Controls to “prove” compliance
- Lots of documented procedures...

28. 3. 2001

8

FGSec PKI

## Standing of Issuer

### *Assurance is required that:*

- the CSP is well managed - controls in place  
independent - no conflict of  
interest  
adequately funded
- the staff are adequately trained  
honest

## Validation Service Level

### *Assurance that a Relying Party can obtain timely information about certificate validity.*

- Suspension and Revocation requests must  
be processed and the directory and CRL  
updated promptly.
- Access to CRL and/or Directory (or OCSP)  
must be highly available.

# Usability of Directory

Assurance that the certificate belongs to the right „Hans Müller, Zürich“.

- We need to be able to search the directory
- How much information do we need ?
- How much information does the Data Protection legislation permit ?

28. 3. 2001

11

FGSec PKI

# RFC 3039

The subject field SHALL contain an appropriate **subset** of the following attributes:

countryName;	commonName;
surname;	givenName;
pseudonym;	serialNumber;
organizationName;	organizationalUnitName;
stateOrProvinceName	localityName
postalAddress.	

**Other attributes** may be present but **MUST NOT be necessary** to distinguish the subject name from other subject names **within the issuer domain**.

Of these attributes, the subject field SHALL include at least one of the following:

- Choice I: commonName
- Choice II: givenName
- Choice III: pseudonym

28. 3. 2001

12

FGSec PKI

## Scope and Liability

- Certificates (and or CP/CPS) can limit the use of a certificate both qualitatively and also quantitatively
  - e.g.
    - this certificate is only to be used for encryption*
    - or
    - this certificate is only valid for transactions up to USD 1000*
- The liability limit is per transaction not per certificate !

## Independent Review

- Accreditation evaluation
- Auditors
- Specific Technical or Procedural reviews organised by internal audit, quality control, security officer etc.

# Cryptography

Another broad field !

- Appropriate algorithms
- Adequate key lengths (Issuer and Subscriber)
- Secure key generation

28. 3. 2001

15

FGSec PKI

# Private Key storage

The subscriber is responsible for the (mis)use of his private key. A secure key store is required to restrict access to the private key.

This can take the form of:

- Browser/MailClient database
  - password protected if the user wishes !
- A Smart Card with class 1, 2 or 3 card reader
- A Certificate Server

28. 3. 2001

16

FGSec PKI

# Signature Security

## What You Sign Is What You See ?

What do you understand by a  
„Secure signature creation device“

- An E-Mail client/Browser installed on a PC
- The display on a class 3+ reader
- A Mobile Phone
- A custom application on a custom platform ?

## CP and CPS

- More or less information about most of these topics is to be found in the CP and CPS of the issuer.
- Clearly there will be some topics like IS which will not be discussed in detail in a public document.
- Certification schemes will be available; for example in the EU for issuers of qualified certificates. (applicable for Signature)

## Vision

- How many key-pairs per user/person ?
- Key Storage → Where? How ?
- Secure Signature Device
- Simple Trust Levels

28. 3. 2001

19

FGSec PKI

## Why Simple Trust Levels ?

- CPS is typically too long and onerous to read
- A skilled reader is needed to evaluate the contents
- We cannot use an infinite number of levels
- We need more than 2 levels

*Qualified / Not Qualified*

28. 3. 2001

20

FGSec PKI

## Simple Trust Levels

- Scale of 0 to 5
- Approximate guide not rigid framework
- Pragmatic i.e. “or equivalent”
- Compliance & Sanctions ?

28. 3. 2001

21

FGSec PKI

## The Levels

	Level 0	Level 1	Level 2	Level 3	Level 4	Level 5
Identification	<b>NONE</b>	<b>E-MAIL</b>	<b>ID</b>	<b>Qualified</b>		
Issuing Procedures				<b>Qualified</b>		
IT Security				<b>Qualified</b>		
Standing of Issuer				<b>Qualified</b>		
Validation Service Level				<b>Qualified</b>		
Usability of Directory				<b>Qualified</b>		
Scope & Liability				<b>Qualified</b>		
Independent Review				<b>Qualified</b>		
Cryptography				<b>Qualified</b>		
Private Key Storage				?	<b>SmartCard</b>	<b>FIPS</b>
Signature Security				?	?	?

***always “or equivalent”***

28. 3. 2001

22

FGSec PKI

## Levels 0 and 1

- **Level 0**      No identification  
                    e.g. test certificate
- **Level 1**      Weak Identification  
                    e.g. based on E-Mail address

28. 3. 2001

23

FGSec PKI

## Level 2

- **Identification**      based on Personal Appearance with ID
- **Issuer Security**      Issuer Keys in FIPS module  
                                    External audit  
                                    Liability > 20'000  
                                    Key Generation was reviewed  
                                    Issuer & Subject key lengths
- **Validation & Directory Service Levels**  
                                    Revocation service: CRL Max Delay 60 min,  
                                    Service 7x24, Availability 99.5%, MTTR 10 min

28. 3. 2001

24

FGSec PKI

## Level 3

- Certified issuer of Qualified Certificates for appropriate countries

*Qualified applies to Digital Signatures*

*Non-repudiation but what about authentication ?*

- Key usage options for user to have  
Non-Repudiation separate from other uses.

*Doubt about "bits" being legally significant, non-critical needed for browser compatibility ...*

28. 3. 2001

25

FGSec PKI

## Level 4

- Issuer can guarantee that private key exists only on a smart card or equivalent ,
- plus as 2 and/or 3

*Which gives the relying party more confidence  
a secure key store or  
a qualified CSP ?*

28. 3. 2001

26

FGSec PKI

## Level 5

- As 2 or 3 plus Issuer can guarantee that subscriber's private key exists only on a FIPS tamper resistant security module or equivalent
- Appropriate procedures

*suitable for Issuer Root keys*

**NB:** don't forget all the above is **“or equivalent”**

## Questions

- **How will users understand what is going on ?**
- What is a Secure Signature Device ?  
(EESSI is active)
- Will accredited CSPs occupy the extreme high-end of the market or the middle ground ?

## Conclusions

- Perhaps these issues only concern security professionals and will not bother users  
After all credit cards are used extensively over the Internet despite lack of security and frequent incidents.
- All this is only critical for “Digital Signature” which is not (yet) a mainstream application of PK Technology