

Public Key Infrastructures

Vision, Trends and Real-World Implementation
20.4.2007

Dr. Elke Stangl, PKI Consultant

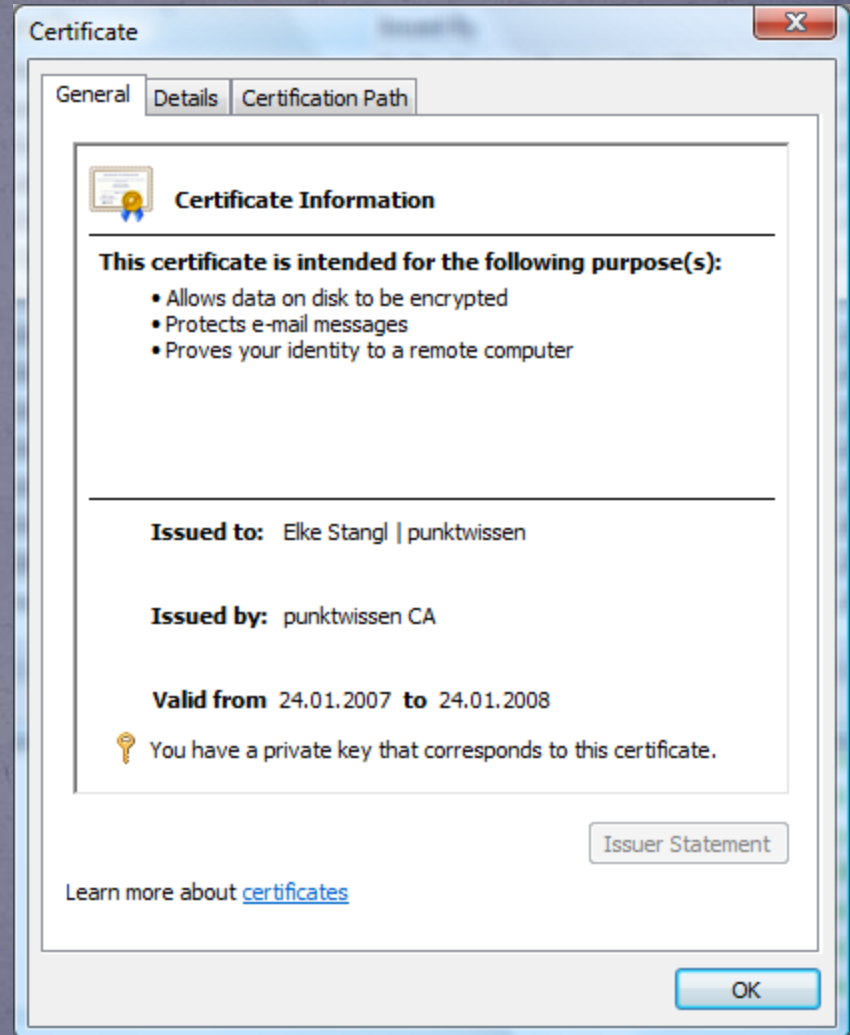
www.punktwissen.com

What is PKI?

- Based on **Public Key** cryptography
 - Alice and Bob want to communicate without exchanging keys
 - Pair of keys: Public / private
 - Trent is introduced: **Trusted Entity**
- Tools, protocols, services, clients (**Technology**) and **processes** (= **Infrastructure**) involved in managing the lifecycle of **digital certificates**
- Technical representation of an organization's **trust boundaries**
- NOT: A silver bullet that solves **all identity management and security issues**.

What is a Certificate?

- Electronic counterpart of **passport** or **driver license**
- Issued to **entities**: Humans, machines, services
- Linkage of
 - Something which identifies an entity
 - Contact data, naming attributes, org. information
- Attributes and extensions according to **X.509**



Why do We Want PKI?

- **Compliance** <insert buzzword like SOX here>
- Modern knowledge worker lifestyle results in **new risks**:
 - Stolen notebooks
 - Remote access to corporate networks
 - Protection of the (virtual) network perimeter
- Part of bigger picture: **Identity management**
 - Caveat: Resulting in projects and solutions that try to "solve anything"
- **Replace island-type existing solutions**
 - Many applications contain tools to create "their own certificates"
 - Can be simple or can be management nightmare

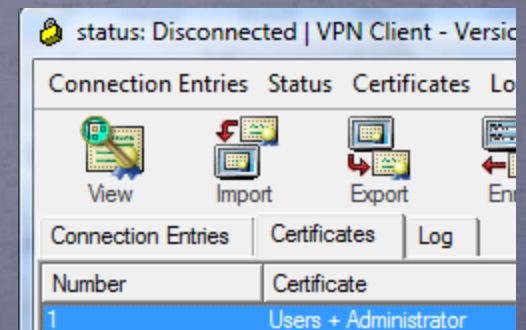
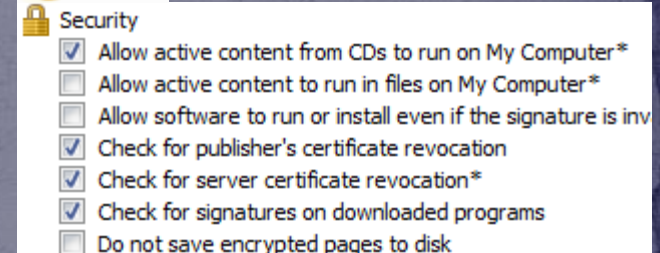
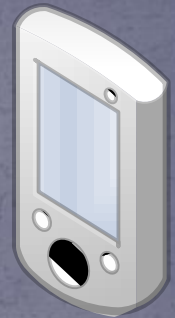
What is PKI ? (cont'd)

- ... and **why are there challenges**
- Certification Authorities issuing certificates. End-entities (have to) trust CAs → **Lots of Trends with complicated relationships**
- Repositories publishing CA certificates and end-entity certificates → **URLs that may not be accessible**
- **Processes, processes, processes** → Most underestimated part of PKI solutions
- **Policies, policies, policies** → Integration of non-IT departments, company politics, paperwork



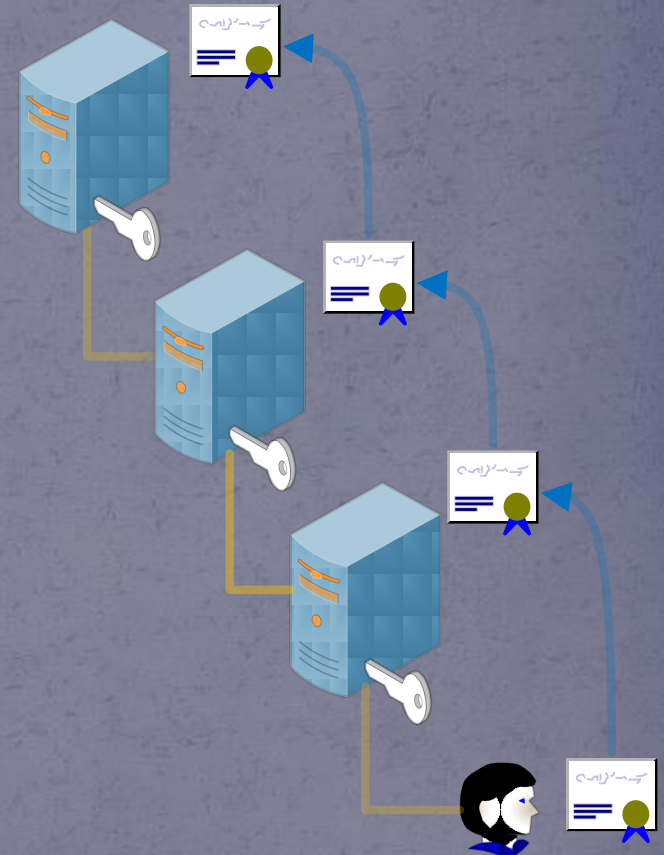
What is PKI ? (cont'd 2)

- ... and **why are there challenges**
- Many kinds of Alices and Bobs
 - Certificate-enabled clients
 - Certificate enabled relying parties
- 1000 ways to implement the standards or make use of **optional attributes** in certificates
- 1000 ways to configure **certificate validation** ("You are allowed to enter if your passport is expired for not more than 6 months")



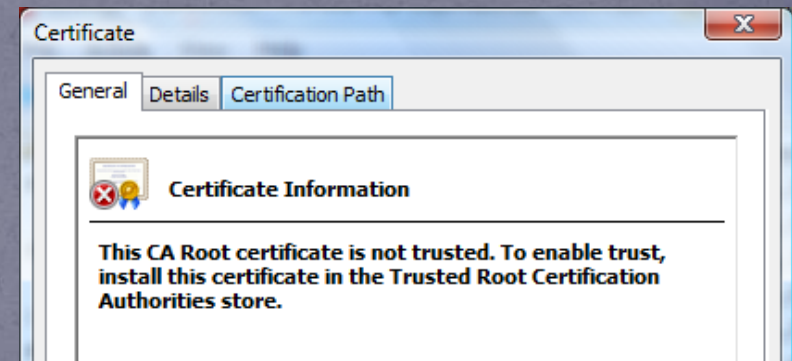
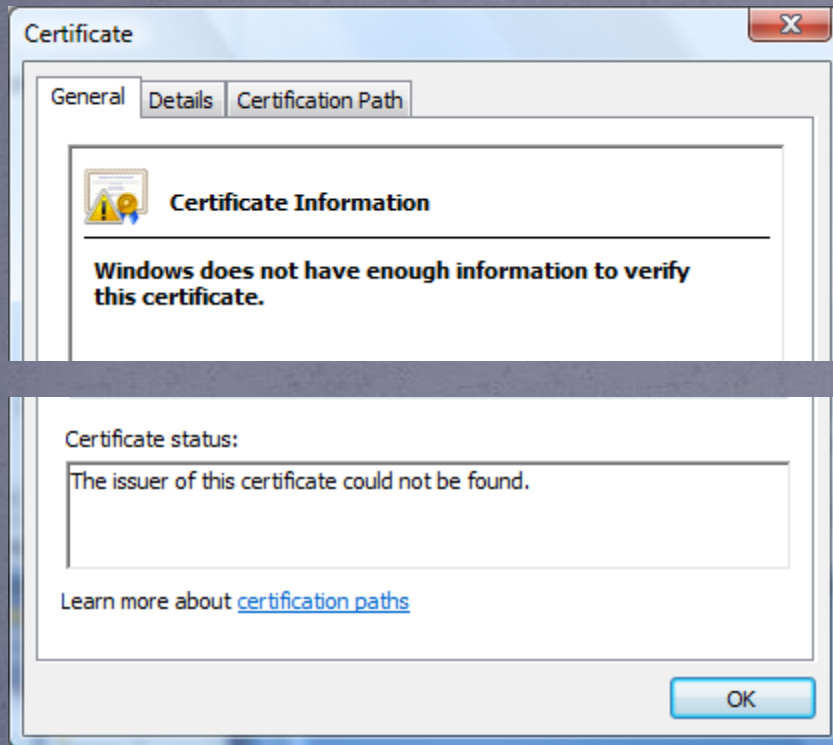
Challenge: Path Validation

- Relying parties check:
 - Validity and contents of attributes (hopefully)
 - URLs that point to the certificate of the parent certification authority (hopefully)
- Each cert says:
 - "Go HTTP://<hopefully existing URL>" to find the next cert. In the chain



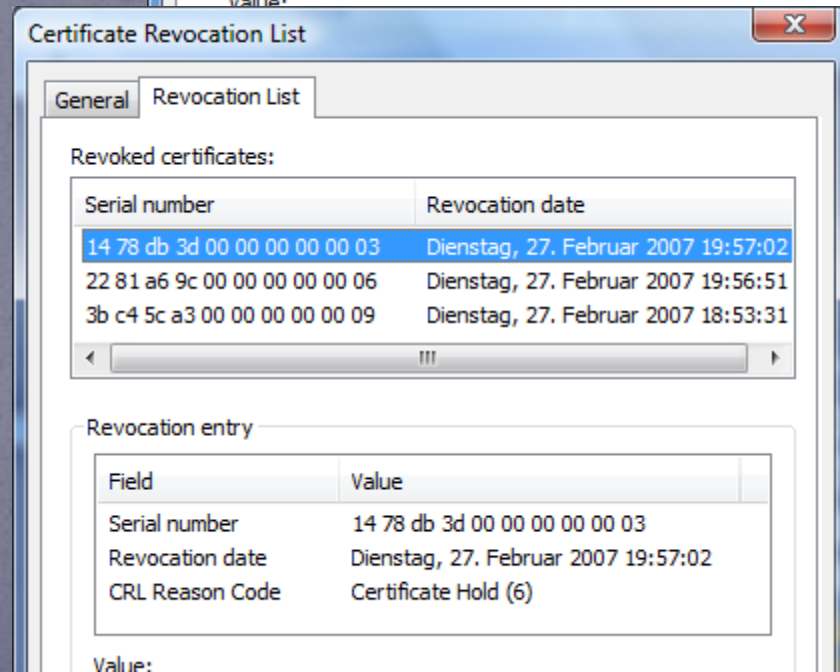
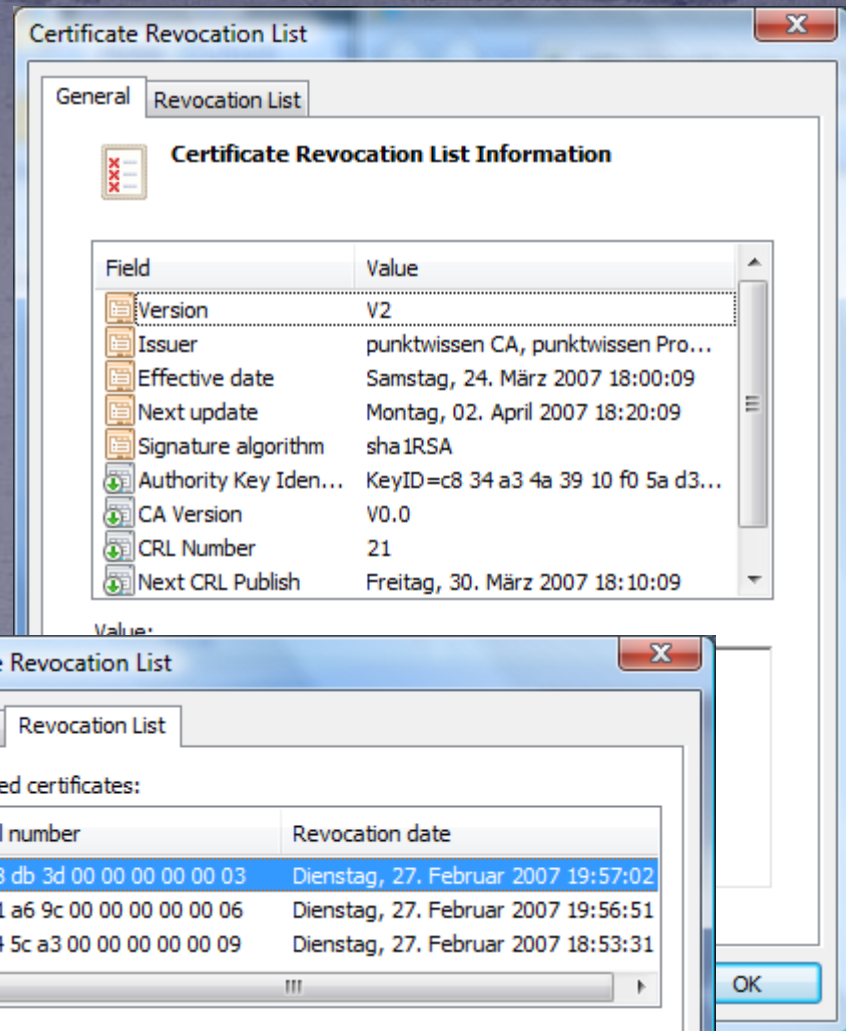
Challenge: Path Validation (cont'd)

- Validating the path is NOT the same as...
- Trust



Challenge: Revocation

- How can a license / passport be withdrawn when the document can be copied and spread over the whole world? → **Revocation services, revocation lists (black lists)**
- Revocation lists are cached
- Main source of PKI design and implementation errors



Challenge: Revocation (cont'd)

- ... and **optional attributes**
- Some applications do not check revocation at all
- Embedded URLs should tell relying parties where to find a revocation list

Certificate Details window showing basic fields:

Field	Value
Version	V3
Serial number	14 68 e7 80 00 00 00 00 02
Signature algorithm	sha1RSA
Issuer	punktwissen CA, punktwissen ...
Valid from	Mittwoch, 24. Jänner 2007 23...
Valid to	Donnerstag, 24. Jänner 2008 ...
Subject	elke@punktwissen.com, Elke S...
Public key	RSA (1024 Bits)

E = elke@punktwissen.com
CN = Elke Stangl | punktwissen
OU = IT Security and PKI Consulting
DC = universe
DC = everything

Certificate Details window showing advanced fields:

Field	Value
Certificate Template Name	User
Enhanced Key Usage	Encrypting File System (1.3.6...
Key Usage	Digital Signature, Key Encipher...
SMIME Capabilities	[1]SMIME Capability: Object I...
Subject Key Identifier	e1 2c 99 b2 bf 94 b0 0e 82 fb ...
Authority Key Identifier	KeyID=c8 34 a3 4a 39 10 f0 5...
CRL Distribution Points	[1]CRL Distribution Point: Distr...
Authority Information Access	[1]Authority Info Access: Acc...

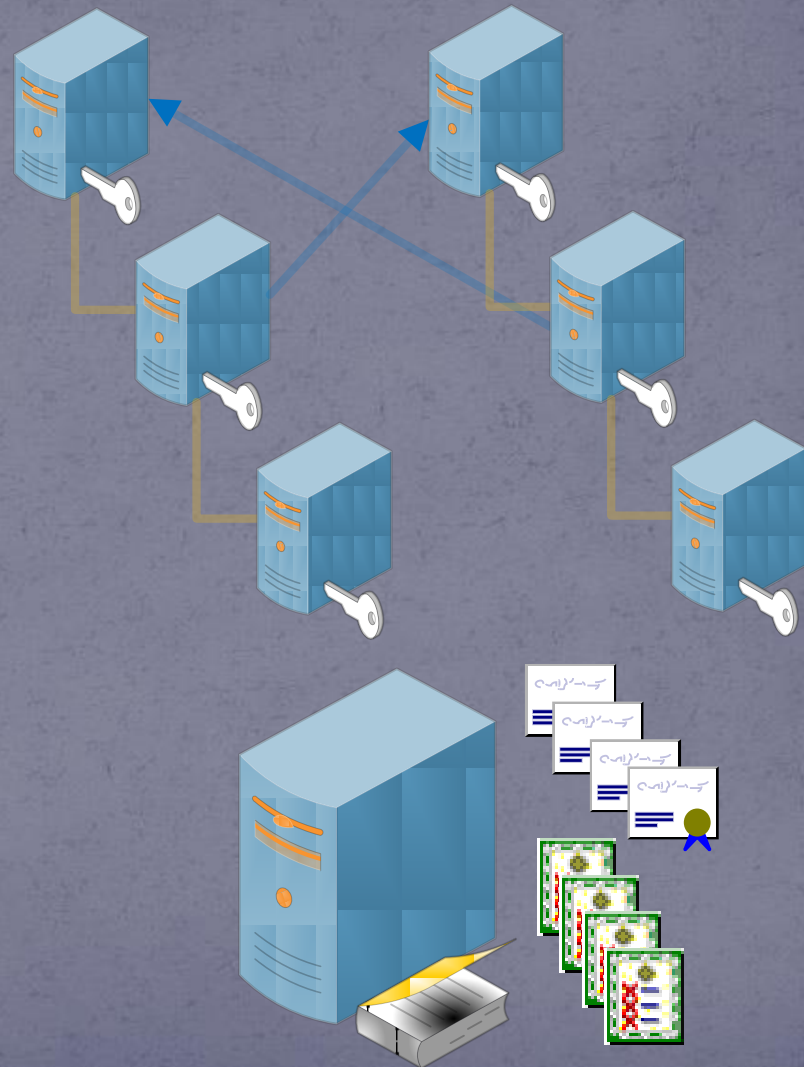
[1]CRL Distribution Point
Distribution Point Name:
Full Name:
URL=http://punktwissen.com/punktwissenCA.crl
URL=http://punktwissen/CertEnroll/punktwissenCA.crl

PKI is Based on Ancient Concepts

- **X.509** certificates and certificate revocation lists
- **LDAP** directories
- **RSA** public key cryptography
- (Disclaimer: There are new standards and concepts available as well: XrML certificates, OSCP, Elliptic Curve Cryptography)
- Compare to the change of using:
 - SMTP
 - HTTP
 - TCP/IP in general

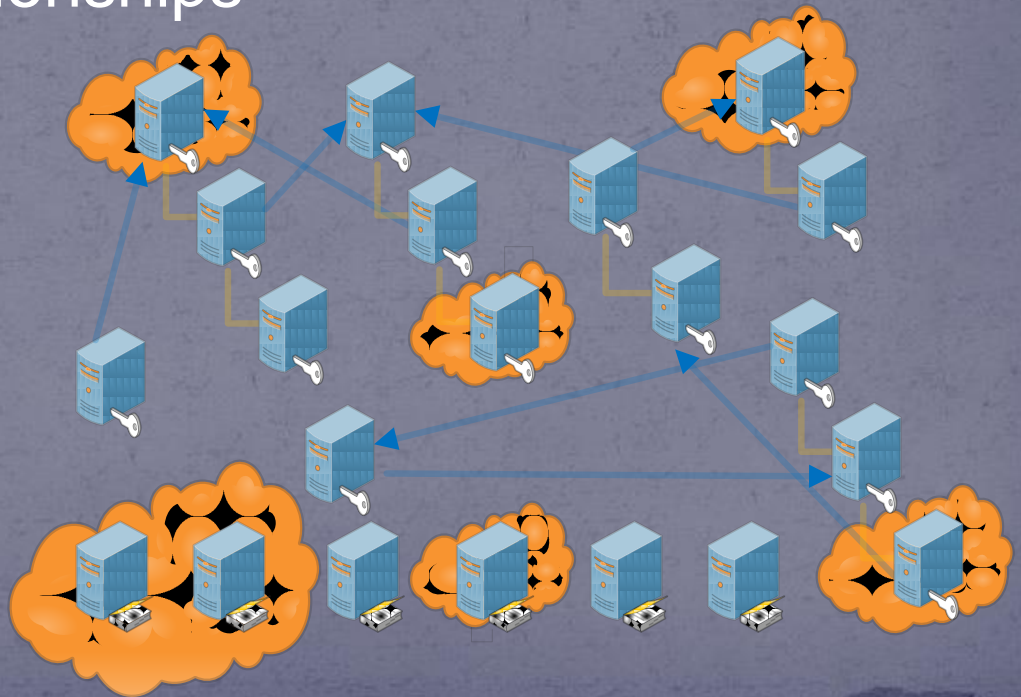
Built with a Simpler World in Mind

- Few hierarchies
- Less attributes
- Not used by "every application"
- Unique names.
Sample Issuer Name
in RFC3840
OU=NIST; O=gov;
C=US
- Few directories



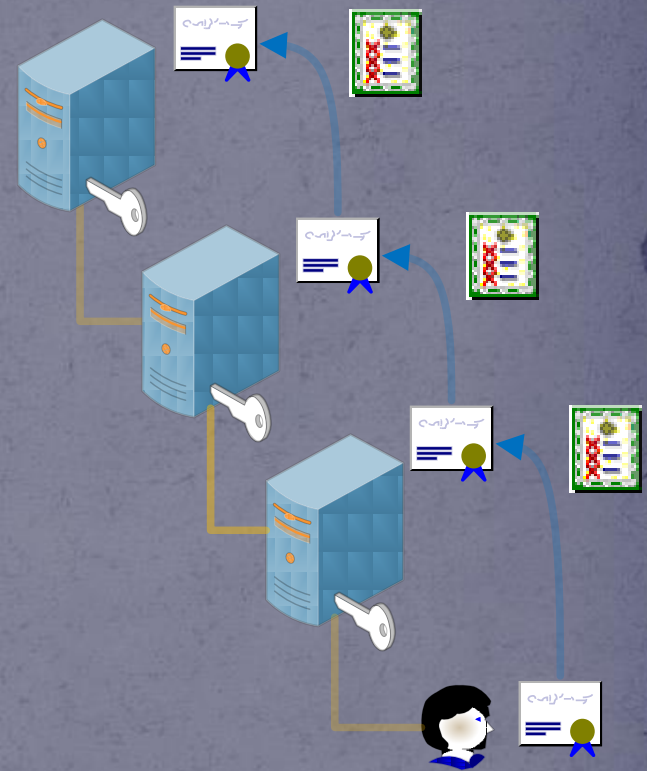
Usage in a Complex World

- "Every device has its certificate"
- Mobile users and devices
 - Each entity is member of different realms of trust
- Granular trust relationships
- Frequent changes



(Some) PKI Challenges

- X.509v3 support by applications: As you like it
- Path validation
 - Accessible repositories
 - Long-lived names
 - Processes for cert. distribution
- End-entity certificate lifecycle **management**
 - Issuance
 - Renewal
 - Revocation
- End-entity cert. may be stored in hardware – to be managed
- Careful design required taken into account each client's / app's peculiarities

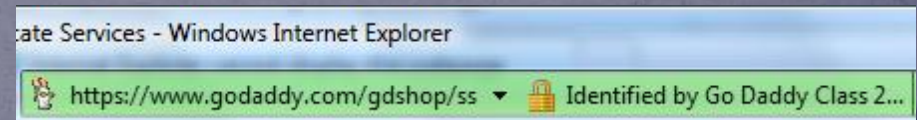


PKI Project Challenges

- Requirements of PKI clients may impact hierarchy design
 - Not all PKI clients are known at design time
 - Limitations are not known or not tested
- Involvement of lots of different departments
 - IT Operations
 - Legal
 - Development
 - Line of Business Application Owners
 - Helpdesk
 - ...

Secure Sockets Layer

- SSL: Everybody knows the yellow padlock
- New: Extended Value SSL certificates (Become green!)
- Mitigation of man-in-the-middle attack.
 - Ever heard of credit card fraud like that?
 - Other attack vectors are more popular
- Who cares about expired or untrusted SSL certificates or missing revocation information?



Network Protection by 802.1x



- 802.1x do not establish a connection unless user and/or machine are authenticated
- Goal: Keeping untrusted and infected PCs out of your network
- Does not protect from infected trusted PCs and users
- Renewal: Don't lock yourself out of the system!
- Revocation: Better disable the user/machine
- How to deploy machines at the user's desk?

Encryption

- Different requirements than for signature or authentication
- High-assurance signature keys must not be archived, encryption keys should be archived
- Recovery processes have to be carefully designed
 - What happens if an employees loses the key "at the end of the world"?
- Employees' private (?) data
- Disk, file, folder:
 - Are file names confidential?
- E-mail, SMIME: Server-side protection preferred:
 - Sealing at the post office, not at the desktop
- Sent e-mails are encrypted as well

PKI Operations Challenges

- It is more difficult than expected to assign a person to a task due in two years.
- Change management: "I need a certificate with <unusual extension X> for <application Y>"
- Helpdesk training: "I cannot connect to the network!"
- User loses his/her smartcard
 - User thinks that the card has been stolen
 - User detects that the card is still there
- Machine cannot access the network to renew the certificate because it does not have a valid certificate
- Delegation of administrative roles
 - Enrollment agents are powerful (create card to act on behalf of the Managing Director or the system administrator)
 - Do you have enough employees to staff all trusted PKI roles?

PKI Ambiguity

- Authentication versus authorization
- Many per-application certificates versus one multi-purpose certificate
- Huge identity management PKI versus specialized island-type PKI
- Seamless user experiences / part of networking infrastructure / no disturbing pop-ups versus notifying the users when something strange is going on
- Passport versus driver license

Fundamental Questions

- (lacking "right answers")
- Where should entities be authenticated?
- Where should entities be authorized?
- How many certificates should one entity have?
- Are certificates more sort of passport or sort of driver license?
- How are human beings going to check presented certificates? (Are they?)
- How are applications going to check presented certificates?