MÁV INFORMATIKA Ltd.

Building a Certificate Authority: Lessons Learned

Róbert Kisteleki, senior PKI consultant
kistelekir@mavinformatika.hu
http://www.mavinformatika.hu/

WWW2003 Budapest
2003/05/24

MÁV INFORMATIKA Kft.

Contents

- About MÁV INFORMATIKA Ltd.
- PKI CA projects
- Requirements for being a CA in Hungary
- Our implementation
- Thoughts about the Law
- Open questions
- Possible abuses – and remedies
- Conclusion

MÁV INFORMATIKA Ltd.

MÁV INFORMATIKA Ltd.:

- subsidiary of MÁV, the Hungarian State Railways
- founded in 1996 and still 100% owned by MÁV
- purpose: outsourcing IT services mainly for but not limited to MÁV
- more than 550 employees in Budapest and 6 more cities around Hungary
- income in 2002: EUR 20,000,000 (4,8 billion Ft)

MÁV INFORMATIKA Ltd.

MÁV INFORMATIKA Kft.

Company profile:

- outsourced IT services
- software development, system integration
- IT consultancy

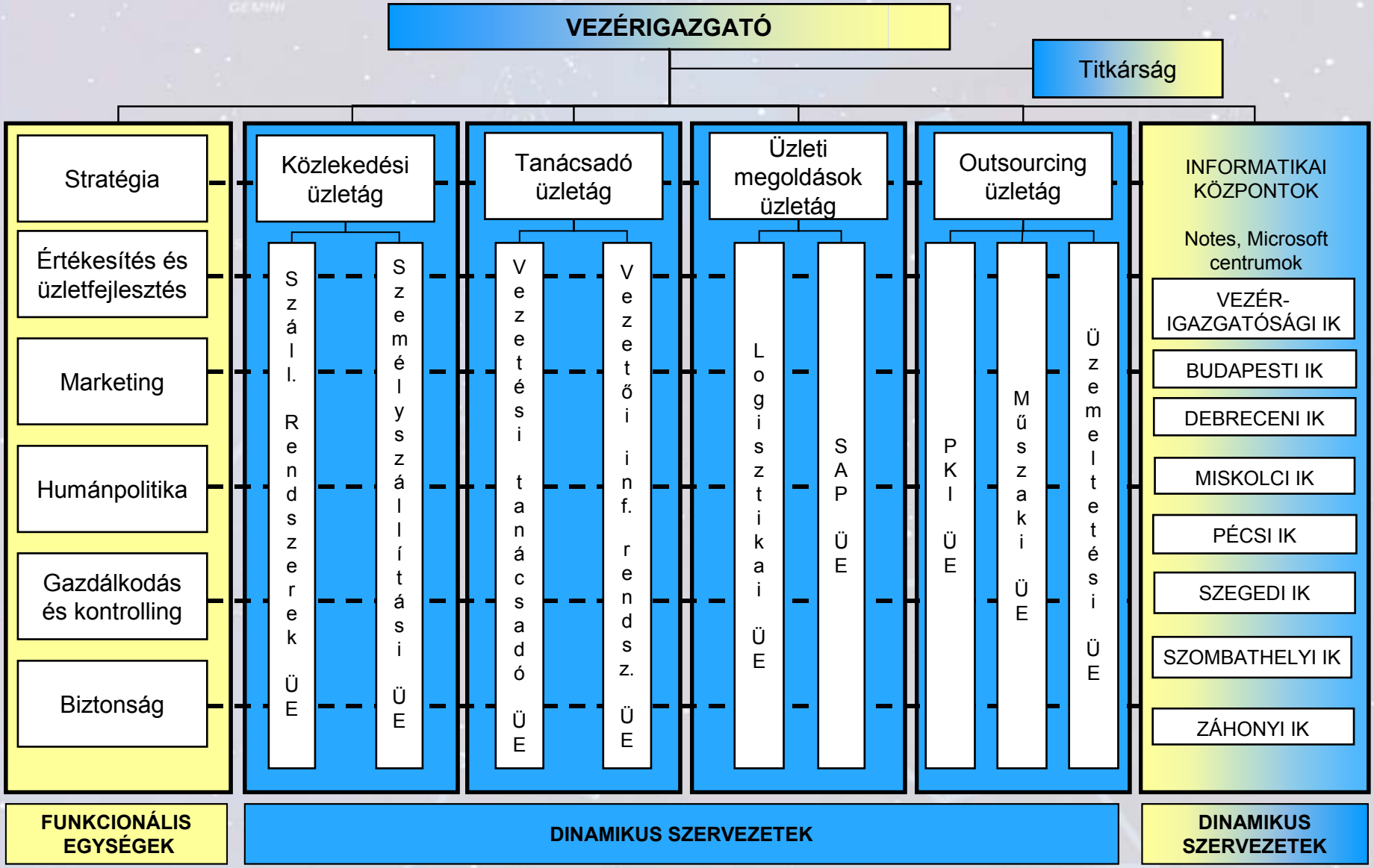
Market position*:

- 3rd largest IT outsourcing company in Hungary
- 4th largest software development company

*: according to: IDC, EITO-BBJ

MÁV INFORMATIKA Ltd.

MÁV INFORMATIKA Kft.



MÁV INFORMATIKA Kft.

MÁV INFORMATIKA Ltd.

IQNet

THE INTERNATIONAL CERTIFICATION NETWORK

CERTIFICATE

IQNet and MSZT

hereby certify that the organization

MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

H-1012 Budapest, Krisztina krt. 37/a.

for the following field of activities

IT consulting, system development and system integration, installation and operation of IT networks, outsourcing of IT systems, technical support and services, supply of IT products (EA scope: 33, 29)

has implemented and maintains a

Quality Management System

which fulfils the requirements of the following standard:

ISO 9001:2000

Issued on: 03-10-2001

Validity date: 21-09-2001 – 20-09-2004

Registration Number:

MSZT-503/0660-553

IQNet

Dr. Fabio Roversi
President of IQNet

Pónyai György
General Director of MSZT

Members of IQNet (registered association):

AENOR *Spain* AIB-Vincotte International *Belgium* APCER *Portugal* CQS *Czech Republic* CISQ *Italy* DQS *Germany* DS *Denmark* ELOT *Greece* FCAV *Brazil* FONDONORMA *Venezuela* HKQAA *Hong Kong* IRAM *Argentina* ICONTEC *Colombia* JQA *Japan* KEMA *Netherlands* KFQ *Korea* MSZT *Hungary* NCS *Norway* NSAI *Ireland* ÖQS *Austria* PCBC *Poland* PSB *Singapore* SFS *Finland* SII *Israel* SIQ *Slovenia* SQS *Switzerland*

IQNet is represented in the USA by the following IQNet members: AIB-Vincotte International, CISQ, DQS, KEMA, *and* NSAI

MINŐSÍTETT
N A T O
BESZÁLLÍTÁSRA
ALKALMAS

MSZT 1921

MAGYAR SZABVÁNYÜGYI TESTÜLET
HUNGARIAN STANDARDS INSTITUTION

Minőségirányítási Rendszer Tanúsítás
Quality Management System Certification

TANÚSÍTÁSI OKIRAT
CERTIFICATE

Tanúsítjuk, hogy a
We certify that the quality management system of

MÁV INFORMATIKA

Kereskedelmi, Szolgáltató és Tanácsadó Kft.

H-1012 Budapest, Krisztina krt. 37/a.

minőségirányítási rendszere megfelel a szabvány követelményeinek a következő alkalmazási területen,
termék/szolgáltatás előállítás (fő) folyamatai:
informatikai tanácsadás, rendszerfejlesztés és rendszerintegráció,
informatikai hálózatok építése és működtetése, informatikai rendszerek outsourcingja,
műszaki karbantartás és javítás, informatikai termékek értékesítése
has been registered as meeting the requirements of the scope of application,
product/service realization (basic) processes:
IT consulting, system development and system integration, installation and operation of IT networks, outsourcing of IT systems, technical support and services, supply of IT products

MSZ EN ISO 9001:2001 (ISO 9001:2000)

MSZT CERT

A tanúsítási okirat érvényes/ The certificate is valid:... **2001. 09. 21. – 2004. 09. 20.**

A tanúsítási okirat száma / Reg. number:..... **503/0660**

Budapest, ... **2001. október 3.**

Pónyai György
ügyvezető igazgató

IQNet

MÁV INFORMATIKA Ltd.

MÁV INFORMATIKA Kft.

Company culture

PKI CA projects

MÁV INFORMATIKA Kft.

PKI (CA) projects

PKI CA pilot project

- Started in December 2001, ended in June 2002
- Goal was to evaluate the possibilities for building a qualified CA in Hungary
- Ended successfully with a feasibility study as its output
- The real PKI CA project begun based on this feasibility study

MÁV INFORMATIKA Kft.

PKI (CA) projects

PKI CA project

- Started in September 2002, ends nowadays
- Selected PKI solution: Utimaco Safeguard PKI

Results:

- November 2002: MÁV INFORMATIKA Ltd. became an advanced level CA
- April 2003: MÁV INFORMATIKA Ltd. became a qualified level CA

Requirements to a CA

Requirements

Laws and rules

Hungarian Law XXXV/2001 (Digital Signature Law):

- **Conformant with the 1999/93/EC EESSI „Common Framework for Electronic Signature" Directive**
- **Creates a legal background for the usage of electronic signatures**
- **Specifies three levels of electronic signatures and two levels of Certificate Authorities („advanced" and „qualified")**
- **Mostly technology-independent**

Requirements

Laws and rules

Decree 16/2001 of the Minister of PM Office:

- **According to the DS Law it specifies all the requirements for Certification Authorities (especially qualified ones) and their services**
- **Details many financial, liability insurance, personnel, security, business continuity, logging, archiving, auditing, process and other related requirements**
- **Specifies the minimum contents of different CPSs**

MÁV INFORMATIKA Kft.

Requirements

Other standards, directives, regulations...

- 1999/93/EC Directive
- ITU X.509 PKI
- RFC2459 (X.509 PKI profiles)
- RFC3161 (TSS)
- RFC2527(CPS)
- ETSI TS 101 456 (CPS)
- USA NIST FIPS 140-1, 1,2,3,4 (HSM, …)
- CEN CWA 14167-1
- MSZ ISO/IEC 17799
- …

MÁV INFORMATIKA Kft.

Requirements

According to the regulations for advanced CAs:

- **Have to submit a CPS and General Terms to the Communications Authority (HÍF)**
- **These documents are only formally checked**

As of today, there are 5 advanced level CAs.

MÁV INFORMATIKA Kft.

Requirements

According to the regulations for qualified CAs:

- **Have to submit CPs, CPSs and General Terms to the Communications Authority (HÍF)**
- **All the details of these and the legal requirements are verified and audited by HÍF**
- **The auditing has to be renewed annually.**

As of today, there are 2 qualified level CAs.

Our implementation – Trust&Sign

Our implementation

Physical security

The most secure „Trust Center” is a separated computer room with:

- Concrete walls all around
- Multi level security
- ID card operated entrances with security doors
- Alarm system with motion detectors, video cameras
- Non-stop cooling and power supply
- Logged physical key handling, EMC protection

MÁV INFORMATIKA Kft.

Our implementation

Hardware architecture

- All components are at least duplicated
- Data storage is based on SAN (RAID 5)
- PKI key protection is done with HSMs (IBM 4758)
- Backups are encrypted, CD-R and DVD-R based
- Two independent high-speed Internet connections
- Hardware components: Compaq (HP), Sun, Cisco, others

MÁV INFORMATIKA Kft.

Our implementation

Software architecture

- Different OSs on different components (Windows 2K, Linux, Zorp OS, Solaris)
- Custom built HA software module for monitoring the components and switching to spares if necessary
- Logging firewalls (also HA)
- IDS components on different security levels
- All logs are preserved and audited for suspicious events

MÁV INFORMATIKA Kft.

Our implementation

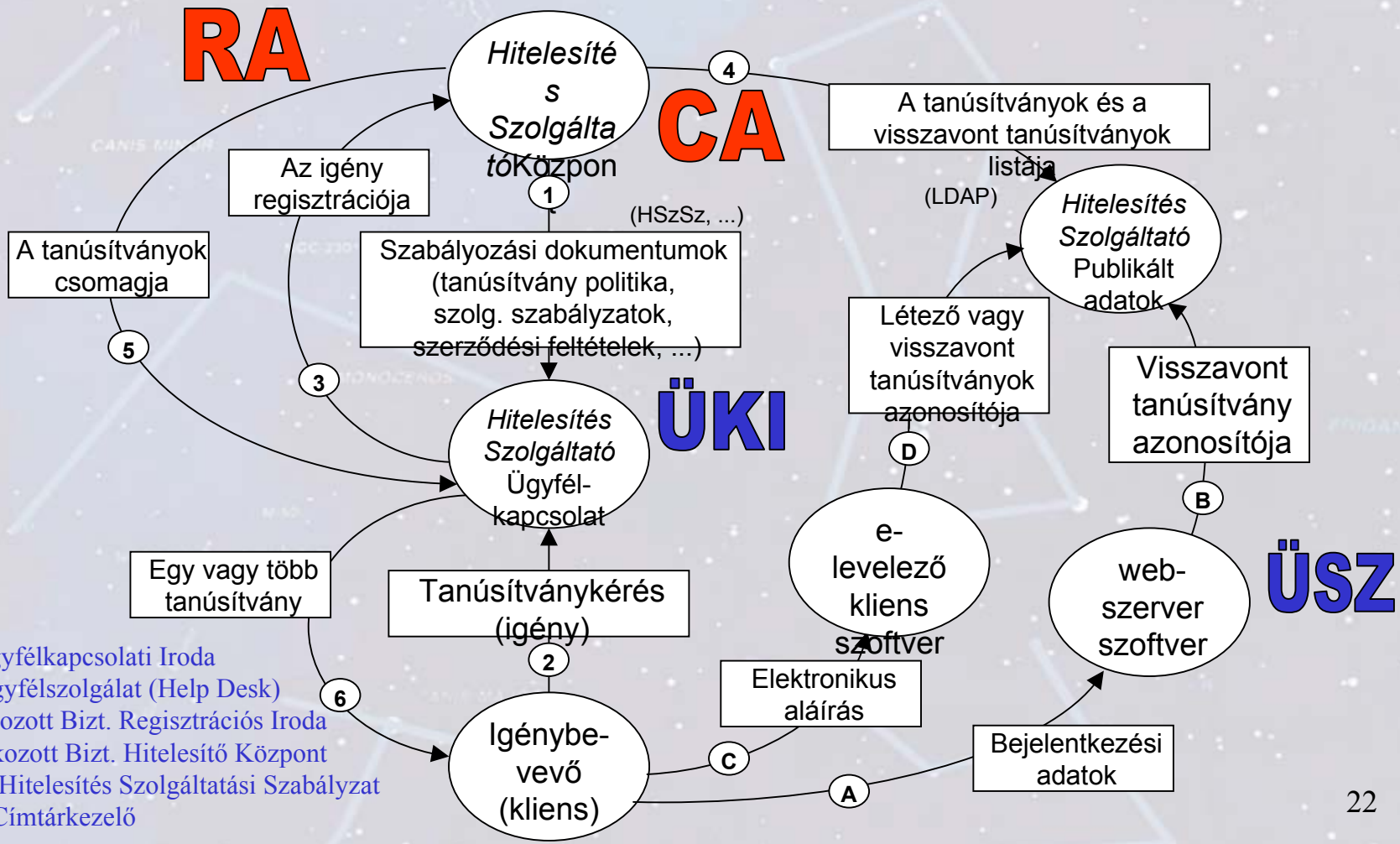
Employees in the service

- All managers, key guards, SOs, ROs, auditors, operators, customer care and help desk personnel, etc. have been working here for years
- The technology oriented people have PKI, firewall, OS, etc. certifications
- Customer care centers are planned in different cities around the country

Our implementation

MÁV INFORMATIKA Kft.

Established processes

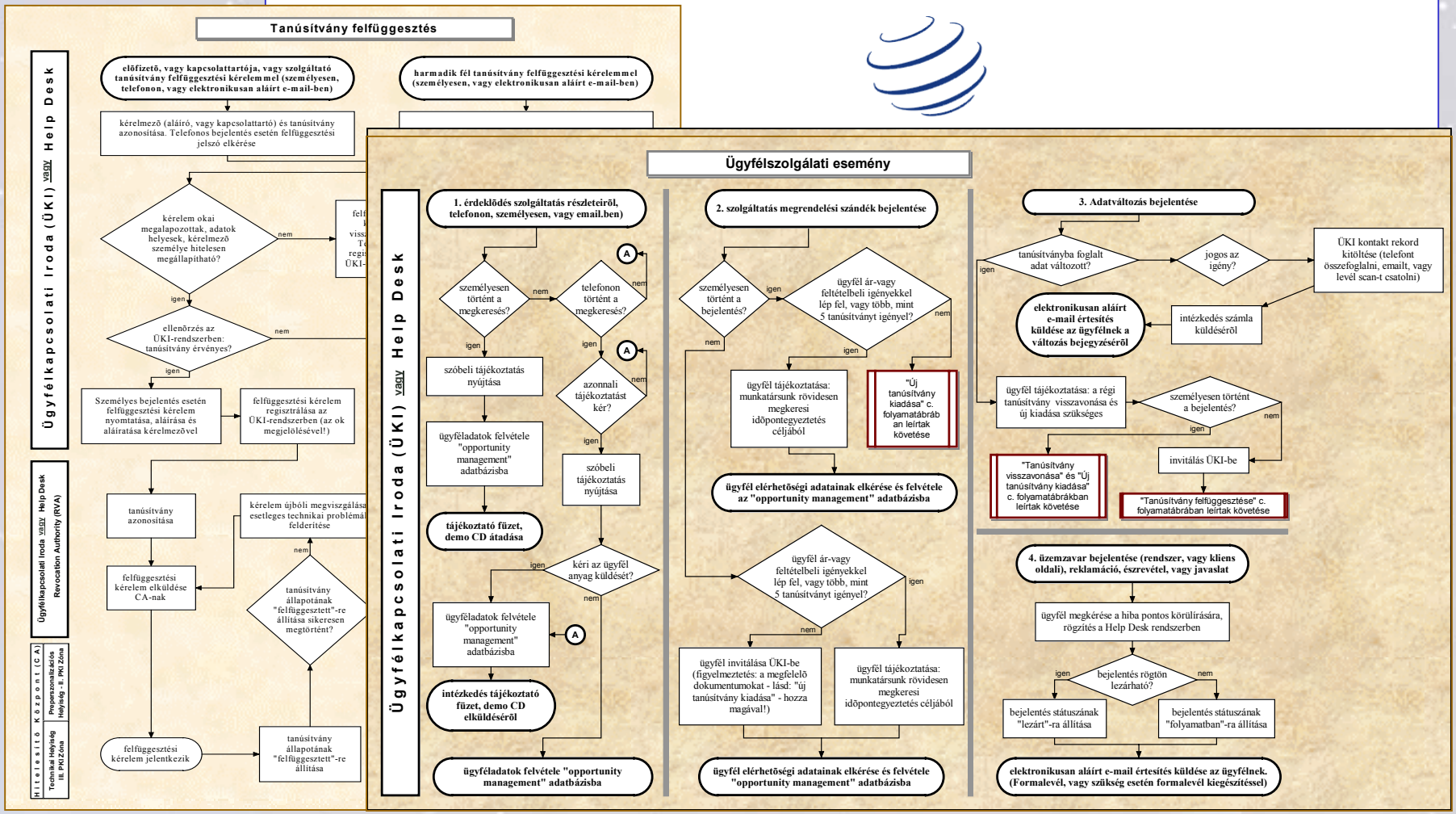


Jelölés:
ÜKI – Ügyfélkapcsolati Iroda
ÜSZ – Ügyfélszolgálat (Help Desk)
RA – Fokozott Bizt. Regisztrációs Iroda
CA -- Fokozott Bizt. Hitelesítő Központ
HSzSz -- Hitelesítés Szolgáltatási Szabályzat
LDAP – Címtárkezelő

MÁV INFORMATIKA Kft.

Our implementation

Established processes



MÁV INFORMATIKA Kft.

Our implementation

Financial background

- The regulation specifies strict criteria especially for insurance related questions
- The CA has to provide bank guarantee for expenses related to certain events specified in the Law

MÁV INFORMATIKA Kft.

Our implementation

Policies and statements

Public documents:

- CPS, CPs
- General Terms of Agreement
- Subscriber Contract
- Different price lists, white papers

MÁV INFORMATIKA Kft.

Our implementation

Policies and statements

Private documents:

- Various system architecture plans and documents
- Security Policy and Rules of Security Book
- Security Risk Analysis
- Book of Operations
- Business Continuity Plan
- Various company related documents and policies

Our implementation

Backup site

The regulation specifies mandatory installation of a backup site in case of an emergency event.

- All the primary site certificate data is transferred to this site to resume the operations when needed.
- The CA is able to construct all keys needed for issuing CRLs on the backup site – yet still securely.
- Backup site has an independent Internet connection.

MÁV INFORMATIKA Kft.

Our implementation

Client support

- Based on the company itself we provide provisioning all around the country
- The company itself is a software vendor, system integrator, and reseller of client software components, development toolkits
- We provide all the „boxed” client softwares provided by our partner, Utimaco Safeware AG.

MÁV INFORMATIKA Kft.

Our implementation

Client support

Personal Device

Cardman Family
SafeGuard Easy
SafeGuard PrivateCrypto
SafeGuard Advanced Security
…

Digital Transaction Security

SafeGuard PKI
SafeGuard Sign & Crypt for Outlook
SafeGuard Sign & Crypt for Office
SafeGuard Sign & Crypt for Notes
SafeGuard Sign & Crypt for SAP/R3
SafeGuard Sign & Crypt for Transaction Client
SafeGuard Sign & Crypt Signature Suite for PDF
SafeGuard Sign & Crypt for ToolKit
SafeGuard Sign & Crypt Signature Verifier

Some thoughts about the Law

Thoughts about the Law

Timestamping vs. Signatures

- No timestamp is needed to create an acceptable qualified digital signature
- The exact time when the signature was made is therefore not known.
- How to verify such a signature (especially against CRLs)?

Thoughts about the Law

Revocation vs. on hold

- „Certificates cannot be revoked retroactively.”
- What if a certificate is lost?
  - Put it on hold by phone „soon”, then
  - Revoke it „later”.
- But CRLs can contain certificates only once, only with one revocation reason!
- Revocation time will be „later”, not „soon”, so the timeframe between them will be lost.

MÁV INFORMATIKA Kft.

Thoughts about the Law

Encryption

- Digital encryption is not forbidden by law.
- But „The signature creation data can solely be used for creating signatures.”
- Is this national security or „practical advice”?
- Qualified signature creation devices can only contain the qualified certificate and key.
- It is very unlikely that users will use two cards in parallel for signing and encrypting...

Open questions

MÁV INFORMATIKA Kft.

Open questions

Signature creation devices

There is practically no „secure signature creation device” (BALE) today.

- Schlumberger’s Crystal has no CSP (yet)
- Oberthur’s AuthentIC applet is not certified (yet)

- Hardware Security Modules are not intended to be used by individuals.

Open questions

Signature creation devices continued

What to certify:

- Smartcard hardware - yes
- Smartcard applet - yes
- Smartcard CSP software – yes
- Smartcard reader - ?
- Smartcard reader driver - ?
- Signature software - yes
- User software - ?
- Operating system - ?
- PC hardware - ?

Open questions

Signature software

Do we need it?

- **There is no support for old hardware/software, nor will there be**
- **We have plug-ins for current software (e.g. Microsoft Office 97/2000/XP, Outlook, Lotus Notes 5)**
- **Future programs will probably have built-in electronic signature support**

MÁV INFORMATIKA Kft.

Open questions

„Know thy user”

- Certificates contain publicly available data, therefore no personal data (SSN, personal ID/number) is included.
- Do you know who the user really is? E.g. when:
  - opening bank accounts,
  - requesting a new passport on a governmental portal
  - loyalty systems
  - etc.
- Same situation with company officials.

MÁV INFORMATIKA Kft.

Open questions

Missing „national CP”

- CAs write their own CPs and conforming CPSs
- There is no common, country-wide accepted CP to conform to, only a recommended structure
- Users will have to know a number of CPs/CPSs to accept certificates from different CAs

- We look forward to a number of issues when (if) a „national CP” is set up.

Open questions

CAs that should be trusted by a user

Number of built-in CA certificates:

- Internet Explorer 6 (Outlook, etc.): 109
- Opera 7.1: 51

Number that should be built-in according to Law in Hungary:

- Advanced level: 5
- Qualified level: 2

Estimation: at least 90% of users will not change the default installed CA settings.

Open questions

CAs that should be trusted by a user - continued

How will this change? – cross certification

- HÍF is thinking about setting up a national root CA
- Hungary is joining the EU in May 2004: what other EU based CAs should be accepted?

Other soulutions generally not supported by today's client software:

- Bridge CA concept (US DoD)
- Gatekeeper (Australian government policy)
- etc.

MÁV INFORMATIKA Kft.

Open questions

Practical usage of qualified certificates

- Qualified certificates can only be issued to and used by existing individuals.
- Most „important stuff” (e.g. invoices, scanned archives) are required have timestamp and qualified digital signature to be legally valid.
- Normally this means that some human „biorobots” will have to sign all these documents...?
- If you give your signature creation data (private key) to a machine, you also give away the responsibility...

Open questions

CRL handling

Fact: CRLs are produced periodically and sometimes on demand, depending on the CA policy.

- Do you accept a signature if a certificate is not on the current CRL?

- Are you sure?

- How does automatic software verification know this?

- CRLs could be huge… (look at Verisign's)

One solution: OCSP, which costs money per transaction in almost all cases (software vendors).

Possible abuses – and remedies

Possible abuses – and remedies

The font attack

What can Alice do if she wants to sign a contract of $9 with Bob, but Bob only agrees to $2?

- One evening Alice secretly changes Bob's favorite TrueType font to another that looks the same, only „9"-s show up as „1"-s.
- Next day Bob get the $9 contract, happily signs it since he can see it showing up as $1.
- In the evening Alice restores the original font.

No one will be able to prove the hack later, but Alice will have the $9 contract...

MÁV INFORMATIKA Kft.

Possible abuses – and remedies

Question: What You See Is What You Sign?

Macros, trojan horses, buggy software can show you one document and sign another.

A „secure signature device” should be able to:

- Show the document to be signed – has a display
- Ask for the signature creation data – has a reader
- Ask for the PIN code – has a keyboard
- Create the signature – has hardware/software in it

Today the device that has this functionality is ... a computer (PC?).

MÁV INFORMATIKA Kft.

Possible abuses – and remedies

Ask for the PIN code

It is not enough to ask for the PIN code only when you insert the smart card! (start a „session”)

- **If the PIN is not asked for every time a signature is made, a background process can sign any document without the user’s knowledge.**

But the sessions should not be too short either...

- **Web based solutions would not work if the user had to enter the PIN every time he/she clicks on a link.**

Possible abuses – and remedies

Non secure components

Using a non secure OS can lead to abuses.

- One can steal PIN codes if he/she can change the keyboard driver to a „patched” one or can install a sniffer.

Using non secure drivers can lead to abuses.

- E.g. the same PIN code can be stealed from the smart card communication if that is not secured.

Possible abuses – and remedies

Remedies

The previous ones were only a few from a few dozen anomalies (challenges) known so far.

A good signature hardware/software closes these holes (i.e. it uses secure communication all the time, it has built-in fonts, it should be aware of the usage context, etc.)

Conclusion

- Building up a reliable CA requires a lot of effort, most of what is not technology related.
- Building a qualified CA needs even more resources.
- Technology is not yet close enough to:
  - Legal issues
  - Practical uses
- Serious applications require strict hardware / software solutions to avoid abuses.

MÁV INFORMATIKA Kft.

End

Róbert Kisteleki

Senior PKI consultant

MÁV INFORMATIKA Ltd.

kistelekir@mavinformatika.hu

http://www.mavinformatika.hu/