

Long-term archiving of electronically signed documents in Hungary

Dr. István Zsolt BERTA, PhD, MBA, CISA
Microsec Ltd.
HUNGARY

istvan.bertha@microsec.hu
www.e-szigno.hu

Microsec Ltd.

- Founded in 1984, owned by six Hungarian individuals
- IT service provider of the Ministry of Justice (from 1990)
- Certification authority and time stamping authority (from 2002), issuing qualified certificates and timestamps (from 2005)
- We developed an application for the creation and verification of XAdES electronic signatures (e-Szignó)
- We provide long-term archiving service for electronically signed documents (from 2007)

Hungarian law on electronic signatures

- It is based on EC directive 1999/93
- Defines four 'electronic signature related services':
 - issuance of digital certificates,
 - issuance of signature creation devices,
 - time stamping,
 - long-term archiving.
- Providers of each service can 'qualified' or 'non-qualified'.
- Qualified service providers are supervised by the National Communications Authority
- Qualified signatures are assumed to be created by the signatory unless the opposite is proven
- Signatures archived by a 'qualified' long-term archiving service provider are assumed to be valid unless the opposite is proven
- It does not cover other aspects of PKI (encryption, authentication)

The situation of PKI in Hungary

- Four commercial certificate authorities issue qualified certificates and timestamps
- One long-term archiving service provider (Microsec Ltd.)
- The Hungarian public administration has a dedicated root CA for public administration purposes only
- Regulations for e-signatures within the public administration: certificate profile, certificate policy, signature format (XAdES)
- Very few PKI applications in the public administration
- Hardly any e-billing applications due to awkward and/or conflicting (accounting ↔ e-signature) regulations
- Promising applications in the Hungarian jurisdiction...

Electronic firm registry system

Firm registry in Hungary

- The Hungarian firm registry is maintained by registry courts.
- Lawyers represent companies at registry courts (e.g. when founding a company)
- Registry courts communicate with other organizations (Tax Authority, Central Statistical Office, banks, etc.)

Electronic firm registry procedures

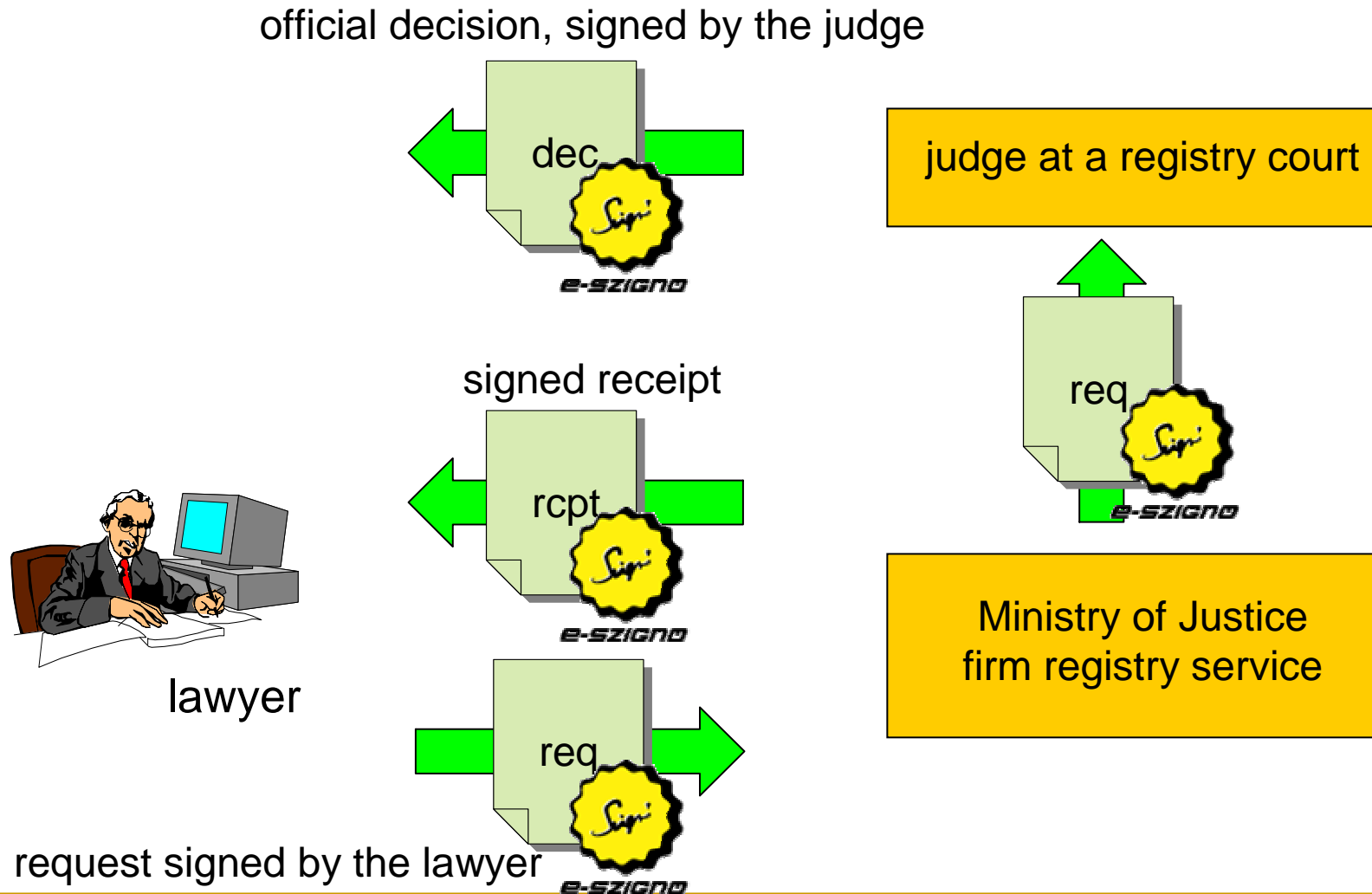
- From September 2005, lawyers are allowed to submit firm registry requests with qualified signatures to the registry courts.
- Such a request is an e-dossier containing:
 - the request in an XML form,
 - scanned documents of the firm with scanned handwritten signatures,
 - electronic document with the electronic signature of the lawyer's client (very rare case),
 - electronically signed statements from the Hungarian Treasury claiming that the necessary fees were paid,
 - the entire e-dossier is signed with the lawyer's qualified electronic signature.

A signed request

The screenshot shows the MICROSEC e-Szignó application interface. The title bar reads "MICROSEC e-Szignó". The menu bar includes "E-akta", "Dokumentum", "Aláírás", "Ellenőrzés", "Átvételi elismervény", "Eszközök", and "Segítség". The toolbar contains various icons for document management and navigation. The main window is titled "e-Cégeljárás" and displays a folder view of "Változás bejegyzési kérelem". The selected item is "A változás bejegyzési kérelem e-akta adatlapja", which is highlighted in blue. Below the folder view, a table displays the metadata of the selected document.

Mező	Tartalom
E-akta címe	Változás bejegyzési kérelem
E-akta típusa	elektronikus akta
Létrehozás időpontja	2006. nov. 7. 14:20:29
Cég elnevezése	AMEROPTIK Optikai Cikkeket Forgalmazó Betéti Társaság
Cég székhelye	1118 Budapest, Beregszász köz 3.
Cégjegyzékszám	01-06-311798

Electronic firm registry procedures (2)



What do lawyers need for using it?

- A computer,
- Internet access, e-mail address,
- a scanner,
- a smart card (SSCD) and a qualified certificate,
- access to a time stamping service,
- a signature creation application for creating XAdES-T signatures,
- a permission from the Hungarian Bar Association.

Organizations connected to the system

- Organizations connected to the system include:
 - Tax Authority (e.g. tax numbers are acquired automatically, notification on forcible collection, etc.)
 - Central Statistical Office (statistical numbers are acquired automatically)
 - Hungarian Treasury (electronically signed verifications on the payment of fees)
 - All banks and financial institutions (a company's account number is automatically reported to the firm registry)
 - ...
- Communication with these organizations is based on (advanced) electronic signatures.
- These messages are created and processed by machines (except for the case of some smaller financial institutions).

Benefits of the electronic registry system

- The process became much faster
 - data is entered only once,
 - in the electronic system, certain requests must be processed in 2 days (30 days in the paper-based case)
- For lawyers:
 - No queuing, open 24 hours a day
 - Significantly less fees
 - Submitting 3 or 4 requests a year electronically already covers the cost of the qualified electronic signature.
- It is expected that the use of this electronic system for firm registry requests shall become mandatory from 2008.

Problems

- There are problems with third parties (banks, other authorities) accepting the official decisions in an electronic form (with the qualified electronic signature of a judge).
- Some registry courts print the electronic documents for working.

In numbers...

- Currently 400 lawyers participate in the system (out of the 2-3000 lawyers who deal with company registration)
- 2000 electronic requests arrive monthly (out of 16000), it was less than 200 a year ago

The role of Microsec

- We developed and we operate the systems in the Ministry of Justice and at the registry courts.
- We developed and operate the software that other organizations user for interfacing with the system.
- We developed the signature creation applications.
- We supplied most lawyers with smart cards, certificates and we provide most of them with time stamping service.

Electronic signing and archiving at Hungarian notaries

Notaries and electronic signatures

- From 2006, all Hungarian notaries (and vice-notaries) are capable of creating qualified electronic signatures.
- Each Hungarian notary (and vice-notary) has:
 - a smart card (SSCD),
 - a qualified certificate,
 - access to time stamping and OCSP services,
 - a signature creation application (e-Szignó)
- Notaries are capable of creating archive electronic signatures (XAdES-A format, using OCSP)

Why is long-term archiving necessary?

- An electronic signature is a mathematical transformation. This transformation is 'easy' with a private key, it is 'hard' without it.
- PKI provides means for proving that the private key was in possession of the right person at the time of signing.
- The validity of an electronic signature may become improvable if:
 - the time of signing is not known (i.e. the signature is not time stamped),
 - the certificate of the TSA expires,
 - the certificate of the TSA gets revoked, or
 - an algorithm used for signing or time stamping becomes insecure.
- This problem can be solved by placing additional time stamps (with a different TSA key or with different technology) on signed documents.

Long-term archiving at notaries

- All notarial deeds are signed with the qualified signature of the notary;
- The e-dossiers containing the signed deeds are archived in a (qualified) long-term archive;
- Paper-based notarial deeds are scanned, signed by notary and sent into our long-term archive;
- Electronic notarial deeds (there are very few of them yet) are directly sent into our long-term archive.
- Current legislation allows a notary to access the documents archived from the same office only; this may change in the future.

The long-term archiving service of Microsec

- Signed documents are submitted (and later accessed) through an SSL connection.
- Our long-term archiving service is based on the principles of the 'LTANS' IETF working group.
- Encrypted documents are stored, they can be decrypted with the decryption key of corresponding notarial offices and by the archiving service (this latter is a very rare event).
- Our archiving service time stamps archived signatures regularly (or when necessary) and thus guarantees the long-term validity of electronic signatures.
- Archived documents contain PDFs.
- The long-term archiving service retains tools for displaying the PDFs exactly the same way even after a long period of time.

The role of Microsec

- We supplied all notaries with SSCD smart cards and qualified certificates.
- We provide them with time stamping and OCSP services.
- We provide them the necessary signature creation applications.
- We provide the long-term archiving service.

Summary

- There are certain applications in the Hungarian jurisdiction, where electronic signatures are successfully used.
- In the Hungarian firm registry system, companies can be registered in a purely electronic way, using qualified electronic signatures.
- Hungarian notaries use qualified electronic signatures for the long-term archiving of notarial deeds.
- Microsec Ltd. provided most of the software, hardware and the PKI services for these applications.

Long-term archiving of electronically signed documents in Hungary

Dr. István Zsolt BERTA, PhD, MBA, CISA
Microsec Ltd.
HUNGARY

istvan.bertha@microsec.hu
www.e-szigno.hu