

# Developing interoperable e-government solutions in Hungary

Csaba Krasznay, Áron Szabó  
*Budapest University of Technology and Economics*  
*Centre of Information Technology*  
*Magyar tudósok körútja 2.*  
*H-1117, Budapest, Hungary*  
*krasznay@ik.bme.hu, aron@ik.bme.hu*

## Abstract

*In 2005 we presented the Hungarian Electronic Public Administration Interoperability Framework on the eGOV INTEROP'05 Conference. In this paper we show the activities leading toward the realization of this project. We describe the legal background, the cooperation between governmental, private and educational parties and a case study of an interoperability test between electronic signature applications. In the last part we explain the future possibilities in the field of e-governmental interoperability.*

## 1. Introduction

The Hungarian Parliament accepted the Act CXL of 2004 on the general regulation of the administrative authority process and services in December, 2004. This law fundamentally changes the operation of public administration. Its 10<sup>th</sup> section defines the rules of electronic administration and the services of public authorities.

## 2. Act CXL of 2004 on the general regulation of the administrative authority process and services

The basic rule is that public authorities must use electronic administration in official cases besides the traditional way. Citizens can submit official electronic documents to the authorities by signing them with at least advanced electronic signature. For those citizens who do not have electronic signature, the central government service provides the possibility of electronic administration. This service is the "Client gate" on the Government Portal, [www.magyarorszag.hu](http://www.magyarorszag.hu).

Citizens have to acquire a username and password to the client gate. They must visit to the office of their local authority with their identity card and fill out a form. This procedure ensures the personal appearance. If the citizen has qualified signature this kind of personal appearance is unnecessary. In both methods the user should give a valid e-mail address for later communication. The username is valid for 5 years.

If the registration is successful, the citizen will be able to get into contact with governmental and local authorities. After the acceptance of official documents, the authority must send an automatic reply to the citizen. They have 3 days to determine that the provided document meets the legal requirements. If everything is in the right form, the authority determines the obligation to pay. If this process is not free of charge the citizen has 8 days to pay.

Electronic administration is possible in the following areas:

- request of appeal and its attachments
- request of judicial assistance
- completion of documents
- inspection of the documents of an official procedure
- summoning
- any submissions of a citizen to the authorities
- information from the authority to the citizen
- etc.

## 3. Executive orders of the Regulation

The Ministry of Informatics and Communications published 5 executive orders in connection with the Regulation. These define the detailed rules of electronic administration, the requirements of certification authorities, electronic signatures and certificates, the

security and interoperability of IT systems, the replication of paper documents to electronic form and the technical requirements of electronic documents in the electronic administration.

The 193/2005. (IX. 22.) governmental regulation is about the detailed rules of electronic administration. Its main purpose is the establishment of various types of communication between the government and the citizen (one-way or asynchronous communication). It defines the general rules of identification. We can also find the rules of registration here. A new concept in the Hungarian legal system is the mutual identification. This states that the advanced or qualified certificate is not enough for the identification. The citizen should fill out a form with his personal data and then sign it with his electronic signature. Then the authority sends the citizen's certificate and personal data to the certification authority to verify that the personal data and the certificate belong together. The regulation also defines the management of electronic submissions (acceptance, delivery, link up of traditional and electronic administration and payment).

The 194/2005. (IX. 22.) governmental regulation deals with the questions of electronic signatures in public procedures. It extends the strictness of the Hungarian e-signature law. It decrees the establishment of a governmental root certification authority to over certify the current CAs. Citizens can only use their certificates in public procedures if they meet the requirements of this regulation. It also regulates the usage of electronic signatures for public servants and authorities.

The 13/2005. (X. 27.) ministerial order defines the rules of the replication of paper based documents into electronic format. The electronic copy must contain the following metadata:

- name of the paper based document
- physical parameters of the original document
- name of the organization and person who made the copy
- name and version of the replication system and policy
- time of the replication
- validity time

An authentic copy shall contain at least an advanced electronic signature and a timestamp.

The 12/2005. (X. 27.) ministerial order defines the detailed technical rules of document formats in public procedures. It enumerates many common document standards, e.g. PDF, RTF. According to the order this

short list can be widened in a special register. Public authorities must accept those documents which are mentioned in this list.

Possibly the most interesting governmental regulation is the 195/2005. (IX. 22.) about the security and interoperability of IT systems. It orders the conscious design of IT systems. Authorities shall initiate quality management process for effective operation. They must create a detailed documentation about their IT system and a risk assessment to ensure the satisfying design. There are some security classes for the procedural actions. The authorities must use these classes based on a future recommendation. Security classes depend on the local policies. There is a possibility to outsource the IT security procedures. Of course the outsourcing company must comply for some regulation. Public organizations shall use a proper access control system both in the backend and the front-end systems. Adequate logging system is also a must as well as a backup and archiving system. They must care about the security of data transmission.

Interoperability is also an important part of this regulation. It orders to strive for interoperability in the design and implementation phase. Authorities should take the standards into consideration especially the open and international standards.

#### **4. Technical recommendations**

The Ministry of Informatics and Communications also published some technical recommendations to ensure interoperability in the public procedures. These recommendations deal with the format of electronic signatures, electronic signature policies, certificate policies, the structure of certificates; timestamps; mutual identification and the interoperability standards catalogue.

Most of these recommendations are developed with the help of international standards. The recommendation about the format of electronic signatures was developed by an independent association with the support of the Ministry. The members of Hungarian Association for Electronic Signatures (MELASZ) formed a workgroup to make an interoperable e-signature format. This workgroup contained the most significant Hungarian application developers who have a solution for this field. Their agreement was converted to the official recommendation.

## 5. Interoperability test

One of the technological conditions of widespread usage of electronic signatures is interoperable functioning. The structure of acceptable signatures that is based on web technology is written down in the XML electronic signature standards ([1], [2], [3]) which are necessary (but not sufficient) to provide interoperability. The way that several applications function, the service providers and the development kits can raise other matters.

These points have been identified by the international standardization bodies such as IETF (Internet Engineering Task Force) and W3C (World Wide Web Consortium) that organized the first independent tests of XML electronic signature creation and verification applications. The tested applications were based on XMLDSIG ([1], [2]) standard, and the work lasted in several rounds from the March of 2000 to the April of 2004.

<http://www.w3.org/Signature/2001/04/05-xmldsig-interop.html>

The XMLDSIG standard has soon come into the center of interest at ETSI (European Telecommunications Standards Institute) which is one of the standardization bodies of the European Union. The Directive issued in 1999 has provided the legal background of usage of electronic signatures, though the technological conditions were given from the '70s. Experts of ETSI extended the XMLDSIG ([1], [2]) standard to fit to the legal environment thus the XAdES ([3]) standard has been born.

*The XAdES-BES satisfies the legal requirements for electronic signatures as defined in the European Directive on electronic signatures.*

/source: [3]/

Applications based on XAdES ([3]) standard are more complex and lifelike therefore more interoperability questions could have been raised. Experts of ETSI have organized several plugtest events between the November of 2003 and the October of 2004 to examine interoperability of applications. Experiences of these plugtests initiated the correction, extension of XAdES standard ([3]).

<http://www.etsi.org/plugtests/History/History.htm>

In Hungary several developments have been started to provide services to information society where security matters are critical. The goals of eEurope 2005 Action

Plan have been highlighted in the development of electronic government solutions (12 + 8 public services), where interoperability is a common requirement.

*Interoperability. [...] It will be based on open standards and encourage the use of open source software.*

/source: [4]/

In Hungary the Act CXL of 2004 on the general regulation of the administrative authority process and services has come into effect on the 1st of November of 2005 thus the interoperable, standardized technological support must be implemented to provide electronic services.

Hungarian experts of electronic signatures congregated in MELASZ have also decided to work out a methodology and organize an interoperability test to software developers of electronic signature creation and verification applications and service providers. The document of signature structure requirements was discussed on several meetings of MELASZ members, where the related standards have been read through and have been extended with comments, refinements. These interoperability requirements have been published as guidelines for software developers (it will be freely available both in English and Hungarian at the website of MELASZ). The official name of this project is MELASZ-Ready.

Interoperability, standardized functioning are elemental requirements of IT security. With applications that are not interoperable, it can happen that users get different output from different solutions to the same input. These differences can mean that whether the electronic signature is acceptable or not, the certificate is good or revoked or at other field of IT security the accessibility of a confidential document is authorized or not. There are several aspects of examining conformance to IT security requirements of an application. An electronic signature creation and verification application should be tested based on interoperability and also on the Hungarian schema of Common Criteria (MIBÉTS) methodology. These two tests complement each other, the differences can be demonstrated by a simple example: MIBÉTS test examines whether the cryptographic strength of SHA-1 hash algorithm is still good enough or shall SHA-256, SHA-512 be used, and that is an interoperability matter whether the SHA-1 is implemented well and meet the requirements of the standard.

MELASZ and the laboratory of Centre of Information Technology of BME (Budapest University of

Technology and Economics) held the first interoperability test on electronic signature creation and verification applications between the 1st of October of 2005 and the 15th of November of 2005. Five software developers participated on the first test and all of them had to fully comply with the requirements of the three-rounded event.

At the first round of the interoperability test XML processing (such as canonicalization, parsing) have been tested. As it was noticed by IETF and W3C interoperability problems can occur at this level, some functions of software developer kits had to be reviewed. Some test input file (based on C14N canonicalization standard of W3C) have been created and sent to participants to generate output. These outputs were examined at bit-level in the first period of test. The W3C standard in connection with canonicalization contains some example to demonstrate the canonicalization rules but these are just on character-level and not bit-level. In half of the cases there were problems with handling of white space characters, especially with end-of-lines (Carriage return and Line feed). On the other hand C14N functions had problems with the canonicalization of a subset of the nodes. At these cases functions could not handle well namespaces, could not get xmlns elements from parent nodes. These differences resulted different strings as input to the hash functions that provided different hash values, therefore C14N problems had to be eliminated in order to keep interoperability.

The second round of interoperability test contained the schema validation. Participants had to create a sample electronic signature file that has been examined in the laboratory by assigning XMLDSIG ([1], [2]) and XAdES ([3]) schema to them. Well-formedness and schema validity are also elemental requirements of interoperability. It can be say, that the best way to keep interoperability is to create electronic signatures that contains every element that are allowed in the standard (even optional elements), and at verification the application should use just the mandatory elements (because optional elements are not necessarily present). During the schema validity optional and mandatory elements should have also been examined whether they comply with definitions written down in related standards and MELASZ documentations.

After the first two rounds, participants installed their product on the computers of the laboratory. The final and also the greatest step was to examine face-to-face functioning: one application generated an electronic signature which was verified by another one. Results, error messages have been noted down into the test-matrix and sent back to developers who corrected the problems.

At the end of the iterative testing most of the interoperability problems have been solved which means that at given conditions that are laid down in MELASZ document these applications can communicate with each other and provide interoperable solutions. At the public administration and electronic government solutions legal requirements meet the technological requirements of modified XAdES-C (and in a long-term, XAdES-A), therefore the interoperability test focused to this format. Electronic signatures must contain timestamps, signing certificates, CA certificates and CRLs or OCSP responses that have been issued after signing time, and grace period. The structure must follow enveloping signature format. In most cases errors of verifications were based on the different logic of functioning such as using Id attributes of tags to find referenced elements, or not including root CA (just intermediate CA) certificates into the structure. Some errors were independent from software developers, but could cause serious problems in functioning such as getting subject or issuer names from certificates (these strings or arrays were represented differently on different platforms, environments). These kinds of problems must have been solved by omitting these data during verification processes.

Based on the success of the first interoperability test others could follow this event. The coverage of examination of electronic signature, electronic government related activities, solutions, standards should be extended by testing devices (e. g. smart cards of public administration), interoperable messages (e. g. working out XML schemas to every message sent in the public administration) or more complex electronic signatures (e. g. electronic archiving of documents, electronic invoices by using XAdES-A electronic signatures).

## 6. Future possibilities

We can see that it is impossible to expect all of these requirements from public authorities. The Ministry states that they will make a call for tenders for the implementation of secure and interoperable e-government systems. They will buy some core applications and distribute it to different authorities. Hopefully these steps can help the development of efficient electronic administration.

The Hungarian Association for Electronic Signatures will continue its standardization work on the field of e-signature and e-invoices. This work will be based on international standards but with some rational limitations. Budapest University of Technology and Economics is ready for future interoperability tests in the field of e-

government and we will continue the development of an interoperability laboratory.

## **7. Acknowledgements**

This work was supported by Mr. Zsolt Sikolya and Mr. Endre Kovács from the Ministry of Informatics and Communications. Special thanks to Mr. János Almási and Mr. István Balázs from the Hungarian Association for Electronic Signatures for their valuable help. The laboratory was established by the support of the National Office for Research and Technology (Hungary).

## **8. References**

- [1] W3C Recommendation: XML-Signature Syntax and Processing.
- [2] IETF RFC 3275: (Extensible Markup Language) XML-Signature Syntax and Processing
- [3] ETSI TS 101 903 v1.2.2: XML Advanced Electronic Signatures (XAdES)
- [4] eEurope 2005: An information society for all
- [5] W3C Recommendation: Canonical XML – Version 1.0
- [6] W3C Recommendation: Exclusive XML Canonicalization – Version 1.0
- [7] Common MELASZ format for electronic signatures – version 1.0