Hungarian Electronic Public Administration Interoperability Framework (MEKIK) – Technical Standards Catalogue

Zsolt Sikolya
Ministry of Informatics and Communications (IHM)
Tel: +3614613366, Fax: +3614613548
zsolt.sikolya@ihm.gov.hu

Péter Risztics
Budapest University of Technology and Economics
Tel: +3614631188, Fax: +3614631387
risztics@ik.bme.hu

Abstract : The huge project of the MEKIK (Hungarian Electronic Public Administration Interoperability Framework) has already been started, the next steps were the specification of the middleware and MEKIK portal and the pilot implementation of technical standards catalogue that would be accessible via this portal. These requirements affected the work in connection with the secure communication and the usage of electronic signature in the public administration. The project – correspondingly to the standards of the catalogue – also covered the general conception of security framework, requirements of certification service providers, signature creation application and devices, cryptographic protocols, legal aspects and secure mobile communication. This article introduces the actualities in connection with the interoperability of electronic public administration.

1 MEKIK project

1.1 Antecedents

In the area of public administration the communication between parties (e.g. between governmental organizations) needs interoperable standards, data models, data communication schemas. The project of Hungarian interoperability framework, called MEKIK was under the control of the Ministry of Informatics and Communications (IHM). The expectation of the European Union is that all of the member countries must have an own „one-window administration" solution that must be interoperable with each other. The aims of the project were the declaration of the needed standards, definition of work-flows including legal regulation. In the project experts have taken into account the works of IDA (Interchange of Data between Administrations) – which is the program of European Commission – at accessibility, multilingualism, security, protection of private data, subsidiarity, usage of open standards, usage of open source code application. These tasks needed a governmental control

therefore the Hungarian Electronic Public Administration Interoperability Framework (MEKIK) became the leader. As the project document says the law must support the interoperability questions of electronic public administration. Most of the interoperability problems were based not just on technology but on management and workflow. During the overall work experts examined solutions, standards in other countries such as in United Kingdom, in Sweden, in Germany, in France, in Denmark, in Australia and in the European Union. The project made suggestions for communication, messages in transactions taking into account the security matters. The technology issues were based on XML (SOAP protocol, XML signature, XML encryption, XSD schemas) and also solutions of future were mentioned (WSDL, UDDI). MEKIK project unambiguously said that security features must be based on PKI (Public Key Infrastructure) technology.

Studies have been made and now the next step is to implement the MEKIK portal with standards catalogue and middleware.

1.2 EIF, e-GIF, SAGA

The sorting of technical standards and maintaining this catalogue is one of the tasks of the MEKIK. This catalogue must be the reference at software development that would be used in the public administration in order to be interoperable with other systems such as British or German public administration, and also at the development of basic 12 + 8 public services these standards must be taken into account. These 20 public services were defined in the eEurope Action Plan 2002: 12 for citizens and 8 for businesses.

In the recent past national interoperability framework projects have been started and technical standards catalogues have been constructed. The third phase of IDA program is IDABC (Interoperable Delivery of Pan-European eGovernment Services to Public Administrations, Businesses and Citizens) is about interoperable and secure e-Government services and communications. In the beginning the processes of regulation were just monitored, but finally it has been decided to take more part in work, and EIF (European Interoperability Framework) project has been started. Hungarian experts – in the Hungarian interoperability framework project, which is part of MEKIK – have taken into account the results of national and IDA's interoperability framework projects such as British e-GIF, German SAGA or basic recommendations of EIF.

The standards in the catalogue can be grouped in several ways, one standard can affect more fields of operation, but two main categories could be made:

- data structure, message structure standards, that can be different in each countries,
- all other (mainly open and accessible) international technical standards.

Data structures, message structures have a core, common part that is based on the European regulation, but there can be also differences, because of the national legal regulations in Member States. The InfoStructureBase (isb.oio.dk/repository) is part of the Danish e-Government project and a strategic element in the architecture for e-Government. It is a well-functioning solution to cataloguing and publishing of data structures, message structures as XSD files (XML schemas) with defined namespaces. In this repository users can browse between schema files of different fields of e-Government and also can use search functions and make queries. Each data structure, message structure has well-defined metadata form that is partly based on Dublin Core elements.

Sorting (defining categories as titles in the catalogues) of international standards of W3C, IETF, ISO, ITU, ETSI, CEN and other standardization organizations is not the same at British, German or European documents. The catalogues in these cases are just simple documents, standards are just listed with identifiers and short descriptions.

Hungarian experts decided to provide the catalogue as a simple document and also as a portal (MEKIK portal), where users can browse and search between standards (similarly to Danish solution). The most important tasks of the MEKIK portal should be providing general information about MEKIK, publishing actual news, storing publications, managing forum and names, links of other organizations and document repository (standards, data schemas).

At editing the catalogue of standards the recommendations of EIF and national standard catalogues (e-GIF, SAGA) were in the point of view.

It will be based on open standards and encourage the use of open source software.

/European Interoperability Framework – EIF/

The use of the XML family of standards is recommended in national eGIFs for data integration. This is usually supplemented with recommendations for supporting standards such as UML or RDF for data modelling, XSLT for data transformation, Dublin Core, possibly with national extensions, for metadata, etc. Some Member States also make reference to Web Services interoperability.

/European Interoperability Framework – EIF/

1.3 Metadata

Each entry in the catalogue (as a simple document) contains the title and identifier of the standard, name of the publisher, short description of the content and status information („under observation", „recommended", „mandatory"). At the portal the basic requirement to make these entries searchable can be satisfied by defining metadata to each document.

The well-known and most used metadata standard is Dublin Core. The core set of elements – contains 15 attributes – was published as ISO (ISO 15836:2003), IETF (RFC 2413) CEN (CWA 13874) standard. IETF also published an extension that specifies the usage of Dublin Core elements in HTML files (RFC 2731). At e-Government solutions an extended version of Dublin Core must be used to describe data, create metadata. MIReG (Management Information Resources for eGovernment) is the project of IDA that aimed to provide a standardized structure and XML schemas for metadata in e-Government (XML schema are available on the homepage of IDA). The planned MEKIK portal would be able to view the core Dublin Core elements in HTML files and also MIReG compatible XML files as metadata in the browser of the user.

1.4 Middleware

The middleware that provides the interoperable layer must be able to communicate and process messages based on the standards listed in the catalogue. Functional requirements of the middleware are identification, authentication and authorization of parties and services, managing message transfer, making entries in the logfile, converting data and managing security services.

Most of the services need cryptographic support. Authentication is a serious step in the process of giving access to resources, and also keeping document integrity and

confidentiality. Both of them needs the correct implementation of managing the challenge-response protocol, creating message digests by hash algorithms (one-way-functions), using private keys (digital signature) and public keys (encryption) to encode or decode messages.

1.5 Secure electronic public administration

The other part of MEKIK project was under the control of Ministry of Informatics and Communications (IHM), Prime Minister's Office (MeH), Ministry of Interior (BM). Its aim was to specify standardized requirements in connection with secure communication in electronic public administration between either client and administration or administration and administration. Specification should have conformed to the needs and workflows that could have different security levels. Solutions of electronic government and electronic public administration are based on internet (TCP and IP protocols) therefore the nature of the network determines basic rules in connection with security. The repeatedly mentioned requirements of secure communication are

- confidentiality (encrypted messages),
- integrity (digested messages with hash functions),
- authentication (digitally signed messages),
- non-repudiation (digitally signed messages),

and secure systems also have the availability parameter.

There were several topics in the huge project that should have been examined from the view of security such as security framework, CA requirements (press the point of key recovery), application requirements, system requirements, access control management, smart card specification, legal aspects and mobile phone authentication.

These categories will be examined in details in the following.

1.6 Security framework

Document about security framework in general defines the levels and categories of security aspects. Experts have taken into account different environment at A2A or A2B and A2C communications and sorted requirements.

The main points of security aspects in the document were the following (5 functional + 1 assurance requirements):

- registration: process of mapping „natural person" to „electronic object" (e.g. generating a PKI certificate with the distinguished name of the person at the highest security level and giving a pseudonym at the lowest security level),
- authentication: secure identification of parties at the beginning of a communication (e.g. challenge-response handshake protocol to prove authenticity with certificate request on the client side at a TLS or SSL connection),
- integrity: data during the communication is not altered (e.g. creating message digests with hash functions that are one-way-functions at S/MIME applications, XML-based cryptographic applications and TLS or SSL connection),
- confidentiality: data during the communication doesn't become public (e.g. encrypted messages at S/MIME applications, XML-based cryptographic applications and TLS or SSL connection),
- non-repudiation: actions during the communication can't be denied (e.g. a digitally sign a document at S/MIME applications, XML-based cryptographic applications and TLS or SSL connection),

- conformance: assurance that the object fulfills the requirements (e.g. an independent audit of an application based on the requirements and methodology of Common Criteria).

Experts defined 3 + 1 security level to these security aspects:

- level 0: no expectation (there is no need to use electronic signature),
- level 1: low expectations (advanced electronic signature is needed with software token),
- level 2: average expectations (advanced electronic signature is needed with hardware token),
- level 3: high expectations (qualified electronic signature is needed with secure signature-creation device).

Based on security aspects and security levels, a 6 × 4 security matrix can be drawn that is referenced in all other documents of MEKIK project.

1.7 CA requirements

Certificate Service Providers can operate several kind of CAs, therefore specifying general requirements can be hard. Experts defined 6 categories based on the 1999/93/EC directive and the Hungarian law about electronic signature and service providers:

- issuing secure signature-creation device with qualified certificate (HSz1),
- issuing secure signature-creation device with authentication certificate for citizens (HSz2),
- secure signature-creation device with authentication and encryption certificate for civil servants (HSz3),
- issuing hardware token with signature and encryption certificate (HSz4),
- issuing software token with signature and encryption certificate (HSz5),
- time-stamping service provider (HSz6).

Legal regulation and technical standards in most cases are about the requirements of CA, labelled HSz1. Technological issues are described in a CEN standard (CWA 14167-1) in connection with trustworthy systems managing certificates for electronic signatures (QC or non-QC), and policy information is laid down in ETSI TS 101 456 standard for certificate authorities issuing qualified certificates (QCP public + SSCD). There is another, separate ETSI standard that specifies requirements of certificate authorities issuing public key certificates in general (ETSI TS 102 042) such as CA labelled HSz2 or HSz3.

Each certificate service provider was categorised based on issuing qualified (QC) or non-qualified certificates (NQC), and using qualified (QCP), normalized (NCP or NCP+) or lightweight policy (LCP). Policy requirements of time-stamping authorities are laid down in ETSI TS 102 023 but from the view of CWA 14167-1 requirements must meet with QC.

This document also defines other parameters in connection with the operation of certificate service providers such as availability and time-synchronization. Strict rules means availability of 99,9% which means maximum 3 hours or 8 hours of outage, at 98% this rate is maximum 24 hours. Time-token must be provided from two, independent, trusted sources in order to keep high rate of availability and precision.

Key recovery is an actual problem that must be solved by experts. There is still no legal regulation for encryption, but it is used in many cases. Losing a token, a smart card is not an extreme situation. In the case of electronic signature the user must report it to certificate service provider and can order another certificate, private key and smart card. In the case of encryption other problems can occur. Encrypted documents need private keys to decrypt them, but it is impossible if that private key is stolen or lost. The solution is using a Key Recovery Agent (KGA), which can store private keys (after key-generation it makes a backup). Two methods are written down in the document. The difference is in the number of used keys, because in the first case private key (used for encryption or signature-creation) is stored at the KGA (that could be accessed if the private key of the user is lost), but user could worry about this stored private key. In the other case another keys are generated just for key-recovery, so user have two key pairs: one for encryption or signature-creation and another one for key-recovery. The authority stores just the private part of key-recovery key pair. During the communication symmetric session keys that are used to encrypt messages are encrypted with public keys (that can be decrypted by private keys). If a user has two key pairs, this symmetric key is sent twice because it can use two public keys for encryption (encryption key pair and key-recovery key pair). These private keys can be downloaded from KGA if any problem occurs.

1.8 Application requirements

Examination of the security of applications focuses on interoperability questions recently therefore common requirements must be set up to help development and evaluation of well-functioning softwares. In several pilot projects experts tried to apply Hungarian methodology for evaluating and certification of softwares and hardwares, called MIBÉTS which is an adaptation of Common Criteria (CC) and Common Evaluation Methodology (CEM). Bases of these examinations, tests must be – as it is written in relating documents of MEKIK project – the standards of CEN such as CWA 14170 and CWA 14171 that defines the requirements of signature-creation application and signature verification. These standards can well extend existing Protection Profiles (based on functional and assurance requirements of Common Criteria) about electronic signature-creation applications (Public Key-Enabled Application Requirements – Department of Defense) and signature-creation devices such as smart cards. Hungary is the member of CCRA (Common Criteria Recognition Arrangement) since 19 of September, 2003 therefore it is recommended to apply methodology of evaluation and certification – based on MIBÉTS – of security products.

1.9 System requirements

Documents of MEKIK project highlight issue of password management, S/MIME applications, TLS (SSL) protocol, XML-related security standards, certificate profiles, signature policies and cryptographic algorithms. Password management is a critical point of authentication. Specifications give good guidelines to choose strong passwords that can be memorized. There is a Hungarian portal with essays about security relating topics (Biztostu.hu) where password cracking is illustrated and can be tried based on dictionary attack technology. Either passwords or cryptographic certificates (the latter is recommended) can be used to authenticate users in the communication, at the start of a TLS or SSL session. The usage of TLS (RFC 2246) or SSL protocol was also examined in the documents of MEKIK project. S/MIME can satisfy the basic requirements of European Union on electronic signature (BES or EPES structure as it is written down in ETSI TS 101 733) but experts also draw attention to deficiencies (such as timestamp, which is needed at e.g. electronic invoices), therefore it is recommended to use XML-based applications to create and verify electronic signatures (RFC 3275 and ETSI TS 101 903), encrypt messages (W3C XML Encryption

Syntax and Processing) or manage keys (XML Key Management Specification (XKMS 2.0)). Other topics related to electronic signatures have been also examined. Certificate profiles have been specified for different usages (signature, authentication for TLS or SSL, encryption) and different roles (individual, organisational person, civil servant), signature policies must be based on ETSI TR 102 038 standard, and applications must use secure algorithms specified in ETSI SR 002 176.

1.10 Access control management

Experts examined user authentication methods at several electronic public administrations such as in Austria or in the United Kingdom, and also draft specifications of NIST. Access methods are based on PKI technology, technical requirements of communication parties are given (e.g. SAML over SOAP that is secured by TLS or SSL) in the documents, the process of authentication and login is written down step-by-step.

1.11 Smart card specification

Hungarian eID card, HUNEID will be the identification card of users in electronic public administration. Smart cards can be used at several situations to authenticate a user or use digital signature on a document to keep integrity with the benefit of that data (e.g. private key) – stored on smart card – can't be retrieved. Experts have also defined the requirements of the environment of smart card, examined the problem of trusted and non-trusted terminals based on the CEN standard (CWA 14891-1). At the specification of interfaces result of European projects, such as eEurope Smart Card Charter (eESC) have been taken into account. Basic standards of physical build-up are described in ISO/IEC 7816, PKCS standards extend these specifications such as PKCS #15 (describing a file and directory structure on the smart card) or PKCS #11 (functions written in ANSI C programming language), requirements of card readers are also declared. Documents contain the use cases in connection with smart cards (e.g. detailed description relating to PIN management) during the whole life-cycle.

1.12 Legal aspects

Legal aspects of using confidential, sensitive data were also examined in documents of MEKIK project. Electronic public services have been categorised from the view of legal aspects, services as examples have been chosen from the official statements of European Commission and European Council (such as COM (2001) 140, COM (2002) 263, COM (2002) 655, COM (2003) 567). Specifications were based on international models, experiences of United Kingdom and Austria have been assimilated. Critical point of electronic public administration was data protection, data management of users that have been examined and expert's suggestions were written down in documents of MEKIK project. These recommendations cover the field of usage of eID card and procedure of registration.

1.13 Mobile phone authentication

Mobile phone with SIM card can be a secure device for using electronic public administrations. This idea is also under examination at ETSI and Hungarian experts pay attention to the results of standardization organization. Standards of ETSI, such as ETSI TR 102 203, ETSI TS 102 204, ETSI TR 102 206, ETSI TS 102 207 have been introduced in documents of MEKIK project. PKI-based applications have been also examined from the view of CEN standards (CWA 14170 and CWA 14171) which describe the requirements of signature-creation applications and signature verification and also visions have been set up in connection with the basic 12 + 8 public services in mobile environment.

3 Summary

Hungarian regulations and specifications in electronic public administration meet the requirements of European Union. Experts pay attention security questions, therefore interoperability – which is a basic requirement in secure communication – of applications and services was in the center of examination. Implementation of the system has been started, existing modules are being examined and reconfigured to be able to provide interoperable and secure electronic public administration services to information society.

4 References

[1] Hungarian documents of MEKIK project are accessible at the following URL: http://www.itktb.hu/engine.aspx?page=elka_oldal

[2] Common list of basic public services http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/basicpublicservices.pdf