E-GOVERNMENT & IDENTITY METASYSTEM

A FEW ISSUES INTRODUCED TO OASIS IMI

***Abstract**: OASIS started the Identity Metasystem Interoperability (IMI) TC. Government-issued electronic identification (eID) play a role in identity management, where the EU Large Scale Pilot STORK is working on interoperability of existing eID in 14 EU and EEA Member States. During discussions at the inaugural meeting of OASIS IMI, a few issues have been highlighted. These mainly stem from situation where qualified certificates or qualified signatures following the EU Signature Directive 1999/93/EC are used during authentication, where gaps are seen to the IMI input specifications. These issues have been:*

- *Affirmative Statements: E-Government applications may ask for wilful acts (or consent) in the authentication step and where SSCDs (as defined in the Signature Directive) are used technical requirements are imposed by the Directive (or national laws)*
- *Crypto-Algorithm flexibility: The input documents have fixed crypto algorithms (i.e. SHA-1, RSA). National algorithm lists and eID rollouts exist asking for flexibility (e.g. SHA-2, ECDSA, ...).*
- *Signature formats: XAdES (an XMLDSIG variant) is a widely used format in Europe with signature cards.*

This list is not meant to give a complete list of where hurdles between OASIS IMI and existing national eID programmes exist. It mainly focuses on the relation to qualified signatures.

This document explain the issues in more detail an gives thoughts on where the OASIS IMI Committee draft could be revised to avoid hurdles in integrating eID systems bound to qualified certificates/signatures.

Authors:

Mario Ivkovic

Herbert Leitold

1 INTRODUCTION

1.1 ABOUT STORK

STORK is a large scale pilot in the ICT-PSP (ICT Policy Support Programme), under the CIP (Competitiveness and Innovation Programme), and co-funded by the European Commission.

It aims at implementing an EU wide interoperable system for recognition of eIDs and authentication that will enable businesses, citizens and government employees to use their national electronic identities in any Member State.

The project includes a total of 29 consortium partners, including 14 EU Member States and Iceland. The consortium is a mix of public and private sector organisations.

Note that, in the STORK context, eID is meant spanning a broad range: from username-password, mobile phone up to smartcards with qualified signatures. This paper limits itself to the latter case where requirements on the signature components are given in laws.

1.2 REQUIREMENTS OF QUALIFIED SIGNATURES

Several EU Member States add qualified electronic signatures[1], which are defined in the EU Directive 1999/93/EC [2], to national eID cards or use qualified signatures in the authentication step. Hence, requirements on the certificate and signature creation arise.

One criterion which defines a qualified electronic signature is that the signature is "*created using means that the signatory can maintain under his sole control*" (1999/93/EC Article 2, 2c), the private key "*can be reliably protected by the legitimate signatory against the use of others*" (1999/93/EC Annex III, 1c), respectively. As a result, several Member States have decided to use smart cards for the signature creation[2].

Furthermore, a secure signature-creation device (SSCD), which is used for the creation of qualified electronic signatures, must not prevent the data to be signed from being presented to the signatory prior to the signature creation process (1999/93/EC Annex III, 2).

This leads to three issues *Affirmative Statements*, *Extensible Cryptographic Algorithms*, and *ETSI Properties*, that may lead to gaps between the IMI specifications and national eID schemes. We think that these potential gaps can be overcome in the OASIS IMI exercise.

[1] Note, that the term "qualified signature" hasn't been defined by the Directive, it is however commonly used.
[2] Note, that we mix between advanced signatures and qualified signature definition. For the purpose of this paper t is no needed to discuss the differences.

2 AFFIRMATIVE STATEMENTS

Member States applications may require an affirmative statement or a wilful act during the identification and authentication process. This section describes the issues which may be hindering an integration of those situations into the Identity Metasystem and outlines possible solutions.

Figure 1 shows the basic architecture of the Identity Metasystem together with the involved entities and used protocols.

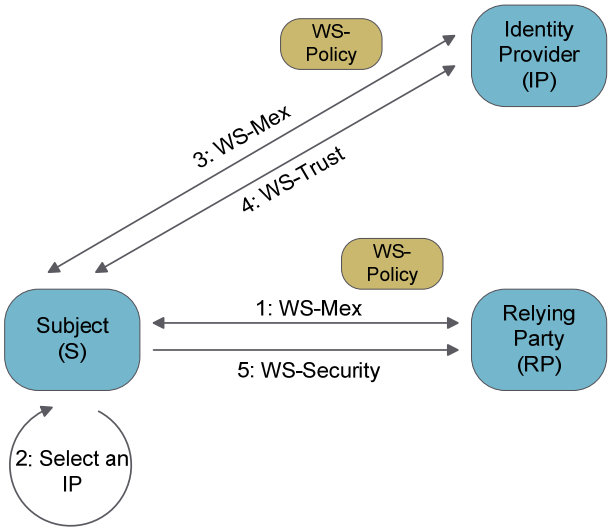

Figure 1: Basic architecture of the Identity Metasystem

2.1 REQUIREMENTS

The following points need to be fulfilled in order to provide the facility that a subject can create and sign an affirmative statement.

- *Information to be signed:* It needs to be possible that a relying party can configure or convey human understandable and readable information which is later signed by the subject.
- *Cryptographic algorithms:* A relying party should have the possibility to choose which cryptographic algorithm it supports (see Section 3).
- *Additional information:* It should be possible to convey additional information which is required for the signature creation.
- *Visualization of the data to be signed:* As described in the previous section, a subject needs to have the possibility to inspect the data prior a signature creation (1999/93/EC Annex III, Section 2).

2.2 POSSIBLE SOLUTIONS

This section gives first thoughts that could be taken to resolve the issues to enable integration into the specifications:

Required information (e.g. data to be signed, algorithms, addition information) could be conveyed to the subject through the use of additional claim-types (figure 1, step 1):

- The information could be either directly sent via a claim or the claim contains only a reference (e.g. a URI) which can be used by the subject or the identity provider to obtain the actual data.
- The data to be signed could be prepared by the relying party and subsequently signed by the subject.
- Alternatively, the identity provider prepares and presents the data to be signed to the subject (figure 1, step 3).

3 CRYPTOGRAPHIC ALGORITHM FLEXIBILITY

At several points in the OASIS IMI committee draft, RSA and SHA1 are defined as the only algorithms which are allowed and supported. For example, an envelope carrying an Information Card must be signed using RSA and SHA1 ([1] line 789), or self-issued tokens must be signed with a 2048-bit RSA key ([1] line 1603).

Due to existing algorithm catalogues of Member States, which inter alia also allow for the use of elliptic curves or RIPEMD-160, etc. it would be desirable if the specification would be more algorithm agnostic.

Furthermore, future changes of the used algorithms, e.g. because of encountered cryptographic weaknesses, should be possible without a change of the specification.

4 ETSI PROPERTIES

The prevalent method to create an advanced electronic signature is the creation of an XMLDSIG signature with additional signed and/or unsigned XADES properties.

Therefore, it is necessary that the protocol supports the generation and transportation of XMLDSIG signatures containing additional properties and especially XADES properties.

5 REFERENCES

[1] OASIS, Identity Metasystem Interoperability Version 1.0, Committee Draft 01, 10 November 2008

[2] Signature Directive: European Parliament and Council, Directive 1999/93/EC, “Community framework for electronic signatures”, December 1999, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML