E-GOVERNMENT & THE IDENTITY METASYSTEM

Technical Requirements and Gap-Analysis for Affirmative Statements

Document Version: 1.0

Creation Date: 06.01.2009

Author: Mario Ivkovic

1 Recap on the need for Affirmative Statements

Several EU Member States add qualified electronic signatures[1], which are defined in the EU Directive 1999/93/EC[2], to national eID cards. Moreover, some Member States have legal regulations which require the use of qualified electronic signatures within the authentication step.

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 decided to use smart cards for the signature creation.

Furthermore, Annex III 2 from the directive states that 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. In other words: Users must have the possibility to see or inspect the data which is going to be signed. In this paper we refer to this signed data as Affirmative Statement[3].

2 Technical Requirements

This section describes the technical requirements which need to be fulfilled in order to create an Affirmative Statement with an applied qualified electronic signature that is necessary for the user authentication in several Member States.

2.1 Transportation of the Data-To-Be-Signed (DTBS) to the User

To create an Affirmative Statement, a Relying Party (RP) must have the ability to convey the DTBS to the user, which the user afterwards can inspect and if she or he wants to sign it. The created Affirmative Statement serves as a declaration of intent within the authentication process.

2.2 XAdES Signatures (ETSI Properties)

In case of XML data, the prevalent method to create a qualified electronic signature is the creation of an XMLDSIG signature with additional signed and optional unsigned properties. Such a signature is called XML Advanced Electronic Signature (XAdES)[4].

However, it is necessary that the IM protocol supports the user-side generation of XAdES signatures over the DTBS which were provided by the RP.

---

[1] Note that the term "qualified signature" hasn't been defined by the EU Directive, it is however commonly used.

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

[3] Affirmative Statement is not a term which has been in the directive. However, the term Affirmative Statement should emphasize the willful act of signing human readable data.

[4] XAdES has been specified by the European Telecommunications Standards Institute (ETSI) http://www.w3.org/TR/XAdES/

2.3 Transportation of Affirmative Statements

The protocol must support the transportation of Affirmative Statements within the token up to the RP. An RP can subsequently verify the willful act of the user to access the service.

3 Gap Analysis

This section describes the gaps which are present in the current version of the specification and how these issues could be solved to support the generation of Affirmative Statements and qualified electronic signatures.

3.1 Transportation of the Data-To-Be-Signed (DTBS) to the User

The current version of the specification doesn't provide the ability to convey the DTBS from the RP to the user.

One possibility would be to use further RP specific parameters in addition to the request for claims to convey the DTBS. The DTBS could be either directly sent via or the parameter contains only a reference (e.g. a URI) which can be used by the identity selector or the identity provider to obtain the actual data.

These additional parameters could be also used to control or specify the creation of the XAdES signature (e.g. supported XAdES versions, cryptographic algorithms, and key sizes).

3.2 XAdES Signatures

This section should describe possible gaps in the present specification which hinder the user-side generation of XAdES signatures. When using Affirmative statements with an applied qualified electronic signature it is not necessary to invoke an Identity Provider (IdP). In such a case, self-issued tokens provide entirely sufficient quality for user authentication. Note that it is not required to apply a qualified signature on the SAML token itself. It is sufficient to convey the signed Affirmative Statement within the SAML envelope.

However, it is also desirable to support the creation of qualified electronic signatures, in particular XAdES signatures, with the interaction of IdPs.

Depending on the actual implementation of Affirmative Statements several issues may arise. Therefore, it would be preferable to develop a solution within the IMI group which fulfills the requirements of a qualified signature and fits into the IMI specifications.

3.3 Transportation of Affirmative Statements

The transportation of Affirmative Statements, within a SAML assertion for example, should be possible and therefore doesn't pose a problem.