INFORMATION CARDS AND AFFIRMATIVE STATEMENTS

Mario Ivkovic and Martin Centner
Institute for Applied Information Processing and Communications (IAIK), Graz University of Technology, Austria

Keywords: Affirmative statements, Citizen cards, e-Government, Identity metasystem, Information cards.

Abstract: E-government services require strong methods of identification and authentication in order to protect personal rights and to comply with corresponding laws. The requirements for the authentication process can be fulfilled by electronic signatures. Identification in e-government applications often relies on government-issued identifiers provided by electronic identity (eID) cards. An eID card with signature creation capabilities is typically called Citizen Card. The Information Cards technology, a recently introduced user-centric identity management framework, gains more and more importance if the field of eID. Expecting a high importance of Information Cards in the future, it would be very reasonable to utilize them for e-government services. In this paper we present an approach to use Citizen Cards together with Information Cards for identification and authentication in e-government services.

1 INTRODUCTION

The Identity Metasystem concept gains more and more importance in the field of eID. For several reasons we think that Information Cards and the Identity Metasystem will play an important role in the near future. The first reason is that Information Cards is an open standard which is the basis for a wide distribution. OASIS published version 1.0 of the *Identity Metasystem Interoperability (IMI)* standard in July 2009. The second indicator for a possible success is the increasing number of implementations. Despite Microsoft's CardSpace, which was the first available implementation on the market, several other vendors released their commercial and non-commercial Identity Metasystem products (e.g. Novell's DigitalMe[1], IBM's Higgins[2], Azigo[3], etc.). The third important reason is the industry interest. On the one hand, some editors of the OASIS standard represent big market players and on the other hand, the so-called Information Card Foundation[4] including industry leaders with the aim to advance the use of Information Cards has been created.

Expecting the wide distribution of the Identity Metasystem in the future, it would be very reasonable to utilize it for e-government services. Identification and authentication in e-government application often relies on government-issued identifiers provided by eID cards with signature creation capabilities. This combination of eID card and signature creation device is typically called Citizen Card. The goal is now to combine identification and authentication mechanisms provided by Citizen Cards with the Information Cards technology. Unfortunately, for several reasons this cannot be done directly. Some e-government services for example, call for written statements signed by the user with a qualified electronic signature which is not supported by the OASIS-IMI specification. Furthermore, in some countries it is not intended that providers of government-issued identifiers are directly involved in the identification process. In other words, because of several reasons some countries don't want to conduct an IdP as defined in OASIS-IMI. OASIS-IMI supports self-issued identifiers and identifiers issued by an IdP during the identification process. However, the IMI protocol does not support the required pre-issued governmental identifiers. Additionally, OASIS-IMI only describes the usage of the RSA signature algorithm. Many Citizen Cards (e.g. the Austrian Citizen Card) use other algorithms, which would result in interoperability issues.

In this paper we show how this issues can be solved by our new introduced *Affirmative Statement*

[1] http://code.bandit-project.org/trac/wiki/DigitalMe

[2] http://eclipse.org/higgins/

[3] http://www.azigo.com/

[4] http://informationcard.net/

Ivkovic M. and Centner M.
INFORMATION CARDS AND AFFIRMATIVE STATEMENTS.
DOI: 10.5220/0002804203330339
In *Proceedings of the 6th International Conference on Web Information Systems and Technology (WEBIST 2010)*, page
ISBN: 978-989-674-025-2

Claim. The Affirmative Statement Claim contains a statement in natural language signed by the user with a qualified electronic signature. The signed Claim also contains the required government-issued identifier. The Affirmative Statement Claim can be added like any other Claim without the need to change the existing specification or implementations. To verify our approach we have extended an existing implementation and successfully tested with existing service providers and a self-written service provider.

Having solved these problems, Information Cards can help to improve or enhance existing solutions. On the one hand we consider general aspects of Information Cards where existing eID solutions can benefit from and on the other hand we consider features and characteristics that could enhance the Austrian eID landscape in particular.

Same Look&Feel for Users: The Austrian eID solution, like other national eID implementations, is partly based on specially developed identification and authentication protocols (see Section 2). If the Information Card technology could be used for e-government purposes, people would have only one means for identification and authentication. They could then use the same technology for Austrian e-government services as well as for private-sector services already utilizing the OASIS-IMI protocol.

No Additional Software for Users Required: Not least because of mobility reasons (e.g. access to services in internet cafes or at kiosks), it is very appropriate to avoid the need for specific software on the client side to access a service. Identity Metasystem implementations that are already integrated into the operating system, could help to clear this hurdle.

No Additional Software for Relying Parties Required: A Relying Party (RP) offering a service usually wants to have wide appeal, but do not want to implement a wealth of identification and authentication protocols. Moreover, it is not very likely that global service providers will implement national solutions. Therefore, the application of Information Cards could be a way towards the propagation of national eID solutions.

Card Roll-out: In Austria the penetration of cards that can be used as Citizen Card is very high (e.g. approximately 8.5 million[5] social security cards and more than 7 million bank cards[6]). If the Austrian eID solution could be combined with the OASIS-IMI protocol, service providers would have a high number of potential users.

The rest of this paper is structured as follows. In the next section we describe the requirements on electronic signatures to fulfill the needs for identification and authentication in e-government applications and we briefly explain the Austrian Citizen Card concept. The third section of this paper describes the concept of Information Cards and the underlying Identity Metasystem. Starting from the idea and the evolution of the Identity Metasystem, we explain the main concepts behind it and describe the protocol flow of a typical authentication process. In the fourth section (Affirmative Statements), we present how the Austrian Citizen Card could be used with Information Cards for identification and authentication in e-government services. In the last section, we finalize the paper with some conclusions.

2 E-GOVERNMENT SERVICES AND THE AUSTRIAN CITIZEN CARD

E-Government services – such as services that provide access to personal and sensitive data – usually require strong methods of identification and authentication in order to protect personal rights and to comply with corresponding laws.

Electronic signatures provide this means of identification and authentication in many electronic authentication schemes. The EU Directive on electronic signatures (Directive 1999/93/EC, 1999) defines a legal framework for electronic signatures. This Directive has been adopted into national legislation by all EU Member States. It defines special requirements for *advanced electronic signatures*, *qualified certificates* and *secure signature-creation devices*. Advanced electronic signatures based on a qualified certificate created with a secure signature-creation device (hereafter referenced to as *qualified signatures*) satisfy the same legal requirements as handwritten signatures and are admissible as evidence in legal proceedings.

The EU Directive on services in the internal market (Directive 2006/123/EC, 2006) requires Member States to ensure that foreign service providers wishing to provide their services in the respective Member State are able to complete all procedures and formalities at a point of single contact. As the Service Directive calls for providing electronic means for completing procedures and formalities, the recognition of qualified signatures by foreign EU Member States is

[5] According to http://www.chipkarte.at

[6] According to http://www.bankomatkarte.at

of ever-growing importance.

Considering the above mentioned EU Directives qualified signatures can be a very strong instrument for identification and authentication with recognition by foreign EU Member States. They are therefore very well suited for identification and authentication in e-government services.

Identification in e-government applications usually relies on government-issued identifiers. Such an identifier may be based on the social insurance number, the tax account number, the number in the register of residents, etc. – whatever allows to uniquely identify a citizen or legal entity. The identifier provided to a particular service may also be a derived identifier that uniquely identifies a citizen within a specific sector of public administration but is different from the identifiers used in other sectors. Such sector specific identifiers were introduced in some countries (e.g. in Austria) to prevent systematic correlation of personal data from different sectors of public administration.

Government-issued identifiers may be provided by electronic identity cards. Such electronic identity cards are often implemented as smart cards that also act as secure signature-creation device for creating qualified signatures. The combination of electronic identity card and secure signature-creation device is often called *Citizen Card*.

The Austrian E-Government Act (EGov-Act, 2004) defines a Citizen Card as a logical unit, independent of its technical implementation that combines qualified electronic signatures with an *Identity Link*. The Identity Link provides a mechanism for electronic identification by linking a qualified certificate to the citizen's government-issued identifier (the so-called *source PIN* derived from the citizen's number in the register of residents). The source PIN may never directly be used as identifier in e-government services. Instead, a sector-specific personal identifier has to be derived from the source PIN.

Two major types of Citizen Cards are currently available in Austria: Citizen Cards based on smart cards such as the electronic health insurance card, bank cards and other electronic signature cards and Citizen Cards based on mobile phones for authorizing a server generated electronic signature.

All Austrian Citizen Card implementations provide their functions via a common interface (*Security Layer*) specified in the Austrian Citizen Card specification (Hollosi and Karlinger, 2004). Smart card based implementations require a software (called *Citizen Card Environment*) to externally offer the Security Layer interface. Such software is available from different vendors and has to be installed on the citizen's PC. In addition, one implementation is available that does not require the installation on the citizen's PC but is provided by a server and uses a lightweight component, executed in the citizen's browser, to access the smart card.

The Security Layer interface is designed to be directly accessible by applications on the citizen's PC or by web applications via the citizen's web browser. For this purpose the Security Layer interface provides a simple XML based protocol over an HTTP interface.

Identification and authentication with the Austrian Citizen Card involves two steps:

1. Deriving a sector specific identifier, reading and validating the Identity Link.
2. Creating and validating a qualified signature.

The first step serves as method for electronic identification based on sector specific identities as discussed above. The second step provides authentication, based on a qualified signature.

The Austrian Electronic Signature Act (Sig-G, 1999) demands that the secure signature-creation device must not prevent the signatory from viewing the data to-be signed. Therefore, for any data to-be signed a meaningful way of displaying it to the signatory must exist. Authentication based on Austrian Citizen Cards fulfils this requirement by requesting the citizen to sign a text written in natural language. The text may look like this:

> I *name and date of birth* apply for access to
> *the service* with my electronic signature.
> *Sector specific personal identifier*
> *Date and time instant*

Some e-government services have additional legal requirements that must be fulfilled. Some services for example call for written statements. As discussed at the beginning in this section, qualified signatures are able to fulfil the same legal requirements as handwritten signatures. Therefore, electronic applications signed with qualified signatures are able to meet the requirements of written form. The needs of E-Government services that require written form for access (e.g. services that provide access to personal and sensitive data) could be met by providing appropriate text to be signed with a qualified signature.

3 INFORMATION CARDS

The idea to develop a new identity system was born in order to banish the use of passwords together with all its disadvantages from the Web. Therefore, Kim Cameron, nowadays the Chief Architect of Identity in the Identity and Security Division at Microsoft, started a blog[7] to publicly discuss the issues and requirements for a possible solution. Out of this long and extensive discussion he extracted the widely known 7 laws of identity and described the concept of the Identity Metasystem, a user-centric identity management framework (Cameron, 2005).

From a user's point of view, the Identity Metasystem serves as digital equivalent of a wallet which is filled with various types of documents representing the user's identity (e.g. identity card, driving license, credit card, . . .). During an identification process the user is able choose which identity document, and thus, which identity data to disclose. The digital equivalent of an identity document within the Identity Metasystem is called Information Card.

The Identity Metasystem has been designed as a system of systems and it is not based on any specific technology (Cameron, 2005):

> ”We need a unifying identity metasystem that can protect applications from the internal complexities of specific implementations and allow digital identity to become loosely coupled. This metasystem is in effect a system of systems that exposes a unified interface much like a device driver or network socket does. That allows one-offs to evolve towards standardized technologies that work within a metasystem framework without requiring the whole world to agree a priori.”

The concept of the Identity Metasystem has been then taken up by OASIS[8] and the Identity Metasystem Interoperability (IMI) technical committee has been formed to develop an open and public standard. Version 1.0 of the Identity Metasystem Interoperability standard has been published in July 2009 (OASIS-IMI, 2009). All remaining descriptions and deliberations of this paper refer to the OASIS standard.

In the following, the basic concepts and involved parties that are necessary for the following protocol description and this paper in general are described.

Subject. A Subject is a person or entity that wants to use a service offered by an RP. A subject owns a Digital Identity.

Identity Provider. An Identity Provider (IdP) is an entity that issues Digital Identities to Subjects. An IdP could be a government agency that issues Digital Identities to the citizens, or a credit card provider for example. It is also possible that a Subject issues a Digital Identity to itself, which is then called a self-issued identity.

Relying Party. An RP is an entity offering a service to Subjects and relies on Digital Identities.

Information Card. An Information Card is a visualization of a Subject's Digital Identity.

Claim. A Claim is a specific information about a Subject asserted by an IdP. Typical Claims are a person's given name, last name or date of birth.

Digital Identity. A Digital Identity is a set of Claims concerning a particular Subject.

Security Token. A Security Token is basically the representation of an asserted Digital Identity that contains a set of Claims. Typically, a Security Token is encoded as a SAML v1.1 Assertion[9].

Figure 1 shows the basic communication steps of an authentication process using the OASIS-IMI protocol. In this example a Subject wants access to a restricted service offered by an RP[10].

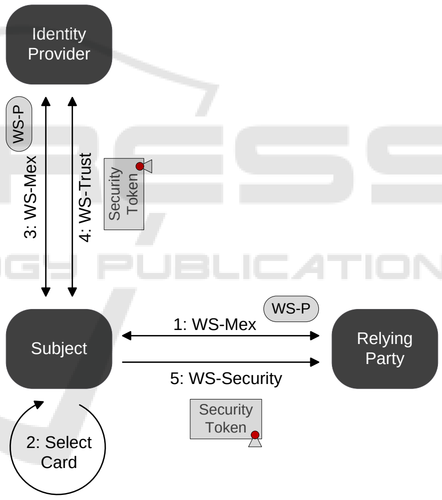


Figure 1: Illustration of the OASIS-IMI identification protocol flow.

In Step (1), the Subject and the RP negotiate the policy that should be applied for this authentication process using WS-MetadataExchange (K. Ballinger et

[7] http://www.identiyblog.com

[8] OASIS, Organization for the Advancement of Structured Information Standards, http://www.oasis-open.org/

[9] Security Assertion Markup Language (SAML) v1.1, http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[10] Please note that this protocol description relates to the generic protocol flow using WS-* protocols between all parties. In case a user wants to access a restricted Web site using a Web browser, which typically doesn't support WS-* protocols, the protocol flow differs from this one. In such a case the communication between browser and RP would be plain HTTP or HTTPS, respectively (OASIS-IMI, 2009).

al., 2006). The policy itself is in turn defined using WS-Policy (S. Bajaj et al., 2006). Based on the received policy the Subject selects an Information Card and thus the Digital Identity that should be disclosed in Step (2). The component that holds the Information Cards and allows to choose which identity should be disclosed is called Identity Selector or Card Selector. The selected card, in case it is not a personal card (a card representing a self-issued digital identity), contains the information that is necessary to contact the responsible IdP. In Step (3), the Subject, or to be precise the Identity Selector on behalf of the Subject, negotiates the policy with the IdP, again using WS-MetadataExchange and WS-Policy. The Subject requests a Security Token based on the previously received policy using WS-Trust (OASIS WS-Trust, 2007) in Step (4). In order to request the token, the Subject needs to authenticate to the IdP. In the OASIS-IMI standard, four different authentication mechanisms are defined. These are username and password, kerberos v5 credential, X.509 certificate credential, and a self-issued Security Token (OASIS-IMI, 2009). A self-issued Security Token is a Security Token issued by the subjects Card Selector using a personal card and not by an IdP as in case of a managed card. In Step (5), the Subject transmits the received Security Token to the RP using WS-Security (A. Nadalin et al., 2004). After receiving the Security Token the RP verifies the token and grants access to the desired service.

4 AFFIRMATIVE STATEMENTS

The previous sections gave an introduction to Information Cards, identification and authentication in e-government and the Austrian Citizen Card. In this section we will present our approach to use a Citizen Card together with Information Cards for identification and authentication in e-government services.

Our aim is to combine the strong means of authentication attained by qualified electronic signatures and identification provided by a Citizen Card with the common user experience of Information Cards. Therefore, it is desirable to have the user's Citizen Card appearing as just another card in the Card Selector, such that the Citizen Card may be used in a manner similar to the use of any other information card.

A Citizen Card carries the same information that is also typically available with Information Cards. Given name, family name and date of birth are Claims often required by RPs. In addition the qualified certificate on the Citizen Card often includes the signatory's e-mail address – another Claim that is typically required by RPs. For RPs providing e-government services, the most important Claim will however be the government-issued identifier (or an derived identifier as discussed in section 2).

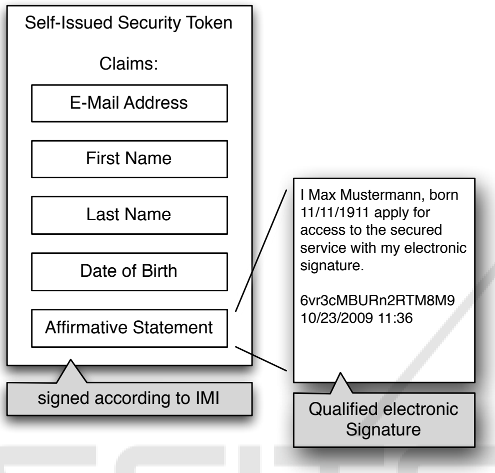
As already mentioned Citizen Card based identification relies on pre-issued identities. The only third party interaction required upon identification and authentication is obtaining revocation status information for the qualified certificate. There is no identity provider involved in the identification and authentication process.

The Information Card model introduces the concept of *self-issued* Security Tokens for authentication without third-party IdP interaction. In the Information Card model, as defined in OASIS-IMI (OASIS-IMI, 2009), self-issued Security Tokens always base on self-asserted identities. We are however going to use self-issued Security Tokens to provide government-issued, and therefore government-asserted and not self-asserted, identity to the RP.

Security Tokens are signed by the issuer before they are used for authentication at the RP. As our aim is to use qualified electronic signatures for authentication, at a first glance it seems obvious to apply a qualified electronic signature directly on the self-issued Security Token. Considering the following issues we have however chosen to follow a different approach.

- OASIS-IMI does not describe the usage of signature algorithms other than RSA. However, many Citizen Cards use different signature algorithms (e.g. ECDSA). Therefore, using such signature algorithms would most likely result in interoperability issues with existing RP implementations.
- As discussed in section 2, national implementations of the Signature Directive require that the signatory must have the ability to view the data before signing. However, there is no standard representation of a Security Token in a form meaningful for an end user. Transformation of the Security Token in an end user readable form before signing would violate the OASIS-IMI specification and would therefore again result in incompatibility to existing RP implementations.

For the given reasons we have decided to define a new *Affirmative Statement* (ASt) Claim. The Claim includes a statement in natural language similar to the one shown at the end of section 2 and has to be signed by the user with a qualified signature for the following authentication process. The ASt Claim also includes the government-issued identifier (either the identifier itself or a derived identifier thereof). This generated Claim is added to a self-issued Security Token, which is then signed as specified in OASIS-IMI (see Figure 2). Therefore, a token-signing key has to be derived from the secret master key of the corresponding information card. If this master key in turn is derived from a secret property of the Citizen Card, there is no need to store any information about the Citizen Card in the Card Selector. Thus, a Citizen Card backed Information Card behaves just like a *roaming* card, which may be easily used with different Card Selectors without the need to transfer information.



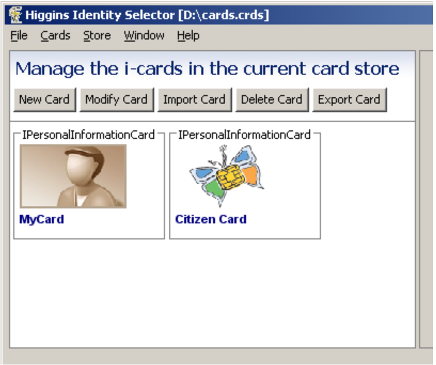
I Max Mustermann, born 11/11/1911 apply for access to the secured service with my electronic signature.

6vr3cMBURn2RTM8M9
10/23/2009 11:36

Figure 2: Self-issued Security Token with an Affirmative Statement.

Security Tokens with the additional ASt Claim can be processed as regular tokens by standard RP implementations.The Affirmative Statement Claim can be retrieved from the RP implementation like any other Claim. It is now the responsibility of a Citizen Card aware service to validate the Affirmative Statement Claim and extract the government-issued identifier. Of course this moves some responsibility to the service implementation. However, RPs which do not require this additional Affirmative Statement Claim can simply ignore it and treat the token like a regular self-asserted Security Token.

Card Selector implementations must be extended to support the introduced Affirmative Statement Claim. They need to be able to retrieve the required information from the Citizen Card and means for requesting the user to sign the Affirmative Statement with a qualified electronic signature. To verify our approach and to gain experience we have extended a Card Selector provided by the *Higgins Project*. Higgins offers several Card Selector implementations (e.g. GTK and Cocoa Selector, Firefox-Embedded Selector, iPhone Selector, Android Selector, . . .). Because of existing Java libraries for the required Citizen Card interaction, we have decided to extend the Higgins Java RCP Card Selector[11] implementation.



Manage the i-cards in the current card store

Figure 3: Citizen Card as Personal Card within the Higgins Card Selector.

To adapt the Higgins RCP Selector for our needs, we have implemented an additional *Personal Card*, in our case called Citizen Card, (see Figure 3) that supports the ASt Claim. If an RP requests an ASt Claim, the extended selector highlights the Citizen Card Information Card as supported card. In case the user selects this card, a Security Layer request (see Section 2 is submitted to retrieve the first name, last name, and date of birth stored on the user's Citizen Card. After retrieving this information the user can decide whether to transmit this card or not. If the user then decides to transmit this card by pressing the submit button, a second Security Layer request is generated and sent to the Citizen Card. With this request the user creates an Affirmative Statement with an applied qualified electronic signature as described above. This Affirmative Statement is then packed into the Security Token which in turn is signed according to the OASIS-IMI specification and transmitted to the RP. Figure 4 illustrates the protocol flow described above.

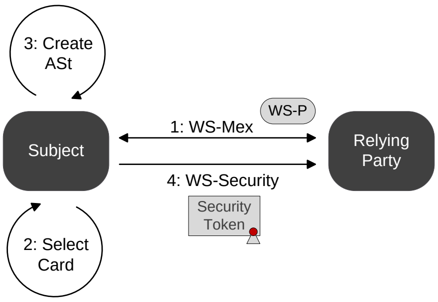


Figure 4: Protocol flow with Affirmative Statements.

[11] http://wiki.eclipse.org/RCP_Selector_1.0

5 CONCLUSIONS

With the presented approach it is possible to use Information Cards for identification and authentication with a Citizen Card without requiring any changes to the underlying protocols. RP implementations do not need to be aware of the Affirmative Statement Claim but need only to be able to hand it over to the application for further processing. Card Selectors however, must be extended to support Citizen Card backed Information Cards. While such integration is not provided in standard Card Selectors, the user may decide to install an extended Citizen Card enabled Card Selector as discussed above. However, it would be possible to integrate standard support for Affirmative Statements in Card Selectors on the same bases as signature creation devices in different operating systems.

Our concept of an Affirmative Statement Claim that solves the issues with existing e-government services has been proposed to the OASIS-IMI technical committee. OASIS added this Claim to their list of issues and the need for an Affirmative Statement Claim has been discussed and perceived in the technical committee.

The reliability and trustworthiness of an IdP is essential for the security of authentication schemes requiring IdP interaction. The approach we presented does not involve IdP interaction but uses qualified signatures for authentication. Thus, it relies on a well established legal framework as well as a system for accreditation and supervision of certification authorities. Therefore, RPs do not need to establish trust to any further parties.

The presented approach also provides Information Cards with a high degree of portability. A Citizen Card may be used with any supporting Card Selector without the need of prior information transfer.

REFERENCES

A. Nadalin et al. (2004). Web Services Security: SOAP Message Security 1.0. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf.

Cameron, K. (2005). The Laws of Identity. http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

Directive 1999/93/EC (1999). Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31999L0093:EN:HTML.

Directive 2006/123/EC (2006). Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32006L0123:EN:HTML.

EGov-Act (2004). The Austrian E-Government Act – Federal Act on Provisions Facilitating Electronic Communications with Public Bodies. http://www.digitales.oesterreich.gv.at/DocView.axd?CobId=31191.

Hollosi, A. and Karlinger, G. (2004). The Austrian Citizen Card. http://www.buergerkarte.at/konzept/securitylayer/spezifikation/20040514/introduction/Introduction.en.html.

K. Ballinger et al. (2006). Web Services Metadata Exchange (WS-MetadataExchange), Version 1.1. http://specs.xmlsoap.org/ws/2004/09/mex/WS-MetadataExchange.pdf.

OASIS-IMI (2009). Identity Metasystem Interoperability, Version 1.0, OASIS Standard. http://docs.oasis-open.org/imi/identity/v1.0/os/identity-1.0-spec-os.pdf.

OASIS WS-Trust (2007). WS-Trust 1.3, OASIS Standard. http://docs.oasis-open.org/ws-sx/ws-trust/200512/ws-trust-1.3-os.pdf.

S. Bajaj et al. (2006). Web Services Policy Framework (WS-Policy), Version 1.2. http:// specs.xmlsoap.org/ws/2004/09/policy/ws-policy.pdf.

Sig-G (1999). Bundesgesetz über elektronische Signaturen (Signaturgesetz – SigG). available in German only, http:// www.ris.bka.gv.at/ GeltendeFassung.wxe?Abfrage = Bundesnormen&Gesetzesnummer=10003685.