Towards global eID-Interoperability

Bud P. Bruegger[1], Detlef Hühnlein[2], Michael Kreutzer[3]

[1] Comune di Grosseto, Italy
bud@comune.grosseto.it

[2] secunet Security Networks AG, Germany
detlef.huehnlein@secunet.com

[3] Technical University of Darmstadt, Germany
kreutzer@dzi.tu-darmstadt.de

Abstract
The ability to use electronic identities (eID) anytime and anywhere is a prerequisite for a dynamic information society. However, there are still many obstacles which prevent the secure, privacy-friendly and ubiquitous use of electronic identities in an interoperable manner. This paper introduces the vision of global eID-Interoperability, describes the state of the art for electronic identities, highlights related challenges and sketches possible steps towards global eID-Interoperability.

1 Introduction

The ability to access electronic services anytime and anywhere is a prerequisite for a competitive and dynamic knowledge-based economy. However there are associated risks which grow at least proportionally to the level of ubiquity. To minimize these risks, it is necessary to provide strong, usable and interoperable methods for authentication, identification and privacy protection.

Electronic identities can be obtained from various sources (governments, social insurance organizations, financial institutions or other private companies etc.) or even be created by individuals themselves like in [CardSpace] and hence may provide significantly different levels of trust, depending on the enrolment process, the strength of the applied security mechanisms and the trustworthiness of the used equipment. The vision of global eID-interoperability (see section 2) consists of well defined and commonly agreed on metrics that cover the various eID characteristics. Further, eIDs need to be used together with arbitrary identification and authentication protocols in order to facilitate ubiquitous access to electronic services. When considering the state of the art in this area (see section 3), there are various challenges (see section 4) which need to be addressed in order to turn this vision into reality. Therefore, section 5 sketches some possible steps towards global eID-Interoperability. Section 6 provides a summary of the present contribution and an outlook on possible further steps.

2 Global eID-Interoperability

Electronic identities can be obtained from a range of sources and therefore represent significantly different levels of trust and are used in the context of different technical protocols for accessing electronic services at a given Service Provider (SP). In the figure, eID issuers are simplifyingly called Identity Providers, IdP; but this is understood in a wider sense that also includes Certification Authorities, which issue X.509 certificates and issuers of other identity tokens, such as SAML assertions or Kerberos tickets.

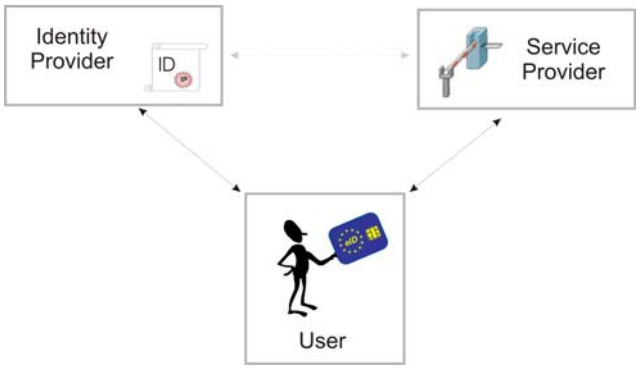

Figure 1: eID System Architecture

Hence, while the eID System Architecture depicted in Figure 1 looks very simple, there are many related social, technical, organizational, economical and last but not least legal issues which make global eID-Interoperability a challenging task. This applies even more when Users, IdPs and SPs reside in different countries and the service access becomes cross-border. Global eID-Interoperability may be defined as follows:

Global eID-Interoperability allows a User with an arbitrary eID – with a given level of eID-Quality and issued by a given Identity Provider/Certification Authority – to access a service offered by an arbitrary Service Provider in an arbitrary domain, requiring a minimum level of eID-Quality and limiting the possible protocols that can be used.

3 State of the Art for eID in a European perspective

Electronic identities (eIDs) have been generally accepted as a key enabler for the secure access to online services in our information society. While a clear focus on eGovernment applications is evident, eIDs may be even more relevant in the private sector and in a service-oriented Europe-wide market place. Therefore it is not surprising that a majority of European member states (see section 3.1) are either already rolling out eIDs to their citizens or are planning to do so shortly.

3.1 A survey concerning national eID cards in Europe

Probably the first country that has issued eID cards is **Finland** who has issued about 100,000 cards today. The Finnish eID implements the X.509 standard and has two certificates, one for authentication and the other for qualified electronic signature. Finland, with the full publication of their specifications and as co-founder of the Porvoo Group, has widely shared its experience and promoted interoperability and harmonization of eIDs in Europe. The Finnish experience has influenced the eID cards of Estonia and Belgium.

Estonia has issued more than 1 Mio. cards and is the first European country which has issued eID cards to a majority of its population. It already has a wide selection of available services including mobile signatures according to [ETSI-102204] and is now concentrating on a campaign to drastically increasing eID use by its population.

Belgium has issued well more than 2 Mio. cards and makes steady and rapid progress in the roll out. It has put strong emphasis on the availability of services and provides the necessary software components in open source for both, public and private sector service providers.

Italy and Spain have been among the first European countries to start eID projects. Their designs are thus less influenced by the Finish work. They are the first large European countries issuing eIDs.

Italy has issued well more than 2 Mio. eID cards (called CIE) that replace the national ID card and are accepted as travel documents. In addition, as a temporary measure to increase eID availability, Italy has issued more than 10 Mio service cards (called CNS) that are equivalent to CIE cards in respect of online access to services but lack the picture IDs and travel document functionality of the CIE card. The general roll-out of the CIE card to the entire population is imminent. The CIE card contains fingerprint templates as biometrics.

Spain has successfully issued close to half a million eID cards and is in the process of gradually increasing the number of issuing centres to eventually cover the entire population.

Portugal, having started their eID program significantly after the above mentioned countries, has moved very rapidly by adopting all the existing (evolving) standards (prCEN 15480, ISO/IEC 24727) as far as possible and has started to issue the first eIDs to citizens. The national authentication infrastructure that complements the eID card has a solution to map from the unique national identifier that is used in the authentication certificate to the several legacy identifiers that are used by other government sectors.

Austria has conceived the concept of the Austrian Citizen Card that is implemented in several different cards (including health cards (eCard), bank cards, student cards etc.). With more than 8 Mio. cards, they have covered their population more than once, with a citizen typically having more than one card. The Austrian Citizen Card has a unique approach to privacy enhancement that was an integral part of both technical design and national legislation. Thanks to a dynamic derivation of sector-specific identifiers by a government-run Identity Provider, Austria prevents the risks of large-scale linkability of personal data across sectors and services. While all the other mentioned eID cards all use X.509 certificates for authentication, the Austrian design refrains from using this standard in order to implement their privacy-enhancement features[1].

Iceland is another newcomer to the eID scene and has already made very rapid progress. Like Portugal, it has adopted all standards (prCEN 15480, ISO/IEC 24727) as far as possible and, with the eID project managed by banks, has included also an EMV application on the card. The first pilot roll-outs have started and there are credible plans to very rapidly issuing cards to the entire (and rather small) population.

Malta has several levels of eIDs ranging from username/password over soft certificates to eID cards for which a tender has been issued. Malta like other newcomer countries is requesting standards-based solutions (prCEN 15480, ISO/IEC 24727).

In addition to bank issued eIDs, **Sweden**'s police is issuing an eID card that has both a contact and a contact-less interface. The latter is an ICAO travel document. The contact-part is issued with only a boot-strapping application while currently it remains unclear who is going to issue trusted certificates for authentication to online services and for digital signature.

Bulgaria has announced that it will start issuing eIDs at the end of October of this year (2007). The card contains either a thumbprint or an iris scan as biometrics.

Both **Germany** and the **United Kingdom** are currently working on eID projects that plan to issue cards relatively soon. Germany is currently working on the legal basis and technical aspects of an electronic version of their identity card (Personalausweis). It may have a contactless interface that contains an ICAO travel document application as well as applications to authenticate towards online services and for digital signature. Germany is among the strong supporters of standards (including prCEN 15480). The activities around the forthcoming national eID card are part of a more comprehensive eCard-strategy (cf. [Kowa07]), which also considers the forthcoming electronic health card (elektronische Gesundheitskarte) and other cards as well as a variety of eGovernment applications such as ELSTER (cf. [Rand07]).

[1] Note that section 5.4 reports on work to use the Austrian concept of privacy enhancement in a manner that is compatible with the X.509 standard and is thus applicable to currently issued eID cards.

The **United Kingdom** has also decided to issue eID cards in addition to passports. Since there is no history of ID cards comparable to that of other European countries and there is currently no national population register, the plan to issue eIDs has been the focus of heated public discussion.

Please refer to [Modinis] for a more comprehensive survey concerning eID activities around Europe.

3.2 Towards a unified eID-middleware for Europe

With the Manchester Ministerial Declaration (November 2005), the importance for interoperable identity management for our Information Society has been formally put on the political agenda of Europe and recognized as a priority and key enabling factor for our development. The declaration confirms the national autonomy in the issuance of national identity documents and electronic identities. Hence there may be various eIDs using different processes and technologies and hence providing different levels of trust. As the eIDs themselves may significantly differ from one domain to another, it is necessary to provide powerful middleware solutions, which are able to handle arbitrary eIDs and nevertheless provide common interfaces to applications which want to use eID services.

This approach was taken in the development of the eCard-API-Framework by the German government [BSI-eCard] which is briefly introduced below.

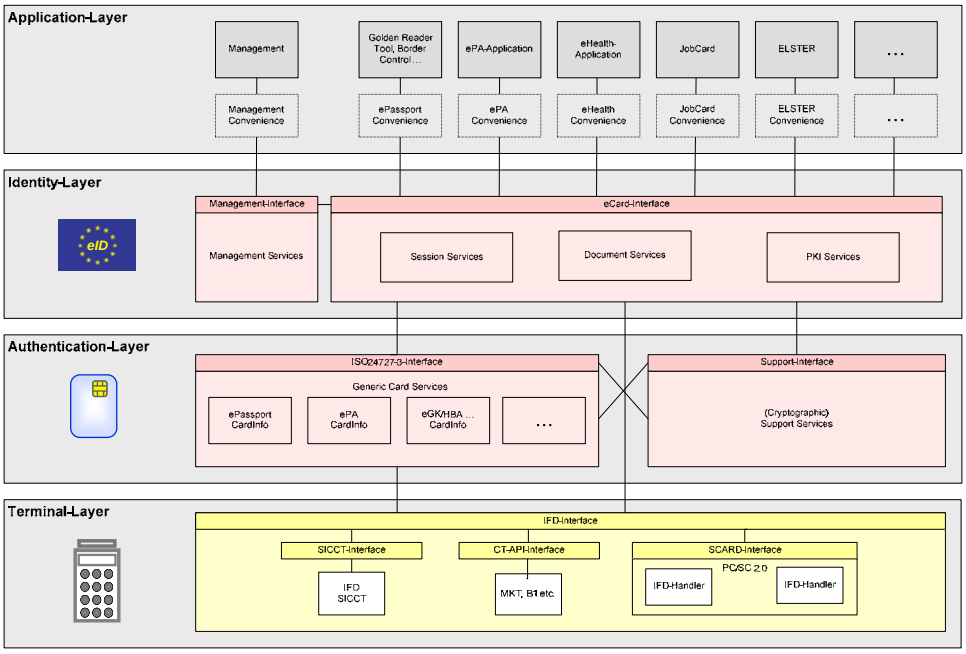

Figure 2: eCard-API-Framework

The eCard-API-Framework roughly consists of the following layers:

- Application-Layer

  The Application-Layer may comprise different applications which access the services provided by the eCard-API-Framework in order to access eID-functions, secure electronic documents by means of (advanced) electronic signatures and/or encryption or to obtain access to some electronic service provided by a Service Provider.

- Identity-Layer

  The Identity Layer provides functions to establish secure sessions and secure documents in various formats by means of (advanced) electronic signatures and encryption.

- Authentication-Layer

  The Authentication Layer provides the basic authentication functionality using arbitrary smart cards. The authentication services are accessed using the "Service Access Interface" which is currently standardized in [ISO24727-3] and [prCEN15480-3]. In order to be able to use arbitrary identity tokens – especially tokens which fail to provide a standardized cryptographic information application according to [ISO7816-15] – the generic card services will use the XML-based `CardInfo`-structure introduced in [HüBa07] and currently discussed in CEN TC 224 WG 15.

- Terminal-Layer

  The Terminal-Layer provides a homogeneous interface for arbitrary card terminals, which is currently standardized in [prCEN15480-3] and [ISO24727-4].

While the lower layers (Authentication-Layer and Terminal-Layer) are about to be standardized by CEN and ISO, it is currently not clear whether the Identity-Layer will also be standardized within the scope of ISO/IEC 24727 and/or CEN 15480. As the standardization of the Identity-Layer may provide the most significant contribution towards global eID-Interoperability, it would be very unfortunate if this opportunity would be missed.

4 Challenges for ubiquitous eID-Interoperability

While there are various initiatives for electronic identity cards and related standardisation efforts (ISO/IEC 24727, CEN 15480 etc.) there are still many obstacles which prevent the secure and ubiquitous use of electronic identities:

- Missing standardization of Identity Layer

  While there are different standardised protocols for the Identity Layer (see section 5.1.1), there is currently a lack of a comprehensive Generic Identity Interface that covers the different existing and emerging approaches and harmonizes the way in which applications request identification and authentication services.

- No common metrics for eID-Quality

  In addition to the technical standardization effort, it is necessary to standardize the notion of eID-Quality[2] such that trust relationships may be federated across domains in a well defined manner. For this purpose it will be necessary to investigate social, technical, organizational, procedural, economical and legal aspects of eID in order to identify the different dimensions of eID-Quality and provide an appropriate metric.

- Support for mobile devices

  In the context of eIDs, the meaning of the term "ubiquity" is two-fold: Firstly it means that some eID issued in one domain may be used in another domain (see section 2). Secondly it means that the use of eIDs may occur anytime and anywhere; this makes it necessary for eID-solutions to support mobile devices.

- Privacy

  The risks associated to the use of eIDs will grow at least proportionally to their level of ubiquity. In particular, it will be increasingly important to adequately address privacy issues if eID-solutions need to be widely accepted.

5 Possible steps towards global eID-Interoperability

This section briefly addresses the different challenges introduced above and sketches possible steps towards respective solutions.

5.1 Generic Identity Interface

While there are multiple standard protocols for the Identity Layer that are discussed in section 5.1.1, there is no comprehensive and harmonized Generic Identity Interface. The latter will be briefly sketched in section 5.1.2.

---

[2] The eID ad-hoc group is currently looking into this by defining the different levels of the European interoperability framework.

5.1.1 Existing protocol standards for the Identity Layer

5.1.1.1 Liberty Alliance and its specifications

Liberty Alliance **[Liberty]** enables the user to easily access a variety of identity-based services on the Web. The key features are Identity Federation, Single Sign On and Single Logout. The notion of federation is closely related to Single Sign On: the user needs to authenticate only once and can subsequently use different services from diverse providers without additional effort. Currently Liberty Alliance as an identity system is respecting privacy in the following way: The subject identifier is chosen to be "… different for each relying party (because the subject will be identified by the unidirectional identifier established with that particular relying party)." In the long run, it is planned that a stronger notion of privacy should be introduced that supports also partial identities, i.e. the selective disclosure of personal data to service providers (see **[Laur07]**).

Liberty Alliance is not restricted to a central storage where all (partial) identities of the users are kept. Users' identity can be stored in multiple places, for example, 3rd party identity providers as well as local storage (e.g. devices).

Further information and the specifications developed within the Liberty Alliance project can be found in [Liberty-Spec].

5.1.1.2 CardSpace / WS-*

CardSpace [CardSpace] preferentially uses the WS-* series of standards (see [MSWSS] and [RoRe04]) and provides a unified user interface for choosing and controlling the identities presented to relying parties. The goal in the long run is to establish a general-purpose Identity Meta System, i.e. a unified, secure and interoperable identity layer for the internet.

Currently, CardSpace allows users to create self-issued (partial) identities. Such an identity can contain one or more personal attributes. Certain transactions may reject self-issued identities and instead require a "managed identity", i.e. one issued by a trusted identity provider such as a bank, employer or a governmental agency. The CardSpace identity management system is based on and uses Microsoft's .NET technology, but there are other similar open source based approaches for user-centric identity management solutions, such as [Higgins], [OSIS] and [SourceID]. For an overview of identity agents, please refer to [RuTr07]. This latter publication also describes the extension of Identity Agents to support other protocols like Liberty, OpenID, etc. in addition to WS-*, i.e., a true Identity Meta System.

5.1.1.3 Transport Layer Security Federation (TLS-Federation)

TLS-Federation is a mature and stable solution for strong authentication to services on the web that uses widely accepted IETF standards such as the Transport Layer Security (TLS) [RFC2246] and Certificate Management Protocol (CMP) [RFC2510]. The federation extension to plain TLS allows to use the same ubiquitous protocols and technology for any kind of (national) eIDs, removing the restriction to only eIDs with X.509 certificates. In particular, when used with non-X.509 eIDs, the eID middleware creates a key pair and uses the standard CMP protocol to request a session certificate on the fly from an Identity Provider (technically a standard Certification Authority). This is directly comparable to the request of a SAML assertion from an IdP.

To protect against identity theft, TLS-Federation applies the most secure off-the-shelf technology for strong authentication (TLS) to a federated approach in which all possible eID technologies are supported. It thus avoids that the federated interoperability framework become the weakest security link and, instead, guarantees that the full security of national-only use of eIDs applies.

Supported eID technologies include but are not limited to X.509 credentials on smartcards (like in the eIDs from Finland, Estonia, Belgium, Italy, Spain, Portugal, Iceland (forthcomeing), Malta (forthcoming), etc.), non-X.509 credentials on smartcards (like the Austrian Citizen Card), X.509 credentials on file system (soft certificate solutions), and username/password centralized identification services.

TLS-Federation can be seen as an innovative use of existing standards and technology much rather than a new approach. The standards are arguably more mature and stable than those of the other federation solutions discussed above; and there is a wider choice of available off-the-shelf software both commercial and open source than for the other solutions since it is implemented on standard PKI, X.509, and TLS functionality. What is new is the use of these technologies in eID middleware (only that of non-X.509 eIDs); but the very same technology has been successfully used at very high volumes for eGovernment applications like ELSTER (cf. [Rand07]), the German tax declaration system that supports more than 80 Mio. transactions a year.

5.1.2 A sketch of possible steps towards a Generic Identity Interface

As there is currently a choice of popular protocols (TLS/CMP, WS-*, Liberty etc.) for the Identity Layer, it would be desirable to have a "Generic Identity Interface" that abstracts from the differences of the underlying protocols and presents authentication and identification in a unified manner: This interface could be – in a very abstract sense – similar to the Generic Security Services API [RFC2743], which, for example, provides a generic call to establish a security context (GSS_Init_sec_context), which in turn may be implemented using different security mechanisms such as Kerberos [RFC1510] [RFC1510] or SPKM [RFC2025]. However, the Generic Identity Interface should probably not directly be based on the structures and bindings of the GSS-API, but rather on XML and web service standards, such as [MSWSS], include federation issues, such as [Liberty] and even support card-to-card-mechanisms like specified for the European Citizen Card prCEN 15480.

Therefore, a good starting point for the design of such a Generic Identity Interface which might cover all the different eID-technologies and identity management protocols, might be a web-service-based variant of the functions `TC_API_Open` and `TC_API_Close` that are about to be standardized in [ISO24727-4].

5.2 Metrics for eID-Quality

In order to allow the federation and application of trust across different domains and countries, it would be helpful to have some sort of commonly agreed "metrics" for eID-Quality. A promising strategy for developing such a metric might be

- to look at the different dimensions of eID-Quality and
- define a function which maps the set of values in the different dimensions to a unique class of eID-Quality.

5.2.1 Dimensions of eID-Quality

Among the dimensions of eID-Quality, which would need to be considered for the development of metrics are the following:

- *Quality of registration process.* To rate the quality of the registration process for an eID, one would ask whether the registration process will include personal appearance at trustworthy institutions, population registers, biometrics, background checks and other security measures, which minimize the risk that such an eID is issued to a wrong person or contains false information.
- *Strength of the security mechanisms.* To determine the strength of the applied security mechanism in the eID and respective identity management protocols one may use the classes (basic, medium and high) and the methodology described in [ISO18045] (Appendix A.8).

- *Trustworthiness of equipment.* To rate the trustworthiness of the equipment (eID-token, client application component, server systems etc.) used for identification and authentication purposes, one may consider the evaluation assurance levels defined in [ISO15408-3] (Section 10).

Other aspects and more sophisticated considerations may be the subject of a forthcoming paper.

5.2.2 Function to map the dimensions to a unique class

Which function is appropriate to map the various quality components to a unique value for eID-Quality depends among other things on the possible values in the different dimensions. If all dimensions have the same classes (e.g. “basic”, “medium”, “high”) and are independent and equally important an appropriate function might be as simple as the minimum function.

5.3 Support for mobile devices

In order to allow the ubiquitous use of electronic identities, it is important to support mobile devices. Among the challenges related to using eIDs with mobile devices are (typically) the following:

- low computing power of mobile devices,
- smaller bandwidth and reliability of mobile networks and
- usability of mobile devices.

In the following, we will briefly discuss some issues related to usability and refer to [SMILE] for the other topics. The usability requirements of mobile user interfaces differ considerably from traditional desktop user interfaces and raise many challenges for interaction designers. Problems that designers of mobile devices have to face are for example:

- *Small screens and low screen resolutions.* It is a difficult task to present data in way that fits the low resolution of mobile devices. It is therefore necessary to follow other paradigms than those used for desktop applications. For example, it can be cumbersome for users to scroll through long pages of text.
- *Restricted possibility for text entry.* Mobile devices typically do not feature a keyboard, which makes it difficult for users to enter text.
- *Context of use.* Mobile applications are often operated outdoors, which has an impact on the readability of the display. Furthermore, users typically operate their mobile devices while moving, which means that they are not able to primarily focus on the application and thus have to finish operations in a fast and efficient way.

These topics and other challenges with respect to using eIDs with mobile devices may be addressed in [SMILE].

5.4 Privacy aspects

National (usually government issued) eIDs play a unique role in all identity management issues that are linked to a physical person; only governments usually have the necessary legal mandate and can cover the substantial cost of a highly secure enrolment process. This is for example evident when looking at the population registers that play a key role during eID issuance, or the use of biometrics for securing enrolment that would hardly be acceptable for private sector players.

While unique, current eIDs are often designed for eGovernment use where privacy issues are much less important than for private sector services. Current eIDs thus typically use a unique national identifier for all purposes and sectors of use. Unless explicit action is taken, there is a high risk to create a legacy where databases of personal data across sectors all use the same identifier as a key to personal data. This would render large-scale linking very easy and the legacy, once created, would be very difficult to correct at a later stage.

We therefore recommend that immediate action to avoid this risk is necessary. The most promising and least costly/disruptive approach seems to be a combination of three best practices: (i) The Austrian approach of dynamic derivation of sector/purpose-specific identifiers, (ii) the Belgian legal approach to prohibit the storage of the national unique identifier in databases, and (iii) optionally the Italian concept of zero-disclosure certificates that avoid to contain any personal data or known identifiers. An international collaboration is currently focusing on this approach and a draft paper is available [BMHHS07]. This approach is compatible with both the most common forms of eIDs that are based on X.509, as well as with the evolving standard of the European Citizen Card (prCEN 15480).

We believe that from this base-line that avoids the creation of harmful legacy, the addition of privacy features in eIDs has to be a gradual and continuous migration process. Before a significant volume of eID use in private-sector services will be reached, it is unlikely for Member States and other decision makers to see a strong needs for certain forms of privacy enhancement and it is even less likely that there will be a significant investment in the necessary technology and infrastructure. The gradual improvement of privacy characteristics in eID best practice realistically happens only once the need for every improvement step is perceived and is limited by economically viability at every stage of development.

The privacy-enhancement steps that we foresee is the use of Identity Providers both, for the creation of sector-specific or one-time-use identifiers at the source (i.e., to protect against linkability of personal data) and for the derivation of partial identities from the certified personal data that is typically contained on eID cards. In this context, the mentioned draft paper [BMHHS07] foresees several levels of privacy-enhancement that increase quality along with the cost of implementation. We plan to incorporate this eID privacy-enhancement approach into the informative parts of the evolving European standard for eIDs (prCEN 15480).

6 Conclusion

In this paper, we provided a short overview of electronic identities in an international perspective with special emphasis on national eID-cards in Europe. Furthermore, we briefly outlined our vision of global eID-Interoperability, highlighting related challenges and briefly sketching some possible steps towards global eID-Interoperability. While there are promising approaches around and about to be standardized or deployed, it is nevertheless evident that there are a fair number of research problems remaining before ubiquitous eID-Interoperability can become reality. Therefore, one may look forward to forthcoming research initiatives such as [SMILE].

References

[BMHHS07] B. P. Bruegger, M. Meints, M. Hansen, A. Hayat, K. Simoens, X. Huysmans: *An Inexpensive Privacy Protection Strategy for eID Cards*, Discussion Paper, available on requested from the authors

[BSI-eCard] BSI: *eCard-API-Framework*, Technical Directive BSI TR-03112, Federal Office for Information Security (Germany), 2007

[CardSpace] Microsoft: *CardSpace*, via http://cardspace.netfx3.com/

[prCEN15480-3] CEN/TC 224/WG15: Identification card systems — European Citizen Card — Part 3: European Citizen Card Interoperability using an application interface, Working Draft for prCEN/TS 15480-3, 2007

[ETSI-102204] ETSI: *Mobile Signature Service - Web Service Interface*, Technical Specification TS 102 204 V1.1.4, via http://www.etsi.org

[Higgins] Higgins Team: *Higgins Trust Framework Project Home*, via http://www.eclipse.org/higgins

[HüBa07] D. Hühnlein, M. Bach: *How to use ISO/IEC 24727-3 with arbitrary smart cards*, to appear at TrustBus'07

[ISO7816-15] ISO/IEC: *Identification cards - Integrated circuit(s) cards with contacts — Part 15: Cryptographic information application*, ISO7816-15, 2003

[ISO15408-3] ISO/IEC: *Information technology — Security techniques — Evaluation criteria for IT security — Part 3: Security assurance requirements*, ISO15408-3, 2005, via http://standards.iso.org/ittf/PubliclyAvailableStandards/c040614_ISO_IEC_15408-3_2005(E).zip

[ISO18045] ISO/IEC: *Information technology – Security techniques – Methodology for IT security evaluation*, ISO18045, 2005, via http://standards.iso.org/ittf/PubliclyAvailableStandards/c030830_ISO_IEC_18045_2005(E).zip

[ISO24727-3] ISO/IEC: *Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 3: Application Interface*, Committee Draft for ISO24727-3, 2006

[ISO24727-4] ISO/IEC: *Identification Cards — Integrated Circuit Cards Programming Interfaces — Part 4: API Administration*, Working Draft for ISO24727-4, 2007

[Kowa07] B. Kowalski: *Die eCard-Strategie der Bundesregierung im Überblick*, in the present proceedings

[Laur07] B. Laurie: *Selective Disclosure*, Version of May 11th 2007, via http://www.links.org/files/selective-disclosure.pdf

[Liberty] Liberty Alliance Project: *The Liberty Alliance*, via http://www.projectliberty.org/

[Liberty-Spec] Liberty Alliance Project: *Specifications*, via http://www.projectliberty.org/specifications__1

[MSWSS] Microsoft Inc.: *Web Services Security Specifications Index Page*, via http://msdn2.microsoft.com/en-us/library/ms951273.aspx

[Modinis] Modinis Consortium: *The status of Identity Management in European eGovernment initiatives*, via https://www.cosic.esat.kuleuven.be/modinis-idm/twiki/pub/Main/ProjectDocs/modinis.D3.5_Identity_Management_Initiative_Report_1_IIR1.pdf

[OSIS] OSIS Team: *OSIS: The Open-Source Identity System*, via http://osis.netmesh.org/wiki/Main_Page

[PRIME] PRIME Consortium: *Privacy and Identity Management for Europe*, via https://www.prime-project.eu/

[P3P] W3C: *Platform for Privacy Preferences (P3P) Project*, via http://www.w3.org/P3P/

[RoRe04] J. Rosenberg, D. Remy: *Securing Web Services with WS-Security – Demystifying WS-Security, WS-Policy, SAML, XML Signature, and XML Encryption*, Sams Publishing, 2004

[RFC1510] J. Kohl: *The Kerberos Network Authentication Service (V5)*, IETF RFC 1510, via http://www.ietf.org/rfc/rfc1510.txt

[RFC2025] C. Adams, *The Simple Public-Key GSS-API Mechanism (SPKM)*, IETF RFC 2025, via http://www.ietf.org/rfc/rfc2025.txt

[RFC2246] T. Dierks, C. Allen: *The TLS Protocol*, Version 1.0, IETF RFC 2246, via http://www.ietf.org/rfc/rfc2246.txt

[RFC2510] C. Adams, S. Farrell: *Internet X.509 Public Key Infrastructure - Certificate Management Protocols*, IETF RFC 2510, via http://www.ietf.org/rfc/rfc2510.txt

[RFC2743] J. Linn: Generic Security Service Application Program Interface, Version 2, Update 1, IETF RFC 2743, 2000, via http://www.ietf.org/rfc/rfc2743.txt

[Rand07] C. Randlkofer: *Die elektronische Steuererklärung (ELSTER) - Status und Ausblick – OpenElster*, in the present proceedings

[RuTr07] M. C. Rundle, P. Trevithick: *Interoperability In the New Digital Identity Infrastructure*, (February 13, 2007), via http://ssrn.com/abstract=962701

[SMILE] SMILE Consortium: *Secure Mobile Identity Layer for Europe*, FP7 proposal, 2007

[SourceID] SourceID Team: *SourceID - Open Source Federated Identity Management*, via http://www.sourceid.org/