A Federated Identity Management Architecture for Cross-Border Services in Europe

Prof. Dr. Reinhard Posch
Federal CIO AUSTRIA

Abstract: Identification is the basis for trusted relationships in business as well as in administration. In Europe Member States have developed rules and methods how citizen and businesses are identified electronically. Cross-border applications still suffer from the fact that these methods differ from the legal, from the organisational but also from the technical point of view. Federated and interoperable identity management can contribute to a seamless way of offering electronic services. Taking into consideration that such cross-border services need to fit into the existing structure models and structures of interoperability are discussed with a special focus on the needs of government applications.

The essence of eID when talking to governments

With physical presence we have a log tradition in giving evidence of the identity. In general "identity documents" are used. These documents contain information about the subject that allows a sufficiently secure link to the actual person plus methods that should prevent from tampering with the document. In the general case these documents are issued by an authority.

In the electronic world we see a slight shift. As technology for electronic identity documents was not available until recently we did see a shift from identity documents to other means with electronic services. Usually the resulting method binds to a purpose in this case. E.g., when identifying at an electronic shop it is obviously sufficient if someone presents a credit card to pay. As the service is in the same dimension as the identification (the value is in both cases money) abuse is unlikely. Therefore it is possible to use low security and even work with userid and password. As we see with electronic banking the picture and risk changes totally when application switches from the type "shop" to "access".

With administration "values" are not monetary values and thus identification becomes a key issue. A further fact is that – unlike with business – it is not the choice of the citizen to get in contact with administration. Both facts have influence on the security demands but also on the privacy demands an eID system has to meet.

In practical applications we see different security levels. However, from a legal point of view there is in most cases little justification for the introduction of security levels. This

issue is not transparent as long as we operate within one administration since the application still will map their security demands into the user interface. However as we walk cross domain this absence of justification to differentiate between security demands becomes a real issue. This fact becomes even more complicated as we do not have the same structure of administrative processes in different administrative domains. Unless there are extensive bilateral agreements we might end up in a situation where we have only two states "identified" "non-identified". Since we still want to offer basically all administrative procedures identification will need quality.

The key players

With the use of eID we identify the user – the subject to be identified and the service the user desires to access. As long as we do not introduce further roles the service would have to take care of the **registration**, the pairing process between the user's identity a and the security presentation that might range from userid/password to card/pin as needed, the **management** that consists of revocation, lost token/ forgotten password management, and the **handling of the security presentation**.

This setup forms a closed circle and all other services would have to offer the same elements and perform the same procedures. If the same security presentations are foreseen, one would also need a compatible security policy at all services concerned.

Interoperability and eID federation has the following main goals:

- Reduce cost both on the service and on the user side. Registration and management are high cost services. Still both have a very low frequency.
- Enhance comfort as the ideal situation would only need one security presentation.
- Offer enhanced services like single sign on etc.

To benefit from these advantages a set of further services and elements need to be defined and added to the simple model described above.

Each service has implicitly or explicitly an application oriented "identifier" of each of its users. To enable synergies of eID registration and eID management some sort of implicit or explicit mapping of these sets of "identifiers" must exist to avoid the need of multiple registration.

These identifiers and the policy of mapping and handling will greatly define the data protection capabilities of an eID system. Generally we can see three classes:

- **disjoint**: no direct interoperability of eID is possible. One still could share security devices and mechanisms etc. but registration and management would need duplication or escort mechanisms. (France would be an example)
- **flat**: a centrally managed identifier that is is used throughout. This raises many privacy concerns that can usually only be kept under control by restrictions of use of the identifier. (Italy, Sweden, and Belgium are examples)
- **derived**: through a security mechanism, that can be a central service or a

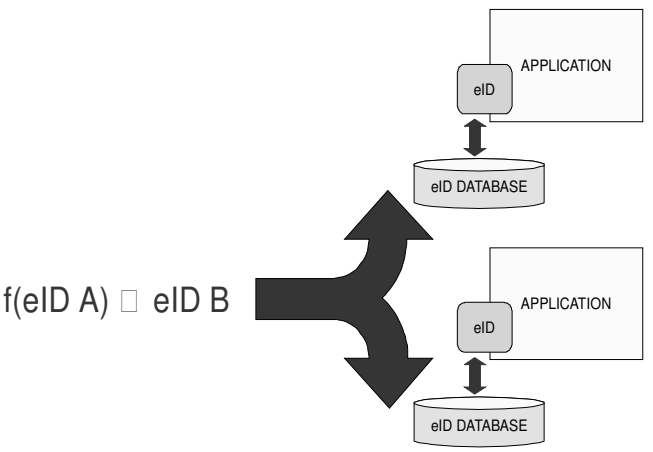
cryptographic mechanism systematic mapping is performed in a way that does not allow cross-relating identifiers (New Zealand, Denmark, and Austria are examples)

When implementing interoperability and federation care has to be taken not to break the given protection principles when crossing the border. This is of high importance as crossing the border twice would result in the same breach within the country.

A first additional service with the implementation of interoperability was identified as the **register of identifiers**. Given these registers of identifiers and given a mapping service among these registers back office interoperability can be implemented.

Back office interoperability and access interoperability has to be clearly distinguished. As we have seen data protection is key with back office interoperation. Technology on the other hand is in the foreground when it comes to access interoperability. The combination of the methods used with these two elements will define the interoperability model.

As we see different schemata with different registers of identifiers we need a further service that translates from one schema into another. This **identifier translation service** needs a high degree of trust as it interfaces with both schemata the source and the destination schema of identifiers. It will be the key question who can operate such translation and also where can such translation be executed. As we hardly see identifier schemes without restrictions of use there must be adequate control by the owner of the identifier over the execution of the identifier translation. If for example the user is deemed to be the owner of the identifier the translation must be under his control. This is also an aspect that will influence applicability of specific interoperability models.



Having in place back office interoperability access interoperability can be implemented. Assuming that access methods are in place that perform authentication of users at a specific point in time and associate an application identifier so that the specific service can be accessed we still need interfaces that allow other technologies coming from other identification domains to perform their security presentations. This results in a further

service that translates security presentations.

This security presentation translation service needs special focus. It occurs directly or indirectly at any service and we cannot assume that we have all services well organised in layered structures. Still security presentation might range from userid and password, client certificates, one time SMS codes to electronic signatures. Viewing effort and cost the major part will be in this last service. Standards and practices offer models for this task SAML [SAML], OpenID [OpenID], CardSpace [CardSpace] etc. have to be mentioned here.

The goals of interoperability

The first goal would be just to provide identified access. This however is not sufficient. Implementations of eID usually include a series of assumptions and many of them are implicit.

It will therefore be necessary not only to map identifiers but also to have a transparent knowledge of the nature of this mapping and keeping this with the target identifier.

The following example should make this more transparent.

With the Austrian eGovernment law [E-GovG] a regulation is in place that focuses inclusion in a way that for people not able or not willing to personally use eID and eGovernment a civil servant can automatically acquire a mandate so that this civil servant can act on behalf of the applicant. While this regulation affects eID and mandates which form an essential part of eID when this person acts towards an Austrian government agency, it is neither applicable to non Austrian agencies nor to companies. This clearly shows that the acting on behalf example and the country of origin must be in the security assertion for eID and must be transparent to the application.[EGOV ABC]

A further goal is to allow inheritance of identification properties. The above example shows one instance where this is key. However there are many more examples like e.g. the identification quality (e.g. qualified certificate).

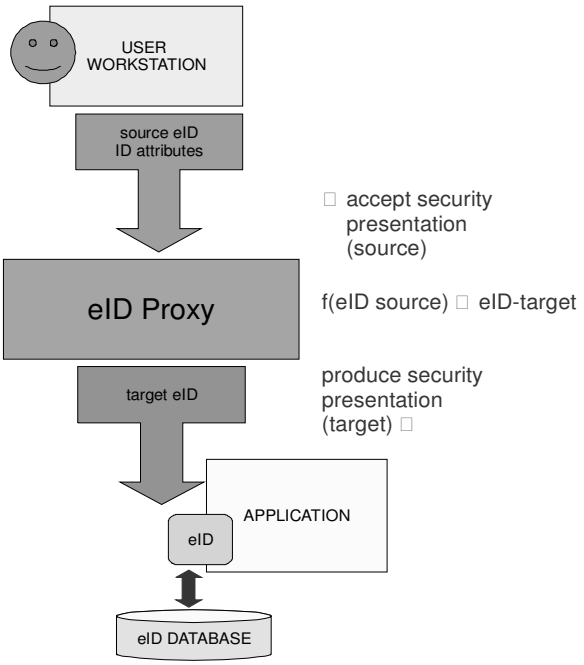
Finally an important goal is to provide inheritance of security and data protection properties. Without such inheritance it would be impossible to implement legally accepted eIDM systems.

Models of interoperability

The choice of models is driven by the legal and organisational environment. Applicability and legality might restrict to a large extent. To provide specific examples a userid / password schema could be mentioned. In such schema a model with central verification might be the only way to manage. Any model that counts on the user's workstation and decentralised operation cannot be used. However, as it comes to data protection such central exchange might be unacceptable as it holds all details about identifications.

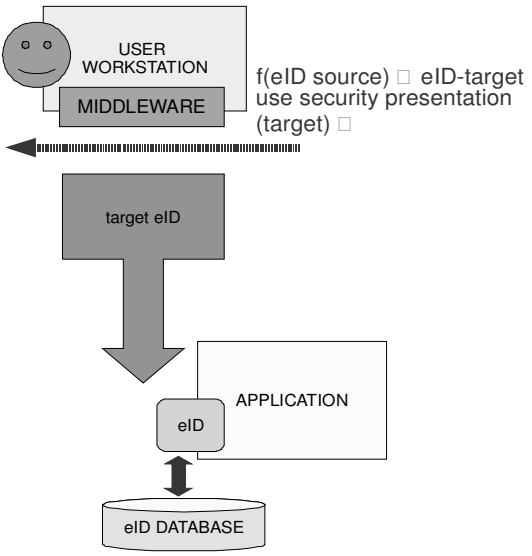
In general we see two models for eID interoperability:

1. the “PROXY MODEL” where an intermediate transforms eIDs – both the identificators and the technology.



   One of the questions to solve in this context is the location of the domain border which in many cases would be the country border. For obvious reasons this can be either above or below the eID PROXY. For the source eID this makes a huge difference.

2. the “MIDDLEWARE MODEL” where a software component at the user performs transformation and mapping.

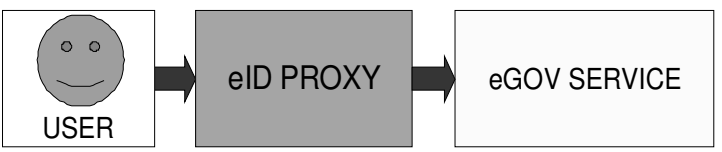


While the domain border is clearly defined here we also see that methods cannot be used where there is a technical risk that a user/aggressor would tamper with the source security presentation. There is no trusted control over the source security presentation. In a more practical sense this means that userid/password like identification cannot be used in this case. Only cryptographic security presentations are eligible.

For the use with administration the biggest difference is the number of involved partners. The PROXY MODEL involves 3 partners (source, target and proxy) and the MIDDLEWARE MODEL involves only two (source and target).

eID and liabilities of government

The difference mentioned in the previous chapters matters with eGovernment applications. The legal basis usually sees an applicant and an agency. For purposes of delivery there is also the postal service in the delivery chain.

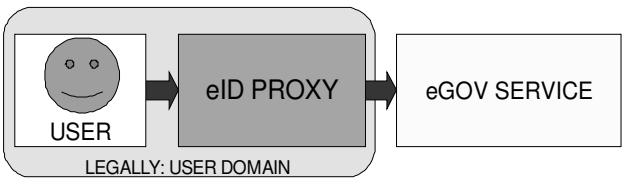


For the time being the only way to have a further party in the loop is through an mandate given by the applicant. This puts the Proxy legally into the user domain. A full proxy situation as shown above would require changes in the administrative procedural laws.

In some cases such mandate could be given to an attorney by the legal framework or it could be set out in law like for children or other special relations. However, such

relationships are in the general case not evident through the register of identifiers and therefore cannot automatically be processed.

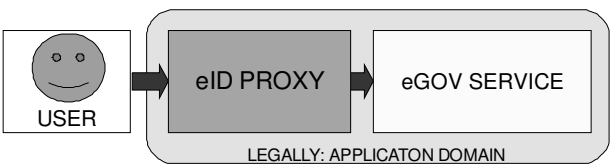
At a first view assigning the proxy legally to the user domain looks promising. However, while it puts the user under full control in terms of data protection it also puts the full risk on the user's side. Any incident or loss of rights in administrative procedures will have to be covered by the user which possibly can on a separate channel claim compensation from the proxy.



Such shift of liability from administration to citizen is hardly justifiable and risks decreasing take-up.

In general there are two ways out of this situation so that the setup where the user talks directly to the administration remains.

- From a systematic point of view the eID PROXY could also be assigned to the application domain.



  While this sounds easy it would have problems when such proxy is physically run by a different organisation or even by the private sector. In these situations the legal situation would need to allow for such a situation – this is not the case where the legal situation foresees explicitly that the administration performs the task – and it would also require specific contracts which makes it complicated to be done as a general approach.

- The second solution was already addressed is the integration into the middleware, where there is obvious user control and consent and no shift of liabilities as no faulting third party is in the game.

The Austrian citizen card strategy

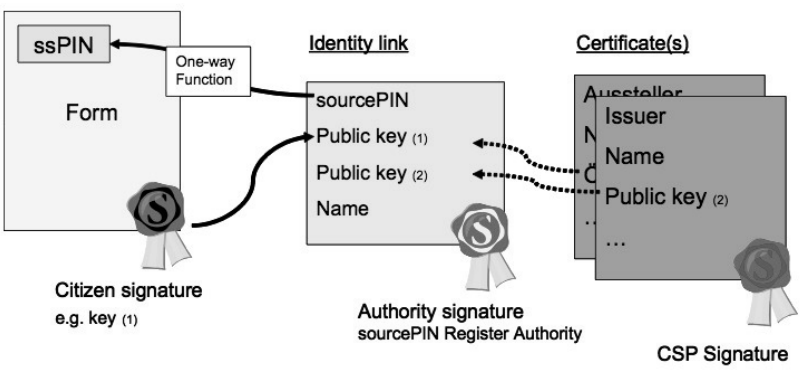
As described in the ABC guide to eGovernment [EGOV ABC] the Austrian citizen card itself is not dependent on any one particular technology. Moreover, there is not just one kind of citizen card. It is up to the citizen to choose what technology to use, from those available, in order to identify him or herself electronically. In principle, any token (not only a chip card) which makes it possible to sign electronically in a secure manner and to

store data in free areas is suitable for use as a citizen card. In the same way as a passport, driving licence or identity card can be used as identification in the "paper world", the electronic world offers a variety of possibilities. Regardless of whether a chip card, mobile phone or USB equipment is used, the important point is that the medium satisfies certain security requirements.

As a result the concept is open and allows basically any token with adequate security to be integrated. This is explicitly backed up in the Austrian eGovernment law [E-GovG].

To establish with certainty a link between an electronic procedure and the person who initiated it and thus to ensure that non-authorised persons cannot access personal data identification must be backed up with the quality of information of the central residence register (CCR). Until now, depending on the public authority concerned, reference numbers such as the social security number or tax number were used in administrative procedures for this purpose.

In order to prevent confusion as to the person involved in electronic procedures, the sourcePIN is used to identify that person uniquely. The sourcePIN is derived from the CRR number by way of an encryption process and stored in the citizen card in an electronically signed form. The sourcePIN can therefore be controlled only by the rightful holder of the citizen card. For data protection reasons, the sourcePIN of natural persons may not be stored directly in applications.

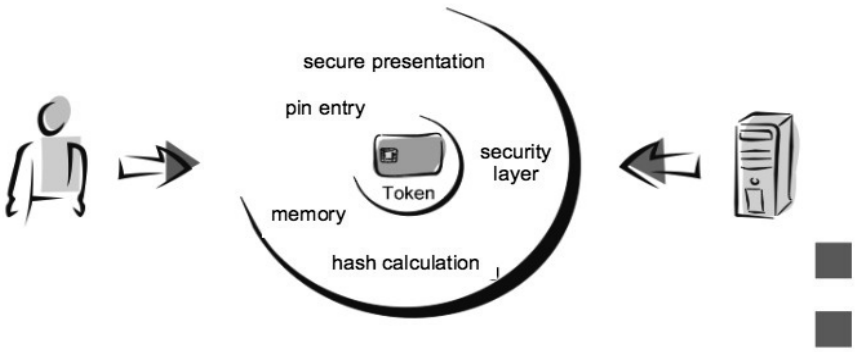


To ensure data protection in administrative procedures, the person must be identified using the sector-specific personal identifier, which is derived from the sourcePIN and the sector code. The application of these two encryption processes (encryption of the CRR number in the sourcePIN and derivation of the sector-specific personal identifier from the sourcePIN) guarantees a high level of data protection and rules out the risk of people shorn of all privacy.

The citizen card concept not only lays down particular security requirements but is also aimed at ensuring choice by permitting several different forms of citizen cards. At present, all Austrian-issued bank cash point (ATM) cards and the health insurance cards “e-card” are compatible and can be used as citizen cards following activation. However, in the spirit of European mobility, even citizen cards issued in the other Member States of the EU can be used, provided they are equipped with an identity link or are capable of being so equipped. At present, citizen cards are issued for example in Belgium, Estonia,

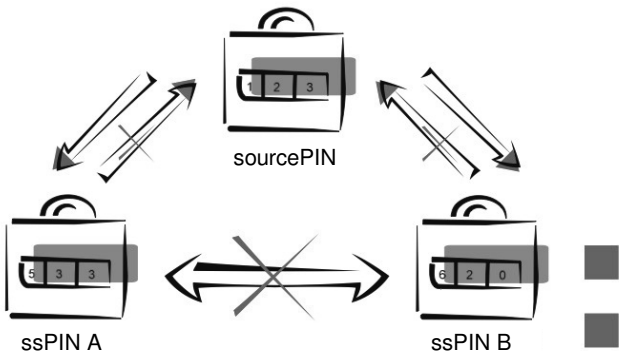
Finland and Italy and it is already possible to use those cards in Austrian e-government federating the identities of the respective Member State.

If the citizen card is used in an online procedure, the citizen-card environment communicates with the procedural application. This communication is not direct but rather takes place via an open interface we refer to as security layer interface. This introduction of an open interface means that applications and the security infrastructure can be developed independently of each other.



When submitting an application to an authority in electronic form, the applicant must be uniquely identified and authenticated. This entails ascertaining whether the person is really the person he or she claims to be and whether the person is actually authorised to submit the application. However, a person's name is not, by itself, sufficient to verify identity and therefore the identity link is used for the purposes of identification and authentication.

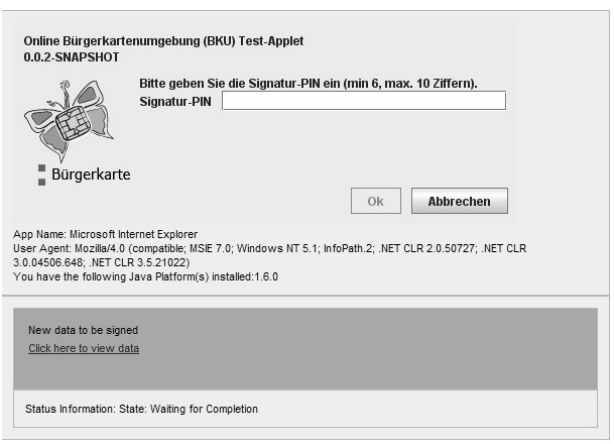
The Identity Link links a person's signature certificate that has been issued by a Certification Service Provider (CSP) to a unique identifying feature – the sourcePIN that is issued by the sourcePIN. This link between the certificate and the person is signed electronically by a public authority (the sourcePIN Register Authority). This creates a cryptographically secured link between the electronic signature of a person (the signer) and a unique identifying feature of that person. The identity link makes it possible to identify a person uniquely and in a way that can be automated in electronic communications with the authority via the sector-specific pin (ssPIN).



This cryptographic measure ensures data protection and with this a very broad use of the eID card. It also allows extension to interoperability at European level and federating identity management.

To practically ensure this protection a middleware approach for deployment and interoperability is followed. Starting 2004 Austria now has some 16 Mio cards in the field that are eligible for activation as citizen cards. A freely available software client is supplied with the card and since 2008 the qualified signature that forms the basis can be obtained free of charge when activated on an e-card (the health insurance card everyone gets from the social security system).

Even with this ease of access there are still hurdles that have impact on take-up. Especially when looking at the implementation of the service directive by the end of 2009 we would see a very complicated situation when integrating all new eID tokens around Europe into this software client especially with the distribution of the client.



Due to this fact Austria moves during the second half of 2008 to a “client -free” citizen card. The above figure shows a beta version that is already in place for access to access the federal ministry's document and workflow system. Assuming a standard PC/SC reader at the user’s environment a java applet based minimal citizen card environment is downloaded at run time. This results two basic advantages:

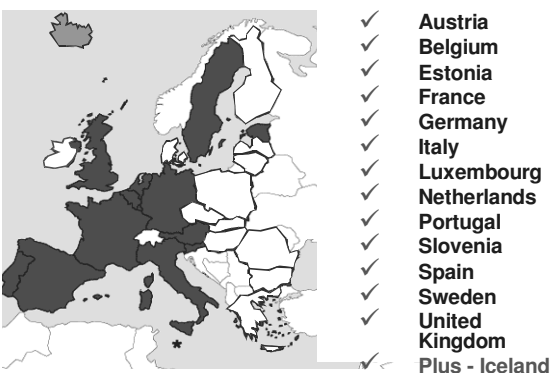
- It presents a sandbox model that is transient and more disjoint from the user's workstation, where the user's workstation might be viewed as the most critical element in terms of security.
- Any additional or new token that should be integrated into the system can immediately be deployed even cross border as it is just the applets not the user's workstation that needs an update.

The resulting scenario gives instant access – multi platform – to any accepted European eID token. This scenario will by the end of 2008 be made available open source so that it can be used by anyone including business.

The interoperability part of this scenario will be developed as a part of the STORK [STORK] project.

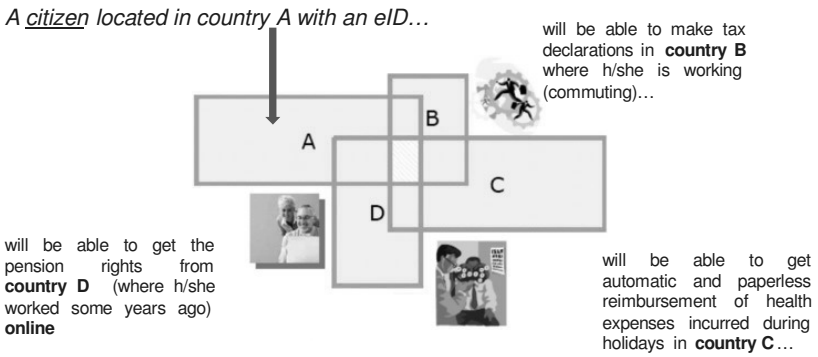
STORK and the EU dimension

Commitments to strengthen cross-border eGovernment are inter alia given with the i2010 initiative [i2010] or the Service Directive [SERVICE]. Vehicles to facilitate these ambitious goals are large scale pilots between Member States. The European Commission has initiated such large scale pilots under the Competitiveness and Innovation Framework Programme, Information and Communication Technologies Policy Support Programme (CIP ICT-PSP). A pilot on interoperability of eID [STORK] brings together 13 EU Member States plus Iceland.



The objectives of STORK are to:

- define common rules and specifications to assist mutual recognition of eIDs across national borders,
- test in real life environments, secure and easy-to-use eID solutions for citizens and businesses
- interact with other EU initiatives to maximize the usefulness of eID services.



To approach interoperability of existing national eID solutions STORK will develop interoperability layers following the two approaches discussed in this paper – the proxy approach and the middleware approach. This shall be tested in several operational applications, namely the five pilots cross-border authentication platform for electronic services, SaferChat for children and juveniles, student mobility, electronic delivery, and change of address. These pilots are expected to be operational for at least a year starting in 2009.

STORK shall identify and overcome obstacles when advancing the heterogeneous existing national eID initiatives to a system that interoperates. The experience gained shall pave the way for federated identity management in Europe.

References

[Cardspace] David Chappell: Introducing Windows CardSpace, Microsoft Vista Technical Articles, April 2006.

[E-GovG] Austrian Federal Act on Provisions Facilitating Electronic Communications with Public Bodies; Federal Law Gazette, part I, Nr. 10/2004, last amended by Nr. 59/2008.

[EGOV ABC] Administration on the Net - An ABC Guide to E-Government in Austria, Digital Austria, January 2007.

[i2010] i2010 – A European Information Society for growth and employment, European Commission SEC(2005) 717, June 2005.

[OpenID] OpenID Authentication 2.0, OpenID Foundation, December 2007.

[SAML] Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, March 2005.

[SERVICE] Directive 2006/123/EC of the European Parliament and of the Council of 12 December 2006 on services in the internal market.

[STORK] Secure Identity Across Borders Linked – STORK, European Commission ICT PSP Grant Agreement 224993, July 2008.