Cross-Border Legal Identity Management

Bernd Zwattendorfer[1], Arne Tauber[1], Klaus Stranacher[1], and Peter Reichstädter[2]

[1] E-Government Innovation Center (EGIZ), Graz University of Technology, Graz, Austria
{bernd.zwattendorfer,arne.tauber,klaus.stranacher}@egiz.gv.at
[2] E-Government / ICT Strategy at Austrian Federal Chancellery, Vienna, Austria
peter.reichstaedter@bka.gv.at

Abstract. Electronic Identities (eID) and their cross-border recognition are on top of the agenda of various e-Government initiatives of the European Commission (EC). Therefore, the EC launched the EU large scale pilot STORK, which was running for about 3.5 years and finished at the end of 2011. In this period, STORK has established a European eID interoperability platform for citizens. The focus of STORK was to achieve eID interoperability of natural persons. However, many e-Government processes are conducted by representatives of legal persons. Hence, this paper proposes an eID interoperability framework for the cross-border identification and authentication of legal persons or professional representatives using electronic mandates. The framework strongly bases on the findings of STORK and introduces an extension of the STORK framework supporting cross-border identification and authentication of legal persons.

Keywords: Electronic Identity, eID, Identity Management, Legal Identities, Legal Persons, Empowerment, Electronic Mandates, STORK, Interoperability.

1 Introduction

Identity Management (IdM) related to secure identification and authentication of citizens defines one of the major challenges in the past years and will last a few more years. A lot of European countries have already rolled-out different kinds of electronic identity (eID) solutions to enable secure identification and authentication of citizens in online processes. Especially in the area of e-Government transactions, IdM is of major interest because in many cases sensitive personal data are processed.

Due to a higher mobility of citizens and businesses within Europe, secure cross-border identification and authentication has gained high importance. However, most European countries rely on their own national approach for IdM, which burdens the economic growth and competitiveness within the European Union. This also makes citizens' mobility within the EU difficult and hinders cross-border transactions. To fill this gap, the European Commission has launched the large scale pilot (LSP) STORK[1] (Secure Identity Across Borders Linked) in the year 2008. The STORK vision was *"to establish a European eID Interoperability Platform that will allow citizens to*

[1] https://www.eid-stork.eu/

H.J. Scholl et al. (Eds.): EGOV 2012, LNCS 7443, pp. 149–161, 2012.

establish new e-relations across borders, just by presenting their national eID" [1]. STORK has built an eID framework on top of various national heterogeneous solutions to make them interoperable. The main focus of STORK lay on secure cross-border identification and authentication of natural persons only.

However, many e-Government transactions are conducted by legal persons or professional representatives. Electronic mandates for the expression of proxyship[2] are one solution for that. Other approaches are the usage of attribute certificates or the assignment of appropriate credentials to the representing natural person. Some EU countries have such an e-Mandate solution in place or are planning to establish one. Similar to the situation of natural persons before STORK, the identification and authentication of legal persons is unresolved in a cross-border context. Hence, the present paper proposes and discusses an eID interoperability framework for the cross-border identification and authentication of legal persons using electronic mandates.

The remainder of the paper is organized as follows. In Section 2, we describe related work with regard to mandate management and the Austrian and Dutch mandate systems as examples. Section 3 gives a brief introduction to the findings of the large scale pilot STORK and explains its interoperability models. The subsequent Section 4 describes the extended STORK architecture enabling cross-border authentication of legal persons or professional representatives for a chosen scenario. Finally, we draw conclusions summarizing the main facts and open issues.

2 Related Work

While IdM for natural persons in the EU has been widely achieved with the roll-out of national eIDs, there is a green-field situation in many Member States (MS) regarding legal IdM. The IDABC Study for eID Interoperability for PEGS [2] reports for representation and mandate management

"[…] that a systematic approach to mandate management and authorization functionality – i.e. the ability to allocate, retract or verify specific permissions of a specific entity - in the examined eIDM systems was still altogether rare. 22 countries out of 32 (69%) have no form of mandate/authorisation management, other than the allocation of certificates or credentials to the representatives of a specific legal entity."

and

"[…] only two countries have implemented systems of mandate/authorisation management which can be characterised as systematic."

Besides Belgium, Austria is the second country mentioned by the 2009 IDABC study. Since then, also the Netherlands have introduced a systematic approach to legal IdM called eRecognition [3]. The following subsections give a brief overview of the Austrian and Dutch systems to demonstrate how legal IdM is realized on a national scale using systematic approaches by accessing central registers.

[2] E.g. a natural person is empowered to act on behalf of another person.

2.1 The Austrian Mandate System

Authentication and identification in Austrian e-Government is based on the so-called citizen card, the Austrian national eID. The citizen card is a secure signature creation device (SSCD) that can be used to create qualified electronic signatures (QES) compliant to the EU Signature Directive [4]. The identification data (name, date of birth and unique national identification number) of the citizen are stored in a special XML-based data structure on the citizen card. The legal basis for the citizen card is laid down by the Austrian e-Government Act [5], which came into effect in 2004. Representation of legal persons has been considered by the Austrian e-Government strategy from the beginning and is thus also an integral part of the Austrian e-Government Act. On this basis, Austria has built an infrastructure for legal IdM using the concept of so-called "electronic mandates" [6]. Electronic mandates are security tokens asserting that a person is empowered to act on behalf of another natural or legal person. The asserting authority is the Austrian SourcePIN Register Authority, a sub-organization of the Austrian Data Protection Commission. From a technical point of view, electronic mandates are well-defined XML structures holding the following information:

- Electronic identity of the representative including name, date of birth and unique national identification number
- Electronic identity of the mandator including name, date of birth and unique national identification number
- Date and place of mandate issuance
- Content and scope of empowerment
- Unique mandate ID
- Any restrictions (financial, timely, etc.)

The Austrian mandate management infrastructure fits seamlessly into the IdM system for natural persons and is based on a just in time (JIT) generation of electronic mandates [7]. This means that the SourcePIN Register Authority acts as an Attribute Provider (AP) by fetching the information for the power of representation, i.e. the mapping between legal and representing natural persons, from constitutive registers, for example the Company Register or the Central Register of Associations. Based on this information, an electronic mandate is created on-the-fly, asserted by the SourcePIN Register Authority through an electronic signature and provided to the identity provider and subsequently to the service provider. Details of this process are discussed in more detail in Section 4 because the Austrian concept is used as sample national legal person management system for demonstrating our cross-border solution.

2.2 The Dutch eRecognition System

Parallel to DigiD[3], the national IdM system for natural persons, the Dutch Ministry of Economic Affairs has provided a systematic approach for legal IdM called eRecognition [3]. This approach is quite similar to the Austrian solution and relies on the

[3] http://www.digid.nl/

so-called eRecognition network to authenticate and identify legal persons. This network consists of the following entities:

- A **service catalogue** where service providers can manage their services.
- An **authentication service** to identify and authenticate the representative (natural person).
- A **mandate registry** containing the information for the power of representation. It establishes the link between a legal person and the representing natural person, e.g. the company manager.
- A **recognition broker** creating and asserting the authentication information for a legal person (represented by a natural person) and providing this information to service providers.

3 Stork

Many European Union countries have already rolled-out national eID solutions or are planning to do so. Those solutions are usually issued by national or regional governments and aim for more secure identification and authentication processes in online transactions. Secure identification and authentication defines a major requirement especially in the fields of e-Government or e-Business where sensitive personal data needs to be processed.

Currently, most Member States rely on smart card-based approaches supporting two-factor authentication. However, in addition e.g. Austria and Estonia offer their citizen its eID solution based on mobile phones. Although the first national eID solutions have approximately been existing since 1999 (e.g. Finland [8]), most solutions are tailored to support domestic and national requirements only and lack in cross-border applicability. Hence, citizens from one European Union country are not able to use their national eID for online services of other European Union countries. This fundamental gap has been taken up by the European Commission in 2008 which introduced the 3-years lasting European large scale pilot project (LSP) STORK [1].

This co-funded project by the EC aimed on implementing and piloting a technical interoperability layer to achieve cross-border acceptance of various national eID solutions within the EU. Hence, the main objective of STORK was not to develop and introduce a new eID concept for all EU Member States but instead taking the heterogeneous existing solutions as a basis and set up a framework on top of it to make them interoperable. However, the focus of STORK was to achieve eID interoperability of natural persons only.

In general, the STORK architecture sets up on two different basic models, the so-called PEPS (Pan-European Proxy Service) and MW (Middleware) model. The first model follows a proxy-based approach where a single gateway is installed and deployed in each Member State. Those individual gateways build a kind of trusted federation network which enables cross-border authentication. On the one side, the aim of these gateways is to hide complexity of national eID solutions from the interoperability layer. The other side is to implement the transport protocol for cross-border identification and authentication data transfer. For taking part within the STORK

interoperability layer and depending on their home country, service providers (e.g. public authorities or private sector enterprises) offering online applications connect electronically to their adequate gateway (PEPS). Within the second model (MW model) no central instance exists and the service provider itself needs to support several eID tokens using a common middleware. In contrast to the PEPS model the middleware is directly installed in the service provider domain. Comparing both models, the PEPS model hides all specifics of national eID infrastructures whereas in the MW model the service provider needs to maintain all different eID tokens that are supported. However, in terms of liability and privacy the MW model has its main advantage as a direct communication channel between the service provider and the end user is possible. In contrast to that, the PEPS acts as trusted intermediary between the service provider and the end user.

Based on these two different basic models, four interoperability models can be distinguished within STORK:

- PEPS – PEPS interoperability model
- MW – MW interoperability model
- MW – PEPS interoperability model
- PEPS – MW interoperability model

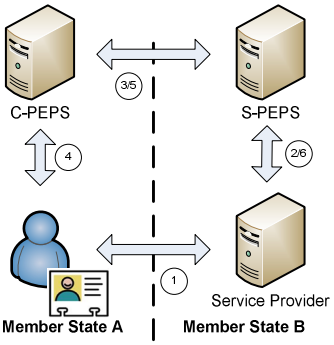

Fig. 1. PEPS – PEPS Model

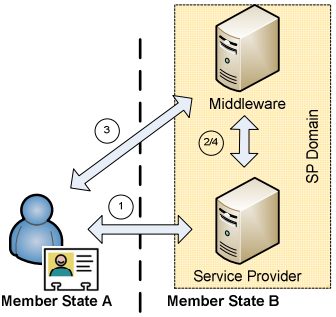

Fig. 2. MW – MW Model

Fig. 1 illustrates the PEPS – PEPS interoperability scenario. In this case, a citizen originating from Member State A wants to access and use a certain service in Member State B which requires authentication (Step 1). Both Member States follow the PEPS approach and each MS has a single gateway (PEPS) deployed. By the help of the STORK interoperability architecture, the citizen of Member State A can use her own national eID token for authentication at the service provider in Member State B. Regarding the process flow, the service provider of MS B forwards the authentication request of the citizen to its national PEPS (Service Provider-PEPS or S-PEPS), cf. Step 2. The S-PEPS presents the citizen a country selection page where she can select the country she is originally from. Based on this information, in Step 3 the S-PEPS

redirects the user to the PEPS of the citizen's home country (Citizen Country-PEPS or C-PEPS). Authentication and identification fully takes place at the C-PEPS involving one or more identity or attribute providers[4] using the citizen's national eID token (Step 4). If authentication was successful the C-PEPS transmits the citizen's identification and authentication data back to the requesting S-PEPS (Step 5). In turn, these data are forwarded to the authentication requesting service provider (Step 6). Based on these transferred data the service provider can either grant or deny access to the requested services. The protocol for structuring the identification and authentication data and its transfer is based on the well-known standard Security Assertion Markup Language (SAML) [9]. Details on this common protocol can be found in the common STORK interface specification [10].

Fig. 2 shows the MW-MW interoperability model on an abstract level. In this use case, both the citizen and service provider country follow the middleware approach. In this approach, no intermediary between the user and the service provider exists. The authentication handling middleware is directly installed and maintained in the service provider's domain. It is assumed that a citizen originating from MS A wants to access a certain service in MS B (Step 1). For authentication, the citizen is forwarded by the service provider to the deployed middleware which integrates all desired national eID tokens (Step 2). In the MW model, in most cases identity information is directly stored on the citizen's eID token and does not need to be fetched from other identity or attribute providers. The middleware extracts the desired identity information from the eID token (Step 3) and forwards these data to the authentication requesting service provider (Step 4).

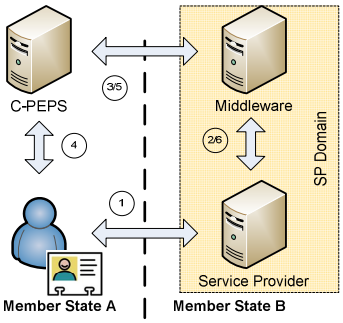

Fig. 3. MW – PEPS Model

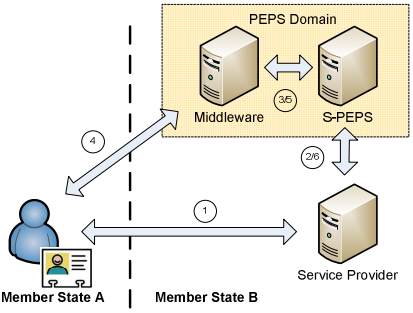

Fig. 4. PEPS – MW Model

The first interoperability model combining both STORK basic models is shown in Fig. 3. A citizen originating from a country that follows the PEPS approach (MS A) wants to use a service at a service provider whose country relies on the MW approach (MS B), cf. Step 1. After requesting authentication, the middleware deployed in the

[4] Identity or attribute providers are not especially illustrated in fig 1. They are assumed to be part of the C-PEPS in this picture.

SP domain does not directly access the citizen's eID token but forwards the authentication request to the corresponding C-PEPS of the citizen's home country (Step 2 and 3). Similar to the PEPS-PEPS scenario in Fig. 1, the citizen identifies and authenticates at the national C-PEPS in his home country (Step 4). The retrieved identity and authentication information is returned to the middleware in country B (Step 5) and further transferred to the service provider who regulates access control (Step 6).

The second STORK interoperability model combining both basic models is shown in Fig. 4. In this case, a citizen originating from a MW country (MS A) wants to access services at a service provider located in a PEPS country (MS B), cf. Step 1. Since the service provider does not support the MW model, similar to the normal PEPS-PEPS model the service provider forwards the authentication request to its corresponding national S-PEPS (Step 2). In this case, the S-PEPS has the middleware installed in its domain where the request is forwarded to (Step 3). Hence, as in the MW-MW model, the middleware directly communicates with the citizen's eID token (Step 4). The middleware installed in the PEPS domain supports all desired eID tokens and manages the MW authentication for the PEPS. Having the citizen successfully authenticated, the identification and authentication information is transmitted to the S-PEPS (Step 5) which in turn forwards these data to the requesting service provider (Step 6). Again, the S-PEPS asserts the SP that the citizen has been successfully authenticated.

4 Extended Architecture

The STORK interoperability framework has been developed to enable secure cross-border identification and authentication in a European context. The main objective of STORK was to develop an interoperability framework by taking existing national eID infrastructures as a basis. The applicability of this framework for cross-border eID authentication has been demonstrated amongst six pilot applications. Details e.g. on the "e-Delivery Pilot" or on the "Safer Chat Pilot" can be found in [11] and [12]. However, the main objective of STORK was to demonstrate cross-border authentication of natural persons only.

Nevertheless, besides unique identification and authentication of natural persons also legal persons play a major role in e-Government or e-Business processes. Unfortunately, legal IdM in electronic processes does not define a trivial task. Across Europe, only a low number of countries have introduced or deployed a legal IdM system within their domain. Examples for such systems have been described in Section 2.

Since delegation and representation of legal persons are valid processes in traditional or paper-based applications, their electronic pendants define also important processes in e-Government or e-Business. However, most electronic representation systems are usually tailored to satisfy domestic and national requirements only. Thus similar to STORK, currently there also exists a gap of cross-border applicability of various heterogeneous legal person or representation systems. To bypass this gap, in our proposed work we took up the STORK interoperability framework to also demonstrate cross-border identification and authentication of legal persons since issues for

transferring data of natural or legal persons across borders are similar. By using our proposed solution, cross-border identification and authentication becomes possible on technical level. To show the feasibility of our solution, we selected one out of the four STORK interoperability scenarios to demonstrate the cross-border transfer of legal person attributes. Therefore, we have set up the STORK infrastructure and connected it to the Austrian national mandate management system (as additional attribute provider) within a laboratory environment. For our demonstration, we took the PEPS-MW model as a basis and coupled the Middleware with this additional attribute provider responsible for national legal person identification. In our extended scenario, legal person identification is based on the name of the legal person and its register number, e.g. the company name and company number. Fig. 5 illustrates the rough and extended architecture of our set up.

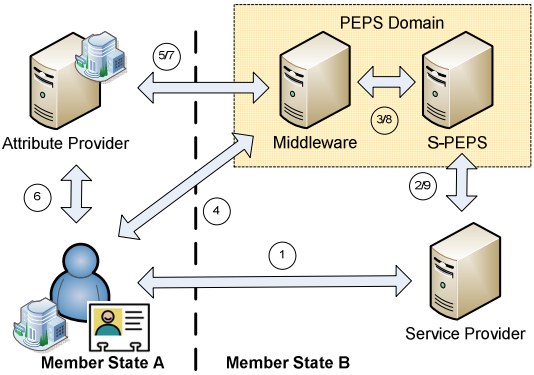

Fig. 5. PEPS – MW Model including legal identity representation

In this proposed scenario, a citizen originating from the middleware MS A wants to access a service provider of the PEPS MS B (Step 1). In contrast to the normal STORK scenario shown and described in Fig. 4, in this case the citizen wants to authenticate and act on behalf of a legal person, e.g. a company, at the service provider. Equally to the normal use case for natural person authentication, after accessing the service provider, the citizen is forwarded to the national S-PEPS (Step 2). However, before being redirected to the S-PEPS the citizen needs to state that she wants to be authenticated as representative for a legal person. This statement can be easily achieved by a simple check box or selection box. By selecting represented authentication, additional attributes are requested from the S-PEPS. Since the citizen originates from a country that relies on the MW approach, the authentication request (including additional requested attributes for legal person representation) is forwarded to the MW component hosted in the PEPS domain (Step 3). In a first step, identification and authentication of the citizen is required (Step 4). Again, this is achieved by direct communication between the MW component and the citizen's eID token. Because the citizen wants to act on behalf of a legal person, after successful citizen authentication

a separate and additional attribute provider needs to be invoked[5] (Step 5). This attribute provider is responsible for trustworthily managing the relationship between the citizen and the represented legal person (Step 6). Moreover, this attribute provider asserts the MW that the citizen is allowed to represent the desired legal person and transmits the corresponding legal persons' name and number (e.g. company name and company's commercial register number) as evidence (Step 7). This information combined with the citizen's identification data is assembled to an authentication token by the MW to be returned to the S-PEPS (Step 8). According to the normal authentication scenario, the identification and authentication data is transferred back to the requesting service provider (Step 9). In addition to the citizen's personal identification data the service provider receives information on the legal person the citizen wants and is allowed to represent within the online service.

Fig. 5 illustrated the cross-border identification and authentication of legal persons using STORK on an abstract level. Fig. 6 digs a little bit deeper into detail and shows all components involved in this scenario using the authentication example of an Austrian citizen representing a legal person. The basic concepts of the Austrian IdM system for legal persons have been introduced in Section 2.1. This section continues and explains the integration of the Austrian legal IdM system into the STORK framework.

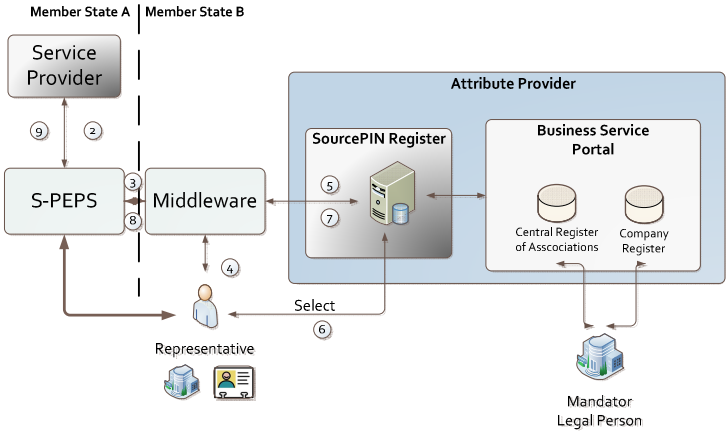

Fig. 6. Cross-border authentication model of an Austrian citizen representing a legal person

Going back to the process flow step where the MW has successfully authenticated the citizen (representative) (Step 4[6]), the MW starts the process to get an electronic mandate for representation. In a first step, the MW submits the representative's identification data to the SourcePIN Register acting as attribute provider (Step 5). This includes the representative's XML identification record (name, date of birth and

[5] In this scenario it is assumed that no representation information is stored on the citizen's eID token.

[6] The numbers of the individual process flow steps are equal in both figures, fig. 5 and fig. 6.

unique national identification number) as well as the representative's signing certificate. The latter is necessary to identify professional representatives like lawyers, notaries or tax consultants representing a particular client. The Austrian IdM system for legal persons provides a particular Object Identifier (OID) in the qualified signature certificate of the citizen card to identify such kind of occupational groups.

The SourcePIN Register uses the representative's identification data to search for all available empowerment information in constitutive registers. This is achieved by querying the so-called Business Service Portal (BSP), which acts as a hub to underlying constitutive registers. Examples of constitutive registers are:

- The Company Register
- The Central Register of Associations
- The Supplementary Register (where e.g. public agencies are registered)

After having retrieved all available empowerment information, the representative is redirected by the MW to the web portal of the SourcePIN Register Authority where all available electronic mandates are presented for selection. The representative now can choose the legal person she wants to represent from a list (Step 6). In case of professional representatives an additional Graphical User Interface (GUI) mask is available where the empowerment data like name and register number of the legal person can be manually entered. This is legally regulated due to their affiliation to a particular occupation group.

Based on the data of the selected mandate the SourcePIN Register creates an XML representation of the mandate, electronically signs it and provides it to the MW (Step 7). The MW can now extract name and register number of the legal person from the XML mandate, create the according STORK attributes and provide them to the S-PEPS (Step 8) and subsequently the SP (Step 9).

The following figures illustrate the single steps of a cross-border authentication process when acting on behalf of a legal person. Fig. 7 illustrates the country selection page of the S-PEPS where the citizen can choose her home country. In addition, a checkbox is shown where the citizen can choose to act as a representative on behalf of a legal person.

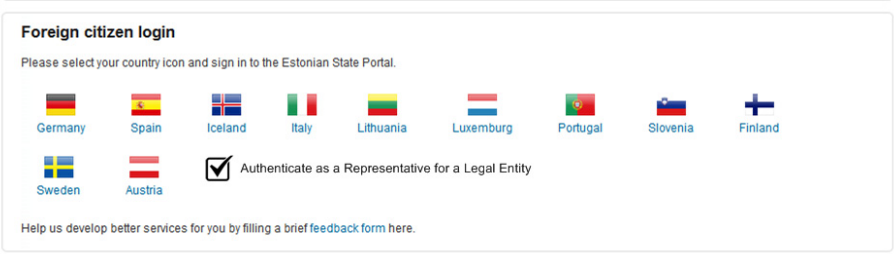

Fig. 7. Country selection and commitment to act on behalf of a legal person

In a next step, the representative is redirected to the MW for authentication. This is shown in Fig. 8 where the representative accesses her eID by entering the signature PIN.

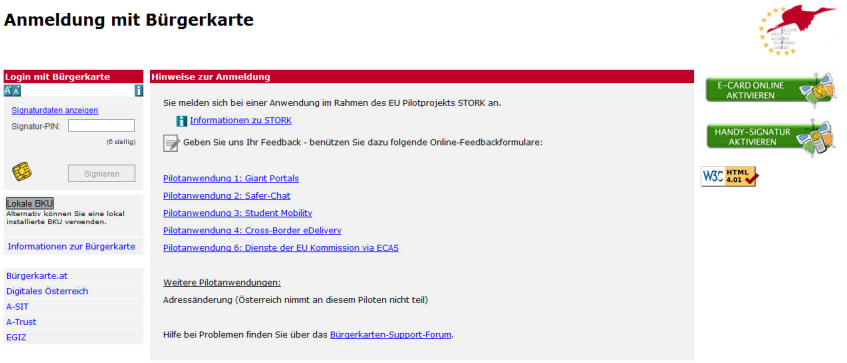

Fig. 8. Authentication dialog of the Middleware to access the representative's eID

After successful authentication, the representative is redirected to the Austrian SourcePIN register to select the legal person she wants to represent (see Fig. 9).

Fig. 9. Selection of the legal person to represent

After selection of the legal person the STORK Middleware forwards the authentication attributes to the S-PEPS, which forwards the data to the service provider. Now the representative can access the service on behalf of the legal person.

5 Conclusions and Open Issues

The present paper has discussed an interoperability framework for the cross-border identification and authentication of legal persons or professional representatives. The proposed solution bases on the findings of the large scale pilot STORK and has been successfully tested within a simulated real life scenario. Nevertheless there exist a few open issues.

Similar to the authentication of citizens, the cross-border authentication framework for legal persons deals with issues such as a missing legal framework, liability, responsibility and accountability. At the moment, there does not exist a similar framework to deal with the new change of handling electronic legal IdM in cross-border scenarios. Other open issues are the evaluation of the necessity of authentication levels for legal identities and a person to person representation, e.g. a natural person is empowered to act in the name of another natural person.

In addition we already presented our solution to the new large scale pilot STORK 2.0[7], which is the follow-up project of STORK. Here, besides enhanced piloting of STORK in various areas (banking, health, etc.) STORK 2.0 will also deal with the identification and authentication of legal persons in a cross-border context.

References

1. Leitold, H., Zwattendorfer, B.: STORK: Architecture, Implementation and Pilots. Securing Electronic Business Processes. ISSE (2010)
2. European Commission, Study on eID Interoperability for PEGS: Update of Country Profiles. IDABC Programme (2009)
3. Herkenning, E.: Scheme for eRecognition – General Introduction, version 1.1 (June 17, 2011)
4. European Union, Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. Official Journal L 013, 0012–0020 (2000)
5. Republik Österreich, The Austrian E-Government Act - Federal Act on Provisions Facilitating Electronic Communications with Public Bodies. In: Austrian Federal Law Gazette, part I, Nr. 10/2004; last amended part I, Nr. 111/2010
6. Rössler, T.: Empowerment through Electronic Mandates – Best Practice Austria. In: Godart, C., Gronau, N., Sharma, S., Canals, G. (eds.) I3E 2009. IFIP AICT, vol. 305, pp. 148–160. Springer, Heidelberg (2009)
7. Leitold, H., Tauber, A.: A Systematic Approach to Legal Identity Management – Best Practice Austria. In: Proceedings of the Information Security Solutions Europe 2011 Conference, pp. 224–234 (2011)
8. MODINIS, The Status of Identity Management in European eGovernment initiatives (2006)
9. Lockhart, H., Campbell, B.: Security Assertion Markup Language (SAML) V2.0 Technical Overview. OASIS Committee Draft 02 (2008)

[7] http://www.eid-stork2.eu/

10. Alcalde-Morano, J., Hernndez-Ardieta, J., Johnston, A., Martinez, D., Zwattendorfer, B., Stern, M.: STORK D5.8.3b Interface Specification (2011)
11. Tauber, A., Zwattendorfer, B., Zefferer, T.: STORK: Pilot 4 Towards Cross-border Electronic Delivery. In: Electronic Government and Electronic Participation- Joint Proceedings of Ongoing Research and Projects of IFIP EGOV and ePart 2011. Springer (2011)
12. Knall, T., Tauber, A., Zefferer, T., Zwattendorfer, B., Axfjord, A., Bjarnason, H.: Secure and Privacy-Preserving Cross-Border Authentication: The STORK Pilot 'SaferChat'. In: Andersen, K.N., Francesconi, E., Grönlund, Å., van Engers, T.M. (eds.) EGOVIS 2011. LNCS, vol. 6866, pp. 94–106. Springer, Heidelberg (2011)