IADIS International Journal on WWW/Internet
Vol. 13, No. 2, pp. 52-68
ISSN: 1645-7641

ENHANCING CROSS-BORDER EID FEDERATIONS BY USING A MODULAR AND FLEXIBLE ATTRIBUTE MAPPING SERVICE TO MEET NATIONAL LEGAL AND TECHNICAL REQUIREMENTS

Thomas Lenz. *E-Government Innovation Center (EGIZ).*

ABSTRACT

Identity-management systems play a key role in various areas for applications and e-Government processes where access to sensitive data needs to be protected and regulated. To protect this sensitive date, the identity-management system provides all necessary functionality to service providers to manage digital identities and handle the identification and authentication process. This identification and authentication process meets legal and technical requirements, which are specified in many European countries. Due the mobility of citizens, cross-border interoperability of national electronic identity systems in the European eID landscape becomes more and more important. If cross-border interoperability comes into play, it becomes difficult to accomplish national legal and technical requirements for identification and authentication. To accomplish national legal and technical requirements, the identification and authentication information must be mapped into national eID characteristics. In this paper, we present a new modular and flexible architecture of an attribute mapping service, which establish an interoperation layer on cross-border identification and authentication attributes to meet national legal and technical requirements. The proposed architecture follows a plug-in based approach that eases the integration of new attributes, or national legal or technical requirements. We illustrate the practical applicability of the proposed architecture by implementing a foreign identity attribute mapping service for the Austrian eID infrastructure. This attribute mapping service meets all national legal and technical requirements of the Austrian eID infrastructure, which are necessary to use foreign identities in the national infrastructure.

KEYWORDS

Identification, Authentication, cross-border Interoperability, Legal requirements, Attribute mapping

1. INTRODUCTION

Electronic identity (eID) is indispensable for a verity of Internet services and online applications. Such Internet services or online applications could be social network interactions, for example, but also are more security-sensitive services such as tax declarations or an eHealth application that protects personal medical data. The more transactions are performed by using online applications processing sensitive data, the higher is the importance for a high level of assurance into a qualified identity and a secure authentication of citizens, according to national legal requirements. E-Government is such an area, where high assurance in the citizen’s identity is needed. With respect to eGovernment, several countries have already developed and deployed electronic identity systems since the beginning of the 21st century. Such of these national electronic identity systems could not only provide personal information of the citizen, like the given name, the surname, or a unique identifier, but also are some additional authentication information, like an electronic mandate or the notification if the citizen is a medical scientist, an advocate or public servant.

Due the mobility of citizens, cross border interoperability of national electronic identity systems in the European eID landscape has become more and more important in the last couple of years. In the case of cross-border eID, the European Commission has recently published the EU regulation on Internal Market electronic identification and trust services (eIDAS) [European Union, 2014], which builds the legal framework for cross-border eID acceptance within the EU. However, the eIDAS regulation is currently only the latest step towards the implementation of a pan-European eID federation. The aim on cross-border eID recognition dates already back to 2005, as the aim was mentioned in the Manchester Ministerial Declaration [European Union, 2005], followed by the EU Service Directive [European Union, 2006] in 2006 and the eID large scale pilot projects STORK and STORK 2.0 . These large-scale pilot projects treaded with an interoperability framework, which can be used to couple different national eID solutions by using well-defined service models [Leithold, H. and Zwattendorfer, B., 2010].

The STORK service models define the infrastructure and the communication protocols between the different national electronic identity systems. However, many countries have national legal requirements that had to be complied with or they use proprietary authentication attributes in there national eID infrastructure. Consequently, it is not enough to specify the communication channel between national eID systems only, but also cross-border identification and authentication data has to be mapped to the national eID characteristics and requirements. In practice, this mapping of cross-border eID information is actually not a trivial task since national regulations and attribute definitions in the citizen’s country could be disparate to regulations and definitions in the service provider country. For example, there are differences in the legal scope of mandates between countries, or the legal form of a company has a different coverage in respect to the law. However, there are also challenges in the cross-border interoperability, which are not recognizable at first view. As an example for such an interoperability challenge, the surname can be mentioned. In many countries the legal requirements of a minimal personal data-set consists of a given name, a data of birth and the surname, but there are also some countries like Island, where there data set does not contain a surname. Therefore, some additional national infrastructure is required to facilitate cross-border eID interoperability.

As a first solution to this problem, Stranacher have proposed an approach for the integration of foreign eIDs into the Austrian eGovernment [Stranacher, K., 2010]. However, this proposal lacks in terms of adaptability, flexibility and modularity to comply new legal requirements or to offer new attribute mapping functionality, which are part of the STORK 2.0 pilot or the eIDAS regulation. To overcome this issue, we present improved architecture of a national attribute mapping service, which can be used in combination with the STORK 2.0 interoperability framework.

The paper is structured as follows. Section 2 gives a short introduction into the STORK interoperability framework and the models, which are in use there. In Section 3, the architectural design of our attribute mapping service is explained. In Section 4, we give details on the implementation of our architecture, by implementing an attribute mapping service for the Austrian cross-border eID implementation. In Section 5, we give some prospects regarding the eIDAS regulation. Finally, in Section 6 we draw a conclusion.

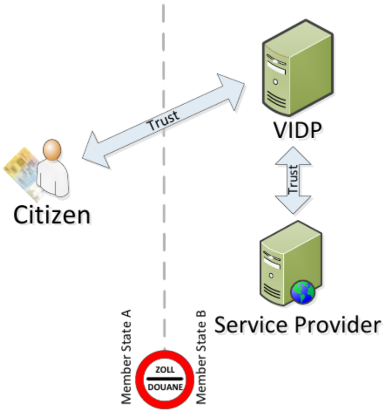


Figure 1. STORK middleware model

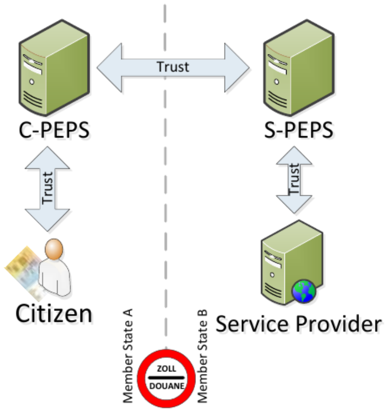


Figure 2. STORK PEPS model

2. STORK INTEROPERABILITY FRAMEWORK

The STORK large-scale pilots treated with an interoperability framework, which can be used to couple a heterogeneous set of national identity management infrastructures. To perform this challenge, the STORK interoperability framework defines two different service models, which can be used to build up an interoperability layer between national eID solutions.

These models are the Pan European Proxy Service (PEPS) model, which are shown in Figure 2 and den middleware (MW) model illustrated in Figure 1 [Zwattendorfer, B., et al., 2013]. Both models use a well-defined communication protocol to interconnect national deployed eID services.

The PEPS model uses a proxy-based approach to encapsulate specifics of the national eID infrastructure. In this model, PEPS is a single point of contact for other countries, which implements a gateway to use the national eID infrastructure cross-border. In contrast to the PEPS model, in the middleware model citizens are directly authenticated at the service provider. Therefore, a service provider has to deploy a so-called V-IDP in the service provider infrastructure, which provides all necessary functionality for citizen identification and authentication. Actually, STORK implements both models and all possible combinations between them, because there are advantages and drawbacks in both interoperability models [Zwattendorfer, B., et al., 2013].

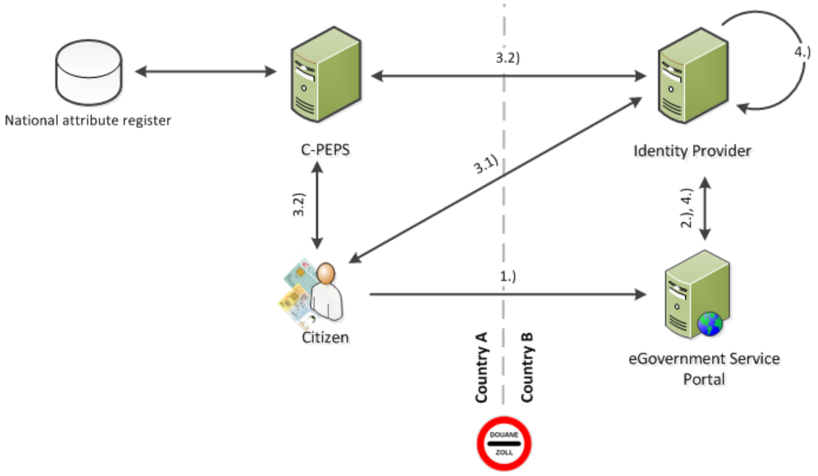
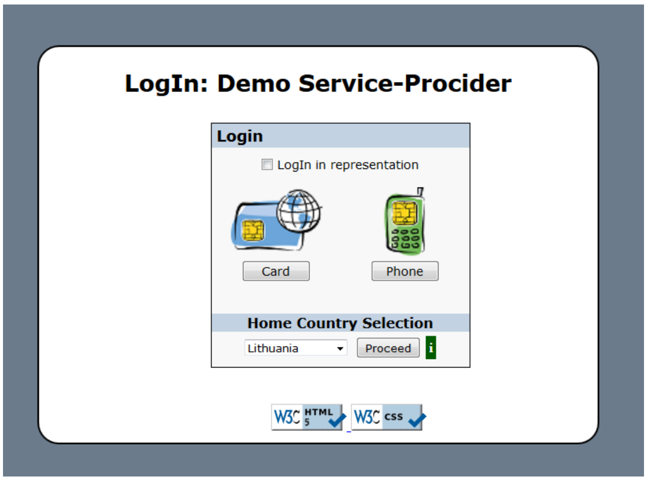


Figure 3. Process flow of a cross-border identification and authentication process by using the STORK framework.

Figure 3 illustrates the identification and authentication process flow, in which a citizen of a country A would use an eGovernment portal, which is deployed in a country B, by using its national eID. This process flow consists of the following steps:

1. A citizen of country A wants to access a protected area at an eGovernment portal in country B.
2. The citizen is redirected to an identity provider and there the citizen has to select is favored identification and authentication model. Figure 4 shows a mockup of a graphical user interface, which allows the selection of the identification and authentication model, which is generated by the national identity-management solution [Lenz, T., et al., 2015].



LogIn: Demo Service-Procider

Login

□ LogIn in representation

Home Country Selection

Lithuania

Figure 4. Identification and authentication model selection.

A direct identification and authentication, regarding the STORK middleware model, can be selected by using the *Card* button, which starts identification and authentication process by using a smartcard based identification and authentication token. If the foreign citizen would use the PEPS model for identification and authentication, he or she could select his or her home country, which is listed in the Hypertext Transfer Protocol (HTTP) [Fielding, R., et al., 1999] drop-down list. Additional, the citizen could select some more options, like an authentication in representation by using electronic mandates or an identification and authentication, which is based on mobile phones. Such a mobile phone based solution is actually deployed in Austria.

3. After selection, one of the STORK service models is used to identify and authenticate the citizen. This identification and authentication process generates identification and authentication attributes, which are received from the identity provider, by using the STORK communication protocol. If the PEPS model is used, also some additional attributes could be generated by using a national attribute register. Such an additional attribute could be an electronic mandate for example. According to Figure 5, the identification and authentication process, which is based on the PEPS model, involves the following steps. This sequence description starts with the selection of the citizen's preferred identification and authentication model, by a click in the GUI shown in Figure 4.

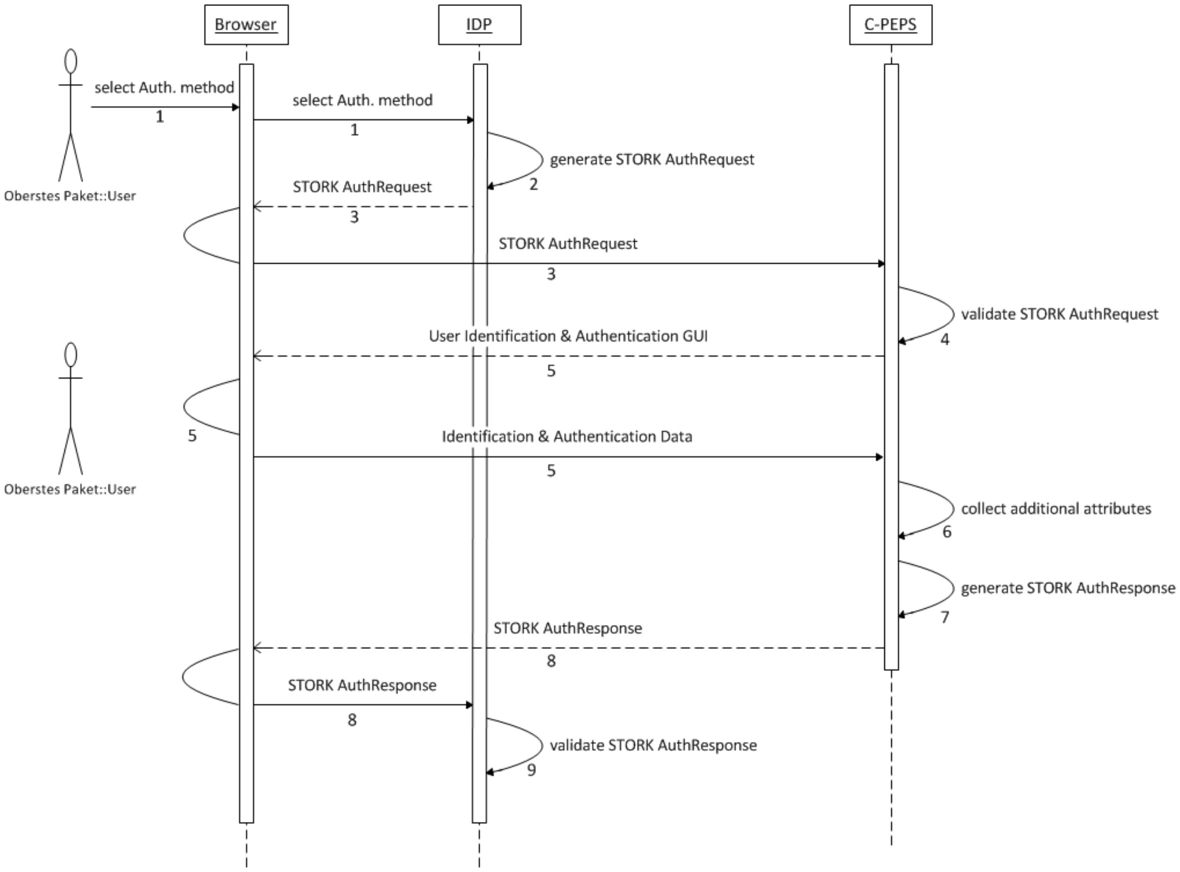

Browser
IDP
C-PEPS
select Auth. method
1
select Auth. method
1
generate STORK AuthRequest
2
Oberstes Paket::User
STORK AuthRequest
3
STORK AuthRequest
3
validate STORK AuthRequest
4
User Identification & Authentication GUI
5
5
Identification & Authentication Data
5
Oberstes Paket::User
collect additional attributes
6
generate STORK AuthResponse
7
STORK AuthResponse
8
STORK AuthResponse
8
validate STORK AuthResponse
9

Figure 5. Sequence diagram of STORK cross-border communication.

1) The citizen selects his or her home country in the GUI shown in Figure 4 and starts the identification and authentication process based on the STORK PEPS model.
2) The STORK communication protocol is based on the SAML2 WebSSO Profile [Hughes, J., et al., 2005] to transfer identification and authentication data cross-border between the identity provider and the C-PEPS. Therefore, the identity provider generates a STORK authentication request [STORK2.0-D4.4, 2015], which is a special type of a SAML2 *AuthnRequest* [Cantor, S., et al., 2005 (A)], and signs this STORK authentication request with an identity-provider private-key. This STORK authentication request includes a set of identification or authentication attribute-names, which are needed to identify and authenticate the citizen cross-border. The XML schema, which is used to request a specific identification or authentication attribute is illustrated in Listing 1.

```
<xsd:complexType name=″RequestedAttributeType″>
  <xsd:sequence>
    <xsd:element ref=″stork:AttributeValue″ type=″anyType″ minOccurs=″0″
                 maxOccurs=″unbounded″/>
  </xsd:sequence>
  <attribute name=″Name″ type=″string″ use=″required″/>
  <attribute name=″NameFormat″ type=″anyURI″ use=″required″/>
  <attribute name=″isRequired″ type=″boolean″ use=″optional″/>
  <anyAttribute namespace=″##other″ processContents=″lax″/>
</xsd:element>
```

Listing 1. STORK requested attribute.

3) The identity provider sends the STORK authentication request to the C-PEPS by using SAML2 POST Binding [Cantor, S. et al. 2005 (B)]
4) The C-PEPS validates the STORK authentication request, by using the identity-provider public-key, which must be included in a C-PEPS certificate trust-store. If the authentication request is valid, the C-PEPS start its national identification and authentication process.
5) The C-PEPS identifies and authenticate the citizen by using its national identification and authentication process. Those identification and authentication processes based on national technical and legal requirements and acquire national identification and authentication data of the citizen.
6) In addition, the C-PEPS may also request additional identification information by using a national attribute register. Such additional information could be like an electronic mandate, an address register, which has information about the citizen's place of living, or an eHealth register, which identify a citizen as doctor, for example.
   7) The C-PEPS builds a STORK authentication response, which is also a special type of a SAML2 *Response* element. This authentication response includes all requested identification and authentication information in a SAML2 *Assertion* element. Every identification or authentication attribute is packaged in a specific SAML2 Attribute element, which are defined in the SAML2 STORK-profile. Listing 2 illustrates two STORK identification attribute elements [STORK2.0-D4.4, 2015], as example. At last, the full authentication response is signed by the C-PEPS.
8) The C-PEPS sends the STORK authentication response to the identity provider by using SAML2 POST binding. The POST binding endpoint URL is automatically discovered from the *AssertionConsumerServiceURL* attribute value of the STORK authentication request.
9) The identity provider validates the STORK authentication response, by using the C-PEPS public-key, which must be included in an identity-provider certificate trust-store. If the authentication response is valid, the identity-provider extracts all identification and authentication information from the SAML2 *Assertion* element.

```
<saml2:AttributeStatement>
  <saml2:Attribute Name=″http://www.stork.gov.eu/1.0/surname″
                 NameFormat=″urn:oasis:names:tc:SAML:2.0:attrname-format:uri″
                 stork:AttributeStatus=″Available″>
    <saml2:AttributeValue xmlns:xsi=″http://www.w3.org/2001/XMLSchema-instance″
                        xsi:type=″xs:anyType″>Mustermann
    </saml2:AttributeValue>
  </saml2:Attribute>
  <saml2:Attribute Name=″http://www.stork.gov.eu/1.0/givenName″
                 NameFormat=″urn:oasis:names:tc:SAML:2.0:attrname-format:uri″
                 stork:AttributeStatus=″Available″>
    <saml2:AttributeValue xmlns:xsi=″http://www.w3.org/2001/XMLSchema-instance″
                        xsi:type=″xs:anyType″>Max
    </saml2:AttributeValue>
  </saml2:Attribute>
</saml2:AttributeStatement>
```

Listing 2. STORK requested attribute.

4. To fulfill national legal requirements and to make the received authentication attributes interoperable with the national eID infrastructure an attribute mapping process is required. This attribute mapping process could be performed by using the attribute mapping service, which we present in this paper.
5. At last, the identification and authentication information is transmitted to the eGovernment service provider and the citizen can access the protected resource.

As shown in Listing 2, the STORK communication protocol defines a set of identification and authentication attributes to transfer identification and authentication information across borders. Table 1 illustrates some important attributes, which are in use for cross-border identification and authentication. This identification and authentication attributes, which are illustration in Table 1 as example, has to be mapped to national legal and technical requirements. Consequently, a semantic attribute mapping service, which builds up an interoperation layer on identification and authentication attribute values, has to map all attributes, which are defined by the STORK interoperability framework. In the next section, we present the architecture of an attribute mapping service, which can be used in both STORK models.

Table 1. A selection of STORK authentication attributes.

Attribute Category	Attribute Name	Description
Natural person	eIdentifier	Unique identifier of a natural person
	givenName	Given name of a natural person
	surname	Surname of a natural person
	dateOfBirth	Date of birth of a natural person
Legal person	eIdentifier	Unique identifier of a legal person
	commonName	Name of a legal person
	address	Postal address of this legal person
Mandate	mandateContent	Scope of an electronic mandate in respect to validity period and legal scope.
	representative	Description of natural person which represents another person.
	represented	Description of natural person or legal person, which is represented

3. ARCHITECTURAL DESIGN

The proposed architecture of an attribute mapping service is based on a sophisticated modular architecture to get a flexible solution for attribute mapping in respect to their legal meaning and situational meaning. Figure 6 illustrates the general architecture of our attribute mapping service.

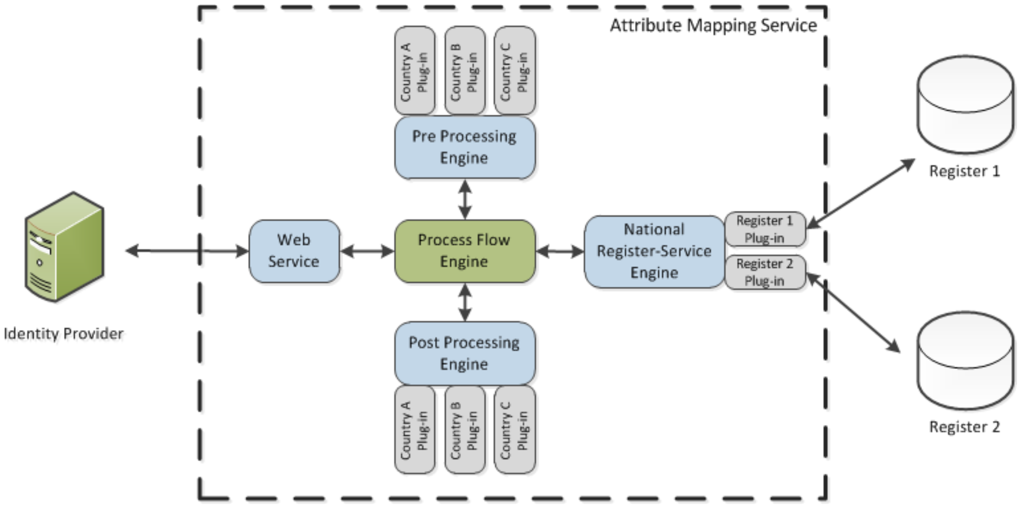


Figure 6. Architecture of the attribute mapping service.

The key component of the entire solution is the Process Flow Engine, which coordinates the different steps of an attribute mapping process. An attribute mapping process can be divided into three steps. In the first step, the attribute values, which should be mapped from one national representation to another national representation, are processed by using the Pre Processing Engine. For each supported source country, an appropriate Country Plug-in can be implemented. Every Country Plug-in implements the mapping from the national attribute representation to a generic attribute representation, which are used in the next steps. The advantage of this modular preprocessing approach is the generalization of the input date to a well-defined data set for the next processing steps.

In the second step, the National Register-Service Engine is used to fulfill national legal requirements or to generate proprietary national identification and authentication datasets. Every national register interaction is implemented as a Register Plug-in, which use the generalized input data to interact with the register. By using this flexible approach, a multitude of national register services could be used during the mapping process to comply all national requirements.

In the last step, the Post Processing Engine is involved, which generates destination country specific authentication information by using the data, which is processed before. We also used a modular approach, which use Country Plug-ins for every destination country, to perform this last step. This modular post processing approach facilitates the usage of our solution in different countries and makes it adaptable to new national requirements.

An additional advantage of these modular preprocessing and post processing is that it allows minimizing the implementation effort for new countries, because a specific mapping operation could be implemented into Pre Processing Engine or into the Post-Processing Engine depending on national attribute value characteristic. For example, if a source country has a proprietary attribute value, which has to be mapped for every destination country, the mapping could be performed in the preprocessing step, easily. In contrast, an attribute mapping should be performed by the post-processing step, if the destination country requires a special proprietary attribute value. The communication between an identity provider and our proposed attribute mapping service is done by using a Web-service, which is realized in the Web Service module.

We have evaluated the practical applicability of the proposed architectural design by implementing an attribute mapping service for the Austrian eID infrastructure to facilitate cross-border eID interoperability with respect to the STORK 2.0 pilot, which is still running.

4. AUSTRIAN FOREIGN-IDENTITY ATTRIBUTE MAPPING SERVICE^

The practical applicability of our proposed architectural design has been evaluated by realizing and implementing an attribute mapping service in practice. To illustrate that, we have implemented an attribute mapping service for the Austrian eGovernment, which fulfill all national legal and technical requirements to use foreign identities in the Austrian eID infrastructure. This new and advanced solutions enhanced the implantation, descript by Stranacher [Stranacher, K., 2010] by using our proposed architectural design. In Subsection 4.1, we shortly describe the legal requirements for foreign identities in Austria. In Subsection 4.2, we present the implementation of the advanced Austrian foreign identity attribute mapping service.

4.1 Legal Requirements

The legal requirements to use foreign identities in the Austrian eGovernment infrastructure, which is the Austrian eGovernment Act [Austrian Federal Law Gazette (BGBI) part 1 Nr. 10/2004, 2008], have been amended in the year 2008. As a result foreign electronic identities fully integrated in the Austrian eGovernment in case they are associated with qualified electronic signatures (a qualified electronic signature requires the usage of a secure signature creation device (SSCD), like a smart card, to generate the electronic signature). A legal requirement of this Austrian eGovernment Act is that if the citizen is not already registered in the Austrian Central Register of Residents, which is the case if the person has a registered residence in Austria, the foreign citizen must be registered in the Supplementary Register. With §6(5) of the Austrian eGovernment Act the possibility to register a person electronically has been given. This is done by the so called eGovernment Equivalence Decree [Austrian Federal Law Gazette (BGBI) Nr. 170/2010, 2010], which determined the identification attributes from a foreign identity must be used. Usually the identification attributes are stored in the subject name of the certificate, which the foreign citizen has used during the identification and authentication process. However, in some cases, the certificate does not include all required identification attributes. Therefore, an additional national register query must be performed to get all required national identification attributes. Consequently, the eGovernment Equivalence Decree define those countries, which provide electronic identities by using a qualified electronic signature for authentication purpose and specifies the identification attributes, which are required for each county. Actually, the following countries are defined to be equivalent: Belgium, Estonia, Finland, Iceland, Italy, Liechtenstein, Lithuania, Portugal, Sweden, Slovenia, and Spain. Consequently, citizens from these counties could use their national eID for login to an Austrian online application [ref].

There are also legal requirements in the Austrian eGovernment infrastructure, if electronic mandates are in use. These legal requirements are defined in the Austrian SourcePin Register Degree [Austrian Federal Law Gazette (BGBI) part II Nr. 57/2005, 2005.]. Additionally, there exist also some technical requirements for electronic mandates, which are defined in the specification of electronic mandate [Rössler, T., et al. 2006]. This technical specification defines the data content and the data structure of an electronic mandate, which is used by the Austrian eID infrastructure.

4.2 Implementation

We use our proposed architecture to implement an advanced attribute-mapping service to use foreign identities in the Austrian eGovernment infrastructure. Figure 7 illustrates this Austrian specific implementation of our proposed architecture.

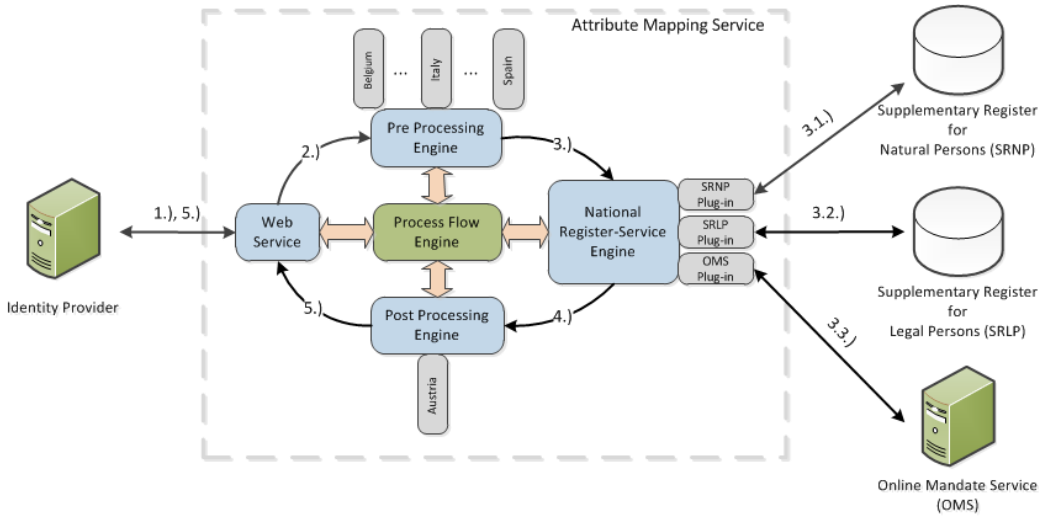


Figure 7. Implementation of the Austrian attribute mapping service.

To present our implementation in detail, we describe an attribute mapping process, which is based on an electronic mandate to represent a legal person, as an example. In this example, a foreign citizen wants to log in to an Austrian eGovernment application by using its national eID and an electronic mandate, which authorize the citizen to represent a legal person, like a company.

1. After identification and authentication is performed by using the STORK interoperability framework, the identification and authentication attributes, which the Austrian identity provider has collected, should be mapped to the Austrian legal and

technical requirements. Therefore, the identity provider connects the attribute mapping service by using a SOAP [Gudgin, M., et al., 2007] based Web service. Beneath the SOAP protocol, the Hypertext Transfer Protocol (HTTP) [Fielding, R., et al., 1999] is used as carrier for the SOAP message. This is reasonable, because HTTP is popular, frequently used and widely supported. SOAP messages being exchanged over the implemented Web service rely on the Extensible Markup Language (XML) [Bray, T., et al., 2006]. The XML schema, which we have defined[1], to exchange messages with the attribute mapping service is shown in Listing 3

```
<xsd:element name= “AttributeMappingRequest “>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name=” Signature” type=” xsd:base64Binary maxOccurs=” 1” />
      <xsd:element name=” STORK” type=” STORKAttributeType”  minOccurs=” 0”
                   maxOccurs=” unbound”  />
    </xsd:sequence>
  </xsd:complexType>
</xsd:element>
```

Listing 3. Attribute mapping request.

According to the defined XML schema, an attribute-mapping request consists of an electronic signature (*Signature* Element), which is mandatory, and a set of STORK attributes, which are located as child elements in the *STORK* element. We use the STORK attribute names to distinguish the single STORK attributes in the *STORK* element.

2. After receiving the attribute-mapping request, the Pre Process Engine starts to process the received attributes. At first, the Pre Process Engine gets the foreign signature from the request and verifies it. Thereby, also the signature certificate is checked if it is qualified. In case the certificate is qualified, the Pre Process engine extracts the citizenship from the certificate by using the country element of the certificate's subject name and selects the corresponding country plug-in. After this general preprocessing, the country specific plug-in starts the country specific date extraction and mapping process, which consists of the following steps in our example.

2.1. At first, the plug-in extracts identification information, which is available in the foreign certificate. This data could be the given name, the surname, a national eID number and information about the certificate. In this step, an additional register query is performed for some special countries, like Liechtenstein, to get additional information, which are not included in the certificate. After collection all required information from the citizen the next preprocess step is performed.

2.2. In the second preprocess step, the STORK attributes, like an electronic mandate are processed. In case of an electronic mandate to represent a legal person, also some additional mappings are necessary. At first, the legal scope of the foreign mandate has to be mapped to an Austrian mandate legal scope, because Austrian online applications

[1] We were forced to define a schema, since existing schemata were not able to meet the Austrian technical requirements.

only support Austrian mandate scopes. Therefore, we implement the mandate legal scope mapping, shown in Table 2.

Table 2. Mandate legal scope mapping.

Representative Person type	STORK legal scope	National legal scope
Natural persons	General Powers	GeneralvollmachtBilateral[2]
	Health Powers	ELGABilateral[3]
Legal persons	General Powers	Einzelvertretungsbefugnis[4]

At second, the legal corporate form of the legal person, which should be represented, has to be mapped to an Austrian legal corporate form. The full legal corporate form mapping is illustrated in Table 3. After these, all foreign identity attributes are mapped into a generic attribute dataset. This generic dataset serves as basis for all further steps in the attribute mapping process.

Table 3. Legal corporate form mapping.

STORK legal corporate form	National legal corporate form
Public Limited Company, Plc	Aktiengesellschaft
Private Limited Company, Ltd	Gesellschaft mit beschränkter Haftung
Limited partnership, LP	Kommanditgesellschaft
Partnership	Offene Gesellschaft
Société en commandite par actions	[5]
Different from previous values	[6]

3. In this step, National Register-Service Engine is used to achieve legal and technical requirements, which are essential if a foreign identity should be used in Austria. To satisfy these requirements, we implement three plug-ins. This plug-ins implements the communication with national registers and national web services, which we will describe in detail in the next sub steps.

3.1. At first, the *SRNP Plug-in* is used to check, if the foreign citizen is already registered in the Central Register of Residents or in the Supplementary Register for Natural Persons (SRNP). If the citizen is not registered, the SRNP plug-in sends a request to the Supplementary Register for Natural Persons to register the foreign citizen, by using the citizen identification attributes from the generic dataset. Actually, the following attributes are required to register the foreign citizen into the SRNP:

- Unique identifier: STORK *eIdentifier* attribute
- Firstname: STORK *givenName* attribute
- Familyname: STORK *surname* attribute
- DateOfBirth: STORK *dateOfBirth* attribute
- IssuingCountry: Issuer country from the citizen signing certificate

3.2. If an electronic mandate is in use, the represented person must also be registered in a national register. In case of a represented legal person, this legal person must be

[2] Austrian type of general powers to represent natural persons
[3] Austrian type of a eHealth power, which is only for natural persons
[4] Austrian type of general powers to represent a legal person
[5] Doesn’t exist equivalence in Austria
[6] Doesn’t exist equivalence in Austria

registered into the Supplementary Register for Legal Persons (SRLP), if this legal person is not already registered there. To perform this SRLP registration, the mapped legal corporate form and some other legal person identification attributes are used. In detail, the following STORK attributes or already mapped attributes are used to register the legal person into the SRLP:

- Unique identifier: STORK *eLPIdentifier* attribute
- Legal person name: STORK *legalName* attribute
- National legal corporate form: Mapped STORK *translatableType* attribute
- Address: Elements of the STORK *canonicalRegisteredAddress* attribute
- Information of the natural person, which represents the legal person
  - Unique identifier: National unique identifier of the natural person
  - Firstname: STORK *givenName* attribute
  - Familyname: STORK *surname* attribute
  - DateOfBirth: STORK *dateOfBirth* attribute
  - Mandate legal scope: Mapped national legal scope of the used mandate

If the represented person is also a natural person, the registration process is equivalent to the registration process of the foreign citizen descript in step 3.1.

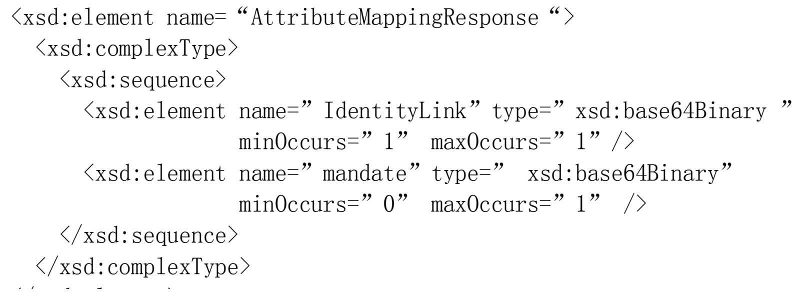
3.3. The electronic mandate, which is used by the foreign citizen, must also be registered to the Austrian *Online Mandate Service* (OMS). This registration process uses the information from the SRNP, the SRLP and the mapped legal scope of the foreign mandate to generate an Austrian electronic mandate just-in-time. The generated electronic mandate is an XML dataset, which includes all information about the represented person and the representative person, like a unique identifier, given name, surname, date of birth, or the common name for legal persons, and the legal scope of the mandate. This XML dataset is signed by the Austrian *Online Mandate Service* (OMS) and therefore, the generated electronic mandate is equivalent to electronic mandate, which is in use from Austrian citizens.

After this, all Austrian legal requirements are satisfy and the attribute mapping process switches to the next step.

4. The last attribute-mapping step is performed by the Post Processing Engine, which generates Austrian specific identification and authentication attributes. Unique identification of Austrian citizen is done by using a special XML data structure, which is called identity link. Consequently, the plug-in generates an identity link for the foreign citizen, by using the information, which is stored in the SRNP.

5. In the last step, the identity link, which was generated on-the-fly for the foreign citizen, and the Austrian electronic mandate, if a foreign mandate was in use, is returned to the identity provider. Listing 4 illustrates the XML response schema, which we have defined, to transfer the mapped Austrian identification and authentication attributes back to the identity provider.

After this, the identity provider could use the mapped identification and authentication attributes to transmit the information to the Austrian eGovernment service provider.



```
<xsd:element name= “AttributeMappingResponse “>
  <xsd:complexType>
    <xsd:sequence>
      <xsd:element name=” IdentityLink” type=” xsd:base64Binary ”
                   minOccurs=” 1”  maxOccurs=” 1” />
      <xsd:element name=” mandate” type=”  xsd:base64Binary”
                   minOccurs=” 0”  maxOccurs=” 1”  />
    </xsd:sequence>
  </xsd:complexType>
```

Listing 4. Attribute Mapping Request.

5. PROSPECTS REGARDING THE EIDAS REGULATION

In the case of cross-border eID, the European Commission has recently published the implementation regulation *EU 2015/1501* [European Commission 2015/1501], which regulates the implementation on the interoperability framework on electronic identification and trust services for electronic transactions in the internal market. This implementation regulation regards the EU regulation on Internal Market electronic identification and trust services (eIDAS) [European Union, 2014] and gives detail information about the technical and operational requirements of the interoperability framework on order to ensure the interoperability of the electronic identification and authentication across borders. Those requirements include in particular the following points:

- Minimum technical requirements related to the assurance level and the mapping of national assurance levels [European Commission 2015/1502]
- Minimum technical requirements of interoperability in respect to data formats and infrastructure requirements
- The minimum set of person identification data uniquely representing a natural or legal person
- Common operational security standards

The most interesting part of the European implementation regulation *EU 2015/1501,* related to this paper, are the minimum sets of person identification data for natural and legal persons. Because some of the interoperability challenge, which we had described before, based on lack uniform person identification data set, like no surname in Island, as example. In this regard, the European implementation regulation EU 2015/1501 defines a minimum set of person identification data, which uniquely represents a natural or legal person in case of cross-border identification and authentication. This minimum data set contains a combination of identification attributes of a legal or natural person. Actually, the following attributes are part of the minimum data sets:

- Natural persons
    - o Current family name
    - o Current first name
    - o Date of birth
    - o Unique identifier, which is persistent as possible in time

- Legal persons
    - Current legal name
    - Unique identifier, which is persistent as possible in time

Since, the regulation *EU 2015/1501* is obligatory for every member state in the European Union, they had to implement, provide, and permit these minimum data set attributes in case of cross-border eID communication. Consequently, the interoperability of cross-border eID to uniquely identifier natural or legal persons becomes much easier during this regulation, because now all member state must support and permit the same identification information. Although, the regulation *EU 2015/1501* is the next step towards harmonization of cross-border eID, but other challenges, like national legal or technical (legal scope of mandates, legal form of companies, national unique identifier formats, or national requirements to register foreign citizens, etc.) remain open. Consequently, an attribute mapping service to meet national requirements will also be with the regulation *EU 2015/1501* still needed.

6. CONCLUSION

Identification and authentication of citizen is an integral component of a variety of Internet services and online applications. The capability for reliably identification and authentication according to national legal requirements is important for service providers, which process private and individual-related data, like eGovernment applications. If cross-border interoperability of national electronic identity systems comes into play, it becomes difficult to accomplish national legal and technical requirements for identification and authentication. It is not enough to define the communication channel between national eID solutions, because cross-border identification and authentication data must also be mapped to national eID characteristics and national requirements.

In this paper, we have presented a new architecture of an attribute mapping service, which establish an interoperation layer on cross-border identification and authentication attributes. Our solution relies on an adaptable and modular architecture that facilitates future extensions. We have demonstrated the practical applicability of our architectural design by implementing a foreign identity attribute mapping service for the Austrian eID infrastructure. The implemented solution meets special legal and technical requirements of the Austrian eGovernment, but its general architectural design is also applicable to other contexts.

The realization of further legal or technical requirements, which arise from the eIDAS regulation, that make use of the presented architecture is regarded as future work.

REFERENCES

Austrian Federal Law Gazette (BGBI) part 1 Nr. 10/2004, 2008. The Austrian E-Government Act, Federal Act on Provisions Facilitating Electronic Communications with Public Bodies, entered into force on 1 March 2004; amended by BGBI 1 Nr. 7/2008 (amendments entered into force on 1 January 2008) including the Corrigendum in BGBI 1 Nr. 59/2008

Austrian Federal Law Gazette (BGBI) Nr. 170/2010, 2010. E-Government Equivalence Decree, Decree of the Federal Chancellor laying down conditions for equivalence under Section 6(5) of the E-Government Act

Austrian Federal Law Gazette (BGBI) part II Nr. 57/2005, 2005. SourcePin Register Degree, Decree of the Federal Chancellor, which regulates the activities of the SourcePin Register agency relating to the SourcePin register in detail.

Bray, T., et al., 2006. Extensible Markup Language (XML) 1.1 (Second Edition). http://www.w3.org/TR/2006/REC-xml11-20060816/

Cantor, S., et al., 2005 (A), Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0, OASIS Standard, https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

Cantor, S. et al. 2005 (B), Binding for the OASIS Security Assertion Markup Language (SAML) V2.0., OASIS Standard, https://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf

European Union, 2005. Ministerial declaration, Manchester, united kingdom, on 24 November 2005. European Union.

European Union, 2006. Directive 2006/123/EC of the European parliament and of the council of 12 December 2006 on services in the internal market. European Union.

European Union, 2014. Regulation (EU) no 910/2014 of the European parliament and of the council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing directive 1999/93/EC. European Union.

European Commission 2015/1501, COMMISSION IMPLEMENTING REGULATION (EU) 2015/1501 on the interoperability framework pursuant to Article 12(8) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, European Commission, 8 September 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1441782373783&uri=OJ:JOL_2015_235_R_0001

European Commission 2015/1502, COMMISSION IMPLEMENTING REGULATION (EU) 2015/1502 on setting out minimum technical specifications and procedures for assurance levels for electronic identification means pursuant to Article 8(3) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market, European Commission, 8 September 2015, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOL_2015_235_R_0002

Fielding, R., et al., 1999. Hypertext transfer protocol – http/1.1. http://www.ietf.org/rfc/rfc2616.txt.

Gudgin, M., et al., 2007. Soap version 1.2 part 1: Messaging framework. http://www.w3.org/TR/soap12-part1/

Hughes, J., et al., 2005, Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0., OASIS Standard, http://docs.oasisopen.org/security/saml/v2.0/saml-profiles-2.0-os.pdf

Leithold, H. and Zwattendorfer, B., 2010. STORK: Architecture, Implementation and Pilots, ISSE 2010 Securing Electronic Business Processes, 131-142

Lenz, T., et al., 2015. A modular and flexible identity management architecture for national eID solutions, 11th International Conference on Web Information Systems and Technologies, pages 321-331

Rössler, T., et al. 2006. Elektronische Vollmachten Spezifikation 1.0.0

Stranacher, K., 2010. Foreign identities in the austrian e-government - an interoperable eid solution. In Center, T. N. C., editor, IDMAN 2010 - 2nd IFIP WG-11.6 International Conference on Identity Management, pages 31 – 40.

STORK2.0-D4.4, 2015, D4.4 Final version of the Technical Specification for the cross-border Interface, Secure idenTity acrOss boRders linKed 2.0, WP4 core team

Zwattendorfer, B., et al., 2013. Middleware architecture for cross-border identification and authentication. Journal of information assurance and security, 8:107–118.