Enhancing the Modularity and Flexibility of Identity Management Architectures for National and Cross-Border eID Applications

Thomas Lenz(✉) and Bernd Zwattendorfer

e-Government Innovation Center, Inffeldgasse 16a, Graz, Austria
{thomas.lenz,bernd.zwattendorfer}@egiz.gv.at

Abstract. Identity-management systems play a key role in various areas of applications and e-Government processes where access to sensitive data needs to be protected. To protect this sensitive data, the identity-management system provides all necessary functionality to service providers to manage digital identities and to handle the identification and authentication process. Identity management per se is no new topic and hence several identity-management systems have evolved over time, which are deployed in almost all European countries. However, identity management is constantly evolving in terms of new technical or legal requirements, higher secure protocols, new identification and authentication mechanism, or new fields of applications. In particular, the need for exchanging or federating identities across domains or even borders requires new interoperable solutions and flexible identity management architectures. In this paper we present a flexible and modular identity management architecture which focuses on federation and interoperability capabilities based on plug-able components. Due to that, new arising requirements can be easily fulfilled by implementing appropriate plug-ins. Hence, our proposed architecture is especially applicable for high qualified identification systems such as national eIDs for e-Government applications and their federation across borders. We further illustrate the applicability of our architecture by implementing it to be used as an identity provider for Austrian eGovernment applications, on the one side being applicable for national authentications and, on the other side, in a cross-border context.

1 Introduction

Electronic identity (eID) is indispensable for a variety of Internet services and online applications. Once the identity of communication entities is established with a level of certainty matching the value associated with the service, the communication partners can gain the confidence and trust needed for mutual transactions. Such transactions can include social network interactions, but also more security-sensitive services such as a tax declaration or an eHealth application that protects personal medical data. In each case, besides using an electronic identity authentication is additionally required to prove a claimed identity to be

V. Monfort et al. (Eds.): WEBIST 2015, LNBIP 246, pp. 123–143, 2016.
DOI: 10.1007/978-3-319-30996-5_7

authentic. Consequently, this authentication step link the identity information to a person, which uses a PIN or password to proved that he or she is the owner of that identity information.

Actually, more and more transactions are preformed electronically, by using online applications ore Internet service, which processing sensitive data. Consequently, the importance for a high level of assurance by secure means of authentication linked to qualified identity is rising sharply. eGovernment is such an area, where high assurance in the citizen's identity is needed. Therefore, several countries have already developed and deployed electronic identity systems for the eGovernment infrastructure since the beginning of the 21st century. This deployed electronic identity systems are still in operation since more than a decade ago, it is not too hard to guess that requirements on identity management solutions have changed over time and new technologies have emerged. Such technologies and requirements are not only things like new authentication protocols, which support a higher level of security, or new identification and authentication mechanisms, but moreover are requirements targeting usability, interoperability, or identity-management federations.

Particularly, identity-management federations such as nationally federated eID solutions or even cross-boarder eID federations became more and more important in the last couple of years. In the case of cross-boarder eID, the European Commission has recently published the EU regulation on Internal Market electronic identification and trust services (eIDAS) [1], 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 [2], followed by the EU Service Directive [3] in 2006 and the eID large scale pilot projects STORK[1] and STORK 2.0[2], which is still running.

Since national eID systems have been deployed nearly a decade, many requirements has been changed. In order to meet these new or changed requirements on e.g. cross-border federation, an improved and enhanced architecture for identity-management systems is inevitable for meeting those requirements. Therefore, we present an improved identity-management architecture in this paper, which will meet current requirements and which is open to future extensions.

This paper is structured as follows. In Sect. 2 general requirements for identity-management solutions are defined. In Sect. 3, we describe related work and discuss it with respect to the defined requirements of Sect. 2. In Sect. 4, we propose an enhanced architecture of an identity-management system which is capable of meeting all the requirements. Afterwards, in Sect. 5 we demonstrate the practical applicability of our proposed identity-management architecture by implementing an identity provider for Austrian eGovernment applications supporting three main identity-management use cases. Finally, conclusions are drawn in Sect. 6.

---

[1] https://www.eid-stork.eu/.
[2] https://www.eid-stork2.eu/.

2 Requirements

Identification and authentication are by far no new issues, thus several different identity-management systems have already evolved [4]. In most of these identity-management systems, user identification and authentication are handled by an identity provider, which finally transfers the user information and authentication data to the service provider. Based on these information and data, the service provider is able to decide whether to grant or deny access to its protected resources. Consequently, the identity provider constitutes a very important entity within an identity-management system. Especially if the service provider is a public-sector application providing eHealth or eGovernment services, the support of qualified citizen identification and secure authentication by the identity provider is essential. Hence, such an identity provider needs to fulfill certain requirements to meet the high level of assurance and security required by public-sector applications. For that reason, the following requirements should be fulfilled and kept in mind, if an identity provider for public-sector applications is designed.

- **Security:** An identity provider for public-sector applications is typically used in a security-sensitive area, which handles with highly personal date, like medical information. Public-sector applications require a highly secure identification and authentication process to protect these confidential and sensitive data against unauthorized access. Furthermore, a public-sector identity provider needs to be resistant against attacks that threaten to illegally influence the identification or authentication result.
- **Reliability and Testability:** Service providers that make use of the identity provider must be able to rely on the results of the identification and authentication processes carried out by the identity provider. In addition, it should be possible for the service provider to test and validate the authentication information to check if the information was provided from a trusted identity provider and not from a attacker.
- **Flexibility:** From a service provider's point of view, an identity provider should be able to provide different standardized interfaces for service-provider communication, to offer a wide range of possible connection scenarios. Therefore, flexibility with respect to service providers can reduce the deployment costs for them. From a citizen's point of view, an identity provider should provide different identification and authentication methods, in order to being able to support a large number of users and to enable a simple usage of different secure tokens.
- **Interoperability:** An identity provider should be work interoperable with other architectures, e.g. if the communication with other identity-management systems is necessary. The requirement of interoperability increases because the interconnection of heterogeneous identity management systems is important for identity federation. Especially, this requirement is important for cross-border acceptance of identity-management solutions and to interconnect national eID systems, like a pan-European eID federation.

- **Adaptability:** In many countries national legal requirements or eID solutions serving domestic needs exist, which an identity provider has to comply with. Such solutions – which cannot be implemented by generic standards – could be a special secure token or a proprietary national infrastructure. Therefore, an identity provider supporting public-sector applications needs to build on an adaptable framework to fulfill national characteristics and to support proprietary protocols or architectures.
- **Easy-to-Use Technology:** The usage of an secure identification and authentication process should not impede usability and accessibility for both citizens and service providers. Therefore, an identity provider should provide a recognizable user interface and enable a safe and known usage with this security-relevant application. Furthermore, this requirement covers several more aspects such as hiding complexity for service providers or platform independence to reduce deployment costs.
- **Modularity:** An identity provider should have a modular architecture, because modularity is in line with flexibility and interoperability. Therefore, a modular architecture facilitates the implementation of new functionalities to meet new requirements with respect to interoperability, standardized interfaces, or new identification or authentication methods.

There exists some other works, which handles with requirements for identity management systems [5,6]. Therefore, we use requirements of this related work in combination with our own experience to defined a non-exhaustive enumeration of requirements. This defined requirements are rather generic to be not bound to a special national identity-management system. In the next section, available identity-management systems are surveyed and their capabilities to meet the above defined requirements are assessed.

3 Related Work

Numerous identity-management initiatives and systems exist, therefore we will briefly introduce a couple of systems that gained importance either due to their broad use, or as they established relevant standards.

First systems used simple directory based solutions, like LDAP (Lightweight Directory Access Protocol), to perform identity management for single organisations. Since the borders between organisations decrease, interoperable identity-management becomes more and more important. In order to manage this, identity management has to be dynamic and adaptable in different and more complex situations to handle more then one specific context. This resulted in more adaptable solutions, like Kerberos [7], which is one of the earliest systems that allows secure authentication in unsecure TCP/IP networks.

With the increasing popularity of the World Wide Web, more sophisticated identity-management solutions, which allow secure authentication on application level, became popular. Therefore, within the Web new identity-management systems emerged, such as Shibboleth[3] or the Kantara initiative[4] (formerly the Liberty Alliance Project). Both projects influenced the development of the current version of the Security Assertion Markup Language (SAML 2.0) [8]. SAML has been developed by OASIS and defines one of the most important standards dealing with Single Sign-On or identity federation. A similar framework constitutes WS-Federation [9], being part of the WS-Security [10] framework. Another decentralized authentication system on the Web defines OpenID[5].

All above mentioned identity-management solutions could be used to perform a secure identification and authentication process, but most of them are limited to a single or few authentication protocols or standardized interfaces, which are used for service provider communication. Another issue is that they may not meet national legal requirements for qualified identification or authentication in security-sensitive areas of application as those identity-management systems have been designed generic. For instance, several countries use proprietary protocols or special eID infrastructures, like electronic mandate services for example, which can be used to add additional information to an authentication process. Furthermore, interoperability and federation with other eID solutions gains importance. While some of the previously described identity-management systems support federation, this is only possible when interconnecting systems with the same basic architecture or underlying protocol. However, currently used national eID systems have a heterogeneous structure, which means that different communication and variegated implementations are in use which hinder interoperability and identity federation.

In summary, there is currently no perfect solution available, which directly is able to fulfill all requirements stated in Sect. 2. To overcome this problem, we propose an enhanced and flexible architecture for identity-management systems using the example of an Austrian identity provider. The architectural design of the proposed solution is presented in the next section.

4 Architectural Design

The proposed solution of an advanced identity provider is based on a sophisticated modular architecture to satisfy the identified requirements. Figure 1 illustrates our proposal for a modular and adaptable architecture for an Austrian identity provider, which can be used in various ways for identification and authentication purposes. In case of an Austrian identity provider, our architectural solution facilitate authentication for public and private sector applications, electronic mandate services or cross-border authentication. Consequently, our architectural solution could not only be used in national eGovernment applications (public sector), but also are for a highly secure authentication on commercial applications (private sector), like a social network or an online shop, or to identity and authenticate foreign citizens.

[3] http://shibboleth.net/.
[4] http://kantarainitiative.org/.
[5] http://openid.net/.

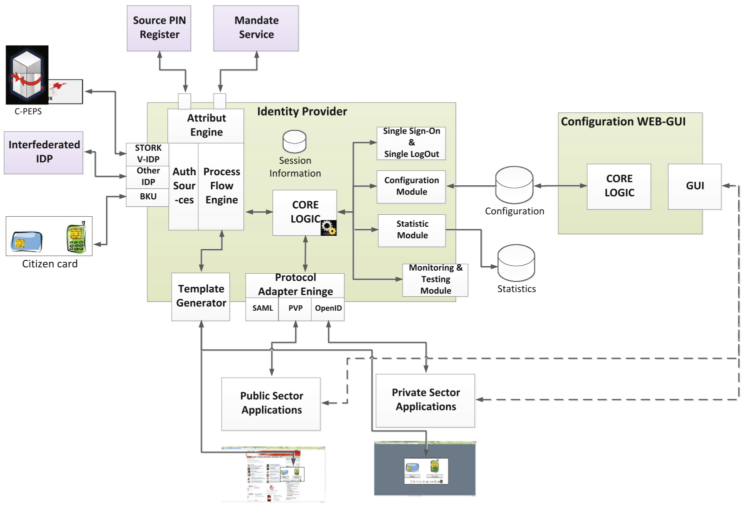

Fig. 1. Enhanced architecture of the Austrian public sector identity provider.

The *Core Logic* is the main item of our proposed solution. This main item coordinates the different steps of an identification and authentication process and handles the communication and interaction between all other modules and plug-ins, which can be used in our architectural design. This functionality is crucial, because an identification and authentication process mostly consists of different steps in which every step has a specific well-defined function. Consequently, it is imported to manage the divided different steps in a correct way, to fulfil the requirement of high secure identification and authentication of citizens. Therefore, our proposed architecture offer different features to support this different steps if an identification and authentication process in a modular way. To better illustrate this modular solution, we will describe it using the example of a generic identification and authentication process. This generic identification and authentication process describes the components and modules of our proposed solution on architecture level, but does not include every single communication step between the user's browser and the identity provider, service provider or other involved entities.

The authentication process is the first phase, if an citizen should be identified and authenticated. This phase is initiated by a communication between the Internet service and the identity provider via a well defined authentication protocol. In our architectural design, the *Protocol Adapter Engine* accomplish this communication task. To fulfil the requirements of flexibility and interoperability, we use a plug-in based to add and remove authentication protocols. For each supported authentication protocol, an appropriate *Protocol Plug-in* can be implemented. This modular Protocol Plug-in approach allows the implementation and usage of different protocols which are concerted to every single application with respect to protocol security and the required scope of operation. Such protocols could be SAML 2.0, which is widely in use, OpenID Connect [11], SAML 1.1 [12] or a national protocol, like the Austrian PVP 2.1 protocol [13], for example.

Our proposed architectural design allows the provision of different identification and authentication methods for users. According to this, a user could select the authentication method, which he or she wants to use, if the identity provider supports more the one identification and authentication solutions in the second phase. This step is carried out by a *Template Generator*, which generates a specific HTML Web interface providing a appropriate user interface to the user. Every Web interface is generated dynamically depending on all actually supported identification and authentication methods, which are implemented as Authentication Plug-ins, and application-specific information. This dynamically generated Web interface satisfies the requirement of an Easy-to-Use technology, because it provides a uniform interface to enable a safe and known usage of this security-relevant process step.

The third phase performs the technical identification and authentication operations. Our solution supports different high secure identification and authentication methods, which are collected and handled by an *Authentication Source Engine*. An identification or authentication step is realized as a single Plug-in. Such Plug-ins implement the communication with a secure token, like a smart-card, a hardware security-module (HSM), or the communication with another identity-management system, by using a well-defined interface, like STORK for example. A *Process Flow Engine* combines the single Plug-ins and these functionality to a well defined identification and authentication process flow. Every process flow, which is offered by the Process Flow Engine, is specified in a XML based configuration file by using an expression language. This expression language can be used to define single identification or authentication task, transactions between single tasks, and conditions for every transaction.

An additional *Attribute Engine* can be used in a fourth phase. This Attribute Engine manages *Attribute Provider Plug-ins*, which can be used to collect additional authentication attributes. Such attributes could be an electronic mandate in case of an authentication on behalf of somebody or other information collected from a national register, like the Austrian *Source-Pin Register* or the Austrian electronic *Mandate Service*. As example, the *Source-Pin Register*could be used to receive an additional unique identifier for this user an the electronic *Mandate Service* could be used to append mandate functionality to an eGovernment process.

At last, the collected identification and authentication information are processed to generate an authentication protocol specific authentication token, which is transmitted to the application by using a Protocol Plug-in. This modular approach allows the definition of various slightly different identification and authentication processes which satisfy the requirement of every application.

An additional feature of our architecture is a generic interface, which can be used to add new functionality to the Core Logic. The generic interface also uses Plug-ins to add new features to the core functionality. Such Plug-ins could implement features like Single Sign-On methods, monitoring and testing functionality, or a plug-in, which collects anonymised statistics information for quality assurance. To fulfil the requirement of an Easy-to-Use technology, a Web based management application, which provides a graphical interface to application administrators, can be used to configure the identity provider.

5 Implementation

The practical applicability of the proposed architectural design has been evaluated by realizing and implementing an identity provider in practice. To illustrate that, we have implemented an identity provider for Austrian eGovernment applications. Our implementation is based on Java, thus achieving platform independence and an easy deployment on heterogeneous server infrastructures. The next sub-sections discuss three practical use cases and their implementation by using our architecture in more detail.

5.1 Use Case 1: Austrian Citizen Authenticating at an Austrian Service Provider

In Austria, unique citizen identification and secure authentication is based on the technology-neutral concept of the Austria citizen card [14]. Currently, the Austrian citizen card is implemented as a client-side approach using smart cards and as a server-side approach involving the citizen's cell phone. Unique identification of a citizen is done by using a special XML data structure which is stored on the citizen card. Authentication is based by the creation of a qualified electronic signature. Since the Austrian citizen card is the official eID in Austria, a basic functional requirement of an Austrian identity provider is the support of the Austrian citizen card. Figure 2 illustrates the involved entities and their interactions in case of an identification and authentication process.

According to Fig. 2, the process of identification and authentication involves the following steps:

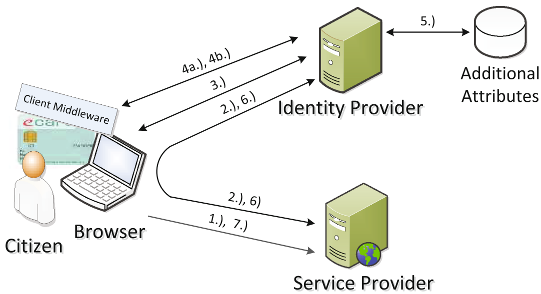

Fig. 2. Involved entities in an identification and authentication process in Austria.

1. A citizen wants to access a protected area on a service provider, which could be a eMail application, but also are a more sensitive application like an eHealth application, by using a HTTP GET or HTTP POST request. This protected area requires the identification and authentication of the citizen, by using the Austrian citizen card.
2. Therefore, the service provider starts an authentication process by triggering the identity provider. The identity provider is triggered by the service provider, which sending an authentication request via a specified authentication protocol. Most authentication protocols use HTTP POST or an HTTP Redirect with GET parameters to send an authentication request from service provider to identity provider via the user's browser. To fulfill the requirements of flexibility and interoperability and to support service providers, which use a diversified set of software implementations, our practical solution implements different authentication protocol plug-ins and hence is able to receive authentication request using different protocol formats. Actually, we implemented four protocol plug-ins to support SAML 2.0, OpenID Connect [11], the Austrian-specific PVP 2.1 S-Profile [13] and SAML 1.0[6] [12]
3. After the authentication request has been processed by the identity provider, the identity provider asks the citizen to select her preferred authentication method. Therefore, the Template Generator module, which is part of the identity provider, generates a web form to illustrate the different authentication solutions, which are supported by the identity provider. For Austria as example, a smart card based solution and a mobile phone based solution exists. After the citizen has selected the preferred solution, the identification and authentication process is started.
4. The proper identification and authentication process is performed by the Process Flow Engine in combination with the Authentication plug-ins. We have implemented different Authentication plug-ins to realize different processes for citizen identification and authentication. In the following two sub-steps, we describe the process, which uses the Austrian citizen card for this purpose, as an example. Therefore, a client middleware, which is just a piece of software (either installed on the citizen's PC or hosted on a server), facilitating access to the underlying citizen card implementation. In this example, a server hosted solution is used to deploy a JAVA Applet based client middleware in the citizens browser [15].
   (a) First, the identity provider identifies the citizen by using the XML data structure from the citizen card through the client middleware. This corresponds to the identification step. The corresponding plug-in implements the communication with the middleware and verification of the XML data structure, which comprises citizen identification information.
   (b) Second, the identity provider requests the citizen, via the client middleware, to create a qualified electronic signature for authentication. This task is also realized as a plug-in which implements the task specific communication and validation operations. Especially, validation is important

[6] In Austria, SAML 1.0 is widely used as legacy protocol by existing service providers.

to comply with the high security requirements for eGovnernment applications. Therefore, the electronic signature must be verified by the plug-in involving appropriate certificate revocation mechanisms, for example.

5. After identification and authentication are completed, the identity provider could use the Attribute Engine to collect additional authentication information of the citizen. Such additional information could be electronic mandates, for example, which are often used in Austria [16]. In our architecture, such additional information can be easily added to the authentication process by realization of an Attribute Engine plug-in. Therefore, we implement the communication with the Austrian electronic mandate service by using the Attribute Engine functionality.
6. If all authentication information is collected properly, the identity provider generates a protocol specific data structure. This data structure includes all authentication information that the service provider has requested and is transferred to the service provider.
7. Based on the received authentication information, the service provider is able to provide the protected resource to the citizen.

5.2 Use Case 2: Identity Federation

This scenario covers the case, where authentication information should be transferred from one identity provider to another identity provider. Such functionality brings considerable advantages to heterogeneous service models, in which service providers are linked to differed identity providers. Such advantages, for example are federated single sign-on (SSO) or interaction of identity providers which implements different identification and authentication methods. Figure 3 illustrates the actors and their relations in a federated service model. In this use case, every service provider is registered at a specific identity provider, similar to Use Case 1 described in Sect. 5.1, but in this use case there is the possibility of an

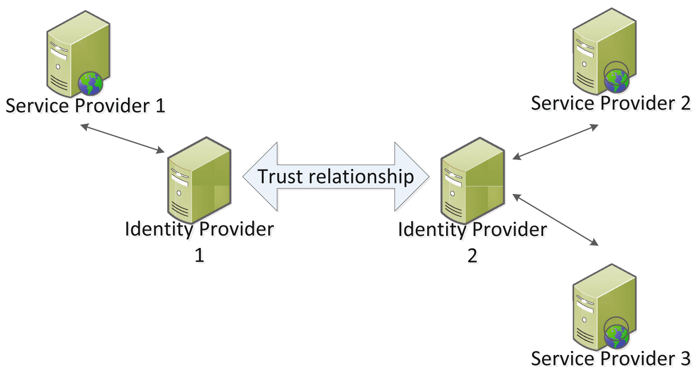

Fig. 3. Overview-Identity federation.

authentication data transfer between the individual identity providers. To transfer the authentication data between the concerned identity providers, a secure and trusted communication channel has to be established. We use the SAML 2.0 protocol to establish a trustworthy communication channel by using the SAML2 WebSSO Profile [17] and an exchange of SAML2 metadata [18]. An advantage of this solution is a high interoperability with other identity-management systems or identity provider implementations, because SAML2 is supported by almost all identity management solutions.

This functionality brings a lot of advantages for citizens and service providers. In the Austrian eGovernment, there actually exists practical applications for such an identity federation. We will present two of these applications next, one for citizens and one for employees of a public authority.

Federated Single Sign-on (SSO). eGovernment applications in Austria use a decentralized identity management approach, which means that service providers deploy there own identity provider for authentication locally in their service provider domain. This decentralized approach has advantages in case of availability and scalability but it is difficult to provide modern user-friendly functionality, like single sign-on for example. To overcome this disadvantage, we implement a single sign-on federation mechanism. Figure 4 illustrates such a federated single sign-on application scenario and the involved stockholders graphically.

The main stockholders in this application scenario are an *eGovernment Service Portal* with its dedicated *Identity Provider Service Portal* and an *eHealth Service* with is dedicated *Identity Provider eHealth*. According to Fig. 4, a citizen authenticates a single sign-on session on an *eGovernment Service Portal* by using the *Identity Provider Service Portal* to perform the identification and authentication process. Consequently, the single sign-on session is linked to the browser session between the *Identity Provider Service Portal* and the Web browser, which is used by the citizen. After this first identification and authentication, the citizen is authorized to enter the secure area of the *eGovernment Service Portal*. This secure

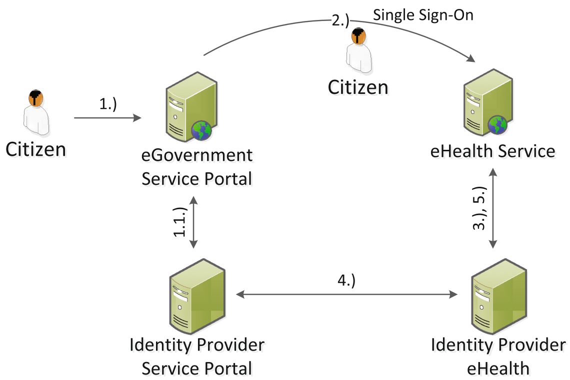

Fig. 4. Federated Single Sign-On for citizens.

area of the *eGovernment Service Portal* could be a One-Stop-Shop for different other eGovernmant applications, like an *eHealth Service* for example.

After this, the citizen wants to use an *eHealth Service*, which operates as a self-contained web application. For this purpose, the citizen clicks a link in the *eGovernment Service Portal* which redirects to citizen to the *eHealth Service* and automatically starts an identification and authentication process for them. But in contrast to a traditional process, in which a full identification and authentication process similar to the process described in Sect. 5.1 must be performed on the *Identity Provider eHealth*, our solution could reuse the existing single sign-on session at the *Identity Provider Service Portal* to authenticate a transaction at the *Identity Provider eHealth*. Figure 5 illustrates the full sequence diagram of this identification and authentication information transfer between the two identity providers.

According to Fig. 5, the federated single sign-on identification and authentication process involves the following steps. This sequence description starts with step 2, shown in Fig. 4, in which the citizen is already authenticated at the *eGovernment Service Portal* and now wants to use an *eHealth Service*.

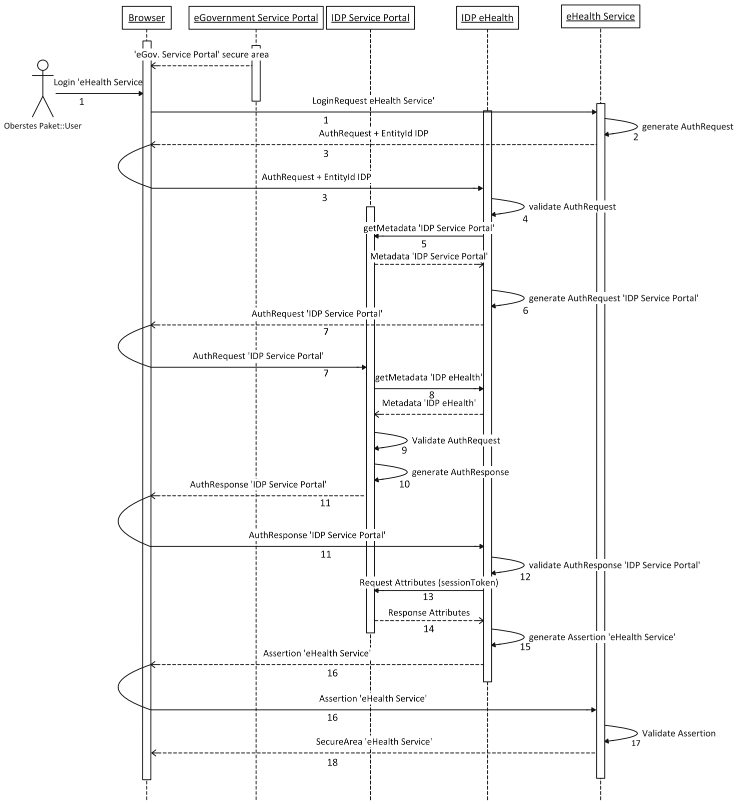

Fig. 5. Sequence diagram of federated Single Sign-On.

1. The citizen wants to use an *eHealth Service*, which operates as a self-contained web application. For this purpose, the citizen clicks a link in the service portal, which starts an identification and authentication process on the *eHealth Service*. This link URL includes the information of a possible active single sign-on session on the service portal IDP as a HTTP GET parameter. This HTTP GET parameter contains a unique identifier of the service provider IDP. In our implementation, we use the SAML2 EntityID of the *Service Portal Identity Provider* as unique identifier.
2. The *eHealth Service* generates an authentication request, by using one of the authentication protocols which the eHealth identity provider offers. By using our implemented solution, the *eHealth Service* could use SAML1, PVP 2.1 or OpenID Connect as authentication protocol.
3. The *eHealth Service* requests authentication from its dedicated identity provider, but in contrast to Use Case Sect. 5.1 the information of an active SSO session at the *Service Portal Identity Provider* is provided, by using the SAML2 EntityID. We use the SAML2 EntityID of the Service Portal Identity Provider, because the EntityID could be easily used by the *eHealth Identity Provider* to determine all necessary information to communicate with the*Service Portal Identity Provider*.
4. The *eHealth Identity Provider* validates the authentication request from the *eHealth Service*. If the request is valid, the federated single sign-on process starts. This federated authentication process can be divided into several steps. In all steps, the SAML2 WebSSO Profile is used to transfer authentication data between the identity providers in an encrypted way. The encryption keys are shared by using the information in SAML2 metadata, which are provided from each IDP.
5. The *eHealth Identity Provider* use the SAML 2 EntityID, received from the *eHealth Service*, to load the SAML2 metadata from the *Identity Provider Service Portal*. Therefore, the SAML2 Well Known Location Method [18] is used to evaluate the SAML2 Metadata URL.
6. The *eHealth Identity Provider* use the information from the SAML2 metadata to generate a SAML2 authentication request for the *Identity Provider Service Portal*.
7. The *eHealth Identity Provider* sends the authentication request to the *Service Portal Identity Provider* by using SAML2 Redirect Binding [19]. The Redirect Binding endpoint URL is also automatically discovered from the *Service Portal Identity Provider* metadata information.
8. The *Service Portal Identity Provider* use the SAML2 EntityID, which is part of the authentication request to get the SAML2 metadata from the *Identity Provider eHealth*, by using the SAML2 Well Known Location Method.
9. The *Service Portal Identity Provider* validates the SAML2 AuthnRequest, by using the SAML2 metadata which was received one step before. If the authentication request is valid, the federated authentication process is continued.
10. The *Service Portal Identity Provider* checks if a valid single sign-on session exists for this citizen. If the single sign-on session is valid, the *Service Portal*

Identity Provider create a SAML2 Assertion, which should be returned to the *eHealth Identity Provider*. This SAML2 Assertion is encrypted, by using the encryption key from the SAML2 metadata and only contains a unique identifier for the citizen, which should be identified and authenticated.

11. The *Service Portal Identity Provider* sends the SAML2 Assertion to the eHealth identity provider by using SAML2 Redirect Binding [19]. The Redirect Binding endpoint URL is also automatically discovered from the *Identity Provider eHealth* metadata information.
12. The *eHealth Identity Provider* validates the SAML2 Assertion received from the *Service Portal Identity Provider*. If the *eHealth Service* requires more attributes as the unique identifier of the user, the *eHealth Identity Provider* could use a SAML2 AttributeQuery request to collect more detail information from the *Service Portal Identity Provider*.
13. Therefore, the *eHealth Identity Provider* creates an SAML2 AttributeQuery request, which contains the unique identifier of the citizen and all attributes which are required. After this, the SAML2 SOAP Binding [19] protocol to build up a direct communication channel between the *eHealth Identity Provider* and the *Service Portal Identity Provider*. This communication channel is used to request all additional attributes, which are necessary to identify and authenticate the user at the *eHealth Portal*.
14. The *eHealth Identity Provider* receives all requested identification and authentication information from the *Service Portal Identity Provider*
15. If all attributes are collected, the eHealth identity provider could generate an *eHealth Service* specific authentication protocol response.
16. This *eHealth Service* specific authentication protocol response is returned to the *eHealth Service* by using a authentication protocol specific communication binding.
17. At last, the *eHealth Service* uses this authentication response to authenticate the citizen and grant access to the secure area.

By using our federated solution, it is possible to combine the user-friendliness of single sign-on solutions with the availability of decentralized services. Additionally, this solution requires no service-provider modifications because all functionality can be implemented on identity provider side.

Public-Authority Network Gateway. eGovernment services are not only used by citizens, they are also used by public officials during there occupation in public administrations. Such public administrations are carried out from a private government network on public eGovernment services. However, such administrative operations often require extensive privileges or additional attributes for security reasons. Figure 6 shows this use case in a graphical example. In this example, a public official would use an eHealth Service as part of his work as a civil servant. Here, the public official could be identified and authenticated in the secure private network area and maybe some additional information attributes could be collected. After this, he could be authenticated as a civil servant at the eHealth service without full re-authentication on the eHealth identity provider,

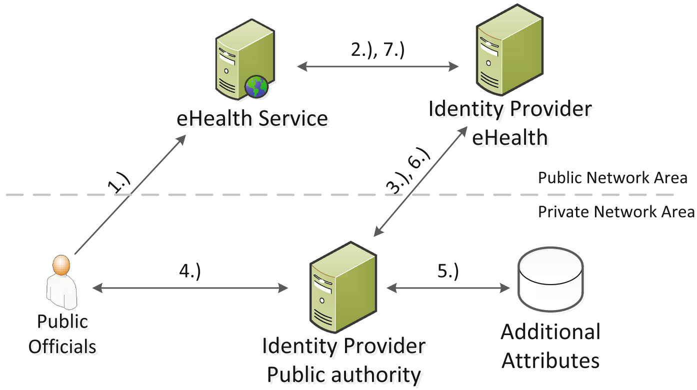

Fig. 6. Authentication of public officials on public eGovernment applications.

by using identity federation. An advantage of this solution is that there is no adjustment at the eHealth service necessary because the functionality for public officials is encapsulated in the identity provider functionality and can be also used for other services providers.

Both application scenarios can be implemented easily by using our architectural design and actually there is a trial period for establishment in Austrian eGovernement applications.

5.3 Use Case 3: European Citizen with European Service Provider

The third use case tackles the requirement of a secure and seamless cross-border electronic identification, which is part of the European eIDAS regulation or the STORK 2.0 large scale pilot [20]. 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. Actually, every EU member state has implemented its own identity management service infrastructure. This circumstance leads to a heterogeneous environment when these individual solutions should be coupled to a cross-border electronic identification solution. The STORK large scale pilots treated with an interoperability framework, which can be used to couple different national eID solutions.

The STORK interoperability framework defines two different 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 is shown in Fig. 7 and the middleware (MW) model illustrated in Fig. 8 [21].

The PEPS model uses a proxy-based approach to encapsulate specifics of the national eID infrastructure. In this model, a PEPS is a national gateway and a single point of service for other countries, which implements the cross-border authentication functionality. In contrast to the PEPS model, in the middleware model citizens are directly authenticated at the service provider. Therefore, the service provider has to deploy a so-called V-IDP in the service provider

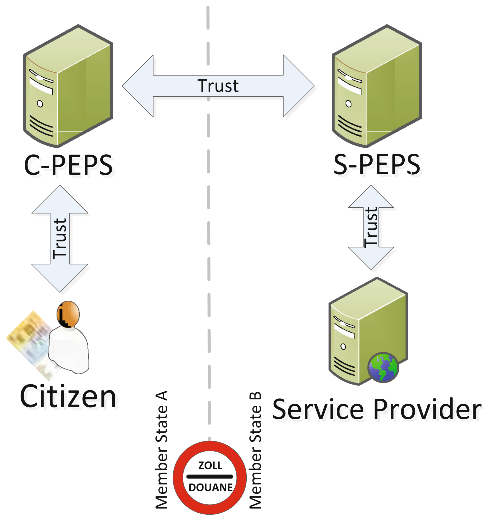

Fig. 7. STORK interoperability framework-PEPS model.

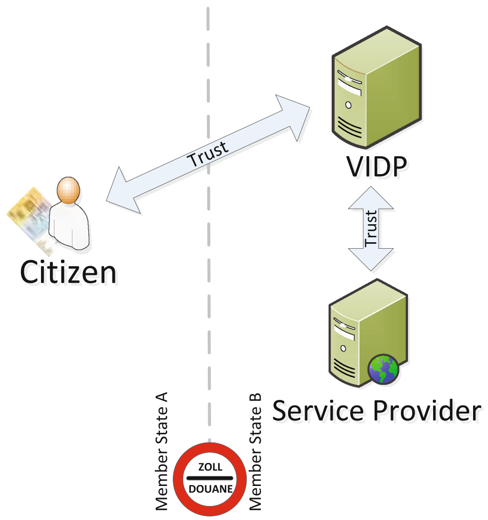

Fig. 8. STORK interoperability framework-Middleware model.

infrastructure. This V-IDP is the server-side middleware, 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 framework models. [21].

Therefore, we implement a solution for our Austrian identity provider, which can be used in both models in order to enable the widest possible utilisation.

From a national point of view, the implemented functionality can be separated into two process flows.

European eID to National Service Provider Flow. This process flow covers the case in which a European citizen, which does not have an Austrian eID, should be identified and authenticated to use an Austrian service provider. Therefore, we implement an authentication plug-in, which offers all functionality for PEPS communication to support the PEPS model, and functionality to identify and authenticate foreign citizens directly, which is identical to the middleware model. This direct identification and authentication is actually implemented for some European member states. Additionally, a mapping from European authentication information to national authentication information is required to fulfill Austrian legal requirements and to provide all necessary information to Austrian service providers [22].

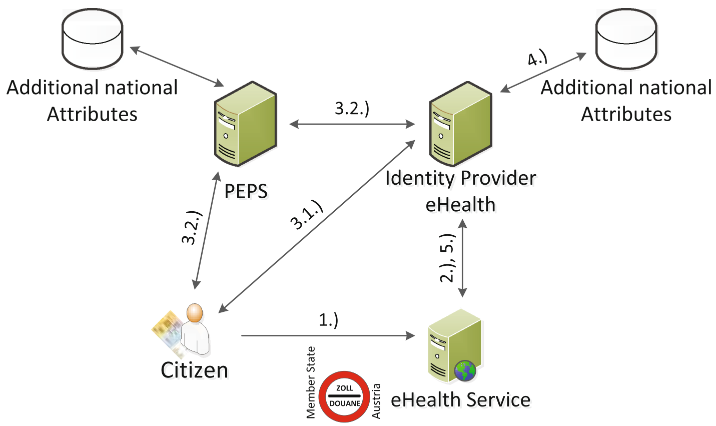

Fig. 9. Process flow to authenticate an European citizen at an Austrian service provider.

Figure 9 illustrates this inbound process flow.

1. A citizen of a member state wants to access a protected area at an Austrian service provider.
2. The citizen is redirected to the identity provider and there the citizen has to select the his or her favourite identification and authentication model.
3. After selection, one of the following solutions is performed.
   (a) **Middleware Model:** In this case, the identification and authentication process is performed at the Austrian identity provider by using the citizen's secure token directly. Consequently, only information that can be provided by the secure token can be used for identification and authentication.

   (b) **PEPS Model:** In this case, the citizen is redirected to the PEPS in the citizen's member state and there the identification and authentication process is performed. By using this model, some additional attributes could also be provided by using member state attribute infrastructure, which is connected to the PEPS. Afterwards, the authentication information is returned by using the STORK communication protocol.
4. To fulfill Austrian legal and technical requirements, the authentication data has to be processed by the Austrian identity provider. Therefore, we use the attribute plug-in functionality of our architecture to implement a register query plug-in, which uses the Austrian attribute mapping service [23] to fulfill these legal and technical requirements. This attribute mapping service uses the identification and authentication date received from STORK protocol to map this information to the Austrian proprietary datasets for identification information, which is a XML data structure. Additionally, this service also maps electronic mandate information, if an electronic mandate is used for identification and authentication by the foreign citizen.
5. At last, the authentication information is transmitted to the Austrian service provider and the citizen can access the protected resource.

National eID to European Service Provider Flow. The second process flow characterises the identification and authentication of an Austrian citizen to access protected resources at a European service provider. To perform this assignment, we implemented a new protocol plug-in, according to our architecture, which implements the STORK communication protocol for service provider communication. Therefore, this protocol plug-in can be used to authenticate an Austrian citizen by using his secure token.

If our solution is deployed as a single point of contact in Austria (C-PEPS) according to the PEPS model (see Fig. 7), then the member state service provider and the intermediate service provider PEPS (S-PEPS) can use the functionality of our identity provider just like an Austrian service provider can do. In this case all national legal requirements for additional attribute consuming, like the usage of electronic mandates, can be easily fulfilled.

The situation is different if the middleware model is used and our identity provider is deployed as a V-IDP which operates in the service provider infrastructure outside of Austria, because some national legal requirements cannot be achieved directly in this deployment situation. This circumstances affect mainly the attribute plug-ins, which are used to provide additional information after identification and authentication steps. In order to solve this problem, we benefit from our modular architecture design because the affected plug-ins can be easily replaced by a modified implementation, which are used in case of V-IDP deployment.

Figure 10 illustrates this deployment, in which a modified attribute plug-in for electronic mandate collection is used, as example. In contrast to the PEPS deployment, a request to the Austrian infrastructure is only necessary if requested authentication information cannot be provided by the V-IDP directly.

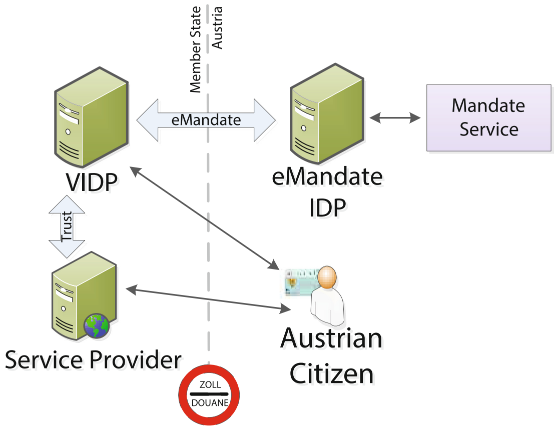

Fig. 10. Our IDP solution used as V-IDP with modified attribute plug-in.

The advantage of this solution is obtained by combining the benefits of the middleware model with the entire functionality of an Austrian identity provider.

By combining the inbound and outbound process flow, our solution can also be used to authenticate an European citizen to an European service provider. According to this, our implemented solution is also directly usable in other European states and not only in the Austrian national eID infrastructure.

6 Conclusions

Internet services and online applications are an integral component of our daily live. Such Internet services or online applications could be social network interactions and eMail applications, 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 users. Consequently, identification and authentication of users is an integral component of general Internet services or eGovernment applications in particular. In this paper, we have presented a new architecture for identity-management systems, to provide a flexible, interoperable and easy-to-use identity provider for service provider identification and authentication. To facilitate future extensions or new requirements of identity-management systems, our solution relies on an adaptable and modular architecture. Although, the presented architecture has been implemented as an identity provider for the Austrian eID infrastructure which had to be fulfil special Austrian legal and technical requirements. But the general architectural design is also applicable to other contexts and the module implementation of the Austrian identity-provider implementation can be easily adapt to national technical or legal requirements.

We illustrate three use cases to demonstrated the practical applicability and flexibility of our implemented identity provider for the Austrian eGovernment infrastructure, which is based on our proposed architectural design. These use cases cover the use of the presented solution to identify and authenticate Austrian citizens and public officials in various ways and assure interoperability of our solution in a European context. All of this 3 use cases are implemented and practically used in different national or European online applications. In detail, the practical implementation of use case 1 is used for productive applications in the Austrian eGovernment. The implementation of the use cases 2 and 3 are actually evaluated in different national and European pilot programs. The realization of further use cases or additional functionality, like two-factor authentication in case of single sign-on, that make use of the presented architecture is regarded as future work.

References

1. European Union: 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 (2014)
2. European Union: Ministerial declaration, Manchester, United Kingdom, on 24 November 2005. European Union (2005)
3. European Union: Directive 2006/123/ec of the European parliament and of the council of 12 December 2006 on services in the internal market. European Union (2006)
4. Bauer, M., Meints, M., Hansen, M.: D3.1: Structured overview on prototypes and concepts of identity management systems (2005)
5. Kölsch, T., Zibuschka, J., Rannenberg, K.: Privacy and identity management requirements: an application prototype perspective. In: Camenisch, J., Leenes, R., Sommer, D. (eds.) Digital Privacy. Lecture Notes in Computer Science, vol. 6545, pp. 735–749. Springer, Berlin Heidelberg (2011)
6. Ferdous, M.S., Poet, R.: A comparative analysis of identity management systems. In: Smari, W.W., Zeljkovic, V. (eds.) HPCS, pp. 454–461. IEEE (2012)
7. Neuman, C., Yu, T., Hartman, S., Raeburn, K.: The Kerberos Network Authentication Service (V5) (2005)
8. Lockhart, H., Campbell, B.: Security Assertion Markup Language (SAML) V2.0 Technical Overview. Technical report (2008)
9. Kaler, C., McIntosh, M.: Web Services Federation Language (WS-Federation) Version 1.2 (2009)
10. Nadalin, A., Kaler, C., Monzillo, R., Hallam-Baker, P.: Web Services Security: SOAP Message Security 1.1. Technical report (2006)
11. Sakimura, N., Bradley, J., Jones, M., de Medeiros, B., Mortimore, C.: OpenID Connect Core 1.0 (2014)
12. Maler, E., Mishra, P., Philpott, R.: Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML) V1.1. Technical report (2003)
13. Rainer, H., Pfläging, P., Zwattendorfer, B., Pichler, P.: Portalverbundprotokoll Version 2 S-Profil (2014)

14. Leitold, H., Hollosi, A., Posch, R.: Security architecture of the Austrian citizen card concept. In: Proceedings of the 18th Annual Computer Security Applications Conference, pp. 391–400 (2002)
15. Orthacker, C., Zefferer, T.: Accessibility challenges in e-government: an Austrian experience. In: Cunningham, S., Grout, V., Houlden, N., Oram, D., Picking, R., (eds.) Proceedings of the Forth International Conference on Internet Technologies and Applications (ITA 2011), pp. 221–228 (2011)
16. Rössler, T., Hollosi, A., Liehmann, M., Schamberger, R.: Elektronische Vollmachten Spezifikation 1.0.0 (2006)
17. Hughes, J., Cantor, S., Hodges, J., Hirsch, F., Mishra, P., Philpott, R., Maler, E.: Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0. Technical report (2005)
18. Cantor, S., Moreh, J., Philpott, R., Maler, E.: Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0. Technical report (2005)
19. Cantor, S., Hirsch, F., Kemp, J., Philpott, R., Maler, E.: Binding for the OASIS Security Assertion Markup Language (SAML) V2.0. Technical report (2005)
20. Leitold, H., Lioy, A., Ribeiro, C.: Stork 2.0: Breaking new grounds on eid and mandates. In: GmbH, M.M.F. (ed.) Proceedings of ID World International Congress, pp. 1–8 (2014)
21. Zwattendorfer, B., Sumelong, I., Leitold, H.: Middleware architecture for cross-border identification and authentication. J. Inf. Assur. Secur. **8**, 107–118 (2013)
22. Ivkovic, M., Stranacher, K.: Foreign identities in the Austrian e-government. In: de Leeuw, E., Fischer-Hübner, S., Fritsch, L. (eds.) IDMAN 2010. IFIP AICT, vol. 343, pp. 31–40. Springer, Heidelberg (2010)
23. Lenz, T.: A modular and flexible attribute mapping service to meet national requirements in cross-border eid federations. In: 13th International Conference on e-Society 2015, pp. 207–214 (2015)