Clemens Orthacker, Bernd Zwattendorfer - "Seamless eID Integration into Web Portals" - Electronic Government: Proceedings of ongoing research and projects of EGOV 09, 2009, pp. 297-304

SEAMLESS EID INTEGRATION INTO WEB PORTALS

Clemens Orthacker[1], Bernd Zwattendorfer[2]

Web portals, bundling related services or sites, usually rely on simple username/password authentication mechanisms for identification and authorization purposes. Many European Union Member States have rolled out diverse national eID solutions that meet the legal requirements for strong authentication. Although such national eID solutions already exist, the seamless integration into (eGovernment) Web portals is still an open issue. Within this paper we introduce a concept of a Web service that is able to integrate various legacy national eID solutions and that transforms identity information into a standardized representation. Finally, this representation is used to seamlessly authenticate the citizen at the Web portal. Using registrationless eID solutions allows to decouple the authentication process from the portal's user management. The presented concept was evaluated by adopting the Austrian and Belgian eID and by integrating the service into the open-source portal of the Liferay Inc.

1 Introduction

Authentication constitutes the process of verifying a person's identity to be authentic. In every system authentication is an essential mechanism ensuring that a user is the very person he or she claims to be. Based on trustworthy identity information, a system may provide means to grant or deny access to protected services or resources. Exceptions where no authentication is needed are usually just information retrieval of publicly available data. Therefore, electronic identity is considered as key enabler for eGovernment in the Ministerial Declaration of Manchester [1] which states, that

"by 2010 European citizens and businesses shall be able to benefit from secure means of electronic identification that maximise user convenience while respecting data protection regulations. Such means shall be made available under the responsibility of the Member States but recognised across the EU."

On national level, eIDs are already in place in many Member States. Most of the national solutions are PKI (public key infrastructure) based and rely on the use of smart cards. However, still other eID solutions based on several different technologies exist. An overview of initiatives in all Member States is given in a study carried out for the European Commission in the MODINIS programme [2].

[1] A-SIT Secure Information Technology Center - Austria, Inffeldgasse 16a, A-8010 Graz, Clemens.Orthacker@a-sit.at
[2] A-SIT Secure Information Technology Center - Austria, Inffeldgasse 16a, A-8010 Graz, Bernd.Zwattendorfer@a-sit.at

Within the eGoverment sector many organizations or institutions rely on eID solutions for protecting their services. Related eGovernment services and sites are often assembled in Web portals. In general, Web portals do not support strong eID authentication mechanisms but confide on ordinary username/password authentication techniques.

This paper introduces a concept to decouple the actual authentication process from the Web portal's user management and to seamlessly integrate national eID solutions into existing Web portals by means of a Web service. The so-called *Authentication Service* authenticates a citizen presenting his or her national eID and transforms the identification and authentication results to a portal internal, standardized protocol message, namely the Security Assertion Markup Language (SAML) assertion [3]. The research presented in this paper resulted from the project "eGov-Bus" [4] that has been supported by the European Community under Information Society Technologies priority of the Sixth Framework Programme.

2 Problem Description

On Member State level various different eID authentication and identity management approaches exist. The various national solutions are heterogeneous in technical, organizational and legal aspects. While smart cards are somehow the dominant technology, solutions based on mobile phones, username/password systems, or public key infrastructures without hardware tokens are also available in Member States (cf. MODINIS study [2]).

Due to the heterogeneity of eID technologies, the various solutions are in general not interoperable. Especially the seamless integration of eIDs into Web portals is an open issue. For this case, the so-called Authentication Service wraps legacy eID solutions and converts them into a specified SAML representation, which allows integration into a service oriented architecture (SOA). The Web portal itself is agnostic about the various authentication mechanisms; it merely receives authentication and identity information wrapped in a SAML message from the trusted Authentication Service.

3 Related Work

Numerous identity management systems and approaches addressing eID interoperability exist. In this section we address a few that the authors consider major ones.

3.1 Liberty Alliance Project

The Liberty Alliance [5] Project's aim is to develop open standards and guidelines for federated identity management and identity-based Web services. It provides a single sign-on solution using de-centralized authentication and authorization. Secure management of user data considering privacy and policy issues is covered as well. Members of the Liberty Alliance Project are both private companies as well as educational and governmental organizations.

Liberty Alliance focuses on identity federation (providing single sign-on) and specifies a framework for identity management. It does not aim to integrate *existing* Member State eID solutions and (due to its complexity) is not applicable for integration into individual service provider infrastructures for mere user authentication purposes.

3.2 Windows CardSpace

Windows CardSpace (formerly InfoCard) [6] is part of the Microsoft .NET frameworks. CardSpace defines an identity management technology for identification and authentication at Web sites or Web services. CardSpace is included in Windows Vista and can be additionally installed on Windows XP.

The main objective of CardSpace is the facilitation for users to securely prove their identity against Web sites or services (relying parties). CardSpace provides a more secure authentication mechanism than e.g. simple username/password schemes.

CardSpace builds upon the analogy of plastic cards in a user's wallet. Thereby CardSpace acts as wallet (identity provider) and contains a collection of various cards. If a user wants to access protected resources on a Web site supporting CardSpace (relying party) he or she is requested selecting an appropriate card out of his or her wallet and transmitting it to the Web site. The Web site verifies the identity information contained in the card and grants or denies access to the resource. In case of successful verification the user is authenticated to the Web site without typing any password.

The tight integration in the client's browser and operating system renders integration of various existing Member State eIDs difficult, since they rely on proprietary software ("Middleware") to interact with identity tokens.

3.3 STORK

The STORK project [7] is a large scale pilot in the ICT Policy Support Programme (ICT-PSP) under the Competitiveness and Innovation Programme (CIP) and is co-funded by the European Union. The aim of this project is to develop an interoperable, cross-border system for the recognition of the various Member States eID solutions and enabling secure authentication.

STORK proposes two conceptual eID frameworks, the Pan European Proxy Service (PEPS) approach and the Middleware approach, depending on the national eID employed. These approaches basically cover the Authentication Service's scope. STORK is an ongoing project, common specifications and first implementations are expected for 2010.

4 Authentication Service

The idea of the Authentication Service is to decouple the Web portal from various national eID approaches. Hence, the Authentication Service integrates single national eID solutions and transforms the authentication and identification mechanisms to an internal protocol message. Analysis of the current standards for eID and communication of authentication information showed that the Security Assertion Markup Language (SAML) standard provides a cross-domain authentication data exchange format widely adopted and approved in identity management and should serve as standardized protocol for the Web portal internal eID representation. Thus the Authentication Service acts as trusted intermediary transforming different heterogeneous national eID solutions to a standardized and Web portal internal eID representation using SAML.

In more detail, the Authentication Service consists of two logical parts, the validation of the national eID and the transformation to an internal eID representation. Figure 4-1 sketches the architecture of the Authentication Service.

eID Validation:

eID validation constitutes the intrinsic part where credential and identity verification is performed. For this operation, the Authentication Service integrates national specific eID modules depending on the eID identification and authentication mechanism used. E.g., for integration of the Austrian Citizen Card, the identification and authentication module MOA-ID [8] is integrated and adapted to meet the authentication requirements of the Web portal.

eID Transformation:

eID transformation is responsible for converting the authenticated eID into the portal internal representation. The transformation process is implemented by a security token service (STS) that issues such internal eID representations (SAML assertions). These representations are further used for secure exchange of identity information.

Depending on available information of the authentication mechanism used, different identity attributes are provided by the user. Thus the internal eID representation can contain following information:

- Unique identifier
- First name
- Last name
- Date of birth
- E-mail address
- Nationality

Additionally, similar to IDABC Authentication Assurance Levels [9], the SAML representation includes the authentication level describing the "quality" of the authentication scheme used. This allows the Web portal to infer the degree of confidence for a performed authentication without knowing the actual eID that was used for authentication.

An eID credential may be valid at a certain authentication level (security level) depending on the authentication mechanism used for eID validation. Thus the Authentication Service distinguishes three different authentication levels concerning the strength of the authentication mechanism selected. The defined levels are:

- low level: any kind of eID not meeting any of the higher level requirements (including for example no cryptographic security, simple username/password schemes)
- medium level: electronic identities certified by any authority
- high level: legally valid electronic identities certified by public authorities (generally relying on two-factor authentication)

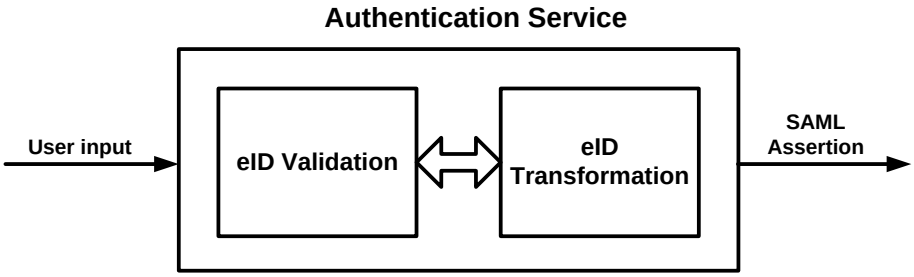

Figure 4-1- Authentication Service Overview

5 Architecture

The Authentication Service is implemented as Web service. The high-level communication with the Authentication Service implements a simple request/response protocol, providing an envelope format for the credentials under investigation.

The requests as well as the provided responses are to be secured (for example, a statement about the validity of a given eID credential has to be authentic and data integrity needs to be ensured). The standard way to secure SOAP messages is WS-Security, for transport layer security the secure SSL/TLS protocol is currently quasi-standard in many systems.

The implemented format of the internal eID representation is SAML and therefore a high-level messaging format supporting the secure transmission of SAML assertions is necessary. The implementation of the Authentication Service relies on the so called SAML Browser/Artifact Profile [10]. Within this profile, a reference to a SAML assertion is generated (SAML artifact) which is sent to a service provider to retrieve the assertion from the issuing party (identity provider). Within a distributed environment the Authentication Service acts as a pseudo identity provider that issues such SAML assertions (internal eID representations). In contrast, the Web portal acts as service provider because it fetches the assertion including the identity information from the Authentication Service.

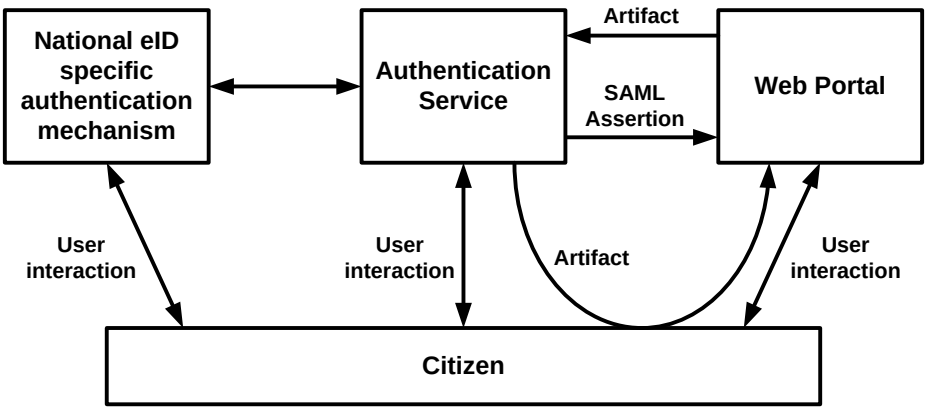

Figure 5-2 - Authentication Service Architecture

Figure 5-2 illustrates the architecture of the Authentication Service when integrated into a Web portal environment. Additionally, the different interfaces and communication channels, respectively, between the Authentication Service, the Web portal, the national eID specific authentication mechanism and the citizen are shown. In the following sub-sections these interfaces are described in more detail.

5.1 Citizen – Authentication Service

The authentication user interface is implemented using JSR 168 portlet technology [11]. This portlet presents a choice of supported authentication mechanisms where the user can select his or her national eID. Currently, the validation of the Austrian and Belgian eID is provided. In addition, if Member States do not support national eIDs, citizens can be authenticated by a simple username/password scheme or digital certificates.

The login-portlet does not perform authentication but redirects the user to the Authentication Service passing the selected authentication mechanism as parameter. The Authentication Service may be operated remotely by a trusted third party. Depending on the parameter received from the login-portlet, the Authentication Service forwards the authentication request to the specific national authentication module wrapped by the Authentication Service[3].

5.2 National eID specific authentication mechanism – Authentication Service

The interface between these two components heavily depends on the national eID solution. The Authentication Service sets an appropriate authentication request to the service corresponding to and developed for the particular eID. If necessary, user interaction takes place between the user/citizen and the eID authentication module. The response, whether the user has been identified and authenticated successfully or not, is returned to the Authentication Service. The type of this response depends on the national eID again.

5.3 Web portal – Authentication Service

If the citizen authentication has been performed successfully, the Authentication Service internally transforms the national eID representation into a portal internal representation. The Authentication Service transforms any authentication to SAML, regardless what national authentication mechanism was originally used.

Depending on the information provided by a national authentication module, the SAML assertion may contain following information:

- Citizen's unique national identifier
- Additional descriptive information to the authenticated person, e.g. name or date of birth
- The authentication level of the authentication process performed
- Citizen's home country two letter country code [12], if available

In order to communicate this eID – and thus the citizen's authentication status – to the Web portal, an interface and protocol to obtain the issued SAML assertion are implemented. By providing this interface, the Authentication Service acts as Identity Provider (IdP).

The SAML Protocol [3] defines a simple request-response protocol allowing a requesting entity (requester) to obtain SAML assertions containing authentication statements after successful authentication of the request's subject (usually the requester). According to the Browser/Artifact Profile of SAML [10], the Authentication Service sends a generated artifact

[3] No citizen authentication at national or regional eGovernment services is actually performed; rather, the citizen is authenticated at the Web portal using his or her accustomed national or regional eID technology.

through the citizen's Web browser to the Web portal via a HTTP redirect message. An artifact identifies a protocol message, allowing the recipient to resolve the requested message (either request or response message). The Web portal acts as SAML requester and sends a SAML request message containing the previously received artifact to the Authentication Service, which acts as Identity Provider. The SAML assertion is returned to the Web portal included in the corresponding response message. When dereferenced, the artifact gets invalidated and subsequent resolution requests fail to resolve the assertion issued by the Authentication Service.

The Authentication Service accepts artifact resolution requests only from the specified Web portal, which usually has to sign requests in order to authenticate the messages. The communication between the Web portal and the Authentication Service to obtain the authentication response carrying the SAML assertion is defined in the SAML Browser/Artifact Profile. It consists of a request message containing an AssertionArtifact element sent by the Web portal and the corresponding response returned by the Authentication Service. The AssertionArtifact element in the request message carries the artifact previously received from the Authentication Service via HTTP redirect. The returned response message is signed by the Authentication Service and its integrity should be validated by the Web portal before extracting the included assertion. The response message includes a response element holding exactly one SAML assertion.

Finally, after validating the authenticity of the SAML assertion the Web portal can use the information received for user authentication or even for registration, if the user accesses the portal the first time.

6 Conclusions and Lessons Learned

Many governmental institutions offer electronic services via the World Wide Web. In more and more cases such services are bundled through Web portals and combine various services relating to a special topic. Common open-source or proprietary Web portals rely on non-cryptographic authentication mechanisms such as username/password schemes only. For governmental services, these types of authentication are not sufficient. For some applications, high quality identification and strong authentication of citizens is necessary, thus the adoption of a national eID solution is required. Because of these cases a need for an easy and seamless integration of eIDs into Web portals arises.

In our work we have specified and developed a concept for a Web service that is capable of integrating various national eID solutions (or additional authentication mechanisms) and transforming identity information into a SAML-based eID representation understood by a Web portal that is otherwise agnostic about the diverse national eID authentication schemes of its users. In this context it is essential to decouple user authentication from the portal's internal user management. Registrationless authentication schemes are therefore a precondition to this approach.

For evaluation, this service has been implemented as SOAP Web service. As part of this implementation we have integrated two national eID solutions, the Austrian Citizen Card [13] and the Belgian eID [14]. Additionally, authentication via simple username/password schemes or digital certificates is supported. For testing and evaluation, the Authentication Service has been integrated into the open-source portal of the Liferay Inc. [15].

7 References

[1] Ministerial Declaration, Ministerial eGovernment Conference "Transforming Public Services", Manchester (United Kingdom) , November 2005, http://archive.cabinetoffice.gov.uk/egov2005conference/documents/proceedings/pdf/051124declaration.pdf

[2] MODINIS-IDM Study on Good Practices in Identity Management in eGovernment, https://www.cosic.esat.kuleuven.be/modinis-idm/

[3] Mishra, Prateek; Philpott, Rob; Maler, Eve: Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V1.1, OASIS, September 2003, http://www.oasis-open.org/committees/download.php/3406/oasis-sstc-saml-core-1.1.pdf

[4] Project eGov-Bus, http://www.egov-bus.org

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

[6] Windows CardSpace, Microsoft, http://www.microsoft.com/windows/products/winfamily/cardspace/default.mspx

[7] The STORK project, http://www.eid-stork.eu/

[8] MOA-ID Specification, http://www.cio.gv.at/onlineservices/basicmodules/moaid/specification/

[9] Authentication Assurance Levels, http://www.whitehouse.gov/omb/memoranda/fy04/m04-04.pdf

[10] Mishra, Prateek; Philpott, Rob; Maler, Eve: Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML) V1.1. OASIS, September 2003, http://www.oasis-open.org/committees/download.php/3405/oasis-sstc-saml-bindings-1.1.pdf

[11] JSR 168 Portlet Specification, http://jcp.org/aboutJava/communityprocess/final/jsr168/

[12] ISO/IEC 3166-1:1974, Codes for names of countries and dependent territories, ISO Standard, 1974

[13] Austrian Citizen Card, http://www.buergerkarte.at

[14] Belgian Personal Identity Card (BELPIC), http://eid.belgium.be/

[15] Liferay Inc., http://www.liferay.com/