Secure and Privacy-preserving Cross-border Authentication: the STORK Pilot 'SaferChat'

Thomas Knall[1], Arne Tauber[2], Thomas Zefferer[2], Bernd Zwattendorfer[2], Arnaldur Axfjord[3] and Haraldur Bjarnason[3]

[1] Datentechnik Innovation GmbH, Seering 5,
8141 Unterpremstätten, Austria

t.knall@datentechnik-innovation.com

[2] E-Government Innovation Center, Inffeldgasse 16/a,
8010 Graz, Austria

{Arne.Tauber, Bernd.Zwattendorfer, Thomas.Zefferer}@egiz.gv.at[2]

[3] Ministry of Finance, Arnarhvoli,
150 Reykjavík, Iceland

{Arnaldur.Axfjord, Haraldur.Bjarnason}@fjr.stjr.is

Abstract. Secure user authentication, provision of identity attributes, privacy preservation, and cross-border applicability are key requirements of security and privacy sensitive ICT based services. The EU large scale pilot STORK provides a European cross-border authentication framework that satisfies these requirements by establishing interoperability between existing national eID infrastructures. To allow for privacy preservation, the developed framework supports the provision of partial identity information and pseudonymization.

In this paper we present the pilot application SaferChat that has been developed to evaluate and demonstrate the functionality of the STORK authentication framework. SaferChat makes use of age claim based authentication mechanisms that allow for an online environment where kids and teenagers are able to communicate with their peers in a safe way.

We first identify relevant prerequisites for the SaferChat pilot application and then give an introduction to the basic architecture of the STORK authentication framework. We finally show how this framework has been integrated into the SaferChat pilot application to meet the identified requirements and to implement a secure and privacy preserving cross-border user authentication mechanism.

Keywords: e-ID, interoperability, authentication, privacy, security, e-Learning, Moodle, STORK.

1 Introduction

The secure and reliable authentication of users over the Internet has turned out to be a crucial requirement for various online services. This especially applies to security sensitive fields of application such as e-Banking or e-Government.

In many European countries, national eID infrastructures provide means for secure user authentication over the Internet. These infrastructures are usually isolated solutions as they need to meet country specific legal requirements and take into account special national circumstances. In a converging European society, missing interoperability between national eID infrastructures threatens to compromise the success of ICT based cross-border services. The European commission has launched several large scale pilots to address the key issue of interoperability and to facilitate citizens' personal mobility within the EU. These initiatives are explicitly mentioned in the e-Government action plan [1] as enablers of a single European digital market, which is one of the main goals of the European Digital Agenda [2].

In order to overcome eID interoperability issues and to facilitate secure cross-border authentication, the European Commission has launched the large scale pilot (LSP) STORK[1] [3], which attempts to establish interoperability between national eID infrastructures. Interoperability is achieved by means of a cross-border authentication framework that builds upon existing national solutions.

Besides achievement of interoperability, the improvement of privacy protection mechanisms for user authentication processes is another core objective of STORK. In various use cases, disclosure of users' full identities is neither required nor desired. For many applications, awareness of partial identity data such as the current age of users or even just the assurance that users fulfill minimum age requirements is sufficient. The STORK authentication framework successfully meets the requirement for provision of partial identity information. For each authentication process, the STORK framework allows for a flexible selection of requested identity attributes. Hence, STORK allows for secure but still privacy preserving cross-border authentication of users based on existing national eIDs.

To illustrate STORK's cross-border authentication framework, the pilot application SaferChat has been developed. SaferChat makes use of the popular open source e-Learning platform Moodle [4] and enhances it by means of an improved authentication scheme that allows for secure user authentications across national borders. This is basically achieved by combining Moodle's off-the-shelf authentication features with functionality provided by the STORK authentication framework.

Another objective of SaferChat is to demonstrate STORK's capabilities to preserve privacy. E-Learning platforms such as Moodle are indeed perfectly suitable for this purpose. Consider chat rooms that are intended for users of an e-Learning platform to collaboratively work on common assignments. Access to these chat rooms shall not be restricted to certain users based on roles for instance [5]. Instead, all students belonging to a predefined age range shall be granted access. In such scenarios, only reliable proofs about users' ages are required, while all other identity information may

[1] STORK is an acronym for "Secure Identity Across Borders Linked".

remain undisclosed. Again, the STORK authentication framework allows for implementation of the required secure and reliable age based access control.

In this paper we present the pilot application SaferChat in more detail. We show how SaferChat, which sets up on the e-Learning platform Moodle, implements a chat room module that securely authenticates users by means of national eID infrastructures and the STORK interoperability framework. Furthermore, we show how SaferChat preserves the privacy of users by making use of partial identity information only, while keeping the full identities of users undisclosed.

The paper is structured as follows. Section 2 introduces predefined requirements for the SaferChat pilot application. We show that the STORK authentication framework is perfectly suitable to meet these requirements. Details of this framework's architecture and functionality are introduced in Section 3. Section 4 presents the architecture of the SaferChat pilot application and shows how the STORK authentication framework has been integrated in order to meet the given requirements. Finally, conclusions are drawn in Section 5.

2 Requirements

For the SaferChat pilot application, four key requirements have been identified. In the following subsections, these prerequisites are described and motivated in more detail. Later, we show how the STORK authentication framework has been used to meet the identified requirements.

2.1 Secure User Authentication

A key requirement for the SaferChat pilot application is secure user authentication. In most cases, user authentication at e-Learning platforms such as Moodle relies on username and password based schemes. This authentication method is known to have several vulnerabilities [6][2]. To improve security, application of strong user authentication schemes has been identified as key requirement for SaferChat.

Usually, secure authentication schemes are based on a so-called two-factor authentication. In two-factor authentication processes, users prove their identity by means of something they possess (e.g. a smart card) and something they know (e.g. a secret PIN[3]) [7].

In various European countries, two-factor authentication based schemes are used in national eID infrastructures and allow for a secure authentication of citizens within e-Government or e-Banking processes. To achieve a comparable level of security for the SaferChat pilot application, secure user authentication based on existing national eID infrastructures has therefore been defined as key requirement for SaferChat.

[2] For instance, dictionary attacks may compromise the security of username and password based authentication schemes.

[3] PIN is an abbreviation for "Personal Identification Number".

2.2 Provision of Related Identity Information

The implementation of an age based access control mechanism to chat rooms is a basic objective of the SaferChat pilot application. To achieve this goal, reliable and trustworthy information about users' ages is needed.

Unfortunately, the already identified demand for secure user authentication does not guarantee that related identity attributes such as the user's age are available after successful completion of an authentication process. Authentication mechanisms verify the claimed identities of users but do not allow for any presumptions regarding related identity information.

As SaferChat requires reliable information about users' ages, provision of trustworthy related identity attributes can be identified as another key requirement for SaferChat.

2.3 Privacy Preservation

Independent from the provided level of security, privacy considerations often play an important role in authentication processes. In various authentication schemes, all available identity attributes are provided during an authentication process. As most applications require only certain parts of the entire identity information, transmission of users' full identities unnecessarily compromises users' privacy.

SaferChat is a prime example for an application that requires only partial identity information. To implement SaferChat's age based access control to chat rooms, reliable and trustworthy information about users' ages is needed. All other possibly available identity data such as name, place of birth, or residence address may remain undisclosed. To protect users' privacy, an enhanced authentication and attribute provision mechanism that allows for secure user authentications based on partial identity information is thus another key requirement of the SaferChat pilot application.

2.4 Cross-border Applicability

In our globalized world, the fundamental idea of a unified Europe continuously decreases the relevance of national borders. This applies especially to Member States (MS) of the European Union, for which a trend towards a single European market and a common European society can be observed. In such a scenario, the cross-border applicability of ICT based services is an increasingly important issue. European citizens should not be restricted to ICT services of their home country, but should be able to use selected services from other European countries too. Considering the SaferChat pilot application, the assurance of cross-border capabilities allows students of different countries to collaborate using a common e-Learning platform. Cross-border applicability is thus another key requirement of the SaferChat pilot application.

Assuring cross-border applicability for web based services is actually no big deal. In fact, various commercial Internet based services can be used irrespective of the user's actual home country. Unfortunately, the previously identified requirements for secure user authentication, reliable provision of identity attributes, and privacy preservation complicate the assurance of cross-border applicability significantly. In particular, missing interoperability between existing national eID infrastructures renders their application for the secure cross-border authentication of users difficult.

By striving for interoperability between national eIDs, STORK tackles this issue and provides means for secure user authentication across national borders. Details on design and architecture of the STORK authentication framework are presented in the next section.

3 STORK Interoperability Layer

The main objective of the STORK project was the design and development of an interoperability layer that supports secure cross-border authentication between European countries. The results of this development have been integrated and tested in several pilot applications where the SaferChat pilot defines one of them. In this section we provide some details of the general STORK interoperability architecture and show how individual components act together.

At the moment, several European Member States have already rolled-out national eID solutions in their country or are planning to do so. Usually, those eID solutions are designed to satisfy domestic needs only and lack in cross-border identification and authentication ability. This is where STORK bridged the gap and tried to make different national eID solutions interoperable. Although the eID landscape in Europe is very heterogeneous it is important to mention at this point that STORK did not try to reinvent the wheel by introducing a new and common European eID concept but aimed in connecting existing national eID infrastructures.

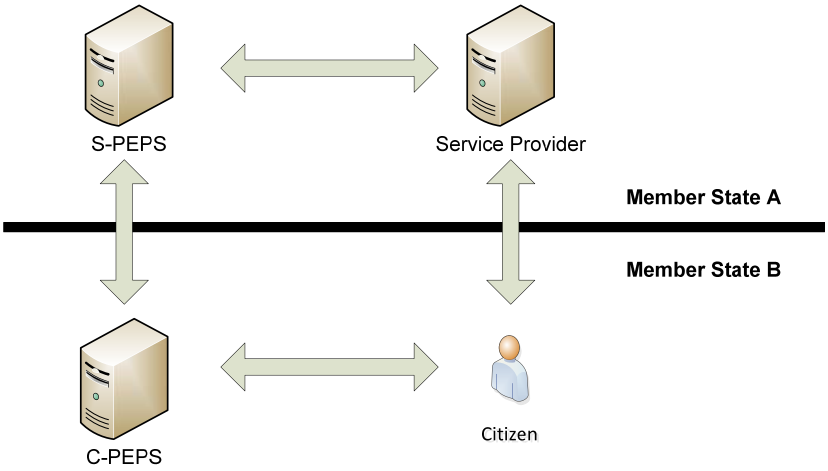

Fig. 1. PEPS Model

Generally, the STORK architecture builds upon two central authentication models where the individual national eID solutions can be classified in [8]. The first model defines a proxy-based approach where each Member State installs and hosts a central gateway. This so-called PEPS (Pan-European Proxy Service) is on the one hand responsible for the transfer of identification and authentication data across borders and on the other hand decouples national eID infrastructure specifics from the interoperability layer. The second base model of the STORK project defines the so-called Middleware (MW) model. In this model, no central instance per MS exists but each service provider integrates and supports several eID tokens using a common Middleware.

Fig. 1 illustrates the PEPS Model. In this case, a citizen originating from Member State B wants to access a protected service in Member State A that requires authentication. Both Member States follow the PEPS approach and have a national gateway deployed in their country. In a first step, after accessing the service provider (SP) in MS A the citizen is redirected to the respective S-PEPS (Service Provider PEPS) in MS A because it is assumed that no security context between the citizen and the service provider has been established before. The S-PEPS provides the citizen with a web page to select the citizen’s originating country. Based on this information the citizen is redirected to her national C-PEPS (Citizen PEPS) in MS B, which is responsible for the actual authentication process. The C-PEPS invokes all necessary identity and attribute providers of the citizen’s home country to successfully authenticate the citizen. After successful authentication, the C-PEPS transforms the identity and authentication information into a common STORK format and transmits these data back to the requesting S-PEPS. The S-PEPS in turn asserts the service provider that the citizens has been authenticated successfully and thus access to the protected resource can be granted.

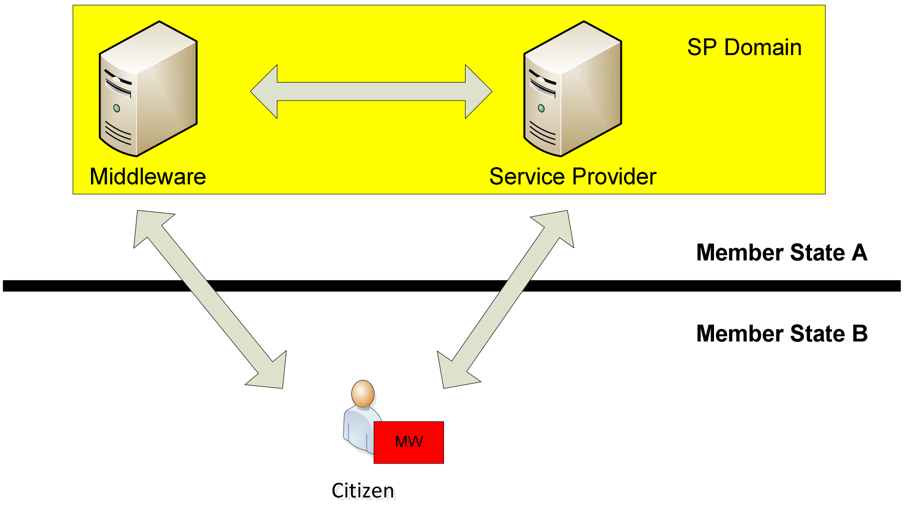

Fig. 2. Middleware Model

The basic MW model is illustrated in Fig. 2. In this picture, a citizen originating from a middleware country B wants to authenticate at a service provider in another middleware country A. In this example, after accessing the service provider application the citizen of MS B is redirected to the installed MW component. This server-side middleware is usually directly located in the service provider domain and supports all desired token-based identification and authentication mechanisms. Assuming the support of the eID token of MS B, the server-side middleware usually directly communicates with the citizen's eID token through a locally installed software on the citizen's personal computer. In comparison to the PEPS model, citizen's identity information is not stored at identity and attribute providers but right on the personal eID token. The identity information received by the middleware component is forwarded to the service provider, which either grants or denies access to the requested service.

The main advantage of the MW model depicts the direct communication channel between the citizen and the service provider whereas in the proxy model the PEPS acts as intermediary in between. Nevertheless, in the MW model the service provider needs to integrate and maintain all eID tokens that should be supported whereas in the PEPS model the PEPS hides all specifics of the national eID infrastructure from the service provider.

One of the objectives of the STORK project was to combine these two models in an interoperability framework to additionally support authentication for citizens between these models. Combining both models the next two interoperability scenarios can be identified:

- MW – PEPS model
- PEPS – MW model

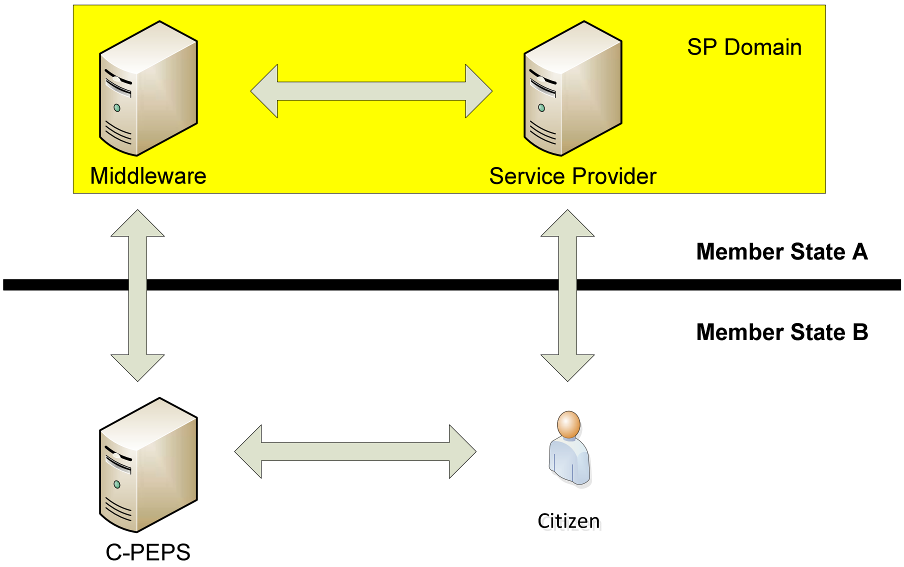

Fig. 3. MW-PEPS Model

Fig. 3 illustrates the first interoperability model where a citizen from a country, which originally follows the PEPS approach, wants to authenticate at a service provider located in a country supporting the MW model. In this authentication process, the first authentication steps are equal to the ones in the traditional MW model. However, instead of directly communicating with the eID token the citizen is redirected by the server-side middleware to the foreign C-PEPS. The foreign C-PEPS carries out the actual authentication with the citizen. The identification and authentication data are returned to the server-side middleware, which in turn hands over these data to the service provider.

The opposite model, in which a citizen of a MW country wants to authenticate at a service provider located in a PEPS country, is shown in Fig. 4. In this interoperability model, the STORK concept foresees a server-side middleware to be installed in the PEPS domain. Instead of being redirected during the authentication process from the S-PEPS to the C-PEPS as illustrated in the classical PEPS model (see Fig. 1) the authentication request is forwarded to the middleware component in the PEPS domain. Equally as in the traditional MW model, the server-side middleware component directly communicates with the citizen's eID token. Subsequently, the identity data are forwarded by the MW component to the requesting S-PEPS and service provider.

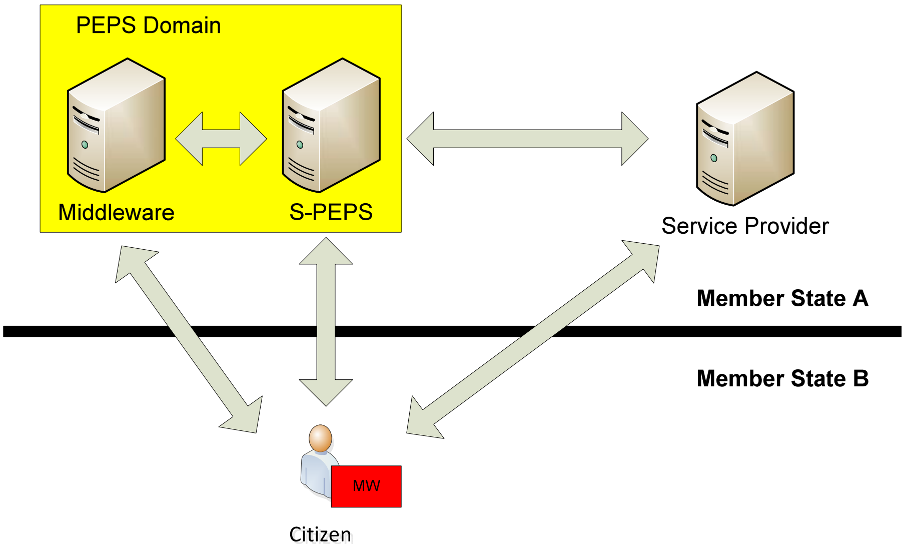

Fig. 4. PEPS-MW Model

Generally, the used protocols and exchanged messages between PEPS and middleware components are based on the secure and well-known standard SAML (Security Assertion Markup Language) [9]. Within STORK the standard protocols have been slightly enhanced to better fit the requirements of the project. Details on the used protocols and messages can be found in the STORK interface specification [10].

4 Integration of STORK into SaferChat

The pilot application SaferChat has been developed to demonstrate the capabilities of the STORK cross-border authentication framework with special regard to privacy issues. The core functionalities of SaferChat have been defined in [11]. More detailed information about the SaferChat pilot application is provided in [12].

In this section we introduce the architecture of the SaferChat pilot application in more detail. We first provide an overview of the Moodle framework, on which SaferChat has been based on. Subsequently, we reconsider the STORK interoperability layer and show how it has been integrated into the SaferChat application.

4.1 Moodle

Moodle is a web based open source e-Learning platform that was developed by Martin Dougiamas in 1999. Its name originates from the former acronym for *Modular Object-Oriented Dynamic Learning Environment*. Since its introduction in 1999, Moodle has been experiencing a continuously growing popularity all over the world. Currently, there are about 50.000 registered Moodle installations in more than 200 countries.

From the user's perspective, Moodle basically provides a set of online courses. Authenticated users may be assigned with different roles such as "Student" or "Teacher". Depending on their role and their assigned courses, users have access to different resources and features. For instance, teachers may define courses, upload assignments, or define online examinations. Students may for instance download working materials, collaborate in certain tasks using Moodle's Wiki functionality, or socialize in chat rooms.

Moodle follows a modular approach and encapsulates supported features in separated modules. By default, Moodle is shipped with a set of core modules. Additional functionality can be added easily by creating custom plug-ins. This way, the original Moodle installation can be extended by new features or alternative authentication methods for instance.

Its worldwide popularity and its open module-based architecture make Moodle perfectly suitable to demonstrate STORK's applicability. In the following, we show how Moodle's functionality has been enhanced by integration of the STORK authentication framework.

4.2 SaferChat Architecture

In this section we present the basic architecture of the SaferChat pilot application. We show how STORK and Moodle seamlessly complement one another to allow for secure and privacy preserving e-Learning solutions.

Fig. 5 illustrates the basic architecture of the SaferChat pilot application and its interface to the STORK authentication framework. SaferChat consists of two core components: an enhanced Moodle installation and a supplementary Moodle Connector. Users interact with the Moodle instance that has been equipped with the STORK authentication plug-in through their web browsers as usual. To carry out eID based user authentications, Moodle makes use of the Moodle Connector. The Moodle Connector itself acts as gateway to the STORK authentication framework. During the authentication process, users interact with the STORK authentication framework to prove their identity and to provide requested attributes.

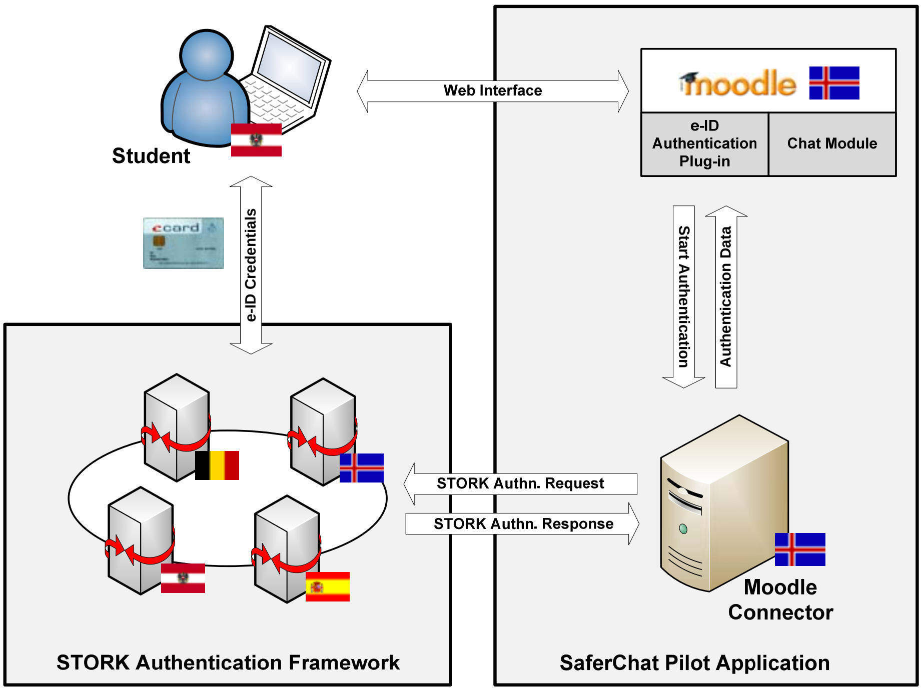

Fig. 5. SaferChat Basic Architecture

In the following subsection we introduce the major components of the SaferChat pilot application in more detail. We then go through the exemplary authentication process shown in Fig. 5 to illustrate Moodle's enhanced authentication scheme.

4.2.1 Moodle Instance

An off-the-shelf Moodle instance builds the basis of the SaferChat pilot application. To meet the predefined requirements, several enhancements have been applied to this Moodle instance.

The STORK authentication framework is used to meet the four identified key requirement of the SaferChat application. Therefore, Moodle has been enhanced by means of an additional STORK authentication plug-in. This plug-in supports the cross-border user authentication at Moodle using different national eIDs. If a user starts cross-border authentication, the process is delegated to the STORK interoperability infrastructure. After successful completion of the authentication process, the plug-in obtains the authentication data from the Moodle Connector and uses these data to authenticate the user at Moodle.

To demonstrate STORK's features for privacy preservation, Moodle's default chat module has been enhanced in such a way that age information can be used in order to grant or deny access to chat rooms. This age verification relies on authentication data provided by the STORK authentication framework. The enhanced Moodle chat module allows to set-up multiple chat rooms each being individually restricted to a certain age range.

4.2.2 Moodle Connector

The second core component of the SaferChat pilot application is the Moodle Connector. The Moodle Connector acts as intermediary between the enhanced Moodle instance and the STORK authentication framework. The Moodle Connector handles the communication with the STORK authentication framework and implements STORK specific protocols and interfaces. Thus, the Moodle Connector allows the Moodle STORK authentication plug-in to be kept lightweight.

Whenever user authentication based on national eID is triggered by Moodle, the Moodle Connector generates an appropriate STORK compliant authentication request to be transmitted to the STORK authentication framework. After completion of the authentication process, the Moodle Connector obtains a corresponding authentication response from the STORK framework. In case of a successful authentication process, the obtained response contains the requested authentication data. The Moodle Connector extracts the obtained authentication data and provides it to the Moodle instance in a usual way.

By encapsulating the interaction with STORK, the Moodle Connector minimizes required modifications of Moodle specific parts. This way, the Moodle Connector contributes to a clear architectural design and retains Moodle's modular nature.

4.2.3 Exemplary Authentication Process

Fig. 5 shows a typical use case for the SaferChat pilot application. According to the sketched scenario, an Austrian student attempts to join a chat room at an Icelandic Moodle instance. To authenticate at this instance using the Austrian eID, the student manually chooses the eID based authentication method. This activates the STORK authentication plug-in, which delegates the authentication process to the Moodle Connector and specifies the student's age as required identity attribute.

The Moodle Connector generates a STORK compliant authentication request and hands it over to the STORK authentication framework. After identification of the student's nationality, Austria's national eID infrastructure is contacted. Acting as identity provider, the Austrian eID infrastructure carries out the authentication process and obtains the requested identity attributes from the student's eID credentials.

The collected identity information (i.e. the student's age) is returned to the Moodle Connector via the STORK authentication framework by means of a STORK authentication response. The Moodle Connector extracts the requested identity attribute (i.e. the student's age) and returns this information to Moodle's eID authentication plug-in. Moodle is now in possession of the student's age and can decide whether to grant or deny access to chat rooms.

Note that although a qualified authentication process based on an approved national eID infrastructure has been carried out, only relevant identity attributes have actually been revealed. Thus, the illustrated example shows how the STORK authentication framework allows for secure and privacy preserving user authentications based on national eIDs.

5 Conclusions

Due to the emergence of ICT based services, various aspects of our daily lives have already been mapped to the digital word. This includes security and privacy sensitive processes such as financial transactions and e-Government services. At the same time, a converging European society has lowered the importance of national borders and raised the need for cross-border solutions. Given these preconditions, four key requirements for security sensitive ICT based services can be identified: secure user authentication based on approved national eID infrastructures, reliable provision of related identity attributes, privacy preservation, and cross-border applicability.

To meet these key requirements, the European Commission has launched the large scale pilot STORK, which aims to establish a cross-border authentication framework that builds upon existing national solutions. The key objective of this framework is the provision of means for secure and privacy preserving cross-border authentication of citizens. To evaluate and demonstrate the functionality of the STORK authentication framework, several pilot applications have been developed.

In this paper we have focused on the pilot application SaferChat that mainly aims to demonstrate STORK's privacy preserving features. Privacy preservation is basically achieved by supporting the provision of partial identity information. For each authentication process, required identity attributes can be selected dynamically. This way, only required identity information is revealed while all other identity data remain undisclosed.

SaferChat is based on the open source e-Learning platform Moodle, which has been enhanced by an improved authentication method and a new chat module. SaferChat allows users to securely authenticate at Moodle and implements an access control mechanism for chat rooms solely based on the verification of users' ages.

SaferChat is currently being piloted in Iceland and Austria. In both countries, a SaferChat instance has been deployed that is used by several Austrian and Icelandic schools. Due to the positive experiences that have been gained during more than nine months of productive operation, an extension to several other European countries has already been taken into consideration. The success of the SaferChat pilot application substantiates the privacy preserving capability of the STORK authentication framework. Supporting the provision of partial identity information, the STORK authentication framework significantly facilitates the development of secure and privacy preserving cross-border services.

References

1. European Commission: The European eGovernment Action Plan 2011-2015, COM(2010) 743, Brussels (2010)

2. European Commission: A Digital Agenda for Europe, COM(2010) 215 final/2, Brussels (2010)
3. Leitold, H., Zwattendorfer, B.: STORK: Architecture, Implementation and Pilots. Securing Electronic Business Processes. ISSE (2010)
4. Moodle, http://moodle.org/
5. Ferraiolo, D.F., Cugini, J.A., Kuhn, D.R.: Role-based access control (RBAC): Features and motivations. NIST (1995)
6. Kessler, G.C.: Passwords – Strengths and Weaknesses. In: Cavanagh, J.P. (ed.) Internet and Networking Security, Auerbach (1997)
7. Yang G., Wong D., Wang H., Deng X.: Two-factor mutual authentication based on smart cards and passwords. vol. 74, pp. 1160-1172 (2008)
8. Berbecaru D. et. al: D5.7.2 Functional Design for PEPS, MW models and interoperability. STORK Deliverable (2010)
9. OASIS, Security Assertion Markup Language (SAML), http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
10. Alcalde-Morano J., Hernández-Ardieta J.L., Johnston A., Martinez D., Zwattendorfer B., Stern M.: D5.8.1b Interface Specification. STORK Deliverable (2009)
11. Bjarnason H., Knall T., Axfjörð A.F.: D6.2.1 SaferChat - Functional Specification. STORK Deliverable (2009)
12. Bjarnason H., Knall T., Axfjörð A.F, Jónsson G. K.: D6.2.3 SaferChat Detailed Planning. STORK Deliverable (2009)