Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2009

Strong Authentication for Web Services using Smartcards

D S. Stienne
University of Plymouth

Nathan Clarke
Edith Cowan University

Paul Reynolds
France Telecom R&D

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2013
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/8

Strong Authentication for Web Services using Smartcards

D S Stienne[1]
Nathan Clarke[1,2]
Paul Reynolds[3]

[1]University of Plymouth
[2] secau - Security Research Centre - Edith Cowan University
[3]France Telecom R&D

Abstract

The popularity of the Internet and the variety of services it provides has been immense. Unfortunately, many of these services require the user to register and subsequently login to the system in order to access them. This has resulted in the user having to remember a multitude of username and password combinations in order to use the service securely. However, literature has clearly demonstrated this is not an effective approach, as users will frequently choose simple passwords, write them down, share them or use the same password for multiple systems. This paper proposes a novel concept where Internet users authenticate to web services (service providers) by the use of a smartcard – taking away any requirement for the user to provide credentials. The smartcard is useful in this context as it is a trusted device that is capable of applying cryptography in a tamper resistant environment. The development of the concept is based upon an extension to Authentication Authorisation Infrastructure (AAI) models, where a trusted authority (Identity Provider) will provide and manage the smart card to end-users. In devices such as mobile phones, a smartcard is already present (e.g. the SIM) to facilitate this and it is envisaged such a card could also be produced for desktop environments – similarly to what many banks are currently implementing.

Keywords

Smart Card, Authentication, AAI, Identity Federation, SAML

INTRODUCTION

Internet users have to prove their identity when accessing services or personal information from web services (service providers). This authentication is generally achieved through the use of identifiers and passwords. With the emergence of the Internet and its substantial popularity, users have to manage a growing numbers of login/passwords which represent their identity across different Service Providers (SPs). The management of these is often difficult as the user does not remember every identifier associated with each web service. In addition, the use of passwords raises a problem of security, with for example having an identity compromised, theft or misused (Schneier, 2004). Indeed, password authentication relies upon the use of a secret knowledge shared between two parties that could be easily disclosed either by the user's behaviour or by a bad implementation of the authentication protocol at the Service Provider. In the first case, the user is responsible to protect, manage and update his passwords on a regular basis and to utilize a different one for each service (Warren, 2006). However, this is not the case for all users who often write them down on paper or a post-it, or just use the same password for every service. As such, Service Providers also have to be careful about the implementation of such an authentication technique and the reliability it is assumed to have. In addition, other threats such as eavesdropping could also reveal the secret information if the channel between end-user devices is not secured (Warren, 2006). Currently, the most frequent form to secure the exchange of credentials is to use the Secure Socket Layer (SSL) protocol with a server side certificate, but this is not always utilised. Taking this into account, the research has proposed a novel approach where a smartcard will be utilised to provide transparent authentication of the user from his device. This approach removes any inconvenience for the user in having to remember username and password information for each service and provides the opportunity to improve the level of security through using asymmetric cryptography.

This paper is organized in five sections, beginning with an overview of smart cards technologies. The paper will then proceed to discuss current research in to the area of federated identity, specifically focussing upon the work of Shibboleth and Liberty Alliance. The third section provides a detailed description of the novel approach; and the penultimate section discusses the overall concept, with a discussion on the advantages and disadvantages. Finally, the conclusions are presented in section four.

BACKGROUND LITERATURE

Smartcard Technologies

By definition, there are different categories of smart cards; passive and active (Scheuermann, 2002). Passive tokens simply store a secret that is subsequently presented to an external system for processing validation. Active tokens also store a base-secret, but this information is never released to the external system. Instead, the token is capable of processing the secret with additional information and presents the result of the verification to an external system. Active tokens or cards are built around a microprocessor and relatively small amounts of memory. The cards benefit from a highly secure tamper resistant environment which makes it difficult for the contents of the memory to be misused active (Scheuermann, 2002). It was due to these very attributes that SIM cards were developed for mobile phones – so that network operators would have a trusted relationship between the handset and network. This tamper resistant environment built upon a relatively cheap and scalable technology has the potential to be useful in storing other information such as user's web identities. Moreover, with over 3 billion mobile phones in use, a solid foundation for the use of these smartcards already exists (GSM Association, 2009).

Therefore, smartcard technologies comply with the defined ISO 7816 standard which describes how this card is produced along with the interactions with smartcard readers. However, the deployment of such a strong authentication solution is currently very limited as it requires the involvement and interoperability between different Service Providers. As a result, the research intends to propose the utilization of the smartcard within a specific framework. The framework is based upon current AAI models, where a trusted entity called an Identity Provider (IdP) will be present to provide and manage the smart card concept to end-users (Service Providers playing the role of web services). Thus, the next section reviews two existing AAIs.

A Review of Authentication Authorisation Infrastructures

The research chose to review two well-known AAIs: Shibboleth (2009) and Liberty Alliance (2007).

Shibboleth is an Internet 2 project which has developed an open solution to solve the problem of sharing resources between different Service Providers. These have their own authentication and authorisation policies which impede sharing resources between them. The Shibboleth project chose to develop a novel idea where a home organisation is present to authenticate the user in different Service Providers. In addition, the home organisation manages the identity of the user. This identity is composed of different attributes which can be disclosed to Service Providers for authentication purposes. Consequently, when a user requests an access to a resource stored from a Service Provider, the Service Provider sends its attribute rules to the home organisation and the home organisation supplies the necessary information back to the Service Provider. The Service Provider then chooses to grant or deny the access to the resource. The advantage of such an architecture is that the Service Providers do not have to manage the authentication of the user; this task being delegated to the home organisation and authorisation decisions are performed by the Service Provider.

The Liberty Alliance project is a European project which was initiated in 2001. It involves key organisations such as France Telecom, British Telecom, Intel, Sun Microsystems amongst others working as a consortium. They cooperate in order to write open standards and define requirements to provide federated identity management. By definition, the concept of federation allows the user to manage his identity across different Service Providers and to navigate directly from Service Provider to Service Provider without the need to re-authenticate (single sign on). This situation is possible when Service Providers are part of a circle of trust where an Identity Provider authenticates the user in his federated services. Both IdP and SP parties must comply with the Liberty Alliance federation framework in order to function across common protocols to exchange their information (DeLooze, 2007).

Whereas Shibboleth is open source software (i.e. released under apache software licence), the Liberty Alliance does not provide any software, but releases specification drafts defining abstract protocols and delegating the task of developing it practically to organisations which wish to implement the federation framework.

Integration of Smartcard into the AAI model

As previously mentioned, within the AAI model, there is an IdP or home organisation (Shibboleth term) which is present to authenticate the user and provide the corresponding user's identity to different Service Providers. These AAIs bring two main advantages: the first one is that the authentication of the user is delegated to the Identity Provider and the second one is that the Identity Provider knows how to name a user at different Service Providers.

However, the research wants to propose a novel concept, where the user can authenticate *directly* to Service Providers (without depending on authentication at the IdP). This case will be possible (see figure 1) by the use of a smartcard where user's identities at different Service Providers will be downloaded remotely from the Identity Provider into smartcard.

This is made possible, primarily due to the trusted nature of the smartcard technology. Once identities are downloaded, the user can provide them to Service Providers totally independent of the Identity provider. This enables the reliance upon the Identity Provider to provide authentication – representing a possible single point of failure in the system. It also reduces the volume of traffic as fewer communications are necessary to complete the transaction and is arguably more scalable from a technology perspective when considering the billions of authentications that might be required daily. Consequently, the role of the Identity Provider will change from existing AAIs (Shibboleth and Liberty) from being used to verify the authenticity of every user to every service, to a management role that creates the initial trusted relationship.

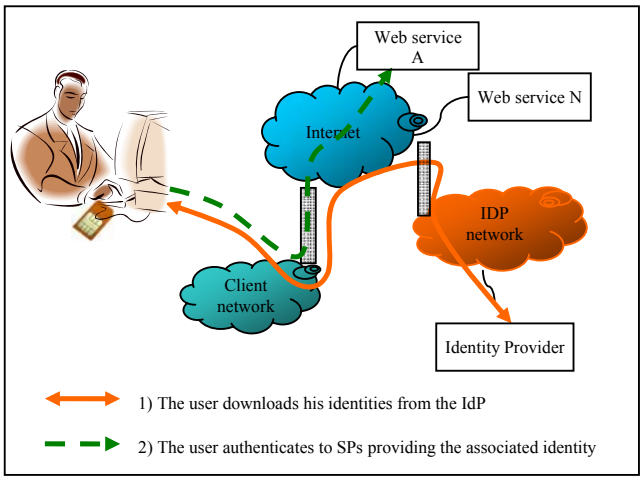

Figure 1 - Smartcard deployment with the AAI model

The following sub-sections introduce several components of the concept, starting with an overview of the Identity Provider and Service Provider association which uses an Internet open standard in order to be interoperable. Subsequently, the second section provides a description of the smartcard features released to the end users by the Identity Provider. The third section illustrates how user's web identities at Service Providers are built, and finally, how the user authenticates to Service Providers.

Identity Provider and Service Providers Association

The research considers that the association between Service Providers and Identity Providers takes place in the context of a *federated* environment. By definition, a federated environment is a set of entities which communicate together with common practices and policies in order to exchange information about their users and resources (Maler, 2006). In our novel concept, both Identity Providers and Service Providers will have to be interoperable, complying with the same methods to exchange information. Furthermore, stakeholders will have to establish trust between each others.

Interoperability: The research has chosen to utilize an Internet open standard called the Security Assertion Markup Language (SAML) produced by the Organisation for the Advancement of Structured Information Standards (OASIS). In reality, SAML is the convergence of work undertaken by Shibboleth and Liberty Alliance project (OASIS, 2004a). By definition, this open standard will provide an efficient mechanism to create and exchange information regarding a user at a particular Service Provider.

Trust: In the AAI model, we need to establish a trust between different entities. In this case, when the Identity Provider produces web identities of the user using SAML assertions, Service Providers will have to trust these assertions. According to the trust model guidelines of the OASIS consortium (OASIS, 2004b), trust is established between two axis: authentication and business agreements (BA) criteria (see figure 2). Considering the strong authentication solution; the research has selected to favour the "Pairwise/Direct" model where Service Providers and Identity Providers have a BA and authentication is made by the use of digital certificates and Public Key Infrastructure (PKI) technology (OASIS, 2004b).

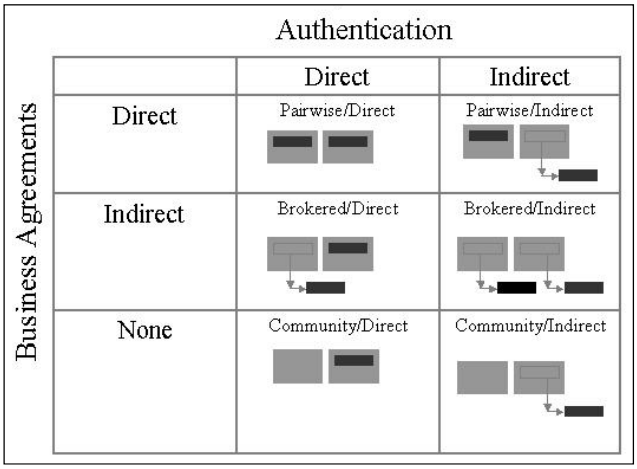

Figure 2 - Trust model category [9]

By definition a PKI is an infrastructure where a Certification Authority (CA) allows different entities to establish trust. This establishment is achieved through the use of digital certificates issued by a trusted CA. Each Service Provider and Identity Provider will exchange their own digital certificate in order to establish trust for a future exchange of SAML assertions.

SAML Assertions

In the SAML concept, SAML assertions are produced by an SAML authority (Identity Provider) and Service Providers are called SAML consumers. By definition, SAML assertions are codified using eXtensible Markup Language (XML) in a data structure which contains information about a user. Therefore, these SAML assertions may contain more data, for instance; authentication statement, authorisation statements, or advanced attributes about a user (OASIS, 2005a). In our case, SAML assertions will be used to create the identity of the user at the corresponding Service Provider.

Typically, when the user desires to use the strong authentication solution for the first time at a particular Service Provider, the Identity Provider will provide the assertion data remotely as illustrated in Figure 3. The structure of the assertion starts with a unique assertion identifier, an issue instant (the time when this one has been created) and the issuer name (i.e. IdP name) followed by the Subject section which then specifies the unique name identifier of the user at the Service Provider and the unique name identifier at the Identity Provider. This information is mandatory as the Service Provider will identify the user through these name identifiers.

In addition, this section includes a subject confirmation method where the user will have to prove his identity when providing the assertion to an Service Provider. Since assertions will be stored in a smartcard, the research has chosen to provide the smart card with a pair of public and private keys and a public key certificate to digitally sign the assertion. Consequently, the "subject confirmation method" field will contain the public key certificate of the smartcard.

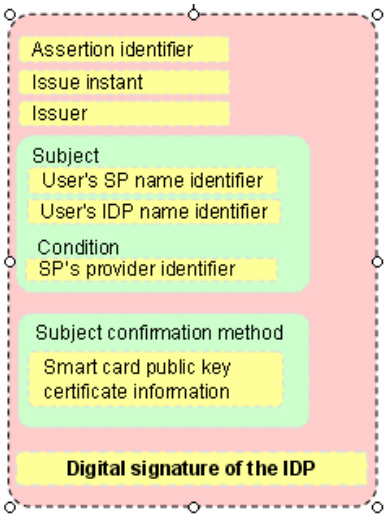

Figure 3 - SAML assertion that will be created by the Identity Provider

Subsequently, the condition field is present to limit the scope of the assertions to one specific Service Provider. Finally, the entire SAML assertion is digitally signed by the Identity Provider in order to guarantee the integrity of the assertion. As a result, when the assertion is provided remotely into the smartcard, it cannot be modified.

Smartcard Features

As previously mentioned the smartcard is a secure token capable of storing/processing data and protecting access to it. When the smartcard is issued to the end user, part of the memory will be dedicated to store SAML assertions (see figure 4). In addition, the card will be provided with a pair of public and private keys. The private key will be used in order to digitally sign the assertion when authenticating at the Service Providers. As a result, the smartcard will be capable of signing the corresponding assertion and will be provided with a cryptographic function in the chip based upon the RSA encryption standard. This cryptographic function is defined by the PKCS#1 standard (RSA, 1993). Furthermore, when signing messages, the user must have a public key certificate which guarantees that the private key used to sign message is bound to his identity. Typically, the public key certificate is issued by a CA and trusted by Service Providers as part of the BA with the Identity Provider.

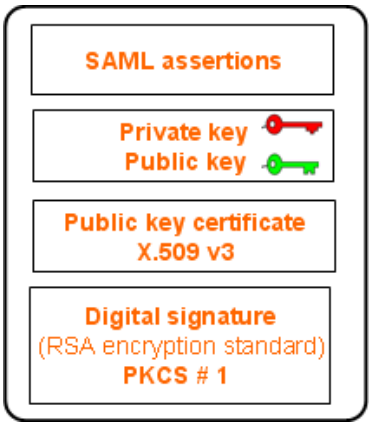

Figure 4 - Smart card feature released by the IDP

When initialising for the first time the strong authentication solution at the Service Provider, the user will be redirected to the Identity Providers website and this one will provide the SAML assertion remotely on to the smartcard. The following time, when the user requests access to his Service Provider, the assertions will come directly from the smartcard rather than having to use the Identity Provider.

User Authentication to Service Provider

Once the user's assertions have been provided to the smartcard, they can be used to authenticate the user to the corresponding Service Provider. As mentioned, Service Providers consume SAML assertions and make authorisation decisions based on these. The communication with Service Providers is made through the web browser of the user. The research supposes that the web browser is able to communicate with the smart card in a secure manner. Thus the exchange of these assertions is made by sending XML messages over the Hyper Text Transfer Protocol (HTTP) using the Reverse Simple Object Access Protocol (SOAP) binding (POAS) defined by the SAML standard (OASIS, 2005b). If supported by the web browser of the user, this binding allows both parties to exchange SAML assertions. Typically, the POAS binding is designed with an authentication request and response protocol where the Service Provider issues an authentication request to the user, and the web browser must respond with an authentication response (OASIS, 2005b).

A generic authentication response is illustrated in Figure 4. In this figure, the response made by the web browser contains the request identifier of the Service Provider and the issue instant of the request. In addition, the content of authentication response contains the corresponding SAML assertion related to the Service Provider. Finally, the entire response message is digitally signed by the private key of the smartcard. As mentioned in the previous part, the digital signature is mandatory as it provides a mechanism to confirm that the user is the owner of the SAML assertion.

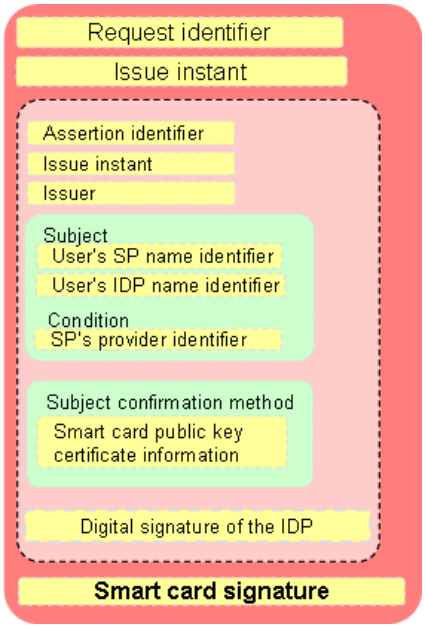

Figure 5- Authentication response

Once received by the Service Provider, the SAML assertion will have to be checked carefully: firstly, by verifying the smartcard's signature and the validity of the public key certificate of the smartcard, and secondly, by verifying the signature and the public key certificate of the Identity Provider. Depending on the result of these checks, the Service Provider makes authorisation decisions by granting or denying access to the user.

Currently, the signature of the authentication response by the private key of the smartcard only provides message integrity and non-repudiation at the application level. Indeed, security will have to be established as well at the transport level in order to guarantee confidentiality when sending authentication request or response. As a result, HTTP messages will need to be sent over Secure Socket Layers (SSL) in order to secure the communications path between the client (i.e. the web browser) and the Service Provider.

DISCUSSION

The research proposes to use a generic smartcard to authenticate the user on his web services utilising part of an existing AAI. The proposed system has a number of advantages over existing solutions and these are presented below:

Service Provider
If a service provider wants to offer a strong authentication solution to his customers, he will not have to face the cost of deployment of a smartcard solution. Rather through simply establishing a BA with an Identity Provider, the Service Provider is able to benefit from that solution. Furthermore, in order to be compatible with the AAI, Service Providers will have to comply with SAML, which is an Internet open standard facilitating the interoperability between them and the Identity Provider. Development, implementation and management of this should therefore be minimised.

End-User
The direct advantage for the end-user is that they benefit from a strong authentication solution to verify identity to their various Service Providers. They will not have to remember a different set of logins and passwords, as the smart card will contain user's web identities, thereby minimising user inconvenience and providing a seamless authentication mechanism. Furthermore, the smartcard brings advanced security features by confirming web identities with digital signatures.

Identity Provider
The research favours the deployment of the smartcard component using an Identity Provider. This can be seen as an introduction of a new type of Internet service which proposes strong authentication solution to Internet users. Of course, this type of service has a cost, but end-users could potentially accept this cost to benefit from a strong authentication solution. Moreover, by moving away from the Identity Provider having to authenticate each and every request, smaller infrastructure demands are made upon the Identity Provider. In addition, if the existing technology, such as the SIM card in a mobile phone, could be harnessed the cost of deployment could be reduced significantly.

Technical Requirements
The web browser of the users' device will typically need an extension or plug-in to interact with the smartcard. Interacting with this is half the problem; as the web browser will have to communicate with the Identity Provider to get the SAML assertions and to communicate with Service Provider for authentication. The research does not indicate how to provide the web identity of the user remotely to the smart card. In addition, during the implementation of the solution, the plug-in will have to recognise incoming authentication requests from the Service Provider. As a result, the plug-in will have to support the POAS binding defined by the SAML open standard .

CONCLUSION
The research has proposed a concept where a smartcard could be used as a strong authentication technique to authenticate the user on his web services. The solution is based upon existing AAI models and identity federation where an Identity Provider is present to provide user's web identities to Service Providers. In the novel concept, these web identities are provided remotely into the smartcard by the Identity Provider. These web identities are constructed with an existing open standard called SAML in order to guarantee interoperability between different stakeholders. Furthermore, in such an architecture, the Identity Provider takes the lead in the deployment of this solution; as a result, Service Providers do not have to manage the cost and deployment of the smartcard which is certainly the criterion which impedes the development of smart card solutions currently.

REFERENCES
DeLooze, L., 2007, "Providing Web Service Security in a Federated Environment", Security & Privacy Magazine, IEEE, Volume 5, Issue 1, Jan.-Feb. 2007 Page(s):73 – 75 [Accessed 24 July 2007]

GSM Association, 2009, "Market Data Summary", GSM Association. Available at http://www.gsmworld.com/newsroom/market-data/market_data_summary.htm [Accessed 12 August 2009]

Liberty Alliance Project website, 2007, "The Liberty Alliance project", [Online] Available from :http://www.projectliberty.org/ [Accessed 12 August 2009]

Liberty Alliance, 2004, "Liberty ID-FF Architecture overview" Thomas, W., eds., [Online] Available from http://www.projectliberty.org/liberty/content/download/318/2366/file/draft-liberty-idff-arch-overview-1.2-errata-v1.0.pdf [Accessed 20 June 2007]

Maler. E., 2006, "SAML, the Liberty Alliance and federation" [Online] available at : http://www.xmlgrrl.com/publications/SAML-Liberty-IIWb-Dec2006.pdf [Accessed 25 July 2007]

OASIS, 2004a, "Trust model guidelines" Linn eds. [Online]. Available at http://www.oasis-open.org/committees/download.php/6158/sstc-saml-trustmodels-2.0-draft-01.pdf [Accessed 30 July 2007]

OASIS, 2004b, "Assertions and protocols for the OASIS Security Assertions Markup Language (SAML) V2.0" Cantor, Kemp, Philpott, Maler eds. [Online]. Available at http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf [Accessed 25 August 2007]

OASIS, 2005a, "Bindings for the OASIS Security Assertion Markup Language (SAML)" Canotir, Hirch, Kemp, Philpott, Maler eds. [Online]. Available at http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf [Accessed 26 August 2007]

OASIS, 2005b, "Security and privacy considerations for the OASIS Security Assertion Markup Language (SAML) V2.0" Hirsch, Philpott, Maler eds. [Online]. Available at http://docs.oasis-open.org/security/saml/v2.0/saml-sec-consider-2.0-os.pdf [Accessed 27 August 2007]

RSA, 1993; "PKCS #1: RSA Encryption Standard" RSA laboratories eds. [Online]. Available at ftp://ftp.rsasecurity.com/pub/pkcs/doc/pkcs-1.doc [Accessed 25 July 2007]

Scheuermann, D.;2002,"The smartcard as a mobile security device", Electronics & Communication Engineering Journal, Volume 14, Issue 5, Oct. 2002 Page(s):205 – 210 [Accessed 6 July 2007]

Schneier, B., 2004, "Customers, passwords, and Web sites"**;** Security & Privacy Magazine, IEEE Volume 2, Issue 4, Jul-Aug 2004 Page(s):88 [Accessed 14 September 2007]

Shibboleth website, 2007, "Shibboleth project documentation", [Online]. Available from : http://shibboleth.internet2.edu/ [Accessed 12 August 2009]

Warren, H., 2006; "Passwords and Passion", Software, IEEE Volume 23, Issue 4, July-Aug. 2006 Page(s):5 – 7 [Accessed 1 September 2007]

COPYRIGHT

Stienne, Clarke and Reynolds ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors