Propuesta de arquitectura de uSSO en eduroam empleando tecnología de Infocard

Proposal for uSSo architecture in eduroam using InfoCard technology

Enrique de la Hoz, Antonio García, Iván Marsá-Maestre, Miguel Ángel López-Carmona

Resumen

En este trabajo planteamos la integración de la tecnología de InfoCard en eduroam para proporcionar un servicio de inicio de sesión único unificado (uSSO). Durante los últimos años, la federación de servicios ha estado entre los temas más candentes para los investigadores de todo el mundo. Entre las iniciativas más interesantes se encuentran aquellas que tratan de llevar dicho servicio de inicio de sesión único más allá de la web. Por ejemplo, en el ámbito europeo se han formulado algunas propuestas muy interesantes para integrar las federaciones integradas en eduGAIN con el otro gran esfuerzo paneuropeo de federación, eduroam. Nuestro objetivo es llegar a proporcionar ese mismo servicio pero con dos premisas fundamentales: que la propuesta sea lo más sencilla posible y que las modificaciones a incorporar en el equipamiento ya existente sean mínimas tanto en clientes como en servidores.

Palabras clave: arquitectura de uSSO, InfoCard, eduroam, eduGAIN, autenticación, identidad digital.

Summary

In this paper we consider the integration of InfoCard technology and eduroam as a means of providing a unique unified Single Sign-on (uSSo). In recent years, the service federation has been one of the hottest topics for researchers all over the world. Some of the most interesting initiatives are those that try to take this unified single sign-on service beyond the web. For example, a number of very interesting proposals have been put forward in Europe for integrating the integrated federations in eduGAIN with the other great pan-European federation force, eduroam. Our aim is to provide that same service but with two basic premises: the proposal should be as simple as possible and the modifications to be incorporated into the already existing equipment should be minimal, both in clients and servers.

Keywords: uSSo architecture, InfoCard technology, eduroam, eduGAIN, authentication, digital identity.

El uSSO es el servicio de inicio de sesión único unificado

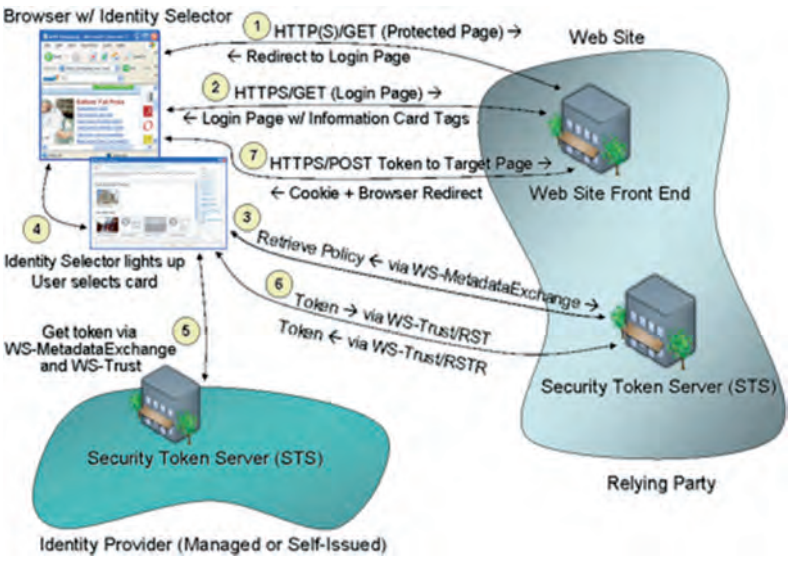
1. Introducción

InfoCard es un tecnología basada en estándares web bien conocidos[1, 2, 3] que permite a los usuarios gestionar su información personal en la forma de tarjetas de visita digitales expedidas por distintas autoridades y emplearlas en distintos contextos donde sean aceptadas con el objeto de acceder a servicios en línea.

InfoCard permite a los usuarios gestionar su información personal

Podemos entender InfoCard como una metáfora que permite abstraer a los usuarios de la complejidad subyacente de los protocolos (SAML, OpenID) que habitualmente se emplean para el manejo de la identidad digital. En la siguiente figura se muestra el diagrama completo de una interacción InfoCard.

FIGURA 1. AUTENTICACION CON INFOCARD EN UN SITIO WEB



La tecnología InfoCard permite a los usuarios elegir la identidad que deseen emplear en cada contexto

El modelo persigue que la identidad digital pueda integrarse en un marco de emisión y consumo de testigos de autenticación/autorización que los usuarios percibirán como una simple entrega de una tarjeta conteniendo cierta información acerca del mismo a un determinado servicio.

Los principales objetivos de esta tecnología son los siguientes[4]:

1. Posibilitar la utilización de la identidad digital en la forma de testigos de seguridad que transporte atributos que puedan usarse como información de autenticación y/o autorización empleando mecanismos basados en servicios web.

Esta tecnología permite salvaguardar la privacidad del usuario proporcionando un entorno amigable

2. Proporcionar a los usuarios con una flexibilidad suficiente la elección de la identidad que deseen emplear en cada contexto permitiendo que controlen el uso de su identidad en distintos contextos.

3. Facilitar la interoperabilidad con proveedores de identidad (Identity Providers, IdP de ahora en adelante) y partes confiantes (relying parties, RP de ahora en adelante) mediante el uso de protocolos abiertos.

4. Ser independiente de los tipos específicos de testigos de seguridad y los atributos que se empleen para de esta manera funcionar como un canal para el flujo de la información de identidad entre IdPs y RPs bajo el control del usuario.

5. Salvaguardar la privacidad del usuario proporcionando un entorno amigable que permita al usuario identificar de forma fácil intentos de comprometer su información personal.

6. Proporcionar un proveedor de identidad sencillo que permita a los usuarios construir y emplear identidades auto-emitidas en interacciones web siempre que esto sea aceptable (el emplear identidades auto-emitidas, se entiende).

Este trabajo propone el uso de InfoCard como tecnología clave para proporcionar uSSO en un entorno donde hay desplegada una arquitectura basada en eduroam con cambios mínimos sobre dicha infraestructura.

El resto del trabajo se estructura del siguiente modo: en primer lugar, se presentarán algunas propuestas para arquitecturas de inicio de sesión único unificado (uSSO). A continuación, se presentará nuestra propuesta para una arquitectura de uSSO en eduroam basada en InfoCard. Para finalizar, se mostrará un prototipo de la arquitectura, los resultados preliminares y las conclusiones.

2. Arquitecturas de uSSO en eduroam

Eduroam (Education Roaming)[5] es un servicio de itinerancia inter-institucional basada en la arquitectura 802.1x[6] y en una infraestructura jerárquica basada en RADIUS[7]. Esta iniciativa permite que los usuarios de las instituciones participantes accedan a Internet desde otras instituciones distintas a la propia usando las credenciales de su institución origen, todo esto con una mínima sobrecarga administrativa. Además, y dependiendo de las políticas locales de las instituciones visitadas, los participantes podrían acceder a recursos adicionales a su voluntad.

Sin embargo, la infraestructura eduroam desplegada es únicamente útil para la autenticación de usuarios. No hay una diferenciación de servicio en función del usuario que solicite dicho servicio. Si tenemos en cuenta que no se dispone de información adicional sobre el usuario (como por ejemplo atributos sobre el mismo), no existe información que podamos emplear para dicho fin. Cuanto más detallada sea la información de la que se dispone, mejor y más detallada será la diferenciación que se podrá proporcionar a la hora de prestar el servicio. Sería, por tanto, deseable que las instituciones participantes pudieran intercambiar información sobre los usuarios de cara a proporcionar el mejor servicio posible.

Sería deseable que las instituciones participantes en eduroam pudieran intercambiar información sobre los usuarios

EduGAIN[8] trata de cumplir con los requisitos descritos en el párrafo anterior. El proyecto DAMe (Deploying Authorisation Mechanisms for Federated Services in the eduroam Architecture)[9] dentro de EduGAIN perseguía dos objetivos fundamentales:

1. Un primer objetivo consistía en tratar de cubrir la necesidad de las instituciones participantes en eduroam de configurar políticas de acceso a la red detalladas y basadas en roles acordes a las necesidades de sus usuarios y las normativas nacionales en cada caso.

2. Un segundo objetivo trataba de proporcionar SSO en entornos heterogéneos como los desplegados en las instituciones europeas participantes en eduroam con una aproximación transversal, relacionando la autentición en eduroam con una autenticación de tipo AAI basada en web.

Sería deseable que las modificaciones que hubiera que acometer en los sistemas de los usuarios finales, fueran mínimas

En un futuro próximo, se espera que DAMe se despliegue en Europa[10]. Uno de los principales inconvenientes de esta propuesta es que requiere una serie de modificaciones no sólo en los componentes de la arquitectura de eduroam sino también en los equipos de los usuarios finales. Llevar a cabo estas modificaciones en los sistemas de los usuarios finales es habitualmente más complejo si cabe que acometer modificaciones en la propia arquitectura de eduroam, como se ha mostrado en el propio despliegue de la misma. Por tanto, sería deseable que las modificaciones que hubiera que acometer en dichos sistemas fueran lo mínimas posibles para posibilitar un despliegue rápido y eficiente de una arquitectura de uSSO.

Es este hecho el que nos lleva a proponer la utilización de soluciones y tecnologías estándar que ya estén

desplegadas en la mayor parte de los sistemas clientes. InfoCard es una de ellas. InfoCard permite la autenticación y autorización de usuarios en entornos de SSO de una forma sencilla y, lo que es más importante, comprensible para el usuario final.

Nuestra propuesta trata de establecer un puente entre eduroam y la tecnología de InfoCard de manera que la mera autenticación eduroam pudiera servir de arranque de una sistema de SSO basado en InfoCard minimizando la intervención requerida por parte del usuario.

3. Propuesta de arquitectura de uSSO para eduroam basada en InfoCard

Tal y como hemos mencionado anteriormente, nuestra propuesta de arquitectura de uSSO para eduroam, trata de unir dos federaciones: eduroam y eduGAIN. Ambas son diferentes con respecto a las tecnologías empleadas y en cuanto a los servicios que ofrecen: acceso a la red en el caso de eduroam y acceso a recursos web proporcionados por algún proveedor de servicio (service provider, SP de ahora en adelante).

La propuesta de arquitectura uSSO trata de unir eduroam y eduGAIN

Podríamos modelar los servicios que eduGAIN proporciona como un conjunto de SP que requieren ciertos atributos (o claims) para autorizar el acceso a los usuarios. Estos atributos provendrían de la institución origen de cada usuario. Típicamente, cuando un usuario trata de conectarse a un SP en un dominio distinto al suyo propio, será redirigido al IdP de su institución. Habitualmente, este proceso se lleva a cabo mediante un mecanismo de tipo WAYF (where-are-you-from) mediante el cual el usuario indica de donde proviene. El usuario es autenticado por su propio IdP, y los atributos son enviados al SP que los había solicitado en primera instancia.

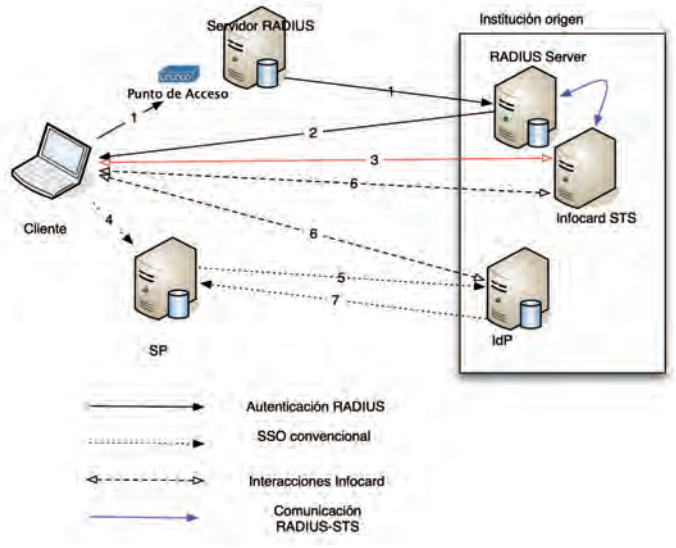
Consideramos que este procedimiento podría simplificarse considerablemente gracias al empleo de tecnologías de InfoCard. Bajo este supuesto, cada institución mantendría un IdP con un servicio de emisión de testigos de seguridad (Security Token Service, STS de ahora en adelante). De esta manera, cuando fuéramos a acceder a un SP, éste expresaría sus requerimientos en la forma de un conjunto de atributos que se podrían obtener empleando una tarjeta InfoCard. Esta tarjeta tendría que haber sido expedida por alguna de las instituciones adheridas a la federación. Si cada usuario dispusiera de una tarjeta expedida por su institución origen, podría emplearla para obtener estos atributos y enviarlos al SP que los requiriera sin tener que pasar por un servicio WAYF. Además, el usuario controlaría en todo momento qué valores son efectivamente enviados de una forma visual e intuitiva.

Cuando un usuario se conecta a un SP en un dominio distinto al suyo, será redirigido al IdP de su institución mediante el mecanismo WAYF

Nuestra propuesta trata de hacer que el empleo de esta tecnología pueda extenderse a eduroam de modo que los usuarios puedan obtener estas tarjetas de modo automático una vez que acceden a eduroam ligando la validez de estas tarjetas a su sesión en eduroam.

Una vez que el usuario accede a eduroam, recibiría una tarjeta (que llamaremos tarjeta de información eduroam o eduroam InfoCard) que podría emplear para autenticarse en cualquiera de los servicios de la red. Con una única exposición de las credenciales del usuario (en la autenticación de eduroam), sería posible un acceso a todos los recursos que se integrarán en la confederación. En la siguiente figura se muestra un ejemplo de un caso de uso típico:

FIGURA 2: uSSO EN EDUROAM EMPLEANDO INFOCARD



Las tarjetas de información deben usarse para obtener testigos de autenticación ante el STS correspondiente

En primer lugar, el usuario trata de acceder a la red empleando eduroam[1]. En nuestra propuesta, tras ser autenticado correctamente, el usuario obtendría también una tarjeta de información que hemos denominado eduroam InfoCard. Cada uno de los dominios de eduroam tendría que añadir un servidor capaz de emitir tarjetas de identidad y testigos de autenticación a partir de las mismas (el componente STS al que hemos hecho referencia anteriormente).

En la aproximación convencional, cuando el usuario, una vez en eduroam, trata de acceder a un proveedor de servicio es redirigido a un proveedor de identidad donde deberá autenticarse, previo posible paso por un servicio WAYF (Where-Are-You-From). Si bien es posible seguir manteniendo esta forma de proceder, resulta más natural si empleamos este esquema el entregar directamente al SP los atributos que necesite para proporcionar el servicio al usuario[4]. Para ello se empleará la tarjeta de información eduroam[5]. Una peculiaridad de este tipo de tarjetas frente a las tarjetas de información convencionales consiste en que las tarjetas permitirán obtener la información solicitada no sólo si el usuario se autentica correctamente frente al STS, sino que también deberá estar conectado en ese momento a eduroam. Esta modificación se introduce para conseguir un cierre de sesión coherente: si el usuario abandona la red eduroam, la tarjeta que se ha creado para el uso dentro de esa misma red debería, por tanto, dejar de ser válida[6]. Si todas estas comprobaciones son exitosas, se expedirá el testigo conteniendo los atributos requeridos[7].

Las únicas alternativas realistas serían el uso de autenticación por usuario y contraseña o mediante una tarjeta autoemitida

Dependiendo de cómo se emplee la tecnología de InfoCard, se obtendrá una experiencia más o menos cercana al SSO. Las tarjetas de información no son testigos de información en sí, sino artefactos. No es posible emplearlos como testigos de autenticación sino que deben ser usados para obtener testigos de autenticación ante el STS correspondiente. Para ello, es necesario autenticarse ante dicho componente. En la actualidad hay definidos tres métodos para este fin:

- Usuario-contraseña.
- Kerberos.
- Certificados cliente X.509
- Un tarjeta de información auto-emitida.

En entornos prácticos, las únicas alternativas realistas serían el uso de autenticación por usuario y contraseña o mediante una tarjeta autoemitida. Aunque en las primeras etapas de nuestro trabajo empleamos autenticación por usuario/contraseña, dado que buscamos una experiencia real de SSO, decidimos pasar a emplear una tarjeta de información autoemitida. Cuando se emplea este mecanismo, el STS/IdP, a la hora de autenticar una tarjeta de información, actuará como una RP que espera consumir un atributo llamado PPID que puede ser producido por una tarjeta auto-emitida.

Cada tarjeta auto-emitida tiene un identificador que combinado con la identidad de un RP (que se obtendría del certificado del mismo) puede producir el valor que hemos denominado PPID (Private Personal Identifier). Esto significa que ante distintos RP se generarían diferentes valores de dicho atributo. Para que un STS emplee este método de validación de una tarjeta de información, debe conocer el identificador de la tarjeta y el selector de identidad del cliente debe conocer de forma segura la identidad del STS. Aunque esto último es fácil de conseguir, no es tan sencillo comunicar al STS el identificador de la tarjeta porque sería necesario disponer de un canal seguro entre el cliente y el STS.

Proponemos el uso de un método EAP tunelizado como PEAP

La emisión automática de tarjetas de información que se autentiquen empleando tarjetas de información auto-emitidas evitando, por lo tanto, la necesidad de que el usuario introduzca ningún par usuario-contraseña, será el método seleccionado porque se ajusta perfectamente al modelo descrito anteriormente.

Para poder conseguir esto, el STS y el cliente deberán haber compartido de forma segura el identificador de la tarjeta auto-emitida (que habrá sido generada por el propio cliente) que se quiere emplear para autenticar la eduroam InfoCard. Para automatizar este proceso, proponemos que el identificador de la tarjeta se transporte como un atributo en el mensaje EAP en el paso 1 de la autenticación descrita arriba. Para evitar que este valor pueda ser capturado, proponemos el uso de un método EAP tunelizado como PEAP cuya extensibilidad utilizaremos también para añadir información adicional al diálogo RADIUS. El servidor RADIUS recibirá esta petición, autenticará al usuario y se comunicará con el IdP-STS de la institución origen del usuario para pedirle una tarjeta de información eduroam para ese usuario. Esta petición contendrá el identificador de la tarjeta auto-emitida que desea utilizarse para resguardar la eduroam InfoCard e información de la sesión, de modo que esta información pueda ser tenida en cuenta en el proceso de generación de la tarjeta, que quedará asociada a la sesión eduroam del usuario. Una vez que el servidor RADIUS reciba la tarjeta, enviará al usuario una referencia a la tarjeta en la respuesta EAP. Haciendo uso de esta referencia, el cliente la descargará automáticamente y la importará en el selector de identidad habilitando al usuario para la utilización de este modelo de tarjetas de información sin que tenga que realizar ningún paso extra al de su autenticación en eduroam.

Se ha implementado un módulo para simpleSAMLphp para la creación, gestión y manejo de las tarjetas de información

Siguiendo este modelo, la única modificación necesaria en los sistemas cliente, sería una cierta integración entre el suplicante de red 802.1x y el selector de identidad para permitir que el usuario seleccione una tarjeta de información auto-emitida en el proceso de autenticación eduroam. Más allá de esto, no es necesaria modificación alguna en los clientes.

4. Resultados

Se ha desarrollado una maqueta del sistema propuesto empleando para ello FreeRADIUS como servidor RADIUS y Linux con wpa-supplicant[11] como suplicante y DigitalMe[12] como selector de identidad. Toda la funcionalidad añadida al servidor RADIUS para la interacción con el STS se ha implementado como un módulo perl, con lo que las modificaciones al código del mismo han sido mínimas. Para la creación, gestión y manejo de las tarjetas de información, se ha implementado un módulo para

simpleSAMLphp[13] que se hace cargo de todo el proceso. El desarrollo de este módulo es otra de las contribuciones de este trabajo.

Se puede observar un vídeo con una demostración del funcionamiento del sistema en esta url: *http://it.aut.uah.es/enrique/research/demo.html*

En la actualidad se está trabajando para extender este modelo a clientes no Linux para lo cual se trabaja con el suplicante multiplataforma open1x[14]. También se está trabajando para solucionar el problema de la transferencia de la información de contabilidad de usuarios entre dominios, necesaria para saber cuando un usario termina la sesión en eduroam.

5. Conclusiones

En este trabajo se presenta una arquitectura de uSSO para un entorno eduroam empleando para ello el modelo de InfoCard. Para ello, se trata de automatizar el procedimiento de obtención y validación de las tarjetas de información en el lado del usuario para minimizar la interacción requerida por parte del mismo y facilitar el despliegue de un modelo comprensible y seguro como es InfoCard.

La solución se basa en soluciones estándar y requiere modificaciones mínimas sobre todo en el lado del usuario que se ha revelado como el elemento que es más difícil modificar en un despliegue de este tipo. Por último, se ha desarrollado lo que permite la utilización de InfoCard en el paquete de gestión de identidad simpleSAMLphp y que podría utilizarse en este u otros entornos.

Se ha desarrollado la solución que permite la utilización de InfoCard en el paquete de gestión de identidad simpleSAMLphp

6. Agradecimientos

Este trabajo ha sido financiado parcialmente por RedIRIS y por el proyecto TIN2008-06739-C04-04 del Ministerio de Educación y Ciencia. Los autores desean agradecer a Samuel Muñoz Hidalgo su trabajo en la construcción del prototipo.

Referencias

[1] C. Kaler, A. Nadalin, et al. *Web Services Trust Language (WS-Trust) Version 1.1*, May 2004.

[2] K. Ballinger, B. Bisset, et al. *Web Services Metadata Exchange (WS-MetadataExchange) Version 1.1*, August 2006.

[3] G. Della-Libera, M. Gudgin, et al. *Web Services Security Policy Language Version 1.1*, July 2005.

[4] Arun Nanda. *A Technical Reference for the Information Card Profile V1.5*. August 2008.

[5] L. Florio, K. Wierenga, *Eduroam, providing mobility for roaming users*, EUNIS 2005, June 2005.

[6] IEEE802.1X. IEEE *Standard for Local and metropolitan area networks, Port-Based Network Access Control,* 2004. *http://www.ieee802.org/1/pages/802.1x.html*

[7] C. Rigney, S. Willens, A. Rubens, and W. Simpson. *Remote Authentication Dial In User Service (RADIUS),*
IETF RFC2865, June 2000.

[8] D. Lopez et al.: *GÉANT2 Authorisation and Authentication Infrastructure (AAI) Architecture – second edition, GÉANT2 Deliverable DJ5.2.2,2,* April 2007 Microsoft Corporation, *A Guide to Interoperating with the Information Card Profile V1.5*, August 2008.

[9] DAMe Project: *http://dame.inf.um.es/*

[10] López, G., Cánovas, í., Gómez-Skarmeta, A. F., and Sánchez, M. 2008. *A proposal for extending the eduroam infrastructure with authorization mechanisms.* Comput. Stand. Interfaces 30, 6 (Aug. 2008), 418-423.

[11] Linux WPA Supplicant. *http://hostap.epitest.fi/wpa_supplicant/*

[12] DigitalMe Identity Selector. The Bandit Project. *http://www.bandit-project.org*

[13] SimpleSAMLphp Project. *http://rnd.feide.no/simplesamlphp*

[14] Open1x.org. *http://open1x.sourceforge.net/*

Enrique de la Hoz
(enrique@aut.uah.es)

Antonio García

(antonio@aut.uah.es)

Iván Marsá

(ivmarsa@aut.uah.es)

Miguel Ángel López-Carmona

(miguellop@aut.uah.es)

Área de Ingeniería Telemático, Departamento de Automática
Universidad de Alcalá