DESCRIPCIÓN DE LOS COMPONENTES DE UN SISTEMA FEDERATIVO TIPO EDUROAM

Gustavo Vélez
Freelance
gustavovelez@hotmail.com

(Tipo de Artículo: **Reflexión**. Recibido el 21/05/2012. Aprobado el 26/05/2012)

RESUMEN
Las federaciones de identidad están surgiendo en los últimos años con el fin de facilitar el despliegue de entornos de uso compartido de recursos entre las organizaciones. Como una característica común de estos entornos es el uso de mecanismos de control de acceso basado en la identidad del usuario, desafortunadamente, la mayoría de las federaciones se han dado cuenta que la identidad del usuario no es suficiente para ofrecer un control de acceso más grano y el valor agregado. Por lo tanto, la información adicional, como los atributos de usuario, deben ser tenidos en cuenta. En este artículo se hace la descripción de los componentes de un sistema federativo tipo Eduroam, teniendo en cuenta el uso de atributos de usuarios adoptando las decisiones de autorización durante el control del proceso de acceso.

Palabras Clave
Eduroam, sistema federativo, identidad del usuario, control de acceso, federaciones, recursos compartidos.

DESCRIPTION OF THE COMPONENTS OF A FEDERATED SYSTEM OF TYPE EDUROAM

ABSTRACT
Identity federations are emerging in recent years to make easier the deployment of environments of shared-use resources between companies. A common feature of these environments is the use of mechanisms for access control based on the identity of the user; unfortunately, most of federations have found that the identity of the user is not enough neither to provide a more grained access control nor the added value. Therefore, additional information, such as user attributes, must be taken into account. This article describes the components of a federated system of type Eduroam, considering the use of user attributes adopting authorization decisions during the control of access process.

Keywords
Eduroam, federated system, user's identity, access control, federations, shared resources.

DESCRIPTION DES COMPOSANTS D'UN SYSTEME FEDERE DU TYPE EDUROAM

RÉSUMÉ
Les fédérations d'identité sont apparues ces dernières années pour faciliter le déploiement d'environnements d'usage partagé de ressources entre les entreprises. Une caractéristique commune de ces environnements est l'usage de mécanismes de contrôle d'accès en se basant sur l'identité des utilisateurs, mais la plupart des fédérations ont compris que l'identité des utilisateurs n'est pas suffisante pour offrir un contrôle d'accès plus grain et la valeur ajoutée. Par conséquent, toute l'information additionnelle, comme les attributs des utilisateurs, doit être considéré. Dans cet article on fait la description des composants d'un système fédéré du type Eduroam en considérant les attributs des utilisateurs en adoptant les décisions d'autorisation pendant le contrôle du processus accès.

Mots-clés
Eduroam, système fédéré, identité d'utilisateur, contrôle d'accès, fédérations, ressources partagés.

1. INTRODUCCION

En los últimos años se ha experimentado el surgimiento de enfoques federados en los recursos compartidos. Las federaciones, entendidas como vínculos de confianza, se establecen entre las diferentes organizaciones autónomas con el fin de otorgarles a los usuarios el acceso a los recursos compartidos con una sola identidad. Ejemplos importantes de estos enfoques son la creación de federaciones del mundo académico y los conceptos alrededor del Grid Computing.

De hecho, muchos aspectos de este enfoque federado han sido planteados por varios proyectos, como por ejemplo, Santo y Seña [1] y Liberty Alliance [2]. Sin embargo, otros aspectos generalmente relacionados con la gestión de identidad integral aún están abiertos, especialmente frente a las propuestas. En cuanto a la movilidad del usuario y la movilidad de la Fuerza de Tarea TERENA [3] se establece como un foro para el intercambio de experiencias y conocimientos sobre las tarifas de itinerancia de las diferentes actividades de desarrollo en la Unión Europea. Como resultado de este esfuerzo, este grupo de trabajo ha definido y probado una arquitectura entre los Sistemas Nacionales de Investigación y Redes de la Educación NREN de *roaming*, llamada Eduroam [4], sobre la base de AA de servidores RADIUS [5] y el estándar 802.1X [6]. El Eduroam les permite a los usuarios y a las instituciones participantes acceder a Internet utilizando su casa como credencial de la institución, todo esto con una carga administrativa mínima.

Dependiendo de las políticas locales, en las instituciones que utilizan este servicio los participantes de Eduroam cuentan también con recursos adicionales a su disposición, llegando al punto de utilizar el sistema como mecanismo de autenticación y autorización a fin de intercambiar información —credenciales— acerca de los usuarios. El objetivo principal del proyecto DAME [7] es definir esta autenticación unificada a través de un sistema de autorización para servicios federados alojado en la red Eduroam, con el fin de permitir el uso de las credenciales del usuario cómo medio autorizador.

Estos servicios federados pueden ir desde el control de acceso a la red de servicios distribuidos, como Grid Computing. Eduroam define la federación cómo el proceso de autenticación de gestión. Con el fin de lograr esto, DAME hace uso de la infraestructura NAS-SAML [8], un sistema de control de acceso a la red basado en la arquitectura AA a partir de atributos de autorización. La propuesta se basa en lenguaje de marcado de aserción de seguridad SAML [9] y el extensible Control de acceso Markup Language XACML [10], normas que se utilizan para expresar y acceder a las políticas de control basadas en los atributos, las declaraciones de autorización y los protocolos de autorización.

De acuerdo con esto en este artículo se establece información que proporciona una visión general del servicio Eduroam, definiendo la infraestructura subyacente de *roaming* y describiendo el NAS-SAML y el acceso a la red de servicios de control que proporciona la red Eduroam.

2. EDUROAM (Education Roaming)

Es un servicio de *roaming* interinstitucional basado en la red 802.1X y una arquitectura de infraestructura jerárquica basada en RADIUS. Esta iniciativa les permite a los usuarios móviles de las instituciones participantes acceder a Internet en diferentes lugares, utilizando las credenciales de su institución de origen y con un costo administrativo mínimo de sobrecarga.

El servidor de nivel superior de la jerarquía RADIUS lo proporcionan TERENA y los NREN pertenecientes a Eduroam desde los cuales esas infraestructuras se encuentran conectadas. Por último, cada institución que esté dispuesta a unirse tendrá la facilidad de conectarse al servidor a través de los NREN [11].

Un ejemplo de este proceso es cuando el usuario de una institución A busca tener acceso a la red inalámbrica en la Institución B y ambos pertenecen a la federación, en esta situación el control de acceso se lleva a cabo siguiendo el estándar 802.1X, es decir, al usuario conectado al punto de acceso inalámbrico AP en su servidor local, RADIUS le facilita que se lleve a cabo su identificación. Una vez que el servidor identifica que el usuario pertenece a un dominio diferente y con base en el identificador de usuario, la solicitud de autenticación se envía a través de la jerarquía de RADIUS para el servidor en el centro de origen del usuario [12]. A continuación, el usuario se autentica y la respuesta se envía de vuelta a la Institución B, donde el AP permite la conexión solicitada, como se puede observar en la Figura 1.

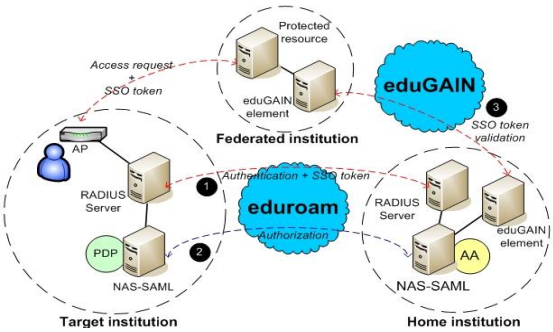

Fig. 1: Infraestructura Eduroam con los mecanismos de autorización [4]

3. ANÁLISIS DE LAS ESTRUCTURAS DERIVADAS DE LA INTEGRACIÓN EDUROAM - NAS-SAML

La integración de NAS-SAML en Eduroam como servicio de autorización puede llevarse a cabo de varias maneras, dependiendo de los requisitos impuestos por las instituciones participante o la aplicación de AA. Por un lado, la entidad objetivo debe recibir la información adicional que describe el usuario de la institución origen; por otro lado, la información obtenida se debe utilizar en la institución de destino para determinar si el usuario puede acceder al servicio que solicita.

Una primera aproximación a dicho proceso, que se puede denominar autorización de fusión, le permite a la institución de origen tener una estrategia para devolver la información sobre el usuario en el mismo canal establecido de autenticación. Es decir, cuando RADIUS recibe la solicitud de autenticación de la institución origen la remite a la infraestructura NAS-SAML, donde se autentica y recuperan algunos atributos adicionales. Esa información puede ser codificada en la respuesta como atributos de RADIUS.

Desde el sistema NAS-SAML se trabaja con el traductor Radius Diámetro [13], el cual se debe utilizar como una puerta de entrada para acceder a la arquitectura NAS-SAML. Una vez el servidor RADIUS destino obtiene dicha información, se lleva a cabo una consulta a un elemento local de la infraestructura NAS-SAML, el PDP, con el objetivo de obtener la decisión de autorización.

Por último, una vez obtenida autorización de entrada, los RADIUS apropiados se devuelven a la AP, de tal forma que este enfoque se puede considerar de óptima relación de dominio entre las comunicaciones. El principal inconveniente de esta alternativa es la extensión y, por tanto, el uso de RADIUS estándar no denominados como atributos para el transporte de la información acerca de los usuarios entre las diferentes instituciones, se debe pasar por alto en cualquier servidor RADIUS intermediario [14].

Con el fin de evitar la modificación del proceso de autenticación se define el Eduroam mediante la introducción de los atributos no estándar; una segunda alternativa se puede definir a través de las llamadas autorizaciones independientes. El proceso de autorización debe comenzar una vez que la autenticación de se ha creado a raíz de los perfiles actuales de Eduroam.

Una vez que el servidor RADIUS objetivo recibe la respuesta de autenticación, la fase de autorización se inicia para determinar el tipo de servicio que se suministrará. Esta etapa también se realiza través de NAS-SAML, en primer lugar, para recuperar la información sobre el usuario de la institución base y, a continuación, para obtener la decisión de autorización en la institución destino. Considerando que este enfoque no modifica el proceso de autenticación, se introduce la necesidad de la definición de una interfaz entre el servidor RADIUS y la arquitectura NAS-SAML —diámetro base— para solicitar decisiones de autorización y las obligaciones derivadas de esa decisión. Además, este enfoque tiene dos inter-dominios comunicacionales que son, en primera instancia, la autenticación y la autorización; por lo tanto, a partir de estos dos puntos se soporta la introducción de una sobrecarga adicional para la autenticación y la autorización y la introducción de una sobrecarga adicional.

Una tercera alternativa, siguiendo el mismo método de autenticación diferenciada y los diferentes pasos de autorización, se podría lograr mediante la ampliación del protocolo RADIUS con un nuevo perfil de la definición de nuevos atributos y mensajes. De esta manera la fase de autorización facilitaría el uso del protocolo RADIUS como un mecanismo de transporte para obtener la información necesaria para el proceso de autorización, en la actualidad esta propuesta está siendo desarrollada por Internet 2 [15].

4. ESTABLECIENDO UNA ACCION GENERADORA DE EDUROAM

Es necesario tener en cuenta que el sistema Eduroam ya ha sido desplegado, en otras palabras, cientos de instituciones lo están utilizando; por lo tanto es necesario introducir cambios gradualmente y manteniendo hacia atrás la compatibilidad. De este modo se han diseñado ambas alternativas, pero sólo se mantienen independientes por el tipo de autorización que se ha aplicado hasta el momento y porque es el más adecuado para las pruebas iniciales en los sistemas comunicacionales.

Frente a la búsqueda de una ampliación de la infraestructura Eduroam, con el fin de ofrecer mecanismos de autorización con el mínimo impacto en las instituciones dispuestas a seguir utilizando el proceso estándar, se ha decidido preservar el mecanismo de autenticación actual en el enfoque aplicado —autorización independiente— para desplegar una nueva autorización desde la infraestructura.

De este modo, empleando estos mecanismos, las instituciones pueden decidir alternativamente sí desean utilizar un servidor RADIUS extendido conectado a la arquitectura NAS-SAML de la autenticación y autorización o un archivo estándar, es decir, sólo la autenticación. En la Figura 2 se muestra este enfoque.

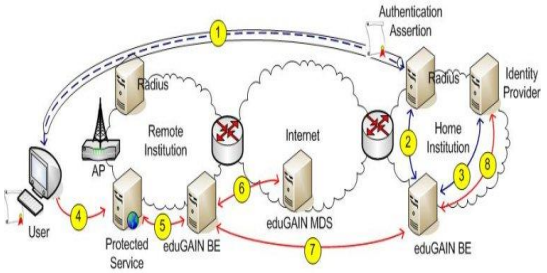

Fig. 2: Implementación de la arquitectura Eduroam [1]

Por otra parte, de acuerdo con el enfoque que se observa en la Figura 3, una vez que el usuario móvil se registra siguiendo el mecanismo de Eduroam estándar, el servidor RADIUS destino utiliza la infraestructura NAS-SAML para conducir el proceso de autorización. Por lo tanto, el servidor principal Diámetro se consulta acerca de los atributos del usuario y, una vez que esta información se recupera, se obtendrá una decisión autorizadora mediante el PDP [16].

Además, un conjunto de obligaciones puede ser devuelto junto con la decisión de autorización que contiene algunas de las propiedades específicas de la red que puedan ser aplicadas por el punto de acceso.

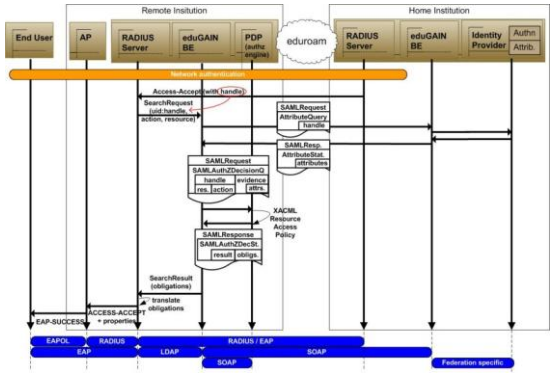

Fig. 3: Propuesta para la ampliación de la infraestructura Eduroam con los mecanismos de autorización [4]

El servidor Diámetro objetivo envía un mensaje en el servidor de casa, incluyendo una sentencia SAMLA ttributeQuery, que contiene la identidad del usuario, es en este momento donde se establecen los atributos establece atributos (AA), desde una política de lanzamiento de atributos. Esta política, basada en XACML, especifica el usuario atributos que se pueden liberar de esa institución de destino.

Una vez establecido lo anterior, los atributos permitidos, y sus valores correspondientes, se envían de vuelta por medio de una sentencia SAML Attribute Statement. Una vez que los atributos son recuperados en la institución destino, se envía una solicitud SAML Authorization Decision Query al Punto de Decisión de Políticas PDP. Esta consulta contiene la identidad del usuario, el identificador de recursos, la acción solicitada y los atributos del usuario. Con esta información el PDP es capaz de obtener la decisión de autorización y de acuerdo con la política de acceso a los recursos que también se basa en la tecnología de XACML.

Por último, el PDP devuelve una respuesta SAML Authorization Decision Statement, que puede contener obligaciones específicas. El mecanismo utilizado por el servidor de diámetro establece el objetivo de encontrar el servidor principal que pueda estar basado en el identificador de usuario, tal como lo define [17].

5. EXPERIENCIA DE EDUROAM EN USA

Como uno de los exponentes más importantes que ha debatido la experiencia del Sistema Eduoram en Estados Unidos se encuentra Ken Klingenstein, quien ha sido muy activo en lo que respecta al actual esfuerzo de la implantación de Eduroam e Internet en el país, a partir de la experiencia InCommon y el Grupo de soluciones comunes [18].

De estas discusiones se obtuvo un compendio de ideas y de intereses y apoyo acerca del tema en general, vislumbrando el esfuerzo de mover Eduroam Estados Unidos hacia delante. Por otra parte, Philippe Hanset aplicó una sesión de presentación y otra BOF para discutir esta temática.

Actualmente, Philippe Hanset se encuentra en las últimas etapas de la aplicación para una beca de la Fundación Nacional de Ciencias en relación con software para Eduroam. Dentro de las ideas principales se tienen: (1) Una colección de herramientas de software, que actualmente no existe, para apoyar el servicio en las áreas de automatización, (2) el monitoreo RADIUS para análisis de registros de seguridad y apoyo, (3) la depuración en una infraestructura que abarque todas las zonas horarias, (4) explorar una integración con perfSONAR, un proyecto Internet, (5) una interfaz entre el InCommon existente y las federaciones Eduroam utilizando el estándar SAML para mejorar el aspecto de cortesía de los dos servicios, que se llevaría a cabo en colaboración con la Federación InCommon y (6) la participación activa en el desarrollo de la generación de Eduroam que se realiza en colaboración con los proyectos GN2 y GN3, financiados por la Unión Europea [19].

Además del desarrollo del software, ce centrará mucho esfuerzo en documentar el servicio y sus herramientas, así como en escribir un Acuerdo de Nivel de Servicio y las políticas asociadas. La infraestructura actual, ya instalado en UTK, se convertirá en un sistema de alta disponibilidad. Hanset ha llevado y sigue llevando la mayor parte de la carga por el esfuerzo Eduroam-Estados Unidos.

6. RECOMENDACION PARA ESTABLECER PROPUESTAS EN COLOMBIA

A través de la experiencia académica de los sistemas de información de las universidades colombianas, surge la propuesta de intervención de un sistema que permita el manejo adecuado de los mecanismos de autenticación y autorización que es el cuello de botella de muchas de esas instituciones.

Este hecho problema se presenta cuando se tiene en cuenta el constante cambio de los usuarios, inducida por su naturaleza abierta y por el establecimiento adecuado de un programa de autenticación y autorización de infraestructuras y, sobre todo, de los esquemas que permitan su integración a través de los mecanismos de las TIC, tanto académicos como administrativos.

Dentro de los objetivos que se establecen para poner en marcha el programa de autenticación y autorización de usuarios académicos se encuentra:

- Establecer un sistema que sirva a las necesidades de cualquier usuario en las instituciones participantes: personal administrativo, estudiantes, investigadores, profesores…,
- Buscar un sistema que les permita a las instituciones seleccionar la tecnología que prefieran para la conexión, con base en un estado de gestión de identidades.
- Establecer esquemas estándar para el intercambio de datos de personal con gran respeto por la privacidad del usuario y su consentimiento.

- Implementar acciones de referencia para la validación y los propósitos de prueba.

- Crear una serie de casos de uso comunes que podrían ser utilizados para el despliegue de los servicios, con un enfoque especial de servidor interactivo.

- Utilizar tanto software de código abierto como sea posible.

Como metodología de intervención el proyecto establece la utilización de tecnologías basadas en la utilización de infraestructuras Eduroam con mecanismos de autorización. Cada institución participante instalará al menos un proveedor de identidad conectado a su gestor de infraestructura y su sistema de datos relacional, de tal manera que las identidades del usuario real se utilicen como servicios pilotos. Además, se busca que algunas de las instituciones desplieguen servicios federados para ser usados por la comunidad.

El software que se necesita para poner en práctica dichos servicios, será utilizado por los miembros del grupo de trabajo designado para dicho fin a través de las respuestas de autorización Eduroam. Con el fin de identificar las necesidades que deben ser abordadas, los miembros más expertos del grupo deben señalar los puntos débiles frente a la implementación de los federativos de dominio Eduroam.

Una vez que los requisitos y las mejoras han sido recogidos, el grupo de trabajo elaborará un documento con las especificaciones y los protocolos de funcionamiento. Durante las fases de diseño y de prueba, esta validación se realizará con base en la producción de los servicios de producción de algunas de las instituciones participantes y el éxito del programa como tal.

7. CONCLUSIONES

Este artículo presenta cómo establece el sistema Eduroam una estandarización de un usuario real y el servicio de *roaming* ampliamente desarrollado por una red inter-NREN, del cual se puede tomar ventaja la utilización de la autorización de los servicios, con el fin de ofrecer un acceso más graneado de la red de control de procesos.

El servicio de autorización basado en NAS-SAML, tratado en el documento, define los componentes de la arquitectura que se deben utilizar con el fin de integrar ambos escenarios. La propuesta de arquitectura proporciona dos alternativas diferentes a fin de tener en cuenta los requisitos de las instituciones involucradas, como el nivel de intrusión en el desplegado y la autenticación de la infraestructura o los requisitos de latencia. El primer enfoque —la autorización de fusión— permite un dominio remoto para obtener las credenciales de autorización en el mismo canal de autenticación, lo que implica unos requisitos mínimos de latencia. Por otro lado, el sistema debe hacer uso de los atributos RADIUS no estándar con el fin de transportar la autorización de las credenciales, las cuales pueden ser distribuidas en los servidores intermedios.

El segundo enfoque —autorización independiente— define el proceso de control de acceso conjunto en dos etapas: el proceso de autenticación, a través de la infraestructura de RADIUS subyacente y el proceso de autorización, a través de la infraestructura NAS-SAML. Este enfoque genera e implica un mayor impacto en la estructura de los sistemas Eduroam, permitiendoles a las instituciones mantener el proceso de autenticación de corte tradicional sin ninguna alteración.

8. REFERENCIAS

[1] S. Cantor & T. Scavo. "Shibboleth Architecture. Technical Overview". 2005.

[2] J. Beatty. "Liberty Protocols and Schema Specification Version 1.1". 2003.

[3] Terena. Trans-European Research and Education Networking Association. Online [Jun. 2011].

[4] K. Wierenga & L. Florio. "Eduroam: past, present and future". *Computational methods in science and technology*, Vol. 11, No. 2, pp. 169-173, 2005.

[5] C. Rigney et al. "Remote Authentication Dial in User Service (RADIUS)". Network Working Group, 2000.

[6] L. Man. "IEEE *Draft* P802.1X/D11. Standards for Local and Metropolitan Area Networks: Standard for Port based Network Access Control". IEEE, 2001.

[7] Dame. Data Mining & Exploration Project. Online [Jun. 2011].

[8] G. López et al. "A network access control approach based on the aa architecture and authorzation attributes". *Journal of Network and Computer Applications*, Vol. 30, No. 3, pp. 900-919, 2007.

[9] M. Eve; M. Prateek & P. Rob. "Assertions and Protocols for the OASIS Security Assertion Markup Language". Oasis Open, 2004.

[10] A. Anderson. "Extensible Access Control Markup Language (XACML)". Technology Report, 2003.

[11] C. De Laat et al. "Generic AAA Architecture". Network Working Group, 2003.

[12] O. Cánovas; G. Lopez & A. F. Gómez-Skarmeta. "A credential conversion service for SAML-based scenarios". *Lecture Notes in Computer Science*, Vol. 3093, pp. 297-305, 2004.

[13] P. Calhoun et al. "Diameter Network Access Server Application". AAA Working Group, 2003.

[14] P. Calhoun et al. "Diameter base protocol". Network Working Group, 2003.

[15] S. Carmody. "Radius profile of SAML". Brown University, 2006.

[16] G. López; O. Cánovas & A. F. Gómez. "Use of XACML policies for a network access control service". *Proceedings of the 2005 conference on Applied Public Key Infrastructure: 4th International Workshop: IWAP 2005*, pp. 111-122, 2005.

[17] S. Skarmeta & D. Chadwick. "A heterogeneos network access service based on PERMIS and SAML". *Lecture Notes in Computer Science*, Vol. 3545, pp. 55-72, 2005.

[18] A. Filip & E. Vásquez T. "Seguridad en redes WIFI Eduroam". Escuela Técnica Superior de Ingenieros, 2010.

[19] Eduroam. Onlilne [May. 2012].