# Sistema de Autorización Única para Plataformas Federadas de Provisión de Contenido[1]

Hristo Koshutanski, Rajesh Harjani, Antonio Maña*, Ernesto J. Pérez, Marioli Montenegro

{hristo,rajesh,amg,ernestopg,marioli@lcc.uma.es}

E.T.S. de Ingeniería Informática, Universidad de Málaga,

Campus de Teatinos, 29071, Málaga, España

## Resumen

El proyecto ConTur propone el desarrollo de una plataforma de gestión de contenidos turísticos provenientes de diferentes fuentes, con el objetivo de mejorar la pobre integración del sector y hacer frente a la rivalidad cada vez mayor de los distintos destinos emergentes. El contenido turístico es proporcionado por medio de servicios federados de la plataforma ConTur y ofrecido por portales Web a los usuarios finales. El suministro de contenido federado implica varias cuestiones de seguridad, tales como si los portales Web de suministro de contenido federado son confiables, o si estos portales respetan los privilegios de los usuarios cuando actúan en nombre de ellos, o si la autorización de usuarios y la gestión de identidades no dificultan el acceso a servicios de la federación de ConTur. Nuestro trabajo se basa en soluciones Single Sign-On para federaciones y proporciona un sistema de *autorización única* para plataformas de suministro de contenidos mejorando el consumo de servicios federados.

## Palabras clave

Autorización única, federación, single sign-on, control de acceso, proxy de seguridad, rendimiento.

---

[1] El trabajo presentado forma parte del proyecto **ConTur** (TSI-020311-2009-4), financiado por el Ministerio de Industria, Turismo y Comercio (http://contur.labs.andago.com).

* Persona de contacto, email: amg@lcc.uma.es, tel: 952137142, fax: 952131397.

## Introducción

Según la Organización Mundial del Turismo y el Consejo Mundial de Viajes y Turismo, el turismo es una de las mayores industrias en el mundo, en gran parte debido a la globalización de la industria a nivel mundial, que ha creado una plétora de nuevos destinos turísticos. De la misma manera, en España el sector turístico tiene un peso muy importante en la economía, aunque como toda actividad productiva, también presenta algunas debilidades:

- Creciente rivalidad de destinos emergentes.
- Dependencia comercial del turismo español con empresas turísticas internacionales.
- Débil integración sectorial que impide tanto la mejora de la competitividad y productividad empresariales, como la comercialización de productos turísticos.

Para paliar estas debilidades, el proyecto ConTur presenta una plataforma de gestión de contenidos capaz de filtrar, catalogar, agregar, fusionar e integrar de forma inteligente, fiable y robusta contenidos turísticos provenientes de diversas fuentes de naturaleza heterogénea dispersas hoy en la web (ej. páginas personales, redes sociales, catálogos institucionales, etc.).

La plataforma ConTur está diseñada para ofrecer contenidos turísticos a usuarios finales a través de una *federación* de portales Web. Para ello, se ha desarrollado un sistema que ofrece un proceso de *autorización única* y que facilita el acceso a los servicios federados.

Los principales requisitos de seguridad necesarios para implementar el sistema de autorización de ConTur son:

- Autenticación y gestión de identidades federadas. Expresar distintos contextos de identidades como certificados digitales y credenciales del tipo ID de usuario y contraseña.

- Autorización única dentro de la federación, permitiendo un acceso flexible a los servicios de los portales Web.

- Modelo de Control de Acceso con autorizaciones específicas de ConTur.

- Mecanismos de seguridad que permitan el acceso seguro, eficiente y escalable a los servicios de ConTur.

**Motivación del trabajo realizado**

Hoy en día podemos encontrar diversos estándares y mecanismos para la gestión de identidades. En trabajos recientes [5] se citan algunos objetivos para las soluciones de gestión de identidades, como que sean (i) voluntarias, en el sentido de que los usuarios puedan elegir entre varios proveedores de seguridad y distintos tipos de credenciales; (ii) seguras y resistentes, (iii) interoperables, escalables y fáciles de utilizar por parte de distintos proveedores de servicios; y (iv) rentables.

Partiendo de aquí, se ha optado por utilizar el estándar SAML v2 [4] como base para gestionar las identidades y autorizaciones, capaz de expresar una gran variedad de información contextual sobre el proceso de autenticación, y donde la futura compatibilidad con mecanismos y tecnologías de identidad externas a ConTur está bien soportada. SAML proporciona declaraciones de autorización y define protocolos para solicitar autorizaciones y responder a los mismos entre entidades federadas.

WS-Trust[2] y WS-Federation[2] definen estándares para la federación de identidades. Nuestro enfoque está centrado en proporcionar un marco de trabajo de gestión de autorización única, en contraste con la interoperabilidad de tokens de autorización de WS-Trust/WS-Federation.

El trabajo [7] examina la noción de autorización única pero en el contexto de una única empresa en lugar de una federación de las mismas. Más cercano a nuestras necesidades se encuentra el trabajo [1] sobre un servicio de autorización federada con su propio (ad-hoc) protocolo de mensajes de autorización, en contraste con nuestra decisión de utilizar autorizaciones federadas de mensajes basados en SAML.

## Arquitectura del sistema de autorización

Los principales factores que han motivado el diseño de la arquitectura del sistema de autorización son:

1. Asegurar que la integración de los aspectos de autorización dentro de la federación ConTur sea fácil y sencilla.

2. Desarrollar mecanismos de seguridad eficientes, reduciendo así la sobrecarga inherente al establecer comunicaciones seguras y confiables.

Teniendo en cuenta estos factores, se han tomado las siguientes decisiones de diseño. La principal es separar la lógica de seguridad de la lógica de negocio, es decir, una separación de los mecanismos de gestión de autorización, administración de políticas del control de acceso, certificación, y autenticación, frente a las aplicaciones de gestión del portal Web y de la plataforma ConTur.

[2] http://www.oasis-open.org/standards

Así, se ha definido el *Proveedor de Seguridad de ConTur* (CSP), en el que confiarán los portales Web para la autenticación y autorización de usuarios. Así mismo, la plataforma ConTur confiará también en que el CSP certifique la legitimidad de los portales Web.

El CSP sirve para dar confianza a todo el sistema, proporcionando servicios dedicados como:

- Registro de usuarios y portales Web.
- Autenticación y autorización tanto de usuarios como de portales Web.
- Autoridad de Certificación, emitiendo certificados a usuarios finales, servidores de portales Web y a los servidores de la plataforma ConTur.

La segunda decisión de diseño fue que los mecanismos de autenticación y autorización fueran transparentes para los portales Web y la plataforma ConTur para así facilitar la evolución del sistema ConTur de cara al diseño y requisitos de políticas. Para ello se ha definido el concepto de *Proxy de seguridad*, que hace posible que la interacción entre los portales Web, el CSP y la plataforma ConTur sea segura. Este componente integra el mecanismo de autorización de los portales Web con la plataforma, y proporciona la funcionalidad de un PEP (Policy Enforcement Point), que reside en los portales Web y que asegura el cumplimiento de las decisiones de autorización del CSP. En el caso de la plataforma ConTur, controla el acceso a los servicios de los portales Web en nombre de los usuarios.

La tercera decisión de diseño fue extender la usabilidad del sistema permitiendo a los usuarios autenticarse a través de identidades externas a la plataforma ConTur; dado que actualmente la mayoría de usuarios tienen identidades electrónicas como el Documento

Nacional de Identidad electrónico (DNIe)[3], u otros certificados digitales firmados por la Fábrica Nacional de Moneda y Timbre[4].

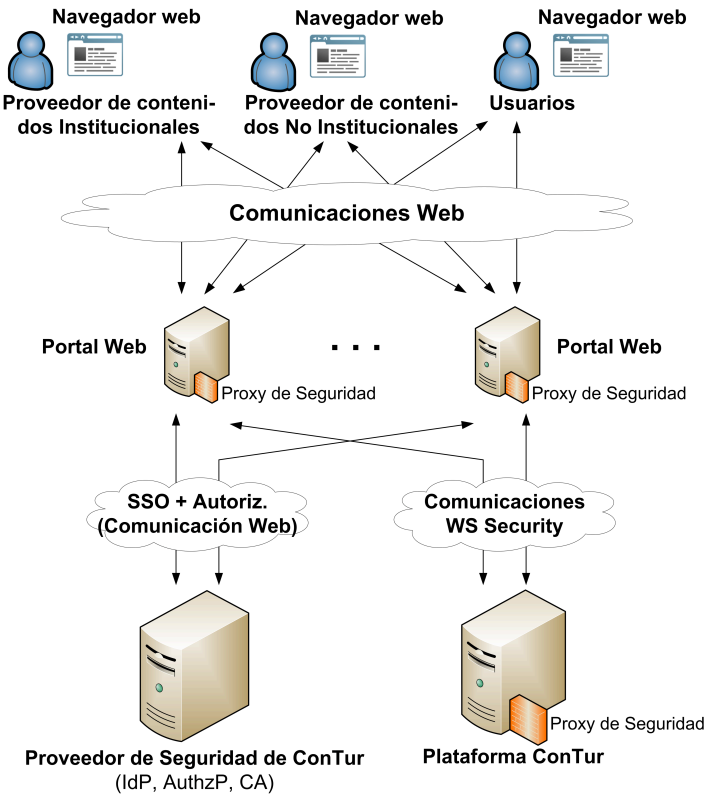


Figura 1. Arquitectura del sistema de autorización de ConTur

La Figura 1 muestra la visión global de la arquitectura de autorización incluyendo los actores principales y las comunicaciones entre ellos.

El sistema ConTur puede definirse como una federación de portales Web para la provisión de contenidos a usuarios finales. La arquitectura de seguridad se define como un *círculo de confianza* entre los portales Web, la plataforma ConTur, y el CSP. Los portales Web necesitan registrarse en el CSP para formar parte de la federación y así poder acceder dinámicamente a los servicios de ConTur[5].

[3] http://www.dnielectronico.es
[4] http://www.fnmt.es
[5] Tras el registro, el portal Web obtiene un certificado para establecer comunicaciones seguras con la plataforma y el CSP.

La federación permite compartir información de identidades de usuarios entre los distintos portales Web de una manera unificada. Una vez que la federación queda determinada, los usuarios pueden aprovecharse del mecanismo de Single Sign-On (SSO) dentro del círculo de confianza. Este mecanismo va a permitir a los usuarios autenticados en el CSP acceder a otros portales Web sin requerir una nueva autenticación. El CSP desempeña el rol de proveedor de identidades confiables a través de todos los portales Web.

## Autenticación de usuarios y gestión de identidades

La arquitectura de seguridad considera dos casos de uso distintos. En el primero, la plataforma ConTur necesita que los usuarios se autentiquen, para poder ofrecerles los servicios que les corresponden en función del grupo de usuarios al que pertenecen. En el segundo, y por razones de negocio, los portales Web requieren que se mantenga la privacidad de sus usuarios, y por tanto necesitan acceder a la plataforma ConTur en nombre de usuarios anónimos (sin revelar su identidad).

*Acceso anónimo a través de portales Web autorizados*

El sistema permite a los usuarios de los portales Web acceder a los contenidos de la plataforma de forma anónima, contando eso sí, con la aprobación del administrador del CSP conforme a una relación contractual con el portal Web.

Para lograr esto, durante el proceso de registro los portales Web tienen la opción de solicitar la activación del acceso anónimo para sus usuarios y seleccionar los privilegios que les serán asignados a estos usuarios.

*Modos de Autenticación de Usuarios*

*Autenticación basada en certificados*. En el caso de que el usuario posea un certificado FNMT o DNIe podrá acceder al portal Web de manera que el CSP acceda a esta

información y autentique al usuario. Si el usuario no posee ninguno de los certificados admitidos por ConTur, entonces debe registrarse en el CSP para obtener un certificado X.509 [6] de ConTur[6].

*Autenticación ligera.* También es posible autenticarse en el CSP usando un nombre de usuario y contraseña. Este mecanismo está diseñado para usuarios que acceden a la plataforma a través de ordenadores de uso público en los que no pueden o no quieren instalar su certificado.

Una vez registrado, el usuario dispone de un perfil de identidad al que puede asociar sus posibles identidades externas (p.ej. DNIe, FNMT). Este perfil de identidad está directamente relacionado, a través de un identificador unificado de ConTur, con el Perfil de Preferencias Turísticas del usuario.

### Autorización única de servicios federados

El principal objetivo del enfoque de autorización única de servicios federados es ofrecer a los usuarios acceso unificado a estos servicios, de forma similar al concepto de SSO pero para la autorización. En otras palabras, los usuarios son autorizados una sola vez para unos servicios dentro de una misma federación, y no se les vuelve a solicitar sus credenciales para esos mismos servicios accedidos a través de otros portales Web de la federación.

El sistema de autorización define un protocolo entre el usuario final y el CSP llamado *Protocolo de Autorización Única de Servicios Federados*, que ofrece a los usuarios la posibilidad de controlar cuáles son los servicios a los que los portales Web podrán acceder en nombre de ellos. De entre los servicios solicitados por el portal Web, el CSP solicita al usuario confirmación de aquellos para los que tiene privilegios de acceso. El

[6] Certificado X.509 y la correspondiente clave privada en un contenedor PKCS12 cifrado con la contraseña de usuario.

usuario seleccionará aquellos servicios que no comprometan su seguridad, teniendo en cuenta la fiabilidad que le merece el portal Web como intermediario en esta transacción de datos.

A continuación describimos el proceso de autorización para un usuario que solicite acceso a una interfaz:

1) El usuario intenta acceder a un recurso protegido del portal Web.

2) El portal Web solicita (localmente) al Proxy de Seguridad[7] autorización para el usuario, indicando la lista de servicios requeridos para acceder al recurso. Si el usuario no está autenticado o no tiene todos los permisos necesarios, se inicia el protocolo de autorización de servicios federados, por lo que el portal Web redirecciona al usuario al CSP, incluyendo la lista de servicios requeridos y la identidad del usuario.

3) El CSP comprueba si el usuario tiene permiso para cada uno de los servicios y le solicita al usuario que seleccione (de entre los que tiene privilegios) los que desea autorizar a dicho portal Web.

4) Cuando el protocolo finaliza, el CSP genera y firma una respuesta de autorización que incluye los servicios autorizados por el usuario.

5) El usuario es redirigido al portal Web, donde se comprueba dicha respuesta de autorización y se le concede acceso a la interfaz solicitada.

A partir de ahora, el usuario podrá acceder a las interfaces que ofrezcan los servicios autorizados por él en cualquier portal Web de la federación.

*Escenario de autorización única de portales Web federados*

[7] A través de una API.

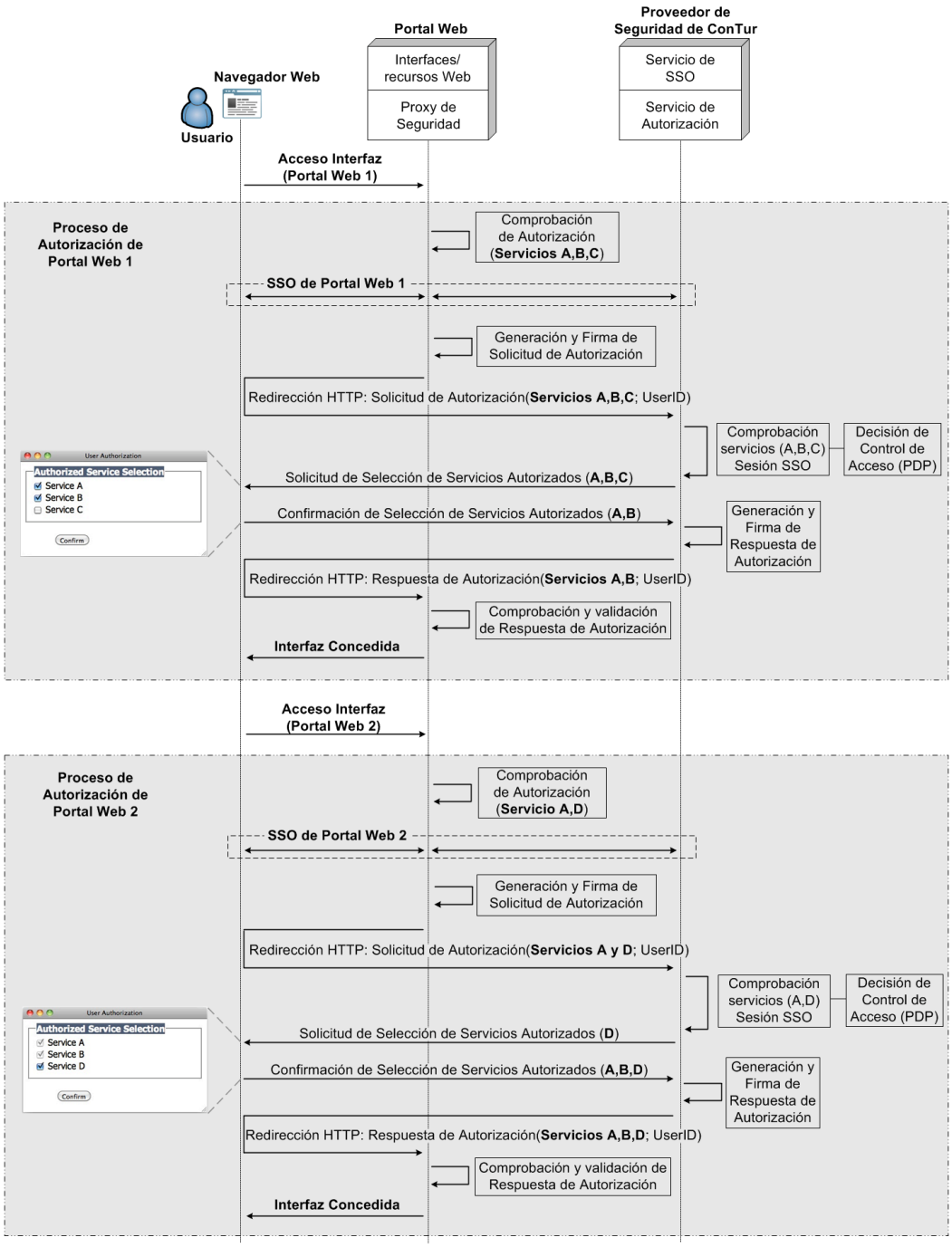


Figura 2. Escenario de autorización única de portales Web federados

La Figura 2 muestra un escenario de autorización con los mensajes intercambiados entre el usuario y los portales Web y CSP. Podemos observar que el CSP comprueba siempre si los servicios solicitados por el usuario han sido ya previamente autorizados en la sesión SSO. Además, la respuesta de autorización contiene siempre todos los servicios activados por el usuario en cualquiera de los portales Web de la federación.

Si el segundo proceso de autorización se realizara en el mismo portal Web, pero accediendo a una interfaz distinta, el proxy de seguridad comprobaría la existencia de una sesión previa, evitando el proceso de SSO. Después, el proxy detectaría que el servicio A ha sido ya activado por el usuario, y no lo incluiría en la solicitud de autorización. Análogamente, para los posteriores accesos a otras interfaces, el proxy evitaría el proceso de autorización siempre y cuando el usuario ya hubiera concedido autorización para los servicios requeridos.

*Protocolo de Autorización Única de Servicios Federados*

Para la consistencia en la gestión de interfaces de portales Web, el sistema no contempla desactivar autorizaciones de servicios concedidas en anteriores interacciones con portales Web de la federación. Así, la última respuesta de autorización contendrá todos los servicios seleccionados por el usuario durante su sesión. Si el usuario quiere desactivar la autorización de sus servicios, deberá cerrar la sesión SSO y comenzar de nuevo el proceso de autorización.

El hecho de que este protocolo ofrezca al usuario la posibilidad de compartir la autorización de servicios a través de varios portales Web, resulta muy útil de cara al usuario que necesite ejecutar los mismos servicios en varios portales.

Se ha definido también un *modo estricto* para la gestión de las autorizaciones a lo largo de la federación de portales Web en la que, para un usuario dado, los servicios previamente activados estarán disponibles para otros portales Web sólo si estos portales los solicitan explícitamente. Por ejemplo, en el segundo proceso de autorización de la Figura 2, el CSP solicita al usuario que active los servicios A y D, pero no B, ya que este no es solicitado por el portal Web. En caso de que el portal necesite este servicio B, entonces el usuario tendría que confirmarlo.

*Autorización de la plataforma ConTur*

Uno de los principales requisitos para la plataforma ConTur ha sido el poder afrontar múltiples comunicaciones simultáneas con distintos portales Web, y por tanto, uno de los principales objetivos técnicos ha sido conseguir una autorización de acceso a los servicios de ConTur escalable y eficiente.

Se ha adoptado el protocolo *SAML Sender Vouches*[8] con certificados para la autorización de servicios solicitados por el portal Web. El concepto básico es que un emisor corrobore la identidad de un sujeto (y posiblemente los atributos de autorización) a un servidor usando un token SAML. Este emisor debe ser una entidad confiable usando su certificado de clave pública. La semántica del protocolo es permitir a un emisor (distinto del sujeto) declarar la identidad del sujeto como responsable de una solicitud de servicio dada. El protocolo usa también un mecanismo de intercambio mutuo de certificados para proteger la integridad y confidencialidad a nivel de mensaje en la transmisión del token SAML.

Este token SAML Sender Vouches estará contenido en el token de respuesta de autorización, indicando los servicios seleccionados por el usuario, y estará firmado por el CSP. De esta manera, en cada solicitud de acceso, la plataforma ConTur comprueba si el servicio solicitado ha sido activado por el usuario, evitando así que portales Web maliciosos accedan a servicios para los cuales no tienen los privilegios necesarios.

## Modelo de control de acceso

La esencia del control de acceso basado en roles, RBAC [2], radica en que los permisos son asignados a roles. Un rol puede ser considerado como un conjunto de privilegios

[8] Definido en Perfil de Token SAML de OASIS v1.1 en http://www.oasis-open.org/specs

que un usuario o un conjunto de usuarios dispone. Así, se realiza una asociación entre usuarios y roles, y la definición de los derechos de acceso de los roles a los recursos.

Más cerca de nuestras necesidades está el control de acceso basado en grupos. De forma similar a RBAC, a los grupos se les asignan privilegios sobre objetos y los usuarios son asignados a grupos. En nuestro caso, el identificador de usuario puede ser también el del grupo. Este enfoque nos ayuda a dar soporte al acceso anónimo de usuarios.

Los grupos y los miembros no se ven afectados por ninguna herencia ni ninguna jerarquía de privilegios, lo que simplifica la gestión de grupos. El proceso de toma de decisiones no requiere una activación de roles explícita. Una vez que un usuario se ha autenticado, se le conceden los privilegios de cada uno de los grupos a los que pertenece.

***Definición del Modelo de Control de Acceso de ConTur***

- $G$ denota un conjunto de grupos.
- $R$ denota un conjunto de servicios (recursos en general).
- $U$ denota un conjunto de usuarios.
- $O$ denota un conjunto de operaciones.
- $P$ denota un conjunto de privilegios. $P \subseteq \{(o,r) \mid o \in O \wedge r \in R\}$.
- $PG \subseteq P \times G$ es una asignación de privilegios a grupos de muchos a muchos.
- $UG \subseteq U \times G$ es una asignación de usuarios a grupos de muchos a muchos.
- *assigned_privileges(u)*=$\{p \in P \mid (u,g) \in UG \wedge (p,g) \in PG\}$, el mapeo de usuario $u$ en un conjunto de privilegios asignados.

```
is_user_authorized_per_privileges(u,{p1,...,pn})={
    return true if {p1,...,pn} ⊆ assigned_privileges(u);
    false otherwise; }
get_user_authorized_privileges(u,{p1,...,pn})={
    return {p1,...,pn} ∩ assigned_privileges(u);  }
```

El último fragmento muestra dos operaciones similares pero con distintos resultados dependiendo del modo de autorización, *estricto* o *flexible* respectivamente. Dependiendo del resultado obtenido y de la política de acceso a interfaces del portal Web, se puede conceder o denegar el acceso, o incluso personalizar la interfaz que el portal muestra al usuario.

*Acceso anónimo de usuarios*. El administrador del portal Web (durante el registro) puede seleccionar aquellos privilegios que serán accesibles para sus usuarios anónimos. Se crea un nuevo grupo cuyo nombre es el nombre del identificador del portal, y se asocia al perfil del portal Web indicando que ofrece a sus usuarios acceso anónimo. La semántica de este identificador de grupo nuevo es la de asignar todos los privilegios seleccionados durante el registro a ese grupo de usuarios, de manera que cualquier solicitud de acceso anónimo por parte de usuarios provenientes de este portal Web, obtengan los privilegios asignados a dicho grupo.

## Rendimiento del mecanismo de autorización

Primeramente hemos medido el rendimiento del proceso de toma de decisiones de autorización del CSP. Para ello, hemos utilizado una Base de Datos MySQL, que nos proporciona una implementación fácil de integrar, y hemos medido el tiempo de ejecución de las consultas SQL correspondientes a la función donde, dado un usuario y una lista de privilegios, se calcula el subconjunto de estos privilegios que el usuario posee (`get_user_authorized_privileges`).

Hemos creado en la base de datos 500.000 usuarios, 20 grupos, y 1000 privilegios (con distintos servicios y acciones) asignados de manera uniforme a los grupos. Cada usuario

pertenece a 5 grupos (aleatorios) mientras que algunos usuarios (creados al final) son asignados a todos los grupos para considerar el peor caso[9].

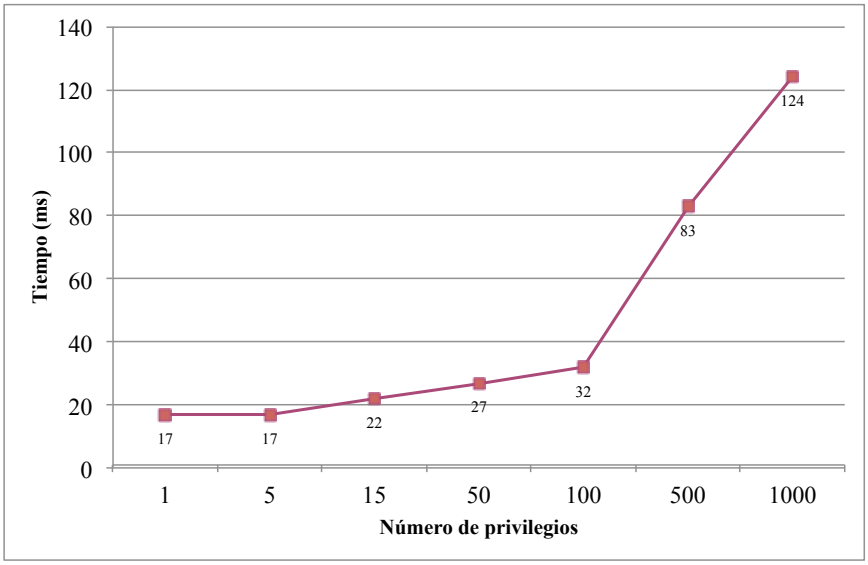


Figura 3. Duración de decisión de control de acceso (milisegundos)

La Figura 3 muestra la media de 100 pruebas por experimento, donde en cada experimento se aumenta el número de privilegios solicitados para la decisión de acceso. La conclusión es que el rendimiento de la decisión de acceso no depende tanto del número de usuarios pero sí del número de privilegios, que se debe al conjunto de operaciones realizadas por el motor de base de datos.

Seguidamente, se ha medido el rendimiento global del mecanismo de autorización de la plataforma ConTur. Para ello, hemos usado el siguiente escenario: el Proxy de Seguridad de la plataforma ConTur se ejecuta sobre una máquina[10], y en otras dos máquinas en la misma red, se ejecuta en cada una un Proxy de Seguridad del portal Web.

[9] El hardware de la máquina: CPU 2.53 Ghz Intel Core 2 Duo, RAM 4GB 1067 Mhz DDR3, MacOSX 10.6.
[10] Hemos utilizado la misma máquina que en el experimento de autorización del CSP.

Cada Proxy de los portales Web generaron y enviaron al servidor de la plataforma 100 solicitudes de acceso a servicios de forma simultánea (usando hebras) en nombre de usuarios finales. Cada solicitud de servicio sigue el mecanismo SAML Sender Vouches.

El Proxy de la plataforma ConTur procesó **24.7** llamadas a servicios Web seguros por segundo. Esta cifra representa un límite superior ya que el tiempo de ejecución del servicio no se tuvo en cuenta (0 milisegundos) para mostrar únicamente la sobrecarga ocasionada por la seguridad.

La evaluación del rendimiento del Proxy de Seguridad del portal Web muestra que se tardan una media de **78** milisegundos por acceso a servicio seguro, excluyendo datos de entrada al servicio y la ejecución real del servicio.

El prototipo actual usa librerías de PicketLink[11] para la gestión de tokens SAML de autenticación y autorización, y Metro[12] para servicios Web seguros.

## Conclusiones

Hemos presentado un sistema de autorización única para una plataforma que proporciona contenidos turísticos de manera federada. Se ha descrito tanto la arquitectura de autorización del sistema como los mecanismos de seguridad desarrollados. También se ha planteado el modelo de control de acceso y los resultados del rendimiento tanto del proceso de toma de decisión, como del acceso a servicios federados de la plataforma a través de servicios Web seguros.

Los resultados de rendimiento del sistema de autorización muestran el potencial de soportar una gran cantidad de usuarios consumiendo los servicios federados de la plataforma.

[11] http://www.jboss.org/picketlink
[12] http://metro.java.net

### Trabajos futuros

Definir la confianza de grano fino en los portales Web federados. Para ello presentamos la noción de Niveles de Confianza asignados a los portales Web, utilizando distintas métricas de confianza para esto. En este caso, los usuarios que accedan a contenido de ConTur a través de distintos portales Web de la federación, tendrán acceso limitado si no poseen el nivel de confianza suficiente.

Aprovechando estos niveles de confianza también podemos ampliar nuestro modelo de control de acceso, teniendo en cuenta datos de contexto en la toma de decisiones [3], de manera que para conceder privilegios a usuarios no se consideren únicamente los privilegios actuales, sino también estos niveles de confianza del portal Web.

## Bibliografía

[1] Colin, Jean-Noël., Le, Tien-Dung., Massart, David. (2009). A Federated Authorization Service for Bridging Learning Object Distribution Models. In 8th International Conference on Advances in Web Based Learning (ICWL 2009). LNCS, Springer, pp. 116-125.

[2] Ferraiolo, D., Sandhu, R., Gavrila, S., Kuhn, D., and Chandramouli, R. (2001). Proposed NIST standard for role-based access control. In ACM Trans. Information and System Security, 4(3):224–274.

[3] Groba, C., Grob, S., and Springer, T. (2007). Context-dependent access control for contextual information. In Proc. of 2nd International Conference on Availability, Reliability and Security, pages 155–161. IEEE.

[4] SAML (2005). Security Assertion Markup Language. http://saml.xml.org/saml-specifications.

[5] Schwartz, A. (2011). Identity Management and Privacy: A Rare Opportunity To Get It Right. In Communication of the ACM, June 2011, vol.54, no.6, pages 22–24.

[6] X.509 (2005). The directory: Public-key and attribute certificate frameworks. ITU-T Recommendation X.509:2005 | ISO/IEC 9594-8:2005.

[7] Yuan, Xue-min; Li, Ting. (2010). A new authorization model of a case-based complex system applied in enterprise informatization. In IEEE 17th International Conference on Industrial Engineering and Engineering Management, pages 299–303.