World Library and Information Congress:
70th IFLA General Conference and Council

22-27 August 2004
Buenos Aires, Argentina

Programme: http://www.ifla.org/IV/ifla70/prog04.htm

Code Number: **055-S**
Meeting: **155. Information Technology**
Simultaneous Interpretation: **-**

Shibboleth: Una solución de Código Libre para compartir recursos

Marianne Afifi
Directora de Electronic Resources & Special Projects Development
Information Services Division LVL 113C
University of Southern California

RESUMEN:
Shibboleth es un proyecto de la National Science Foundation Internet2 Middleware Initiative. Su objetivo es "desarrollar una solución abierta, basada en estándares, con el fin de cubrir las necesidades que tienen las organizaciones para intercambiar información sobre sus usuarios de forma segura y salvaguardando la privacidad"[i]. Las bibliotecas e instituciones académicas observan una necesidad cada vez mayor de proporcionar un acceso protegido y validado a los recursos en línea que ellos producen, licencian, compran o comparten. Los proveedores y editores también están interesados en ofrecer modelos de acceso diferentes a los tradicionales basados en las direcciones IP, servidores proxy y autenticación por nombre de usuario/contraseña. Los investigadores y profesores que utilizan continuamente la web han ido exigiendo, cada vez más, que el intercambio de información proporcione a los participantes ciertos derechos, además de privacidad. Shibboleth se ha desarrollado con el fin de hacer posible la interacción para compartir recursos entre estos miembros de forma sencilla basada en estándares.

En mi presentación resumiré los orígenes de Shibboleth, daré una visión global de su desarrollo y explicaré cómo funciona. También analizaré las razones por las que se considera una herramienta importante para compartir recursos en bibliotecas y otros entornos federados.

Resúmen de la Presentación

- Definiciones y Conceptos
- Shibboleth
- Aplicación a Bibliotecas
- Aplicación a Portales
- Shibboleth y las Federaciones

27 de Agosto de 2004 IFLA Marianne Afifi (afifi@usc.edu) 1

Estoy encantada de dirigirme hoy a ustedes para hablarles de un interesante proyecto que tiene gran relevancia en el tema "Autenticación y Autorización relacionada con los Servicios Bibliotecarios", tema propuesto por la Sección de Tecnologías de la Información de IFLA como objetivo para esta conferencia. El proyecto se llama Shibboleth. En primer lugar, quiero ofrecer algunas definiciones iniciales de los términos que usaré durante mi presentación. Posteriormente presentaré una visión global de por qué Shibboleth ha sido creado, cómo funciona, y hablaré de su relevancia para las bibliotecas, especialmente en los proyectos de portales multi-búsqueda tales como el Scholars Portal.

El desarrollo de Shibboleth ha estado respaldado por diferentes organizaciones. Algunos de ustedes no estarán familiarizados con ellas y por esta razón las enumeraré a continuación. El consorcio National Science Foundation's Internet2 es el patrocinador del proyecto. La investigación del Middleware (programas intermedios) es una de las metas propuestas por Internet2.

Definiciones y Conceptos

- NSF
- Internet2
- Middleware
- Autenticación
- Autorización

IFLA 27 de Agosto de 2004 Marianne Afifi (afifi@usc.edu) 2

National Science Foundation
Fue "creada por la National Science Foundation Act de 1950, como legislación modificada y relacionada de la 42. U.S.C. 1861 y siguientes, y le fue otorgada autoridad adicional por la Science and Engineering Equal Opportunities Act (42 U.S.C. 1885) y el Titulo I de la Education for Economic Security Act (20 U.S.C. 3911 al 3922). …"

"La Ley estableció la misión de la NSF:
Promover el progreso de la ciencia; fomentar la salud, la prosperidad, y el bienestar nacional; y asegurar la defensa nacional"[ii]
http://www.nsf.gov/home/about/creation.htm

Internet2

Es un consorcio compuesto por 206 universidades que trabajan junto con la industria y el gobierno para desarrollar y aprovechar los avances en aplicaciones y tecnologías de redes, acelerando la creación de la Internet del mañana. Internet2 está reactivando la cooperación entre el mundo académico, la industria y el gobierno que promovió la Internet actual en sus orígenes. Los principales objetivos de Internet2 son:

- Crear servicios pioneros de red para la comunidad de investigación nacional
- Posibilitar aplicaciones de Internet revolucionarias

- Asegurar la transferencia rápida de nuevos servicios y aplicaciones de red a la comunidad de Internet en general
  http://www.internet2.edu/about/aboutinternet2.html [iii]

Middleware (Programa intermedio)
o "glue", es una capa de software entre la red y las aplicaciones. Este software ofrece servicios tales como la identificación, la autenticación, la autorización, los directorios y la seguridad. Hoy en día en Internet, por lo general las aplicaciones tienen que ofrecer estos servicios por sí mismas, lo que conlleva estándares opuestos e incompatibles. Middleware, promoviendo la normalización y la interoperabilidad, mejorará las aplicaciones de red mediante un uso más sencillo. La Internet2 Middleware Initiative (I2-MI) intenta conseguir el desarrollo de los principales servicios middleware en las universidades de Internet2.
http://middleware.internet2.edu/ [iv]

Las dos definiciones que considero fundamentales para entender esta presentación son la de autenticación y la de autorización. He seleccionado las definiciones usadas por Clifford Lynch de la Coalition for Networked Information (CNI):

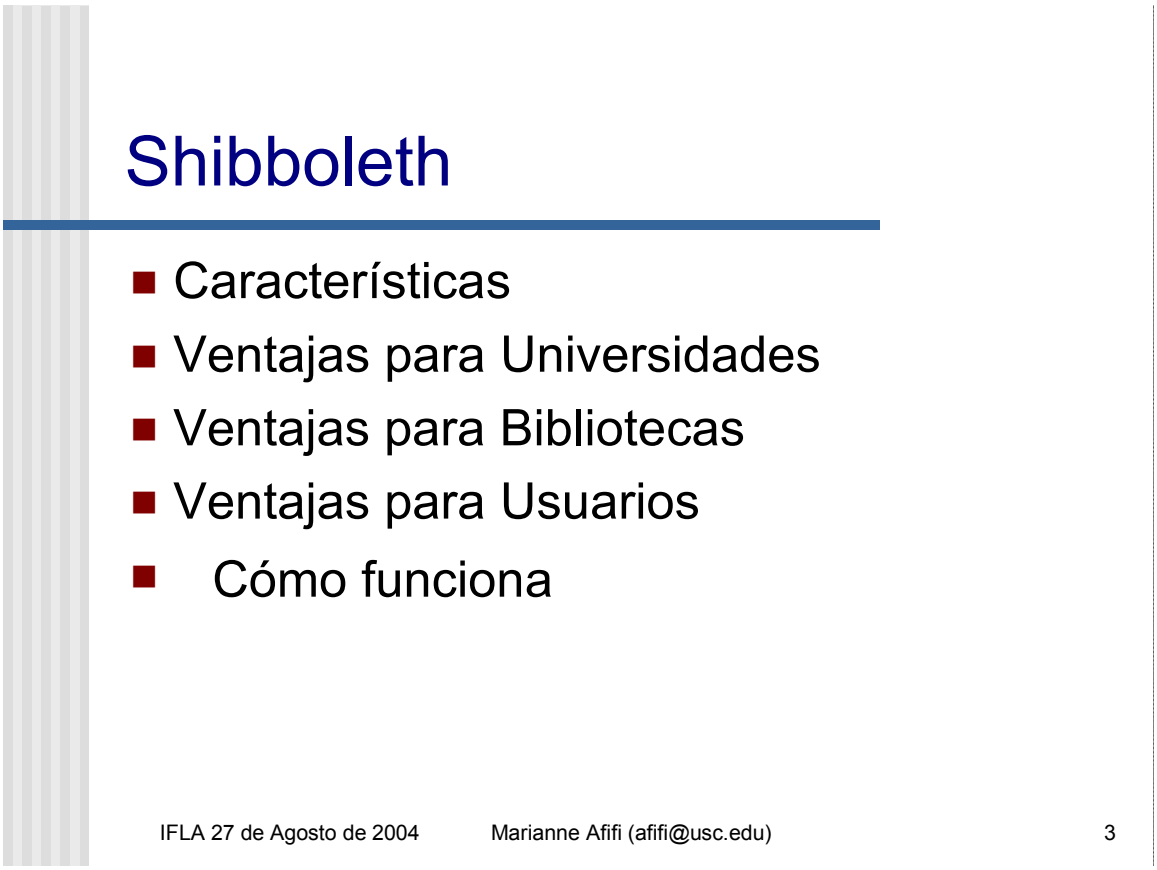
- **Autenticación**

"Autenticación es el proceso por el que un usuario de red establece el derecho a una identidad – fundamentalmente, el derecho a usar un nombre" [v]

- **Autorización**

"Autorización es el proceso que determina si una identidad (junto con los atributos asociados a ella) tiene permitido ejecutar alguna acción, como puede ser acceder a un recurso". [vi]

Estos términos se confunden con frecuencia pero es importante diferenciarlos, aunque actualmente en el entorno bibliotecario, representen muchas veces lo mismo. Por ejemplo, cuando el acceso a un recurso está basado en la validación de la dirección IP, los usuarios son autenticados en virtud de sus direcciones IP, lo que automáticamente significa que están también autorizados. En un entorno Shibboleth los usuarios pueden ser autenticados como parte de un cierto grupo pero pueden no estar autorizados a utilizar un determinado recurso.



Shibboleth

La Segunda Edición del Oxford English Dictionary de 1989 ofrece varias definiciones de la palabra Shibboleth, de las cuales he seleccionado dos que se aplican al proyecto que estamos exponiendo hoy.
"1. Voz hebrea empleada por Jefté como palabra-prueba para distinguir a los Efraimitas fugitivos (quienes no podían pronunciar *sh*) de sus propios hombres los Gileaditas (Jueces xii. 4-6)
3. *fig*. Eslogan o fórmula adoptada por un grupo o secta, con el que se puede distinguir a sus miembros o seguidores, o excluir a los que no lo son".

La palabra Shibboleth es por lo tanto es un nombre apropiado para un proceso de gestión de accesos.

El proyecto de software Shibboleth surgió de la necesidad de los participantes de Internet2 y otras organizaciones con estructuras y exigencias similares, de encontrar un buen método para comunicar información sobre sí mismos y sobre sus usuarios. Shibboleth fue desarrollado para facilitar la comunicación y el intercambio de información entre las partes interesadas tales como universidades, bibliotecas, agencias gubernamentales y entidades comerciales. Debido a la variada naturaleza de los participantes los requisitos de Shibboleth fueron que estuviera basado en estándares, que fuera un recurso abierto, que preservara la privacidad y que permitiera y fomentase la federación entre instituciones. Más adelante veremos cómo los aspectos federativos son especialmente importantes en el uso compartido de recursos. Las actuales estructuras de

comunicación en el ámbito de actuación de las instituciones de Internet2 se basan en tecnologías que tienden a ser complejas y pesadas de administrar. Shibboleth permite a los participantes intercambiar información sin tener que utilizar múltiples métodos de autenticación y autorización no normalizados y de difícil uso. Una vez implementado, Shibboleth permitirá el flujo de información basado en normas y preservará la privacidad de los miembros de las instituciones participantes. Mientras está aún lejana la plena implementación entre los miembros y las comunidades relacionadas, muchas instituciones han iniciado proyectos para probar Shibboleth. Además, las organizaciones también han puesto en marcha esfuerzos a gran escala para crear arquitecturas y estructuras propias que permitan a Shibboleth trabajar con ellas.

Es probable que las universidades implementen Shibboleth para la comunicación entre investigadores, en bibliotecas, para portales, y para sistemas de gestión de cursos (Course Management Systems – CMS). Las conexiones y la interoperabilidad entre todos estos sistemas son especialmente deseables. La importancia de Shibboleth para las bibliotecas será evidente para todo aquel que haya trabajado en áreas de gestión de recursos electrónicos. Los editores, productores y distribuidores habitualmente solicitan listas de direcciones IP u ofrecen acceso a través de nombre de usuario y contraseña que necesitan ser gestionados por la biblioteca. A algunas bibliotecas se les exige que utilicen servidores proxy para identificar usuarios. Otras usan servicios VPN para habilitar a sus usuarios el acceso a la red de ordenadores del campus. Además, unos pocos distribuidores establecen restricciones rigurosas a los recursos, por ejemplo un bibliotecario localizado físicamente en una biblioteca debe introducir un nombre de usuario y contraseña para un usuario. En el siglo XXI estos tipos de métodos de acceso suponen una carga para la biblioteca; la institución y los usuarios se están quedando anticuados rápidamente.

Al igual que los usuarios universitarios son cada vez más diversos, lo mismo ocurre con los usuarios de las bibliotecas. Los usuarios ya no son sólo docentes, estudiantes o personal de la universidad. La educación a distancia, las relaciones entre alumnos, la participación de la comunidad y las actividades universitarias en conjunto han creado varios tipos de usuarios que tienen diferentes privilegios bibliotecarios en distintas localizaciones pero que están todos conectados de alguna manera a la universidad. Actualmente es difícil proporcionar y gestionar el acceso a la biblioteca y a otros recursos para estos grupos de población.

Shibboleth puede mejorar la gestión del acceso a recursos, pero para hacerlo las instituciones deben mantener la gestión de la información de los usuarios en un servicio directorio basado en estándares. El desarrollo de servicios directorio de este tipo generalmente no ha estado basado en estándares, sin embargo sí se han hecho esfuerzos en este sentido. Uno de estos esfuerzos es EduPerson: "una clase de objeto auxiliar para los directorios de campus diseñado para facilitar la comunicación entre instituciones de enseñanza superior. Consiste en un grupo de elementos de datos o atributos sobre individuos pertenecientes a la enseñanza superior, junto con recomendaciones sobre la sintaxis y la semántica de los datos que pueden ser asignados a esos atributos"[vii]. Una vez que los atributos sobre los usuarios están claramente definidos y el servicio directorio basado en estándares se ha creado y gestionado con el paso del tiempo el acceso puede ser mucho más sencillo. Desde el punto de vista de los usuarios, sus datos personales en un entorno Shibboleth están mucho mejor preservados que en otros métodos actuales de autenticación.

La ventaja para la biblioteca es que los recursos se pueden dirigir a poblaciones específicas, lo que puede suponer un potencial ahorro de costes. Por ejemplo, el acceso a una revista cara puede limitarse a los miembros de un determinado proyecto de investigación en lugar de destinarse a toda la población universitaria, lo que permite liberar dinero para otros recursos. Además, los aspectos federados de la implementación de Shibboleth pueden ser ventajosos para un consorcio de bibliotecas, universidades multi-campus, universidades dentro de un estado, alianzas de colaboración en una federación y para los distribuidores. Desde la perspectiva de los distribuidores, el uso de Shibboleth les permite a la larga unificar la variedad de métodos de acceso que actualmente emplean. Aunque el proceso llevará algún tiempo, una vez que los distribuidores hayan puesto en marcha Shibboleth, la incorporación de nuevos clientes que también estén autorizados será muy fácil. Shibboleth además permitirá a los distribuidores ofrecer servicios de usuario más segmentados y específicos y probablemente también necesitará desarrollar modelos diferentes de negocios.

Con el software Shibboleth existe un cambio total en la manera de acceder a los recursos. En los modelos antiguos, los usuarios eran registrados en el sistema del propietario del recurso, por ejemplo el sitio del editor o el OCLC FirstSearch, y debían ser autenticados allí. Shibboleth está diseñado de tal modo que la institución de donde procede el usuario verifica su existencia en la base de datos de la institución y proporciona los atributos necesarios sobre ellos al propietario del recurso. Este proceso se desarrolla del modo siguiente (ver Figura 1):

El usuario va a la página web del propietario del recurso, por ejemplo JSTOR, un distribuidor de una revista científica.

1. JSTOR desconoce de dónde procede el usuario.
2. El sistema de JSTOR SHIRE (Shibboleth Indexical Reference Establisher) le pregunta al servicio WAYF (Where Are You From) sobre la procedencia del usuario.
3. WAYF le pregunta al usuario de dónde procede
4. El usuario redirige la pregunta al Shibboleth Handle Service (HS) de su organización (su origen).
5. El Handle Service busca en la base de datos del directorio de la organización del usuario para encontrar si el usuario existe en la base de datos.
6. Tras la verificación, el Handle Service devuelve la petición al usuario para que envíe sus credenciales.
7. El usuario envía sus credenciales al Handle Service.
8. El Handle Service devuelve un pase (o alias) al SHIRE de JSTOR indicando que el usuario forma parte del sitio origen.
9. El SHIRE entonces envía el pase al SHAR (Shibboleth Attribute Requester), el cual solicita los atributos del usuario y envía una consulta al Attibute Authority (AA) localizado en el sitio origen.
10. El Attribute Authority envía los atributos del usuario a SHAR
11. El SHAR envía los atributos del usuario al gestor de recursos de JSTOR (JSTOR Resource Manager – RM) que permite al usuario el acceso apropiado al recurso.

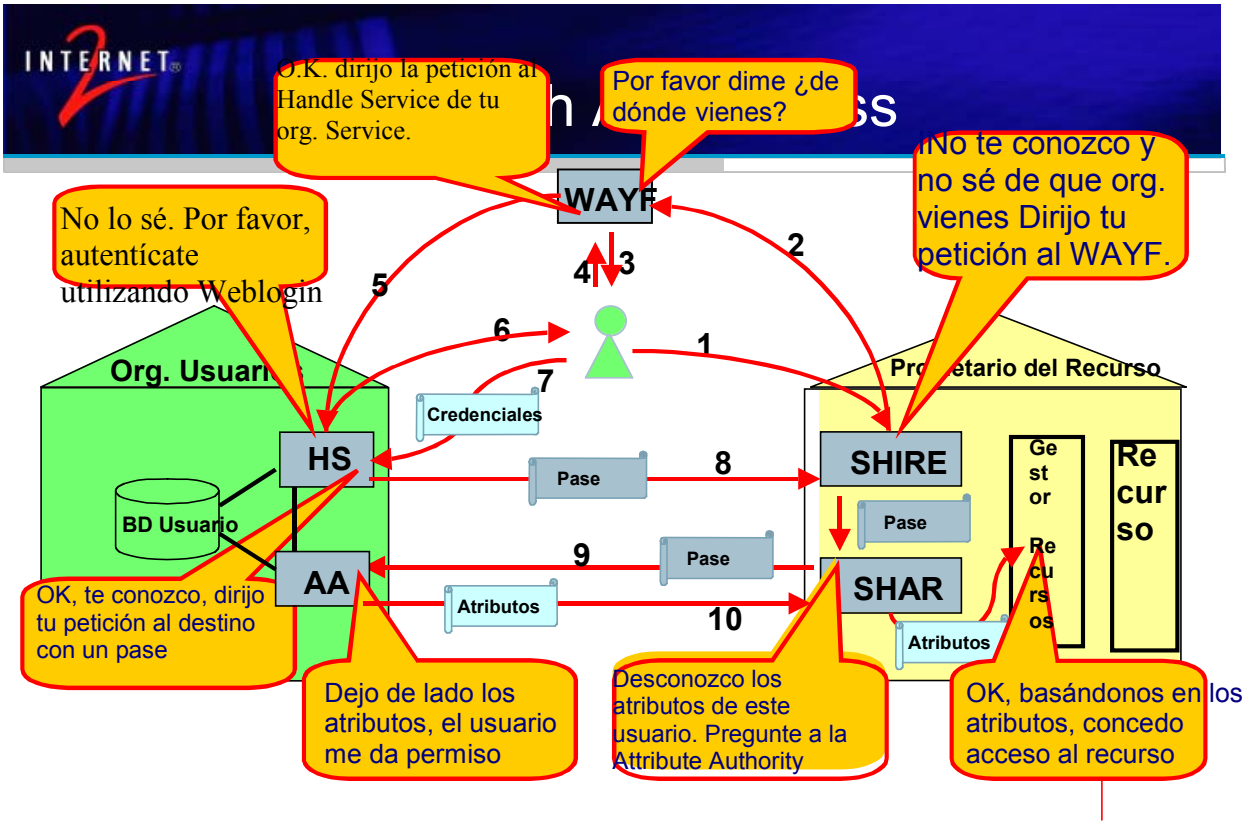
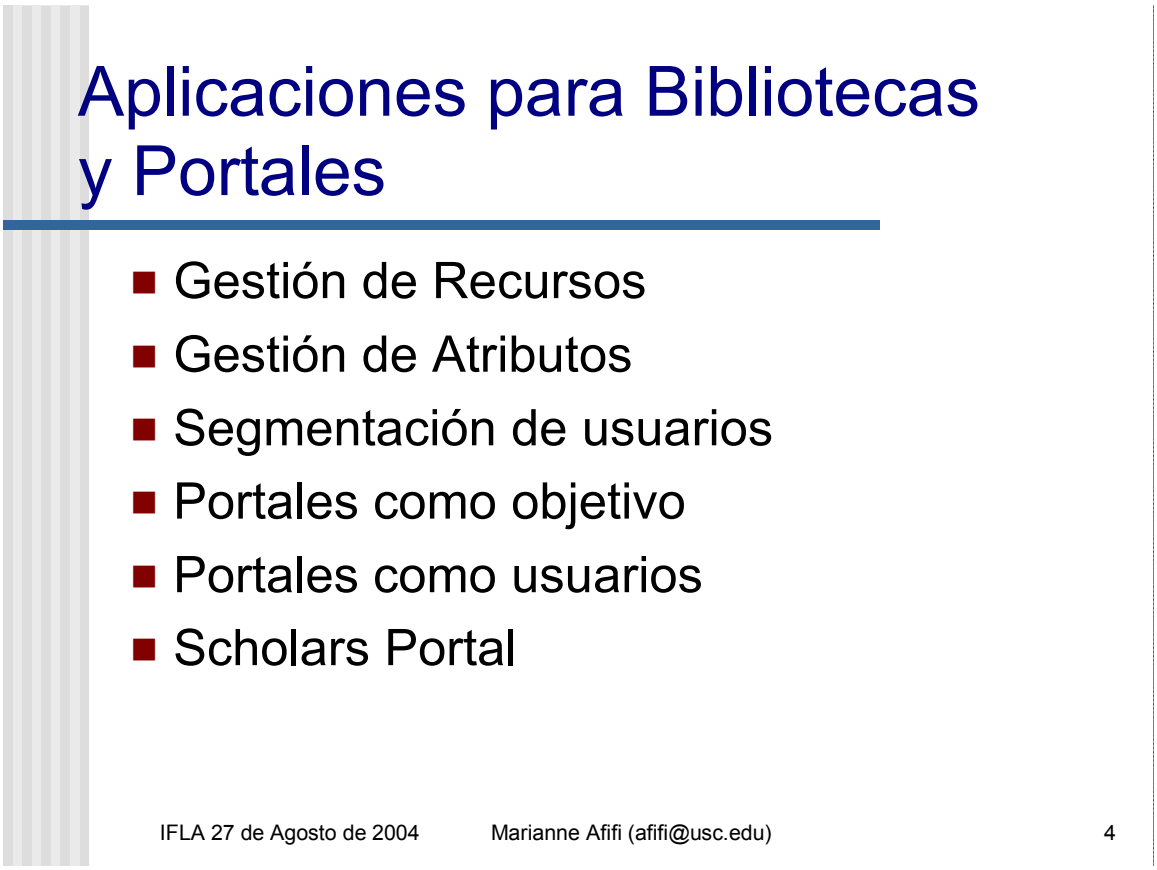


Figura 1. Diagrama cortesía del Dr. Ken Klingenstein, Internet2 de una presentación ofrecida en la Conferencia de la Coalition of Networked Information (CNI) Task Force en abril de 2004 basada en una demo SWITCH (Swiss Education and Research Network).

Aunque la descripción de lo que ocurre entre bastidores puede parecer compleja, la interacción entre varios servicios está prevista totalmente en un entorno web y proporciona un acceso rápido e integrado a los recursos.



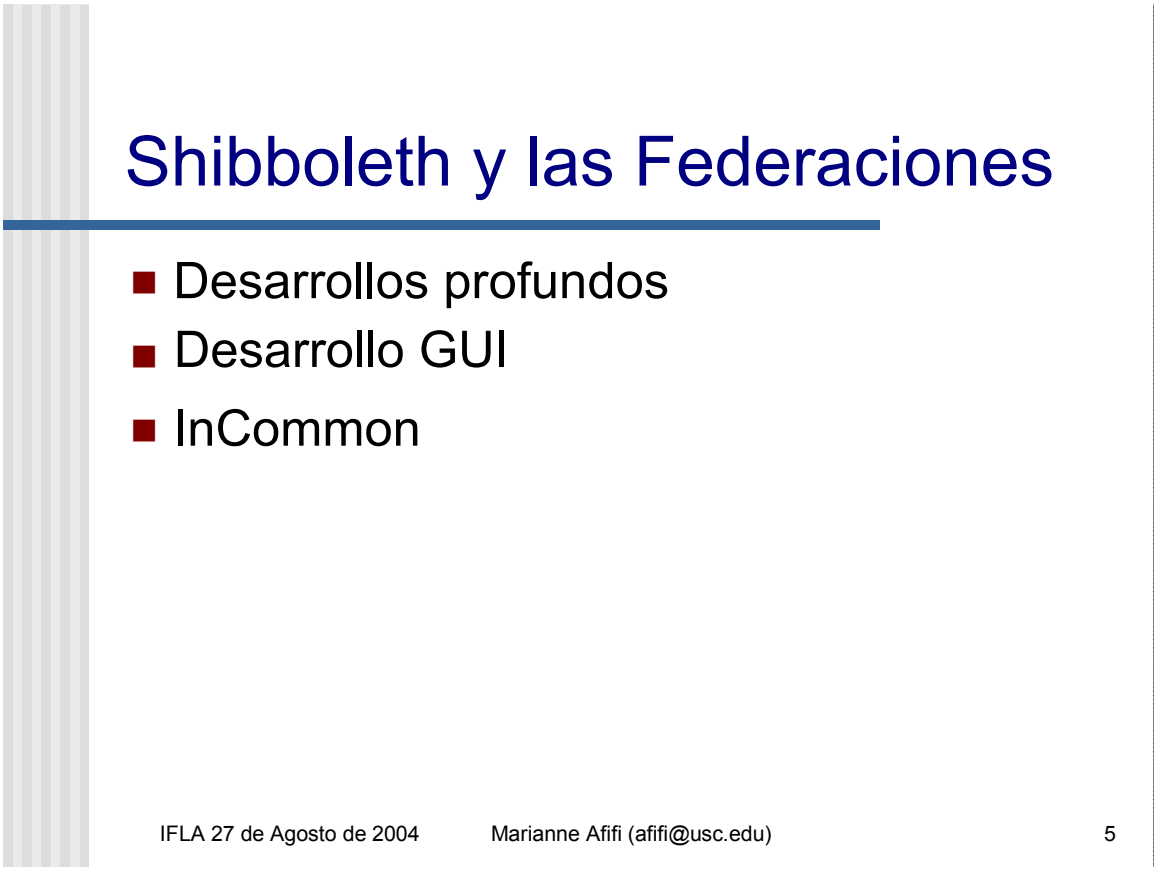
Dos conceptos fundamentales surgen del diagrama: el origen y el destino. Estos conceptos son importantes porque, como veremos los portales pueden desempeñar cualquier papel. El origen es donde reside el Handle Service y el Attribute Autorithy y el objetivo es el recurso. Ambos, el Handle Service y el Attribute Authority, se basan en datos almacenados en la base de datos del usuario de origen (de la institución) que gestiona y controla la información del usuario. Esta información está destinada a lo que el recurso necesita saber sin relevar información de lo que no necesita conocer, como sucede ahora con otros métodos de autenticación. La interacción preserva la privacidad del usuario ya que el gestor de recursos sólo necesita conocer ciertos atributos sobre el usuario, mientras que los actuales métodos de autenticación revelan más información sobre el usuario de la que es necesaria.

Shibboleth y los Portales

Las características de un portal son que la información y los datos se recuperan de varios sistemas y fuentes y se combinan en un entorno web de forma que la información concreta de un grupo de usuarios o un usuario individual se presenta bien automáticamente o bien bajo demanda. Además a los usuarios se les ofrecen servicios como correo electrónico, chat y novedades a través del portal. Las bibliotecas han desarrollado ampliamente estos portales para ofrecer una única fuente para los servicios y recursos bibliotecarios tales como los buscadores temáticos, los metabuscadores y los servicios de referencia en línea.

Don Gourley del Washington Research Library Consortium [viii] ha escrito recientemente un artículo sobre Shibboleth y los portales de bibliotecas y ha presentado algunos escenarios y funciones posibles para ese tipo de portales. En su artículo propone el portal de la biblioteca como un objetivo para Shibboleth.

Un ejemplo de portal que se utiliza como objetivo es el Scholars Portal. Este Portal es un proyecto de ARL que involucra a 7 universidades de Estados Unidos en el desarrollo de un portal metabuscador en colaboración con un distribuidor, Fretwell Downing [ix] . De las siete universidades ninguna utiliza el mismo modo de autenticación y autorización de sus usuarios. Fretwell Downing ha estado trabajando con varias instituciones para satisfacer las necesidades de autenticación de los usuarios del portal. La University of Southern California (USC), un miembro de Internet2 y que tenía implantado Shibboleth, estaba interesado en utilizarlo para el Scholars Portal. La implementación está actualmente en marcha, específicamente USC requiere que Scholars Portal (Zportal de Fretwell Downing) sea un objetivo, lo que significa que Zportal debe acomodarse a SHIRE, SHAR y RM y estar en contacto con el servicio de origen de USC. Por lo tanto los usuarios que quieren utilizar las características de personalización del Scholars Portal usarán Shibbolth para hacerlo. Sin embargo, el acceso a los recursos desde el Scholars Portal todavía se gestiona de manera clásica (principalmente mediante autenticación IP con acceso al exterior del campus a través de Virtual Private Network – VPN). Sólo cuando Zportal sea él mismo origen, y todos o la mayoría de los distribuidores de USC puedan implementar servicios destino, seremos capaces de acceder a la mayor parte de nuestros recursos del modo que Shibboleth pretende.



Shibboleth y las Federaciones

El proyecto Shibboleth se inició en el año 2000, en el 2003 fue lanzada la versión 1.1 de Shibboleth y actualmente se está siendo implementado en un número creciente de universidades y distribuidores. Se está trabajando en la próxima versión, que se supone que será lanzada este año. Futuras actualizaciones incluirán el mantenimiento del portal además de planear otras mejoras. Actualmente Shibboleth GUI Development Focus Group contribuye proporcionando requisitos y opiniones sobre la creación del Shibboleth Attribute Release Policy (ARP) Editor (SHARPE). Este Editor permitirá a las bibliotecas, dentro de una federación, gestionar los atributos de los recursos y de los servicios que actualmente manejan.

Para aprovechar bien Shibboleth, se deben crear entornos federados entre las instituciones participantes que establezcan una infraestructura de empresa con el fin de que la gestión y el acceso a los recursos mejoren en gran medida. Para este fin se desarrolló InCommon que también es un proyecto de Internet2. "InCommon es una federación formal de organizaciones dirigida a la creación de una estructura común para empresas en apoyo a la investigación y la educación. El principal propósito de la federación es facilitar la colaboración a través del intercambio de recursos protegidos, por medio de un estructura de empresa común" [x]. Mientras sólo hay unas pocas federaciones vigentes y su proceso de constitución aún está dando sus primeros pasos, nosotros esperamos que se creen cada vez más ya que este modelo de empresas presagia facilitar el acceso y preservar la privacidad de los usuarios.

Shibboleth cambiará el modo de interacción de diversas comunidades en la red y el modo de acceder a los nuevos tipos de recursos. Es fácil imaginar que surgirán nuevos modelos de comunicación entre instituciones en un entorno privado y seguro.

Más información

- Shibboleth
  - http://shibboleth.internet2.edu//
- SWITCH Authentication and Authorization Infrastructure(AAI)
  - http://www.switch.ch/aai/
- Scholars Portal —
  - http://www.arl.org/access/scholarsportal/
- InCommon —
  - http://www.incommonfederation.org/index.cfm
- Contact: Marianne Afifi —afifi@usc.edu

[1] Shibboleth Frequently Asked Questions (FAQ)
http://shibboleth.internet2.edu/shib-faq.html#001
Nate Klingenstein
4 May, 2002
Retrieved 2/10/04

[ii] NSF Creation and Mission
http://www.nsf.gov/home/about/creation.htm
Retrieved 4/15/04

[iii] About Internet2®
http://www.internet2.edu/about/aboutinternet2.html
21 April 2004, Retrieved April 21, 2004

[IV] Internet2 web site
http://middleware.internet2.edu/
Retrieved March 30, 2004

[v] Cross-organizational Use of Networked Information Resources
Clifford Lynch, editor (cliff@cni.org)
Coalition for Networked Information
Revised Discussion Draft of April 14, 1998
http://www.cni.org/projects/authentication/authentication-wp.html
Retrieved April 21, 2004

[vi] Ibid.

[vii] EduPerson Specification (200312)

http://www.nmi-edit.org/eduPerson/internet2-mace-dir-eduperson-200312.html
Retrieved May 21, 2004
viii Library Portal Roles in a Shibboleth Federation Don Gourley, Washington Research Library Consortium (WRLC), 30 October 2003 http://shibboleth.internet2.edu/docs/gourley-shibboleth-library-portals-200310.html
Retrieved April 21, 2004
ix The Scholars Portal Project. http://www.arl.org/access/scholarsportal/
Retrieved April 21, 2004
x InCommon Home Page
http://www.incommonfederation.org/index.cfm
Retrieved April 15, 2004