UMU-PKIv6: Una infraestructura de certificación avanzada

UMU-PKIv6: An Advanced Public Key Infrastructure

O. Cánovas, A. F. Gómez-Skarmeta, G. López, G. Martínez

La Universidad de Murcia ha desarrollado una solución de PKI capaz de ofrecer tanto servicios de certificación básicos, como servicios avanzados, entre ellos el sellado de tiempo o la validación on-line

Resumen

La Universidad de Murcia ha desarrollado una solución de PKI capaz de ofrecer servicios de certificación básicos, como la emisión, renovación y revocación de certificados de clave pública, así como servicios avanzados, entre ellos el sellado de tiempo o la validación on-line. Además de estos, otras características hacen muy interesante esta solución, como son el uso de tarjetas inteligentes, la certificación cruzada o el soporte del protocolo IPv6. Esta PKI, denominada UMU-PKIv6, es una solución idónea para todas aquellas organizaciones que deseen ofrecer a sus usuarios seguridad en las comunicaciones y protección de datos.

Palabras clave: PKI, IPv6, OCSP, TSP, SCEP, X509, LDAP

Summary

The University of Murcia has developed a solution of PKI able to offer basic certification services, as the issuance, renewal and revocation of public key certificates, as well as advanced services, among them are time stamping or on-line validation. Beside these, other characteristics make very interesting this solution, like the use of smart cards, cross-certification, or the IPv6 support. This PKI, called UMU-PKIv6, is a suitable solution for all those organization that want to offer secure communications and data protection to their users.

Keywords: PKI, IPv6, OCSP, TSP, SCEP, X509, LDAP

1.- Introducción

Debido a la gran cantidad de proyectos sobre seguridad y comercio electrónico en los que se está viendo involucrada la Universidad de Murcia, ha sido necesario el desarrollo de varias aplicaciones que permitan dar soporte a estos proyectos. Una de estas aplicaciones es la Infraestructura de Clave Pública (PKI) UMU-PKIv6, que se está desarrollando dentro de los proyectos Euro6IX European IPv6 Internet Exchanges Backbone e ISAIAS[1].

Una PKI es un conjunto de herramientas que permiten gestionar de modo completo el ciclo de vida de los certificados de identidad basados en el estándar X.509v3, ofreciendo servicios de certificación a usuarios y servicios para proteger sus comunicaciones. Mediante sus servicios, un usuario podrá realizar cualquier tipo de operación desde su propio navegador: solicitar un certificado, renovarlo, revocarlo, buscar el certificado de otro usuario con el cual desea establecer una comunicación segura, etc.

Las principales características que se ofrecen son las siguientes:

- Permite realizar operaciones de emisión, renovación y revocación de certificados de clave pública.
- Uso de directorio LDAP para el almacenamiento de certificados y listas de revocación.
- Operaciones de certificación desde el propio navegador o acudiendo a la Autoridad de Registro.
- Soporte de tarjetas inteligentes para usuarios.
- Definición de una política que establece restricciones en el funcionamiento de la PKI.
- Está desarrollada completamente en Java, lo que permite el uso de cualquier plataforma.

[1] Trabajo parcialmente financiado por los proyectos: Euro6IX: European IPv6 Internet Exchanges Backbone IST-2001-32161 ISAIAS TIC2000-0198-P4-04 - CICYT.

- Esta basada en los estándares definidos por el IETF dentro de su grupo de trabajo PKIX.
- Soporte del clientes VPN: protocolo SCEP[5] y routers 6WIND.
- Soporte para estándares OCSP (On-line Certificate Status Protocol) [6] y TSP (Time Stamp Protocol) [1].
- Certificación cruzada jerárquica y "peer-to-peer".
- Soporta comunicaciones IPv4 o IPv6 entre todos los componentes.

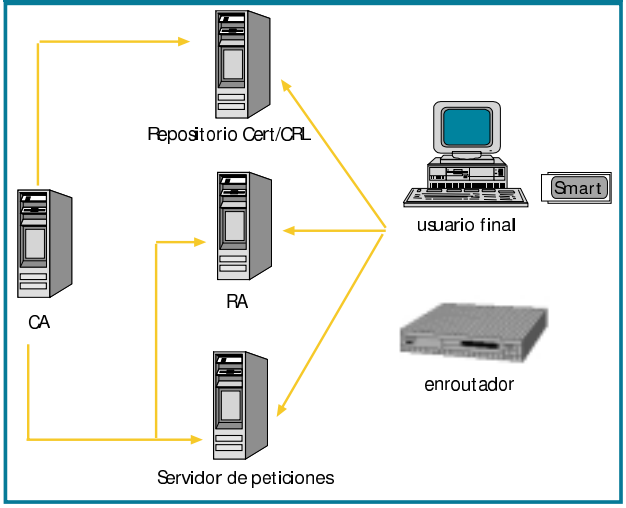
Esta infraestructura soporta el uso de tarjetas inteligentes, en las entidades RA y CA y también en entorno web

2.- Servicios básicos y componentes

UMU-PKIv6 permite a los usuarios realizar los servicios básicos que toda PKI debe ofrecer, estos son los servicios de generación de certificados, que permiten emitir solicitudes desde una RA o directamente por el usuario final a través del navegador web, recuperación de certificados, de modo que un usuario pueda recuperar su certificado o el de otro usuario en cualquier momento, emitir solicitudes de renovación, cuando el usuario desee renovar su certificado, y emitir solicitudes de revocación.

La figura 1 muestra los componentes que forman UMU-PKIv6.

FIGURA 1: ENTIDADES UMU-PKIv6



- *Autoridad de Registro (RA)*. Es la primera entidad de contacto con la infraestructura de certificación. Su función principal es la de validar e identificar a los usuarios que solicitan alguno de los servicios que ofrece la infraestructura. Para realizar sus funciones toma en consideración las opciones determinadas por la política de certificación del sistema.
- *Servidor de solicitudes*. Se encarga de almacenar todas las solicitudes de servicio realizadas por la Autoridad de Registro. Dichas solicitudes serán posteriormente recuperadas por la Autoridad de Certificación para tramitarlas como corresponda.
- *Autoridad de Certificación (CA)*. Entidad encargada de tramitar las solicitudes de servicio realizadas por ciertas entidades del sistema. En general, está encargada de emitir los certificados digitales del sistema, las listas de revocación, firmar las políticas de certificación, y publicar la información en los repositorios de datos tanto internos como públicos.
- *Repositorio público de certificados*. Dicha entidad almacena los certificados digitales y las listas de revocación de certificados emitidas por la CA.
- *Base de datos interna*. Almacena las solicitudes emitidas por la infraestructura.
- *Tarjetas Inteligentes*. Esta infraestructura soporta el uso de tarjetas inteligentes, en las entidades RA y CA y también en entorno web. Los usuarios podrán tener estas tarjetas inteligentes para almacenar su certificado y clave y el certificado de la CA.

El servicio de sellado digital de documentos, TSP, asocia una marca temporal confiable a cualquier tipo de documento

- *Administrador*. Es la entidad encargada de la configuración de los parámetros de funcionamiento de la infraestructura. Entre dichos parámetros se encuentra la política de la PKI.
- *Política de PKI*. Los administradores del sistema tienen el derecho para establecer la política de seguridad que rige el funcionamiento de la infraestructura. Ésta será un reflejo de las prácticas de certificación establecidas por la organización.

3.- Servicios avanzados

UMU-PKIv6 ofrece una serie de servicios de valor añadido destinados a enriquecer más la gama de posibilidades que ofrece la infraestructura.

El servicio de sellado digital de documentos, TSP, asocia una marca temporal confiable a cualquier tipo de documento. Según este protocolo, el resumen digital de los documentos a sellar se le envía al servidor de tiempo con el fin de obtener una sentencia firmada digitalmente por dicho servidor que establezca una vinculación temporal entre dicha información y el instante en el que fue enviado al servidor.

El servicio OCSP fue incluido para dotar al sistema de una mayor precisión a la hora de determinar la validez de un certificado de la que proporciona el uso de las tradicionales CRLs. Con OCSP el usuario o servicio obtiene una validación instantánea del estado en el cual se encuentra el certificado al que se está haciendo referencia.

4.- Certificación cruzada

UMU-PKIv6 permite definir relaciones de confianza entre dominios gestionados por diferentes Autoridades de Certificación. Estas relaciones de confianza pueden ser jerárquicas, de modo que una CA puede permitir CAs subordinadas que expandan la infraestructura, o también pueden establecerse relaciones entre CAs raíces, que son totalmente independientes; estas relaciones de confianza se denominan certificación cruzada "peer-to-peer".

Las figuras 2 y 3 muestran los tipos de certificación cruzada que son soportados

FIGURA 2: CERTIFICACIÓN CRUZADA JERÁRQUICA

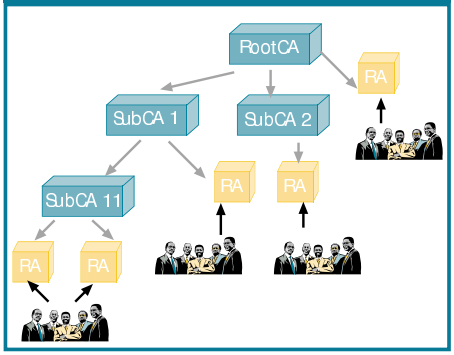
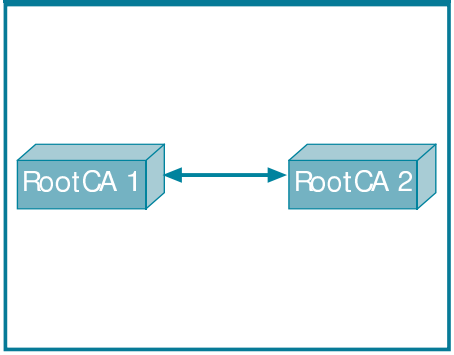


FIGURA 3: CERTIFICACIÓN CRUZADA "PEER-TO-PEER"



5.- Conclusiones

En este artículo se ha presentado una solución de PKI desarrollada por la Universidad de Murcia. Esta infraestructura se caracteriza por ofrece servicios básicos y avanzados de certificación, siendo un sistema flexible y adaptable a cualquier organización que desee ofrecer a sus usuarios seguridad en las comunicaciones. Hay que destacar el uso de políticas de certificación para la gestión del sistema y el uso de Tarjetas Inteligentes, que aporta gran movilidad a los usuarios. También hay que destacar el uso de estándares como OCSP, TSP, el soporte para dispositivos VPN que puede interactuar directamente con el sistema y el soporte IPv6.

Hay que destacar el uso de políticas de certificación para la gestión del sistema y el uso de Tarjetas Inteligentes, que aporta gran movilidad a los usuarios

6.- Bibliografía

[1] C. Adams, P. Cain, D. Pinkas y R. Zuccherato. *Time Stamp Protocol*. RFC 3161, Agosto 2001.
[2] ANTS-CIRCuS Web Pages, ANTS Research Group, http://ants.dif.um.es/circus
[3] O. Cánovas, A. F. Gómez y G. Martínez. "A PKI Scenario for High-Security Communications: Re-issued Certificates", en *Proc. of the eBusiness and eWork 2000 Conference (EMMSEC 2000)*, Octubre 2000.
[4] R. Housley, W. Ford y D. Solo, *Internet Public Key Infrastructure, X.509 Certificate and CRL Profile*, Request for Comments (RFC) 3280, Abril 2002.
[5] X. Liu et al. *Simple Certificate Enrollment Protocol*. IETF draft. draft-nourse-scep-06.txt, Mayo 2002.
[6] M. Myers et al. *Online Certificate Status Protocol*, Request For Comments (RFC) 2560, Junio 1999.

O. Cánovas
(ocanovas@ditec.um.es)
Dpto. Ingeniería y Tecnología de Computadores
A. F. Gómez-Skarmeta
(skarmeta@dif.um.es)
G. López
(gabilm@dif.um.es)
G. Martínez
(gregorio@dif.um.es)
Dpto. Ingeniería de la Información
y las Comunicaciones
Universidad de Murcia