Análisis de infraestructuras de certificación cruzada

Analysis of Cross-Certification Infrastructures

G. López Millán, G. Martínez Pérez y A. F. Gómez Skarmeta

Resumen

La certificación cruzada jerárquica se adapta bien a grandes organizaciones que quieren que su CA raíz tenga control directo sobre el resto de CAs subordinadas. Sin embargo, las certificaciones cruzadas peer-to-peer y bridgeCA encajan mejor en organizaciones donde es necesario un cierto nivel de flexibilidad para establecer y eliminar relaciones de confianza con otras organizaciones bajo demanda. Además, ambas aproximaciones encajan mejor con los modelos de redes inter-dominio de los que se hace uso en Internet. En este contexto, este artículo presenta un caso de estudio basado en los requerimientos de una red de investigación pan-europea compuesta por un conjunto de organizaciones que tienen previamente definida su propia PKI y que quieren establecer relaciones de certificación entre ellas.

Palabras clave: Infraestructura de Clave Pública, Cross Certification, Bridge CA, Peer-to-Peer.

Summary

Hierarchical cross-certification fits well within large organizations that want their root CA to have direct control over all subordinate CAs. However, both the peer-to-peer cross-certification and Bridge CA models suits better than the hierarchical one with organizations where a certain level of flexibility is needed to form and revoke trust relationships with other organizations. It seems that this second approach better fits the current and next-generation inter-domain networking Internet models. In this context, this paper presents a case of study based on the requirements provided by a Pan-European research communication network composed by a set of organizations that may have their own PKIs running, and that are interested to link with others in terms of certification services.

Keywords: Public Key Infrastructure, Cross Certification, Bridge CA, Peer-to-Peer.

Las relaciones de confianza entre PKIs pueden establecerse siguiendo principalmente los siguientes modelos: jerárquico, peer-to-peer y bridgeCA

1.- Introducción

Las relaciones de confianza entre PKIs [1] pueden establecerse siguiendo principalmente los tres modelos siguientes: jerárquico, peer-to-peer y bridgeCA [2]. Cada modelo está pensado para un entorno en el cual el tipo de confianza será más o menos centralizada, distribuida o duradera.

El modelo jerárquico encaja bien en grandes organizaciones, en las que una CA raíz quiere tener control directo sobre los usuarios y CA subordinadas. Esta solución es sencilla de poner en marcha, pero no escala bien cuando entran en juego organizaciones externas. El modelo peer-to-peer, por su parte, está pensado para esta última situación, en la cual diferentes organizaciones quieren establecer relaciones de confianza entre sí. Este modelo escala mejor, pero tiene el problema del incremento en el número de relaciones, dado que para n entidades se pueden llegar a establecer n(n-1)/2 relaciones, y por lo tanto aumenta la complejidad de gestión. Para conseguir la escalabilidad del segundo modelo, sin provocar un excesivo incremento en el número final de relaciones, se definió el modelo denominado de bridgeCA, en el cual existe una CA independiente como punto central de confianza.

El objetivo de este artículo es establecer relaciones de confianza, basadas en los modelos peer-to-peer y bridgeCA dentro de un escenario que simule un entorno real de comunicaciones inter-dominio. El entorno elegido ha sido el proyecto Euro6IX (http://www.euro6ix.org). Esta red, que conecta distintos IXs, ISPs y usuarios sobre IPv6, requiere el establecimiento de servicios [3] que serán compartidos entre cada dominio, de modo que será necesario el establecimiento de relaciones de confianza entre las entidades participantes para poder dotar a dichos servicios de un nivel adecuado de protección.

Dependiendo del tipo de entidad, y las relaciones que necesita establecer con el resto de entidades, se definen dos niveles de relaciones: por un lado, First Level Security Domain (FLSD), que se establecerá

entre dos nodos IX, y se usará cuando se trate de dos entidades bien conocidas, normalmente con intereses mutuos y con una relación estable. Por otro lado, las relaciones del tipo Second Level Security Domain (SLSD), se establecerán entre un nodo IX y un proveedor de red. Estas relaciones vendrán dadas por requerimientos políticos o de negocio y suelen ser más débiles que las primeras.

2.- Definición de un modelo de federación de PKIs

En el escenario definido se supone que cada dominio de seguridad tiene su propia PKI, la cual es gestionada por su propia política interna y tiene su propio modelo (plano, jerárquico o peer-to-peer).

Se propone una solución basada en dos niveles. El primer nivel se basa en un modelo de bridgeCA (BCA) y establece relaciones entre dominios de seguridad FLSD y el segundo en certificación peer-to-peer entre aquellos dominios que tienen una relación de confianza débil o SLSD.

En este contexto sólo se proponen los modelos BCA y peer-to-peer. Cada relación establecida basada en certificación cruzada entre dos dominios necesita ser definida por las organizaciones involucradas a través de un acuerdo mutuo sobre los servicios de seguridad. Por ejemplo, el dominio FLSD-A podría permitir autenticación desde FLSD-B, pero no desde FLSD-C. Estos requisitos deben ser definidos previamente y estar especificados en las extensiones que portan los certificados cruzados emitidos para definirla.

El diseño propuesto debe asegurar que el camino de certificación entre dos dominios que tienen una relación de confianza puede ser construido y validado en tiempo real

3.- Servicios de certificación requeridos

El diseño propuesto debe asegurar que el camino de certificación entre dos dominios que tienen, directa o indirectamente, una relación de confianza puede ser construido y validado en tiempo real. Para conseguir esto es necesario que cada dominio cumpla unos requerimientos. Estos incluyen recomendaciones sobre servicios que deben ser ofrecidos por cada dominio, extensiones en los certificados, protocolos y aplicaciones.

En primer lugar, servicios de PKI. Cada dominio deberá ofrecer un servicio de validación (SV), basado en [4], que permitirá a las partes confiables delegar el proceso de construcción y validación de un certificado a un servicio específico. El SV recibirá peticiones de validación preguntando si un certificado es confiable o no, y será capaz de construir y validar el camino de certificación y decidir sobre él. Además, servicios de repositorio como LDAP o DNSsec deben ser utilizados para contener la información pública de un dominio. Por último, cada dominio deberá soportar un protocolo de gestión de claves, como CMC [5] o CMP [6], capaz de gestionar el ciclo de vida de los certificados.

En segundo lugar, las restricciones a los caminos de certificación son normalmente definidas como extensiones de los certificados que establecen la relación, como se comentará más adelante y en tercer y último lugar, se recomienda el uso de protocolos para construir y validar los caminos de certificación, como DVCS [7], SCVP [8] o OCSP [9].

4.- Gestión de caminos de certificación

Supongamos que el usuario Bob, en un dominio SLSD-C recibe un mensaje protegido con una clave privada de Alice, que se encuentra en el dominio SLSD-A. Bob confiará en el certificado de Alice si existe un camino de certificación entre Alice y una entidad confiable de Bob, y además, si ese camino es válido. Suponiendo que el camino entre Bob y Alice tiene la siguiente forma:

CA (SLSD-C) –> CA (FLSD-1) –> BCA (Euro6IX) –> CA (FLSD-2) –> CA (SLSD-A) –> C(Alice), donde CA (SLSD-X) representa la CA del dominio SLSD-X y las flechas indican relaciones de confianza, este camino debe ser descubierto y validado por el servicio de validación (SV) del dominio SLSD-C.

Para descubrir este camino se hace uso de un algoritmo de construcción de caminos. En una secuencia normal, SLSD-C debería obtener dónde está localizada la información de certificación de CA(SLSD-A), esta información podría estar almacenada en la extensión AuthorityInformationAccess. El SV debe validar esta parte de la cadena, chequeando periodos de validez, emisor, estado, etc.. Para ello, las CRLs pueden ser recuperadas usando las extensiones AuthorityInformationAccess o SubjectInformationAccess, que pueden apuntar a un repositorio LDAP o servidor DNSsec. Para obtener la siguiente CA en el camino de validación, CA(FLSD-2), el servicio SV debe decidir la siguiente CA de la lista de certificaciones cruzadas que tiene CA(SLSD-A), pudiendo esta información estar almacenada, por ejemplo, en el repositorio LDAP, usando para ello atributos específicos. La decisión correcta dependerá del algoritmo usado, que deberá ser capaz de detectar ciclos en el camino y también certificados repetidos.

La validación del camino depende de las extensiones de los certificados que forman la cadena de certificación

Esta secuencia debe continuar hasta que un certificado confiable aparezca en el camino, o hasta que éste acabe con un certificado no confiable. La validación del camino depende de las extensiones de los certificados que forman la cadena de certificación que se analizan en el siguiente apartado.

5.- Requerimientos de Certificación

La siguiente tabla resume las principales extensiones de certificación.

	CA Cross-Cert.Root	CA (BCA/FLSD/SLSD)	End User
CRLDistributionPoint	M	M	M
AuthorityInformationAccess	M	M	M
BasicConstraints	M	M	N
KeyUsage	M	M	O
NameConstraints	M	R	N
PolicyMappings	R	R	N
CertificatePolicies	R	R	R
SubjectInformationAccess	R	R	R
SubjectAlternativeName	O	O	R
PolicyConstraints	O	O	O

Tabla 1: M=obligatorio, R=recomendado, O=opcional, N=no recomend

- CRLDistributionPoint: debe aparecer en cada certificado para asegurar que el proceso de validación pueda acceder a las CRLs del dominio que emite el certificado.
- AuthorityInformation Access/SubjectInformation Access: se considera obligatoria y sirve para localizar los certificados de CA y de certificación cruzada de un dominio.
- BasicConstraints: debe aparecer sólo en certificados de CA y debe indicar la longitud del camino de certificación como optional, de modo que no se limite su longitud.
- KeyUsage: obligatoria en cada certificado de CA para dar prioridad en los caminos de certificación.
- NameConstraints: debe aparecer en cada certificado cruzado; se usa para limitar los nombres de CAs subordinadas y para excluir posibles organizaciones en la autenticación.
- CertificatePolicies: recomendado; indica la política bajo la cual se ha emitido.
- PolicyMapping: usa la extensión anterior para mapear diferentes políticas de certificación, de modo que se puedan establecer relaciones de equivalencia, que son muy útiles para validar el certificado.
- PolicyConstraints: usada para controlar las políticas en una cadena de certificación; puede usar los atributos inhibitPolicyMapping para asegurar que la extensión anterior sea tenida en cuenta hasta un determinado nivel, o requireExplicitPolicy para forzar a los elementos del camino a tener una política confiable.

6.- Conclusiones y vías futuras

Este artículo describe un caso de estudio donde las relaciones entre dominios de seguridad son establecidas para obtener un modelo de confianza basado en el concepto de federación de PKIs, usando como escenario una red real de comunicación inter-dominio a nivel europeo.

Si estos acuerdos se llevan a cabo entre entidades que desean una colaboración mutua y estable, nuestro diseño recomienda el uso de un modelo bridgeCA, consiguiendo una reducción de sobrecarga típica de los modelos peer-to-peer. Si, por el contrario, estas relaciones están basadas en acuerdos que pueden variar con el tiempo, el modelo peer-to-peer resulta más adecuado.

Una vez establecido el modelo de relación, se proponen tanto una serie de recomendaciones sobre el contenido que deben llevar los certificados que definen el modelo como recomendaciones para construir y validar los caminos de certificación que definen la confianza entre los sitios involucrados.

Este escenario se ha diseñado usando como PKI la implementación realizada por la Universidad de Murcia (http://pki.umu.euro6ix.org). Como vía futura, se está trabajando en un entorno de confianza similar para ambientes de roaming, donde un usuario puede desplazarse entre diferentes dominios. Además, se definen las bases para futuros trabajos que integren certificación cruzada con aplicaciones y servicios que basados en sistemas de gestión de confianza X.509.

Este trabajo ha sido parcialmente financiado por los proyectos SENIT IST-2002-001929 y Euro6IX IST-2001-32161.

Este artículo describe un caso de estudio donde las relaciones entre dominios de seguridad son establecidas para obtener un modelo de confianza basado en el concepto de federación de PKIs

Referencias

1.- Housley, R., Polk, W., Ford, W., Solo, D.: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile. Request For Comments RFC 3280. IETF (2002)
2.- Lloyd, S. (ed.): CA-CA Interoperability. PKI Forum (2001)
3.- Gómez, A.F., Martínez, G., Cánovas, O., López, G.: PKI Services for IPv6. IEEE Internet Computing, Vol. 7 (2003) 36-42
4.- Cooper, M., Dzambasow, Y., Hesse, P., Joseph, S., Nicholas, R.: Internet X.509 PKI: Certification Path Building. Internet Draft draft-ietf-pkix-certpathbuild-04.txt. IETF (2004)
5.- Myers, M., Liu, X., Schaad, J., Weinstein, J.: Certificate Management Messages over CMS. Request For Comments RFC 2797. IETF (2000)
6.- Adams, C., Farrell, S.: Internet X.509 Public Key Infrastructure Certificate Management Protocols. Request For Comments RFC 2510. IETF (1999)
7.- Pinkas, D., Housley, R.: Delegated Path Validation and Delegated Path Discovery Protocol Requirements. Request For Comments RFC 3379. IETF (2002)
8.- Malpani, A., Housley, R., Freeman, T.: Simple Certificate Validation Protocol (SCVP). Internet Draft draft-ietf-pkix-scvp-15.txt. IETF (2004)
9.- Myers, M., Ankney, R., Malpani, A., Galperin, S., Adams, C.: X.509 Internet PKI Online Certificate Status Protocol – OCSP. Request For Comments RFC 2560. IETF (1999)

Gabriel López Millán, Gregorio Martínez Pérez,
(gabilm@dif.um.es),(gregorio@dif.um.es),
Antonio F. Gómez Skarmeta
(skarmeta@dif.um.es)
Dpto. de Ing. de la Información y las Comunicaciones
Universidad de Murcia