Cuando la seguridad trasciende las fronteras o sobre como manejar el problema de la autenticación para el acceso internacional de recursos distribuidos

Lic. Francisco Javier Díaz
C.C. Viviana Ambrosi
Lic. Miguel Luengo
Lic. Nicolás Macia
Mg. Lía Molinari
Lic. Paula Venosa
Calle 50 y 115 – 1er Piso – Edificio Bosque Oeste
L.I.N.T.I. - Facultad de Informática – U.N.L.P.

Área Temática: Arquitectura, redes y sistemas operativos

1. Palabras claves

GRID Computing – CA (certification authority) - Certificado digital - PMA (Policy Management Authority) - RA (Registration Authority) - PKI (Public Key Infrastructure)

2. Resumen

Como ocurrió con Internet, una vez más es la ciencia la que inicia el camino de nuevas tecnologías. La necesidad de ejecutar aplicaciones que requieren una gran capacidad de procesamiento, condujo tanto al afianzamiento de las tecnologías GRID, como a la creación de organismos internacionales que cumplan tareas de autenticación para aquellas "entidades finales" que quieran acceder (o ejecutar) estas aplicaciones.
Estas comunidades científicas, que trascienden fronteras, han tenido que desarrollar un lenguaje común, adaptarse a pautas de organización e intercambio que exigen la definición de un marco de interoperabilidad donde la seguridad juega un rol trascendental.
Si se repite el modelo de Internet, donde lo que comenzó en el mundo científico/académico hoy está incorporado a la cotidianeidad de la mayoría de la población mundial, conceptos tales como la identidad federada, autenticación a través de dominios, protocolos genéricos para servicios colectivos, organizaciones virtuales, single sign-on, deben estar en la agenda y en las líneas de trabajo de aquellos que quieren estar al tanto de las exigencias tecnológicas actuales.

3. Introducción.

La necesidad de compartir los recursos distribuidos de la tecnología GRID, es lo que exige la creación y mantenimiento de un dominio común seguro. Accesos a servicios compartidos, con autenticación, autorización, soporte para colaboración multiusuario, single sign-on, usando, además, mecanismos auditables, son esenciales para trabajar en GRID sobre ambientes seguros.
Considerando que la implementación de esta tecnología trasciende las fronteras de un país, se creó un organismo internacional, The International Grid Trust Federation (IGTF), para coordinar y administrar ese dominio de confianza.

IGTF está compuesto por tres PMAs (Policy Management Authorities) que cubren las demandas de Asia Pacífico, Europa y América.

Una PMA es una organización que establece los requerimientos y mejores prácticas para proveer identidad dentro de un proyecto y garantizar un dominio de seguridad que permita el acceso a recursos distribuidos entre diferentes organizaciones.

En el caso particular de este trabajo, esa identidad que se debe garantizar es la de aquéllos que participan en proyectos E-ScienceGrid.

La mayoría de las infraestructuras GRID, y entre ellas las que usan middleware EGEE/LCG, necesitan certificados X.509. Cada usuario, sistema o servicio debe tener un certificado para la autenticación. Esto exige que cada certificado sea firmado por una autoridad de certificación (de ahora en más, CA) que garantiza que ese certificado pertenece a la entidad. Por ello, las PMAs coordinan una infraestructura de clave pública (PKI, Public Key Infrastructure) para las CAs que proveen identidad a las entidades participantes en la Grid, en lo que es el middleware de autenticación. Es decir: las PMAs tienen la responsabilidad de acreditar a las CAs que emiten certificados digitales que serán utilizados para autenticación en la GRID.
Dentro de ese marco la PMA define los llamados requerimientos mínimos (minimun requirements) que garantizan la emisión de certificados confiables y su administración, acredita que las CAs cumplan con esos requerimientos y mantiene una estructura de "referato" sobre las cuestiones que van surgiendo para su incorporación a las mejores prácticas.

Una organización que desee acreditar como CA debe seguir un proceso de acreditación ante la PMA correspondiente. Por ello, una de las responsabilidades de las PMAs es publicar todo lo necesario para guiar este proceso de acreditación.

Cabe aclarar que la PMA no emite certificados para entidades finales ni define políticas para transacciones financieras o con fines de lucro. Tampoco es su responsabilidad definir políticas y prácticas sobre autorización, encriptación, etc.

Para asegurar que las CAs operan de acuerdo a los requerimientos mínimos definidos y los procedimientos aprobados, las PMAs tienen el derecho de auditar a las CAs.

TAGPMA (Americas PMA) cubre América desde Canadá al extremo sur del continente (Argentina y Chile). Fue creada en el 2005 y coordinará, además de las CAs ya en funcionamiento, aquéllas que se preveen surgirán en Latinoamérica en el contexto del proyecto EELA. Este proyecto tiene como objetivo establecer un Grid Testbed común e interoperable entre recursos de América Latina y Europa. La infraestructura Grid debe basarse en el middleware EGEE e interoperar con la infraestructura EGEE.

Un inconveniente común en PKI es donde encontrar los certificados de la CA que necesitan los browsers de los usuarios.
TERENA (Trans Europa Research and Education Networking Association) solucionó este problema a través de **TACAR** (**T**ERENA **A**cademic **CA R**epository), un repositorio de certificados raíz de CAs, donde además publican las respectivas CP/CPS.

En Grid, las llamadas relying parties, es decir, aquellos que reciben certificados (personas, hosts, servicios) aumentan día a día. En Europa está EGEE con 222 sitios, DEISA con 11, SEE-GRID en 10 países, entre otros como UK e-Science, IrisGrid, etc. En América podemos citar EELA con 24 participantes, OSG con 54 sitios, TEraGrid con 9, y en Asia Pacífico, APGrid donde participan 10 países o Pacific Rim Applications and Grid Middleware Assembly con más de 15 sitios.

La interacción de IGTF con The Global Grid Forum (GGF) garantiza que las políticas y prácticas que se proponen son coherentes con las necesidades de la comunidad Grid. GGF agrupa a usuarios, desarrolladores y vendedores que llevan a cabo un gran esfuerzo de estandarización en grid computing. Está constituido por miles de personas tanto de la industria como del ámbito de la investigación, de más de 50 países.

4. Autoridades de Certificación y Autoridades de Registro (CAs y Ras)

Habitualmente la arquitectura general de una CA agrupa una o más RAs (Autoridades de Registración).
Las RAs realizan tareas administrativas relacionadas con el chequeo de la identidad de la entidad que requiere el certificado digital y su participación en un proyecto Grid. Vale aclarar que si bien la entidad requiere el certificado a través de un sitio Web, para validar el requerimiento el solicitante debe presentarse ante la RA para la verificación de su identidad (con documento nacional de identidad/pasaporte) y el aval del director de proyecto.

La CA debe: aceptar requerimientos de certificados, firmar los certificados aprobados, revocar los certificados cuando sea necesario y publicar las listas de certificados revocados.
En su proceso de acreditación, la CA define su llamado CP/CPS (Certificate Policy and the Certification Practice Statement) de acuerdo a la RFC 3647. El CP/CPS define un conjunto de reglas y prácticas que la CA debe respetar en la emisión de certificados. La PMA exige que éste y otros documentos que definen la operación de la CA y las RAs estén publicados en un sitio Web.

Cada CP/CPS debe tener su propio OID (object identification), de manera tal que refleje cualquier cambio que se produzca en el documento.
El prefijo del OID debe ser de una empresa privada, y puede ser obtenido desde el IANA.

La CA debe cumplir con la implementación de lo enunciado en su CP/CPS.
Para dar una idea de las exigencias técnicas que esto representa, debe considerarse que:

- El par de claves de la CA es generado por personal autorizado en una computadora NO CONECTADA a la red o bien un servidor seguro que provea un mecanismo para mantener la clave encriptada en un hardware seguro que cumpla con la norma FIPS140.
- Se debe utilizar software confiable (Open SSL, OpenCA).
- Cada parte genera su propio par de claves a través de una interfase Web.
- El certificado que contiene la clave pública de la CA se entrega a los suscriptores a través de una transacción on line desde el servidor Web, de donde se puede descargar desde el repositorio.
- La clave de la CA debe tener una longitud de 2048 bits, y debe estar protegida por una passphrase de, como mínimo, 15 caracteres.
- La llamada "CA offline", la máquina donde se generan los certificados debe estar en lugar seguro y no conectada a ninguna red. Debe estar, por lo tanto, separada de la llamada "CA online", de acceso público, donde está el repositorio de documentos, certificados válidos, listas de revocación, etc.
- Los backups deben almacenarse en lugares de acceso restringido y a prueba de fuego, inundaciones, etc.

- El sitio público de la PKI (también llamada CA on-line) debe estar protegido por un firewall, correr sólo los servicios esenciales para el proyecto, con acceso restringido y con actualización constante de lo que se requiera para garantizar la seguridad.

La CA debe permitir que las entidades puedan renovar sus certificados, cambiando sus claves o no, garantizado el menor tiempo posible de no operación. Además, debe mantener los viejos certificados para permitir las validaciones y controlar el período de validez, previniendo/notificando a las entidades finales próximos vencimientos de validez.

5. Las CAs de América Latina. Conclusiones

Este documento se inició citando a Internet como el resultado de la incesante búsqueda que la comunidad científica genera para una misión que trasciende fronteras y desdibuja los límites. Más que hablar de países, hablamos de comunidades. No obstante para sustentar esta idea de aldea global es imprescindible contar con mecanismos seguros de intercambio, que acrediten identidad sin burocracia, que permitan la interoperabilidad con una capa mínima de restricciones.

Dentro del proyecto EELA, una única CA constituiría un único punto de falla o ataque, por lo cual no es una solución viable. Además, para algunas arquitecturas de GRID, como GLOBUS-GSI, las estructuras jerárquicas o de "firma cruzada" de múltiples CAs no resultan ser la opción más adecuada. Es por ello que un grupo coordinado de CAs resultaría la opción más conveniente.
En particular, EugridPMA recomienda el establecimiento de una CA por país articuladas en una red de confianza internacional.

Las CAs de América Latina (en particular para Argentina, Brasil, Chile, México y Venezuela) están surgiendo dentro del proyecto EELA bajo la organización TAGPMA. La misma establece una serie de normas y procedimientos muy estrictos para la acreditación.
En América Latina se disparó el proceso de contar con autoridades de certificación en el marco de un workshop realizado en Madrid y Trujillo en enero de 2006.

En nuestro país, la Universidad Nacional de La Plata, a través del CesPI (Centro de procesamiento de la Información) está transitando el proceso de acreditación necesario para erigirse como CA de las actividades de E-Science de la comunidad académica argentina. Docentes e investigadores del LINTI están colaborando para que CesPI pueda lograr este objetivo.

6. Referencias

- DOEGrids Certificate Policy And Certification Practice Statement. Version 2.6. http://www.doegrids.org/Docs/CP-CPS.pdf
- Eugridpma. European Policy Management Authority for Grid Authentication http://www.eugridpma.org/
- IGTF. International Grid Trust Federation. http://www.gridpma.org/
- R. Housley, W. Ford, W. Polk and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and CRL

Profile", RFC 2459, January 1999 http://www.ietf.org/rfc/rfc2459.txt

- R. Housley, W. Polk, W. Ford and D. Solo, " Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" , RFC 3280, April 2002 http://www.ietf.org/rfc/rfc3280.txt
- S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework" , RFC 2527, March 1999 http://www.ietf.org/rfc/rfc2527.txt
- S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, " Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework" , RFC 3647, November 2003 [replaces RFC 2527] http://www.ietf.org/rfc/rfc3647.txt
- TAGPMA. The Americas Grid Policy Management Authority. http://www.tagpma.org/
- The Americas Grid. Policy Management AuthorityCharter. September 20, 2005
- . UK eScience Certification Authority Certificate Policy and Certification Practices Statement, Version 1.1, March 2005 http://www.grid-support.ac.uk/files/cps/cps-1.1.pdf
- "International Grid CA Interworking, Peer Review and Policy Management through the European DataGrid Certification Authority Coordination Group", https://www.cs.tcd.ie/coghlan/pubs/review-condensed-09042004.pdf