Universidad Nacional de La Plata

UNLP PKIGrid CA

Obligaciones de la RA

Operaciones y Estructura RA

Staff:

- Javier Díaz, CA Manager
- Maria del Carmen Lago, RA Manager
- Lía Molinari & Viviana Ambrosi, Responsables de Políticas y Procedimientos internos y externos
- Miguel Luengo, Responsable de Networking
- Nicolás Macia, Responsable de Políticas de Seguridad del Firewall y Sensores
- Paula Venosa, Responsable de Modificación y Testing de OpenCA
- Juan Pablo Giecco, Responsable de Mantenimiento del Sitio https://www.pkigrid.unlp.edu.ar
- Aldana Gómez Ríos, Responsable de Traducción Ingles-Español.

Document OID 1.2.840.113612.5.4.2.3.2.3.1.0S.

16 de noviembre de 2006

Contenidos

1 Nombre del Documento e Identificación

Título del Documento	UNLP PKIGrid CA " Estructura y Operación RA"
Versión del Documento	Versión 1.0
Fecha del Documento	28 de Abril de 2006
Estructura OID del Documento	
Asignado por IGTF	1.2.840.113612.5.4.2.3
Tipo de Documento (Procedimiento)	2
Subtipo de Documento	3
Versión	1
Sub -Versión	0S

2 Definiciones y acrónimos

Autoridad Certificante (CA)

Una autoridad a la que uno o más suscriptores confían la tarea de crear y asignar PKIs. Esa entidad/sistema emite certificados de identidad X.509.

Política de Certificados (CP)

Un conjunto de reglas designadas para indicar la idoneidad de un certificado para una comunidad y/o clase de aplicación particular con requerimientos de seguridad comunes. Por ejemplo, una política de certificado en particular puede indicar la idoneidad de un tipo de certificado para la autenticación de transacciones de intercambio de datos electrónicos.

Declaración de Práctica de Certificación (CPS)

Una declaración de las prácticas que una autoridad certificante emplea al emitir certificados.

Lista de Certificados Revocados (CRL)

Una lista con fecha de vencimiento que identifica los certificados revocados, firmada por una CA y hecha disponible libremente en un repositorio público.

RA

Autoridad Registrante.

3 Estructura RA

Una Autoridad Registrante consiste de un Administrador de RA y uno o más Operadores RA. El Administrador RA debe ser nombrado de la organización donde trabaja, y es responsable de nombrar los Operadores RA y asegurarse de que operen dentro de los procedimientos definidos por el CPS.

Los operadores verifican y registran las identidades de los suscriptores y aprueban las solicitudes de certificados. Esto es, todo el trabajo "real" de un RA.

El administrador nombra los operadores (como también notifica a la CA cuando un operador deja la institución o su cargo como operador).

El administrador es responsable de la RA, es decir, es responsable de que los operadores RA actúen de acuerdo a la política de CA, indicada en el documento CP/CPS, y el remitente definido en las cartas de nombramiento.

Un administrador también puede ser un operador. Hay una carta de nombramiento especial para que un administrador se auto-nombre operador.

Los operadores pueden o no estar en el mismo departamento que el administrador RA. Si están en un departamento diferente, el director de este departamento deberá validar la carta de nombramiento del operador.

El operador deberá actuar de acuerdo a la política y también obedecer el Acta de Protección de Datos (maneja información personal potencialmente sensible). Las cartas de nombramiento tienen que ser emitidas una vez; en particular, el director del departamento solo firmará una vez (A saber, para nombrar al administrador RA –salvo que el jefe de departamento también sea un administrador RA, pero eso no ha pasado hasta ahora).

La organización debe:

- Comunicar al CA quién será el administrador RA.
- Identificar a las personas que serán los operadores, y pedirles que contacten al administrador CA.

4 Obligaciones de la RA

Para ser aprobada internacionalmente, la CA debe operar a un nivel específico de seguridad, llamado seguro medio. Esto significa que los usuarios deben mostrar una Identificación con foto para obtener un certificado. La parte de la CA que verifica las identidades de los usuarios debe entonces estar más cerca del usuario, por lo tanto, este deber se le delega a las Autoridades Registrantes locales (RAs).

El deber de las RAs es esencialmente conservar suficiente información personal para asegurar que la identidad de un Grid pueda ser identificada con una identidad del "mundo real", incluso en una corte, y en segundo lugar, asegurarse de que esta información sea almacenada de acuerdo al Acta de Protección de Datos, es decir, que esté en un área segura.

Las RAs deben asegurarse también de que la misma identidad Grid no se emita para dos personas diferentes (con el mismo nombre), incluso si la primera persona ha dejado de usar el Grid (Principio de Unicidad de Identidad de Grid). El portal CA alerta a los operadores RA si una identidad ha sido usada con anterioridad. Si este es el caso, la información personal de solicitudes anteriores deberá ser consultada si hay alguna duda de que el solicitante es la misma persona.

El administrador RA debe:

- Acordar el nombre de la RA con el administrador CA,
- Definir la comunidad de suscriptores para los cuales la RA aprobará solicitudes, y los requerimientos en adición a los impuestos por el CP/CPS,
- Asegurarse de que sea nombrado de acuerdo a los procedimientos descritos en el CP/CPS,
- Nombrar uno o más operadores RA de acuerdo a los procedimientos descritos en el CPS,
- Asegurarse de que los operadores actúen de acuerdo a los procedimientos propuestos por la CA,
- En particular, asegurarse de que las RA almacenen todos los registros e información adicional de los suscriptores bajo seguridad, y que ésta sea revelada solo bajo las condiciones descritas en el CP/CPS,
- Proveer acceso a los historiales cuando la CA lo requiera.

El operador RA debe:

- Adherir a todas las Obligaciones del Suscriptor,
- Aceptar solicitudes de certificación de entidades autorizadas,
- Para certificados personales, verificar la identidad del Suscriptor y mantener un historial de cómo fue identificado cada Suscriptor,
- Asegurarse de que el DN sea único,
- Para tanto certificados de host y servicio, verificar que el suscriptor sea el administrador responsable del sistema para el recurso identificado por el certificado, o una persona autorizada por el administrador para solicitar un certificado,
- Proveer información al suscriptor sobre cómo mantener un certificado y su clave privada correspondiente,
- Asegurarse de que la información provista por la solicitud de certificado sea correcta;
- Firmar las solicitudes de los suscriptores cuando y sólo cuando todas las condiciones para la emisión de un certificado al suscriptor estén presentes,
- Solicitar revocación del certificado de un suscriptor cuando y solo cuando el operador RA (1) considere que las circunstancias para revocación están presentes y (2) la revocación no haya sido solicitada todavía.

Para certificados de host y servicio, la información personal recolectada por la RA deberá ser usada para identificar a administrador responsable del sistema. *Sólo* la persona responsable por un recurso puede solicitar certificados de host o servicio, *incluso* si ha puesto a otra persona a cargo de correr el servicio.

Los usuarios pueden renovar sus certificados siempre y cuando éstos no hayan expirado y no hayan sido revocados (***renovaciones***). Deberán efectuar una nueva solicitud de certificado, pero podrán probar su identidad usando su certificado actual. La RA estará involucrada en el proceso ya que la RA podrá requerir al usuario que pruebe que continúa trabajando en proyectos de Grid o e-ciencia.

Si los usuarios todavía están en posesión de su clave privada y recuerdan su contraseña, pueden solicitar una ***revocación*** de su certificado ellos mismos sin intervención alguna de la RA. En todos los otros casos, la RA deberá solicitar una revocación de los certificados de usuarios y proveer una razón para la revocación.

5 Certificado de operador de RA

Un operador RA deberá tener un certificado (y la clave privada correspondiente, sin la cual el certificado no sirve de nada).

Hay dos maneras diferentes de obtener uno:

1. La manera “normal”:

   El operador RA atenderá al curso de entrenamiento y acordará un PIN con el CA y luego, desde su casa, enviará una solicitud de certificado (habiendo aprendido cómo hacer esto en el curso) y usar su PIN acordado. La CA aprobará luego la solicitud.

2. La manera “difícil”:

   El operador RA solicitará uno antes de atender al curso de entrenamiento. Para hacer esto, deberá leer la documentación en http://www.pkiUNLPGrid.unlp.edu.ar y luego solicitar un certificado allí.

6 Presentación del suscriptor

Para que la RA pueda autenticar la identidad individual, el suscriptor debe encontrarse en persona con la RA y presentar un documento reconocido oficialmente probando la identidad de la parte dependiente. Solo documentos aceptados por la ley argentina (D.N.I, pasaporte válido, etc.) serán aceptados. El certificado de host puede ser pedido solo por el administrador responsable por el host particular. La RA solicitará que el líder del proyecto confirme que la persona que solicita el certificado es el administrador responsable por e-mail firmado o carta firmada (sección 3.2.3, Autenticación de identidad individual).

Luego de una autenticación exitosa, copias escaneadas del documento de identificación de la parte dependiente y de la solicitud de certificación deberán ser archivadas. El formato de escaneo es TIFF IV compressed, 300 dpi, escala de grises.

7 Referencia

- GOSC (Grid Operations Support Centre) Documentation - http://www.grid-support.ac.uk/
- UNLP PKIGrid CA Certificate Policy (CP) and Certification Practice Statement (CPS). Document OID 1.2.840.113612.5.4.2.3.1.0.2.1