Universidad Nacional de La Plata

UNLP PKIGrid CA

Obligaciones de la CA

Operaciones y Estructura

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.

OID Document 1.2.840.113612.5.4.2.3.2.2.1.0S.

16 de noviembre de 2006

Contenido

1. Nombre del Documento e identificación

Título del Documento	UNLP PKIGrid CA "Estructura y Operación CA"
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 (CP/CPS)	2
Subtipo de Documento	2
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 Definición de roles

Para la operación de la CA, pkUNLGrid define los siguientes roles en la estructura CA, de acuerdo a lo expresado en el CP/CPS:

a) Administrador CA
b) Administrador RA
c) Operador CA
d) Operador RA

Sobre el administrador RA y el operador RA, véase el documento "Estructura & Operación RA".

Responsabilidades del administrador CA

La CA PKIGRID es administrada por el Centro de Cómputos CeSPI de La Plata (Argentina).

El administrador CA (contacto para preguntas relacionadas con este documento de políticas) es el Director del CeSPI.

PKIGrid define las siguientes responsabilidades para el administrador CA, de acuerdo a lo expresado por el CP/CPS:

- Sección 1.5.2 , el administrador CA es la "...persona de contacto para preguntas relacionadas con este documento de políticas".
- Sección 5.3.6, Sanciones por acciones no-autorizadas, "...En el caso de que ocurra una acción no autorizada, abuso de autoridad o uso no autorizado de sistemas de entidades de parte de los operadores de CA y RA, **el administrador de CA puede revocar todos los privilegios implicados**…"
- Sección 5.3.8, Documentación entregada al personal, "Es responsabilidad del administrador de CA suministrar a los operadores CA una copia de los procedimientos del Operador CA UNLPGrid. Es responsabilidad del administrador de CA suministrar al administrador RA una copia de los procedimientos del administrador UNLPGrid…"
- Sección 5.8, terminación de la CA o RA, "...El administrador CA será responsable del archivo subsiguiente de todos los registros al momento de terminación como requerido en la sección 5.5.2. El administrador CA podrá decidir permitir que la CA emita CRLs solo durante el último año (por ejemplo, el tiempo de validez máximo del certificado de un suscriptor) antes de la terminación definitiva…"

- Sección 8.5, Acciones como resultado de deficiencia, "...En caso de una deficiencia, el administrador de la CA PKIGrid anunciará los pasos que deberán seguirse para remediar esta deficiencia…"
- Sección 8.6, Comunicación de los resultados, "...El administrador de la CA deberá hacer el resultado disponible para el público en el web site de la CA con la mayor cantidad de detalles de cualquier deficiencia como ésta crea necesario…"

Responsabilidades del operador CA

a) Es el encargado de guardar la clave privada de la CA.
b) Firma los certificados de los suscriptores.
c) Firma las CRLs.

Por lo menos 2 personas deberán poder cumplir las tareas de operador de CA (1 de 2). (sección 3.2.1. en el CP/CPS, "Número de personas requeridas por tarea ")

4 Obligaciones de la CA

La CA debe:

- Publicar un CP y un CPS, estructurado de acuerdo a RFC 3647;
- Asegurarse de que las operaciones e infraestructura se ajustan al CP/CPS;
- Emitir certificados para suscriptores dignos basada en solicitudes validadas de las Autoridades Registrantes;
- Notificar al suscriptor de la emisión del certificado;
- Publicar una lista de los certificados emitidos;
- Aceptar las solicitudes de revocación de acuerdo con los procedimientos descritos en este documento;
- Autenticar entidades solicitantes de una revocación de un certificado;
- Generar y publicar Listas de Certificados Revocados (CRLs) como descrito en el CPS;
- Identificar y publicar una lista de los servicios para los cuales un certificado es emitido;
- Producir una declaración detallada del procedimiento de acuerdo con el CPS y hacerla disponible para las RA.

5 Procedimientos de Backup

LA CA debe conservar un backup del servidor on line, el servidor off line, historiales para auditoría, las bases documentales de las copias escaneadas de la documentación presentada en la solicitud de certificación y toda información relevante para la operación de la CA.

El backup deberá hacerse en un medio removible. Estos medios removibles (USB sticks y disks) deben estar almacenados en un cuarto a prueba de fuego y con acceso restringido.

El procedimiento de backup debe ser probado para garantizar que la información sea restaurable.

Frecuencia de Backup

La CA deberá hacer los backups todas las noches.

Los historiales para auditoría deberán guardarse en un medio removible WORM cada noche. Cuando no haya actividad, esto no será necesario para el host off line (en los fines de semana, feriados o vacaciones). En el caso del host on line, incluso en los fines de semana, feriados y vacaciones, una modificación (por ejemplo, nueva publicación de CRL) será necesaria para que los historiales para auditoría sean guardados.

6 Referencia

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