Universidad Nacional de La Plata

UNLP PKIGrid CA

Obligaciones del Suscriptor

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 1.2.840.113612.5.4.2.3.2.1.1.0S

23 de Noviembre de 2006

Contenidos

Universidad Nacional de La Plata

1 Nombre del Documento e Identificación

Título del Documento	UNLP PKIGrid CA Obligaciones del Suscriptor
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	1
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.

Entidad de Destino

También llamada Suscriptor, es la persona o servidor para quien el certificado digital es emitido.

RA

Autoridad Registrante.

3 Obligaciones del Suscriptor

UNLPGrid es la infraestructura que soporta las actividades de e-ciencia de la comunidad académica argentina.

Este documento describe el conjunto de reglas y prácticas operativas que deberán ser usadas por la Autoridad de Certificación UNLPGrid. Este y cualquier documento CP/CPS subsiguiente puede ser encontrado en el sitio Web

Los suscriptores deben:

- Leer y adherir a los procedimientos publicados en este documento; generar un par de claves usando un método confiable;
- Para certificados personales, elegir un DN único (véase sección 2.1. de este documento);
- Para certificados de host y servicio, solicitar certificados solo para fuentes por las que son responsables;
- Usar el certificado para los propósitos permitidos solamente. Los certificados solo deberían ser usados o aceptados para actividades que soportan las actividades de e-ciencia. (sección 2.1.1. en el CP/CPS, "…Los certificados emitidos por los CA de PKIGrid deben ser usados solo para actividades de e-ciencia, y no han de ser usados para otras actividades como transacciones financieras...")
- Autorizar el procesamiento y la conservación de datos personales (como requerido bajo la ley de Protección de Datos)
- Tomar toda precaución posible para prevenir la pérdida, publicación o acceso no autorizado a las claves privadas asociadas al certificado, incluyendo:

  - Certificados personales: seleccionando una Contraseña Fuerte, protegiendo la Contraseña de otros;
  - Notificando inmediatamente a la CA de la UNLPGrid y otras partes dependientes si la clave privada se pierde o se halla comprometida;

- Solicitando revocación si el suscriptor ya no se halla en derecho de un certificado, o si la información en el certificado se vuelve incorrecta o imprecisa.

- El certificado de entidad de destino puede ser usado para cualquier aplicación que sea compatible con los certificados X.509, en particular:
  - Autenticación de usuarios, Hosts y servicios
  - Autenticación y encriptación de comunicaciones
  - Autenticación de e-mails firmados
  - Autenticación de objetos firmados

- La vida útil de un certificado es de 13 meses. La CA informará por e-mail 30 días antes de que el certificado expire (y luego de vuelta 7 días antes si el primero no hizo que el suscriptor reaccionara).
- Informar sobre cualquier cambio en los datos personales, en particular el cese de relación laboral con el organismo que lo presentó originalmente.
- Cuando el suscriptor solicite la renovación de un certificado, debe solicitarla al líder del proyecto enviando una confirmación de que el suscriptor sigue trabajando en el proyecto.

3.1 Sobre la presentación de un Suscriptor a la RA

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.

4 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