Universidad Nacional de La Plata

UNLP PKIGrid CA

Política de Certificados y Declaración de Práctica de la Certificación

OID del Documento 1.2.840.113612.5.4.2.3.1.0.2.7S

30 de Octubre de 2007

Contenidos

1 Introducción 9
1.1 Generalidades 9
1.2 Nombre del Documento e identificación 9
1.3 Participantes PKI 11
1.3.1 Autoridades Certificantes 11
1.3.2 Autoridades de Registro 11
1.3.3 Suscriptores 12
1.3.4 Partes Dependientes 12
1.3.5 Otros participantes 12
1.4 Uso del Certificado 12
1.4.1 Usos Apropiados del Certificado 12
1.4.2 Usos Prohibidos del certificado 13
1.5 Administración de Permiso 13
1.5.1 Organización que administra el documento 13
1.5.2 Contacto 14
1.5.3 Persona que determina la idoneidad de CPS para el permiso 14
1.5.4 Procedimientos de aprobación de CPS 14
1.6 Definiciones y Acrónimos 14
2 Responsabilidades de publicación y repositorio 19
2.1 Repositorios 19
2.2 Publicación de información de la CA 19
2.3 Frecuencia de la publicación 19
2.4 Controles de Acceso en los repositorios 20
3 Identificación y autenticación 21
3.1 Nombres 21
3.1.1 Tipos de nombres 21
3.1.2 Necesidad de que los nombres tengan sentido 21
3.1.3 Anonimidad o pseudonimidad de los suscriptores 21
3.1.4 Reglas para interpretar varias formas de un nombre 22
3.1.5 Originalidad de los Nombres 22
3.1.6 Reconocimiento, autenticación y papel de las marcas registradas 22
3.2 Validación Inicial de Identidad 22
3.2.1 Método para probar posesión de clave privada 23
3.2.2 Autenticación de la identidad de una organización 23
3.2.3 Autenticación de identidad individual 23
3.2.4 Información de suscriptores no-verificados 23
3.2.5 Validación de autoridad 23
3.2.6 Criterio de interoperabilidad 23
3.3 Identificación y autenticación de solicitud de cambio de contraseña 24
3.3.1 Identificación y autenticación para cambio de contraseña rutinario 24

3.3.2 Identification and authentication for re-key after revocation 24
3.4 Identificación y autenticación para solicitud de revocación 24
4 Requerimientos operacionales de la vida útil de un Certificado 25
4.1 Solicitud de Certificado 25
4.1.1 Quién puede solicitar un certificado 25
4.1.2 Proceso de enrolamiento y responsabilidades 25
4.2 Procesamiento de solicitud de certificado 26
4.2.1 Realizando funciones de identificación y autenticación 26
4.2.2 Aprobación o rechazo de solicitudes de certificado 26
4.2.3 Tiempo para procesar solicitudes de certificado 26
4.3 Emisión de Certificados 26
4.3.1 Acciones de los CA durante la emisión de certificados 26
4.3.2 Notificación al suscriptor por la CA acerca de la emisión del certificado 27
4.4 Aceptación de certificados 27
4.4.1 Conducta constitutiva de la aceptación de un certificado 27
4.4.2 Publicación del certificado por la CA 27
4.4.3 Notificación de emisión de certificado por la CA a otras entidades 27
4.5 Par de claves y uso del certificado 27
4.5.1 Clave privada del suscriptor y uso del certificado 27
4.5.2 Clave pública y uso del certificado de la parte solicitante 27
4.6 Renovación del certificado 28
4.6.1 Circunstancias de renovación del certificado 28
4.6.2 Quién puede pedir renovación 28
4.6.3 Procesamiento de solicitudes de renovación de certificados 28
4.6.4 Notificación de nueva emisión de certificado a suscriptor 28
4.6.5 Conducta constituyendo aceptación de un certificado de renovación 29
4.6.6 Publicación del certificado de renovación por parte de la CA 29
4.7 Cambio de contraseña de certificados 29
4.7.1 Circunstancias para el cambio de contraseñas de certificados 29
4.7.2 Quién puede solicitar certificación de una nueva contraseña pública 29
4.7.3 Procesamiento de solicitudes de cambio de contraseña de certificados 29
4.7.4 Notificación de emisión de nuevos certificados a suscriptores 29
4.7.5 Conducta constituyente de aceptación de un certificado con contraseña nueva 30
4.7.6 Publicación del certificado con nueva contraseña por la CA 30
4.7.7 Notificación de emisión de certificado de CA a otras entidades 30
4.8 Modificación de certificado 30
4.8.1 Circunstancias de modificación de certificado 30
4.8.2 Quién puede solicitar modificación de un certificado 30
4.8.3 Procesamiento de solicitudes de modificación de un certificado 30
4.8.4 Notificación de emisión de un nuevo certificado al suscriptor 30
4.8.5 Conducta constituyente de la aceptación del certificado modificado 30
4.8.6 Publicación del certificado modificado por la CA 31
4.8.7 Notificación de emisión del certificado de parte de la CA a otras entidades 31
4.9 Revocación y suspensión de un certificado 31

4.9.1 Circunstancias de revocación 31
4.9.2 Quién puede solicitar revocación 31
4.9.3 Procedimiento para solicitud de revocación 32
4.9.4 Período de gracia para solicitudes de revocación. 32
4.9.5 Tiempo dentro del cual la CA deberá procesar la solicitud de revocación 32
4.9.6 Requerimientos de chequeo de revocaciones en partes dependientes 32
4.9.7 Frecuencia de emisión de CRLs (si fuera pertinente) 32
4.9.8 Latencia máxima de CRLs (si fuera pertinente) 32
4.9.9 Posibilidad de chequeo online de status / revocaciones 33
4.9.10 Requerimientos para el chequeo online de las revocaciones 33
4.9.11 Otras formas de publicación de las revocaciones disponibles 33
4.9.12 Requisitos especiales compromiso de contraseña ya cambiada 33
4.9.13 Circunstancias para suspensión 33
4.9.14 Quién puede solicitar suspensión 33
4.9.15 Procedimiento para solicitud de suspensión 33
4.9.16 Límites del período de suspensión 33
4.10 Servicios de estado del certificado 34
4.10.1 Características operativas 34
4.10.2 Disponibilidad del servicio 34
4.10.3 Características opcionales 34
4.11 Fin de la suscripción 34
4.12 Preservación de contraseña y recuperación 34
4.12.1 Políticas y prácticas de preservación y recuperación de claves 34
4.12.2 Políticas y prácticas de encapsulamiento y recuperación de claves de sesión 35
5 Controles de lugar físico, administración y operación 36
5.1 Controles físicos 36
5.1.1 Localización y construcción 36
5.1.2 Acceso físico 36
5.1.3 Electricidad y aire acondicionado 36
5.1.4 Exposición al agua 37
5.1.5 Prevención y protección del fuego 37
5.1.6 Medios de Almacenamiento 37
5.1.7 Eliminación de residuos 37
5.1.8 Backup fuera de la CA 37
5.2 Controles de Procedimiento 37
5.2.1 Roles confiados 37
5.2.2 Número de personas requeridas por tarea 37
5.2.3 Identificación y autenticación para cada rol 38
5.2.4 Roles que requieran separación de funciones 38
5.3 Controles de personal 38
5.3.1 Calificaciones, experiencia y requerimientos de entrada 38
5.3.2 Procedimientos de chequeo de antecedentes 38
5.3.3 Requerimientos de Entrenamiento 39
5.3.4 Requerimientos y frecuencia de repetición de entrenamiento 39

5.3.5 Frecuencia y secuencia de rotación de trabajo 39
5.3.6 Sanciones por acciones no – autorizadas 39
5.3.7 Requerimientos de contra tante independiente 39
5.3.8 Documentación facilitada al personal 39
5.4 Procedimientos de historial (log) para auditoría 40
5.4.1 Tipos de eventos registrados 40
5.4.2 Frecuencia de procesamiento de historial (log) 40
5.4.3 Período de retención del historial (log) 40
5.4.4 Protección del historial (log) para auditoría 41
5.4.5 Procedimientos de backup del historial (log) para auditoría 41
5.4.6 Sistema de colección de auditoría (interno vs. externo) 41
5.4.7 Notificación a sujeto que cause evento 41
5.4.8 Medición de vulnerabilidad 41
5.5 Archivo de Registros 41
5.5.1 Tipos de registros archivados 41
5.5.2 Período de retención de archivo 42
5.5.3 Protección del archivo 42
5.5.4 Procedimiento de backup del archivo 42
5.5.5 Requerimientos para fechar los registros 42
5.5.6 Sistema de colección de archivo (interno o externo) 42
5.5.7 Procedimientos para obtener y verificar información del archivo 42
5.6 Cambio de clave 42
5.7 Compromiso y recuperación en caso de desastre 43
5.7.1 Procedimientos de manejo de incidentes y compromiso 43
5.7.2 Recursos de computación, software y/o datos corruptos 43
5.7.3 Procedimientos de compromiso de clave privada de entidad 44
5.7.4 Capacidad de continuidad luego de un desastre 44
5.8 Terminación de CA o RA 44
6 Controles de seguridad técnica 45
6.1 Generación e instalación del par de claves 45
6.1.1 Generación del par de claves 45
6.1.2 Entrega de claves privadas a un suscriptor 45
6.1.3 Entrega de claves privadas a un emisor de certificados 45
6.1.4 Entrega de claves públicas de CA a partes dependientes 45
6.1.5 Tamaño de claves 45
6.1.6 Generación de parámetros de claves públicas y control de calidad 45
6.1.7 Propósitos de uso de las claves (para el campo de uso de clave X.509 v3) 46
6.2 Controles de Ingeniería de Módulo Criptográfico y Protección de Clave Privada 46
6.2.1 Estándares y controles de modulo criptográfico 46
6.2.2 Control multi-persona de clave privada (n de m) 47
6.2.3 Recuperación de clave privada 47
6.2.4 Backup de la clave privada 47
6.2.5 Archivo de claves privadas 47
6.2.6 Transferencia de clave privada desde o hacia un módulo criptográfico 47

6.2.7 Almacenamiento de clave privada en un modulo criptográfico 47
6.2.8 Método para activar la clave privada 48
6.2.9 Método para desactivar la clave privada 48
6.2.10 Método de destrucción de clave privada 48
6.2.11 Tasación del Módulo Criptográfico 48
6.3 Otros aspectos de administración de pares de claves 48
6.3.1 Archivo de clave pública 48
6.3.2 Períodos operativos de certificados y períodos de uso de pares de claves 48
6.4 Datos de activación 49
6.4.1 Generación e instalación de datos de activación 49
6.4.2 Protección de datos de activación 49
6.4.3 Otros aspectos de datos de activación 49
6.5 Controles de seguridad computacional 49
6.5.1 Requerimientos técnicos específicos de seguridad computacional 49
6.5.2 Medición de seguridad computacional 49
6.6 Controles técnicos de vida útil 49
6.6.1 Controles de desarrollo de sistemas 49
6.6.2 Controles de administración de seguridad 50
6.6.3 Controles de seguridad de vida útil 50
6.7 Controles de seguridad en redes 50
6.8 Fecha 50
7 Perfiles de Certificado, CRL y OSCP 51
7.1 Perfil de certificado 51
7.1.1 Número(s) de Versión 51
7.1.2 Extensiones del certificado 51
7.1.3 Algoritmos Identificadores de Objetos 53
7.1.4 Formas del nombre 53
7.1.5 Restricciones de Nombre 53
7.1.6 Identificador de objeto de Política de Certificado 53
7.1.7 Uso de la extensión de Restricciones de Política 53
7.1.8 Sintáctica y semántica de calificadores de política 54
7.1.9 Procesamiento de semántica para la extensión de Políticas de Certificado críticas 54
7.2 Perfil CRL 54
7.2.1 Número(s) de Versión 54
7.2.2 Extensiones de CRL y campos de CRL 54
7.3 Perfil OCSP 54
7.3.1 Número(s) de versión 54
7.3.2 extensiones OCSP 55
7.3.3 Restricciones de nombre 55
7.3.4 Identificador de objeto de Política de Certificado 55
7.3.5 Uso de la extensión de Restricciones de Política 55
7.3.6 Sintáctica y semántica de calificadores de política 55
7.3.7 Procesamiento de semántica para la extensión de Políticas de Certificado críticas 55
8 Auditoría de desempeño y otras inspecciones 56

8.1 Frecuencia o circunstancias de la inspección 56
8.2 Identidad/calificaciones del inspector 56
8.3 Relación del inspector con la entidad inspeccionada 56
8.4 Temas incluidos por la inspección 56
8.5 Acciones como resultado de deficiencia 56
8.6 Comunicación de los resultados 57
9 Otros aspectos legales y comerciales 58
9.1 Tarifas 58
9.1.1 Tarifas de emisión o renovación de certificados 58
9.1.2 Tarifas de acceso al certificado 58
9.1.3 Tarifas de acceso a información de estado o revocación 58
9.1.4 Tarifas por otros servicios 58
9.1.5 Política de reembolso 58
9.2 Responsabilidad financiera 58
9.2.1 Cobertura de seguro 58
9.2.2 Otros aspectos 59
9.2.3 Cobertura de garantía o seguro para entidades de destino 59
9.3 Confidencialidad de información comercial 59
9.3.1 Alcance de información confidencial 59
9.3.2 Information fuera del alcance de la información confidencial 59
9.3.3 Responsabilidad de protección de información confidencial 59
9.4 Información privada o personal 59
9.4.1 Plan de privacidad 59
9.4.2 Información considerada privada 60
9.4.3 Información considerada no privada 60
9.4.4 Responsabilidad de protección de información privada 60
9.4.5 Aviso y consentimiento del uso de información privada 60
9.4.6 Revelación de información confidencial por procesos administrativos-o judiciales 60
9.4.7 Otras circunstancias de revelación de información 60
9.5 Derechos de propiedad intelectual 61
9.6 Representaciones y garantías 61
9.6.1 Representaciones y garantías de la CA 61
9.6.2 Representaciones y garantías de la RA 61
9.6.3 Representaciones y garantías del suscriptor 62
9.6.4 Representaciones y garantías de las parte dependiente 62
9.6.5 Representaciones y garantías de otros participantes 63
9.7 Renuncia de garantías 63
9.8 Limitaciones de responsabilidad 63
9.9 Indemnizaciones 64
9.10 Período y terminación 64
9.10.1 Período 64
9.10.2 Terminación 64
9.10.3 Efecto de terminación y supervivencia 64
9.11 Notificación individual y comunicación con participantes 64

9.12 Enmiendas 65
9.12.1 Procedimiento de enmienda 65
9.12.2 Período y mecanismo de notificación 65
9.12.3 Circunstancias bajo las cuales el OID deberá ser cambiado 65
9.13 Provisiones sobre resolución de disputas 65
9.14 Ley gobernante 65
9.15 Cumplimiento de la ley 65
9.16 Provisiones misceláneas 66
9.16.1 Acuerdo entero 66
9.16.2 Asignaciones 66
9.16.3 Separabilidad 66
9.16.4 Cumplimiento (tarifas de abogados y dispensa de derechos) 66
9.16.5 Fuerza mayor 66
9.17 Otras provisiones 66
10 Referencias 67

1 Introducción

Este documento está estructurado de acuerdo con RFC 3647, describe el conjunto de reglas y procedimientos establecidos por la UNLP para la operación del servicio de CA de UNLP PKIGrid.

Este documento incluirá tanto la Política de Certificación como la Declaración de la Práctica de la Certificación para la CA de UNLP PKIGrid. La arquitectura general es una autoridad certificante y varias Autoridades de Registro. La autoridad certificante (CA) es una persona natural individual.

1.1 Generalidades

UNLP Grid 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 CA del UNLP PKIGrid, la Autoridad de Certificación (CA) para UNLPGrid, para emitir certificados. Este y cualquier documento CP/CPS subsiguiente puede ser encontrado en el sitio Web

http://www.pkigrid.unlp.edu.ar

1.2 Nombre del Documento e identificación

Título del Documento	Política de Certificación (CP) y Declaración de la Práctica de la Certificación (CPS) para un CA de la UNLP PKIGrid
Versión del Documento	Versión 2.7S
Fecha del Documento	30 de Octubre de 2007
Estructura OID del Documento	
Asignado por IGTF	1.2.840.113612.5.4.2.3
Tipo de Documento (CP/CPS)	1
Subtipo de Documento	0
Versión	2
Sub-Versión	7S (se agrega S por ser la versión en español))

La estructura OID está indicada en el documento “Descripciones y Especificaciones de los Documentos” publicado en el sitio.

Este documento es válido hasta próximo aviso.

1.3 Participantes PKI

1.3.1 Autoridades Certificantes

El CA del UNLP PKIGrid no emite certificados para Autoridades Certificantes subordinadas.

1.3.2 Autoridades de Registro

Las Autoridades de Registro (RA) se crearán por necesidad para apoyar las actividades de investigación académica en el país. Inicialmente la UNLP PKIGrid CA delega la autenticación a CESPI RA.

CeSPI - "Centro Superior para el Procesamiento de la Información" de la Universidad Nacional de la Plata es el centro de servicios informáticos de la UNLP. El CeSPI fue creado en 1969 y provee servicios a toda la Universidad (con más de 95.000 estudiantes, más de 140 programas de grado y más de 200 programas de postgrado) y soporta el 20% de la investigación científica y técnica hecha en Argentina.

Las RA serán responsables de hacer cumplir las reglas de investigación de identidad en nombre de la CA durante el proceso de emisión de certificados a Entidades Finales (EEs).

Las Autoridades de Registro deben ser operadas por organizaciones relacionadas con la comunidad académica argentina. Asumen la obligación de seguir los procedimientos impuestos por la CA para la operación y autenticación de pedidos de certificado.

Los operadores de RA deben ser miembros del staffl de la organización..

Deberá requerirse a las RA que declaren su entendimiento de y adherencia a este CP/CPS, y que cumplan sus funciones de acuerdo con este CP/CPS y las mejores prácticas actuales definidas en el sitio de pkiUNLPGrid.

La CA de UNLP PKIGrid opera una red de Autoridades de Registro distribuidas (RAs). Una lista de Autoridades de Registro es mantenida y publicada en el repositorio on-line. La lista de Ras deberá contener por lo menos el nombre de la RA, la información de contacto de la RA y el dominio de registración de la RA.

La lista de RAs para la CA de UNLP PKIGrid está disponible en el sitio Web de UNLP PKIGrid

http://www.pkigrid.unlp.edu.ar

1.3.3 Suscriptores

La CA de UNLP PKIGrid emitirá certificados para actividades de e-ciencia realizadas dentro de los parámetros de la UNLP Grid. La CA emitirá certificados personales, de servidor y de servicio.

Los solicitantes de certificados deberán pertenecer a la comunidad académica argentina y DEBEN proveer evidencia de su necesidad de trabajar dentro de la comunidad de Grid Internacional (por ejemplo, siendo presentados por un líder de proyectos relacionados con la investigación de la Grid).

Los solicitantes de certificados para Hosts o servicios DEBEN presentar una carta o e-mail firmado y aprobado por el líder de proyecto para probar que el solicitante está relacionado con la administración del host.

1.3.4 Partes Dependientes

Las partes dependientes pueden ser:

- Personas naturales que reciban e-mails firmados, o accedan a hosts o servicios.
- Hosts a los cuales los poseedores de certificados ingresan o envían procesos o trabajos
- Servicios pedidos por poseedores de un certificado

1.3.5 Otros participantes

No se estipula.

1.4 Uso del Certificado

1.4.1 Usos Apropiados del Certificado

Los certificados de CA pueden ser usados solo para emitir certificados y para chequear certificados que afirman haber sido emitidos por la CA de UNLP PKIGrid (véase 1.3.3).

Los certificados de RA pueden ser usados sólo por el agente RA para actividades relacionadas con las RA, no para otras actividades de esa persona natural; estas deben ser realizadas usando certificados de una entidad final.

El certificado de entidad final 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

Los certificados deberán ser usados y/o aceptados sólo para acciones que soporten actividades de e-ciencia.

1.4.2 Usos Prohibidos del certificado

Los certificados emitidos por los CA de UNLP PKIGrid deben ser usados solo para actividades de e-ciencia, y no han de ser usados para otras actividades como transacciones financieras.

No deben ser usados para propósitos que violen la ley argentina ni la ley del país en que la entidad destino (por Ej. Aplicación o host a usar, destinatario de un e-mail) se encuentre.

1.5 Administración de Permiso

1.5.1 Organización que administra el documento

La CA de UNLP PKIGrid es administrada por el Centro de Cómputos CeSPI en La Plata (Argentina).

La dirección de la CA para asuntos operativos es:

Autoridad Certificante UNLP

Calle 115 y 50 S/N

B1900AYB La Plata

Buenos Aires

Argentina

Teléfono: 542214257240

Fax: 542214236610

E-mail: ca@cespi.unlp.edu,ar

El servidor web URL del CA es http://www.pkigrid.unlp.edu.ar

1.5.2 Contacto

El Administrador de la CA (Contacto para preguntas relacionadas con este documento) es:

Díaz, Francisco Javier

CeSPI - UNLP

Calle 115 y 50 S/N

B1900AYB La Plata

Argentina

Teléfono: 542214236609

Fax: 542214236610

E-mail: jdiaz@unlp.edu.ar

1.5.3 Persona que determina la idoneidad de CPS para el permiso

El administrador de la CA de UNLP PKIGrid (Véase 1.5.2) es responsable de determinar la idoneidad de CPS para el permiso.

1.5.4 Procedimientos de aprobación de CPS

El documento aprobado deberá ser enviado a TAGPMA para su aceptación y acreditación.

1.6 Definiciones y Acrónimos

Las palabras clave " DEBE , " NO DEBE , " REQUERIDO , " PODRA , " NO PODRA , " DEBERIA , NO DEBERIA , " RECOMENDADO , " PUEDE" , y " OPCIONAL" en este documento deben ser interpretadas como descritas en RFC 2119.

Las definiciones están organizadas por orden alfabético.

Analista

El analista es una persona que tiene experiencia en todas las fases de la gestión de un proyecto y ayuda a tomar decisiones y resolver problemas.

Autenticación

El proceso de establecer que individuos, organizaciones o cosas son quien o lo que reclaman ser. En el contexto de un PKI, la autenticación puede ser el proceso de establecer que un individuo u organización que pide o busca acceso a algo bajo cierto nombre es, de hecho, el propio individuo u organización. Este proceso corresponde al segundo proceso relacionado con la identificación, como se muestra en la definición de "identificación" más abajo. La autenticación puede también referirse a un servicio de seguridad que garantiza que individuos, organizaciones o cosas son quien o lo que reclaman ser o que un mensaje u otro dato fueron efectivamente originados por un individuo, organización o dispositivo específico. Por lo tanto se dice que una firma digital en un mensaje autentica al remitente.

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.

Autoridad de Emisión de Certificados (Issuing CA)

En el contexto de un certificado en particular, el Issuing CA es el CA que emite el certificado.

Autoridad de Registro (RA)

Una entidad que es responsable por la identificación y autenticación de sujetos de certificado, pero que no puede firmar ni emitir certificados (por ejemplo, se le delegan ciertas tareas en nombre de un CA).

Calificador de Política

La información dependiente de la Política que acompaña un identificador de política de certificados en un certificado X.509.

Cambio de Contraseña

El cambio de contraseña es el proceso por el cual se provee de una nueva contraseña pública al usuario de una CA.

Certificado de Host.

Un certificado para la certificación de un servidor y encriptación de comunicaciones (SSL/TSL). Representará una sola máquina.

Certificado Personal

Un certificado usado para la autenticación para establecer la Identidad de una Persona de la Grid. Representará a una persona individual.

Certificado de Servicio

Un certificado para un servicio particular que corre en un host. Representará un solo dispositivo en un solo host.

Datos de Activación

Valores de datos, no claves, que se requieren para operar módulos criptográficos y que necesitan ser protegidos (Por Ej., un PIN, una contraseña o una llave manual).

Declaración de Práctica de Certificación (CPS)

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

Entidad final

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

Identificación

El proceso de establecer la identidad de un individuo u organización, por Ej., mostrar que un individuo u organización específica es en realidad ese individuo u organización específica. En

el contexto de un PKI, la identificación se refiere a dos procesos: (1) establecer que un nombre dado de un individuo u organización corresponde a una identidad real de un individuo u organización, y (2) establecer que un individuo u organización pidiendo o buscando acceso a algo bajo ese nombre es, de hecho, el individuo u organización mencionado.

Una persona que busca identificación puede ser un solicitante de certificado, un candidato a una posición dentro de un participante PKI, o una persona buscando acceso a una red o aplicación de software, como un administrador de CAs buscando acceso al sistema de CAs.

Líder de Proyecto

El administrador responsable de un proyecto relacionado con la GRID. Es el punto de contacto con la RA, y ha sido elegido para manejar todas las comunicaciones sobre temas relacionados con la política de certificados con el administrador de la UNLPGrid.

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.

Organización Virtual (VO)

Una organización que ha sido creada para representar una investigación particular o esfuerzo de desarrollo independiente de los sitios físicos donde los Científicos o Ingenieros trabajan.

Parte Dependiente

El receptor de un certificado que actúa en dependencia de ese certificado y/o firmas digitales verificadas usando ese certificado.

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.

Renovación de Certificado

La renovación de un certificado es el proceso por el cual un nuevo certificado con un período de validez extendido es creado para un par de claves existente.

Los usuarios pueden renovar su certificado siempre y cuando no haya expirado o haya sido revocado. Pueden reutilizar sus claves privadas (si la RA asegura que no están en riesgo).

Repositorio

Un área de almacenamiento, generalmente online, que contiene listas de certificados emitidos, CRLs, documentos de términos de uso, etc.

Restablecimiento de Contraseña de Certificado

El proceso de restablecimiento de contraseña luego de revocación o expiración del certificado de un suscriptor consiste de una nueva solicitud, que requiere la generación de un nuevo par de claves para el suscriptor. El suscriptor al certificado puede pedir un cambio rutinario de contraseña para su certificado por e-mail firmado, con el mismo remitente que el certificado anterior pero con un **nuevo par de claves.**

Suscriptor

O también llamado Entidad final (EE) es una persona o servidor o servicio para el cual se emite un certificado.

2 Responsabilidades de publicación y repositorio

2.1 Repositorios

Puede accederse al repositorio online de información relativa a la CA de UNLP PKIGrid a través de la URL http://www.pkigrid.unlp.edu.ar

2.2 Publicación de información de la CA

La CA de la UNLP PKIGrid operará un repositorio online seguro que contiene:

- El certificado de CA de la UNLP PKIGrid (disponible en formatos PEM, CRT y DER), y todos los anteriores necesarios para chequear certificados aún válidos,
- Los certificados emitidos por la CA,
- Una lista de Revocación de Certificados (disponible en formatos PEM o DER),
- Una copia de la versión más reciente de este CP/CPS y todas las versiones anteriores,
- Otra información juzgada relevante para el servicio de la CA de la UNLP PKIGrid.
- Un link al repositorio trust anchor de TAGPMA (TACAR, www.tacar.org), donde la raiz de confianza de la CA ha sido previamente publicado.

2.3 Frecuencia de la publicación

- Toda la información publicada deberá ser actual y vigente.
- Los certificados serán publicados en el repositorio de la CA de la UNLP PKIGrid tan pronto como sean emitidos.
- La lista de revocación de certificados (CRL) deberá tener una vida útil máxima de 30 días.
- La CA de la UNLP PKIGrid DEBE emitir una nueva CRL por lo menos 7 días antes de su vencimiento o inmediatamente luego de haber procesado una revocación, lo que ocurra primero. La CRL DEBE ser publicada inmediatamente después de su emisión.
- Esta CP/CPS será publicada en cada ocasión en que sea actualizada.

2.4 Controles de Acceso en los repositorios

El repositorio online es mantenido en base al mejor esfuerzo y está disponible sustancialmente las 24 horas del día, 7 días a la semana, sujeto a mantenimiento previsto y razonable. Fuera del período 08:00-17:00 GMT- 03:00 en días hábiles, puede ser que no sea mantenida “a riesgo “.

La CA de la UNLP PKIGrid no impone ningún control de acceso en su CP/CPS, su certificado, certificados emitidos o CRLs.

3 Identificación y autenticación

3.1 Nombres

3.1.1 Tipos de nombres

El Nombre del Sujeto es del tipo de nombres X.500. El componente CN tiene una de las siguientes formas:

- Para personas el nombre y apellido o un texto directamente derivado de su nombre (se permiten mayúsculas y minúsculas) CN=JavierDiaz
- Para servidores el Nombre de Dominio Enteramente Calificado (FQDN). El nombre DEBE estar en minúsculas. No se aceptan direcciones IP.
- Para servicios el nombre del servicio, el carácter '/' y el FQDN del servidor. El nombre DEBE estar en minúsculas..

  Los Nombres Comunes (CNs) DEBEN estar codificados como PrintableStrings. La longitud máxima del CN es de 128 caracteres para todo tipo de certificados.
- Para certificados de servicios, el carácter "/" también está permitido en el CN y el texto a la izquierda del "/" DEBE estar relacionado con el tipo de servicio que el certificado identifica.

3.1.2 Necesidad de que los nombres tengan sentido

El Nombre del Sujeto en un certificado debe tener una asociación razonable con el nombre autenticado del suscriptor. Los suscriptores deben elegir una representación de su nombre dentro del grupo de caracteres permitidos (véase 3.1.1). El nombre no deberá referirse a un cargo.

3.1.3 Anonimidad o pseudonimidad de los suscriptores

Los suscriptores no pueden ser ni anónimos ni pseudónimos. Ningún certificado de persona natural será emitido a roles o funciones, solo a personas nombradas e identificadas.

3.1.4 Reglas para interpretar varias formas de un nombre

- El componente CN del nombre del sujeto en un certificado para una persona natural deberá contener el nombre de pila y apellido (pueden ser separados por un punto) como aparece en el documento de autenticación que comprueba el nombre del suscriptor. También es posible usar un texto directamente derivado del nombre completo.

CN=JavierDiaz CN=Javier.Diaz

- El CN de un host será el FQDN que pueda ser usado universalmente para acceder a ese host.

CN=pkigrid.unlp.edu.ar

- El CN para un servicio será el nombre de la aplicación seguido por una barra "/" seguida por el FQDN del host en el que la aplicación es ejecutada.

CN=ldap/pkigrid.unlp.edu.ar

3.1.5 Originalidad de los Nombres

El Nombre Distinguido DEBE ser único para cada nombre de sujeto certificado por la CA de la UNLP PKIGrid a lo largo de la vida útil de la CA. La UNLP PKIGrid resuelve esta tarea antes de que el pedido sea generado.

En esta política, dos nombres se consideran idénticos difiriendo solo en el tipo de letra, mayúscula o minúscula. En otras palabras, las mayúsculas y minúsculas no deben ser usadas para distinguir entre nombres.

Los certificados DEBEN referir a individuos o recursos individuales.

3.1.6 Reconocimiento, autenticación y papel de las marcas registradas

No hay estipulación.

3.2 Validación Inicial de Identidad

3.2.1 Método para probar posesión de clave privada

La RA confirma la posesión de la clave privada por verificación de la firma en el Pedido de Firma de Certificado (CSR).

3.2.2 Autenticación de la identidad de una organización

La CA verificará que la organización de la parte solicitante o una unidad de la organización tiene derecho (véase 1.3.3) de obtener un certificado de la CA de la UNLP PKIGrid y que coincida con el pedido.

La primera vez que una organización/unidad quiera obtener un certificado para una persona natura, servidor o servicio, o quiera tener un RA, tiene que anunciarlo oficialmente a la CA de la UNLP PKIGrid. La CA tiene que hacer constar que organización o unidad de organización existe y tiene derecho de solicitar un certificado de la UNLP Grid. También debe tener información competente sobre quién deberá firmar de parte de la institución.

3.2.3 Autenticación de identidad individual

Para permitir a la RA la autenticación de la identidad del individuo, este último DEBE reunirse con la RA en persona y presentar un documento reconocido oficialmente que pruebe la identidad de la parte solicitante. Solo documentos aceptados por las leyes argentinas (DNI, Pasaporte Válido) serán aceptados.

El certificado de host puede ser pedido solo por el administrador responsable del host en particular. La RA pedirá una carta o e-mail firmada/o del líder del proyecto confirmando que la persona que solicita el certificado es el administrador responsable del host a ser identificado por el certificado.

3.2.4 Información de suscriptores no-verificados

No hay estipulación.

3.2.5 Validación de autoridad

Sin definir.

3.2.6 Criterio de interoperabilidad

No hay estipulación.

3.3 Identificación y autenticación de solicitud de cambio de contraseña

3.3.1 Identificación y autenticación para cambio de contraseña rutinario

El cambio de contraseña luego de la expiración o revocación del certificado de un suscriptor es la re solicitud completa, que requiere la generación de un par nuevo de claves del suscriptor y la realización de los procesos de identificación y autenticación para el registro original especificados en el actual CP/CPS.

El suscriptor al certificado puede pedir un cambio rutinario de contraseña para su certificado por e-mail firmado. Este e-mail DEBE contener una nueva solicitud de certificado, con el mismo remitente que el certificado anterior pero con un **nuevo par de claves.** Nota: Esto es diferente a actualizar un certificado: un nuevo certificado está creandose..

El cambio de contraseña antes de que el certificado expire puede hacerse usando una interfaz Web segura. Luego de la expiración del certificado no es posible cambiar la contraseña; una nueva solicitud de registro inicial debe hacerse en su lugar.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a certificate, no re-key is possible. A new application for initial registration MUST be made.

3.4 Identificación y autenticación para solicitud de revocación

A menos que la solicitud de revocación se origine de la UNLP Grid porque ha verificado independientemente que la contraseña estuvo comprometida, la solicitud de revocación debe ser verificada y la parte solicitante debe ser autenticada.

Tal solicitud proveniente de una RA DEBE hacerse en una transferencia firmada enviada a una CA. La CA solo necesita autenticar al solicitante de la revocación si la CA no tiene suficiente prueba de compromiso de la contraseña o de inexactitud del contenido del certificado.

En caso de emergencia la revocación puede iniciarse por vía de comunicación oral con la RA apropiada o la CA de la UNLP PKIGrid. La RA o la CA de UNLP PKIGrid tienen que hacer el mayor esfuerzo por autenticar la solicitud, excepto que haya pruebas sólidas del compromiso de la contraseña.

4 Requerimientos operacionales de la vida útil de un Certificado

4.1 Solicitud de Certificado

4.1.1 Quién puede solicitar un certificado

La CA de la UNLP PKIGrid emite certificados a miembros de la comunidad académica argentina para:

- Personas naturales , y
- Hosts administrados por la organización solicitante, y
- Servicios provistos en un host administrado por una organización competente.

Es recomendable que los solicitantes de un certificado sepan y adhieran a las obligaciones vigentes definidas en el documento "Obligaciones del suscriptor". Este documento está publicado en el sitio del pkiUNLPGrid.

4.1.2 Proceso de enrolamiento y responsabilidades

La parte solicitante genera el par de claves con un tamaño de por lo menos 1024 bits en su sistema a través de la planilla disponible en el sitio web de la UNLP PKIGrid. Luego de que la planilla haya sido completada, la contraseña privada encriptada será almacenada en el sistema donde el navegador corre en un archivo accesible solo para el solicitante (si el sistema operativo permite tal restricción) y el CSR será almacenado en el sistema LDAP.

Los suscriptores deberán:

- Leer y adherir a los procedimientos publicados en este documento
- Usar el certificado para los propósitos permitidos solamente.
- Autorizar el procesamiento y conservación de datos personales (requerido bajo las regulaciones de protección de datos).
- Tomar toda precaución posible para prevenir cualquier pérdida, publicación o acceso no-autorizado a o uso de la clave privada asociada con el certificado, incluidas:
  - (Certificados Personales) seleccionando una contraseña sólida de al menos 15 caracteres;
  - (Certificados Personales) protegiendo la contraseña de otros;
- Notificar inmediatamente a la CA de la UNLP PKIGrid y todas las partes dependientes si la clave privada se pierde o está comprometida;

- Pedir revocación si el suscriptor deja de tener derecho a un certificado, o si la información de un certificado se vuelve incorrecta o imprecisa.

4.2 Procesamiento de solicitud de certificado

4.2.1 Realizando funciones de identificación y autenticación

El operador RA usa el módulo de administración de la UNLP PKIGrid para mostrar todas las CSRs que tengan la validación pendiente. En el caso de una solicitud para servidor/servicio deberá también chequear que el usuario es responsable del host dentro de la organización o unidad dueña del host.

4.2.2 Aprobación o rechazo de solicitudes de certificado

Tras una autenticación exitosa, una copia electrónica del documento de identificación de la parte solicitante y la solicitud de certificado deberán ser almacenadas. Las especificaciones sobre formato de escaneo están indicadas en el documento “RA Structure and Operations” publicado en el sitio Web de la CA.

Si la información de autenticación es inexacta o si una parte solicitante no cumple con los requisitos de autenticación dentro de los 9 días luego de que la solicitud haya sido recibida por la RA, la solicitud será rechazada. Si la parte solicitante insiste en conseguir un certificado deberá iniciar una nueva solicitud.

4.2.3 Tiempo para procesar solicitudes de certificado

El tiempo que se requiere en el lapso comprendido desde la solicitud hasta la emisión depende mayormente del proceso de autenticación, pero el certificado debe emitirse dentro de los tres días siguientes a la recepción de la solicitud.

4.3 Emisión de Certificados

4.3.1 Acciones de los CA durante la emisión de certificados

La CSR deberá ser transferida a una computadora que contenga la clave privada de la CA de la UNLP PKIGrid y que no esté conectada a ninguna red. En este sistema el certificado es creado y firmado. El certificado firmado podrá ser entonces transferido de vuelta al servidor en línea de la UNLP PKIGrid.

El certificado DEBE ser emitido basado en el ultimo CP/CPS aprobado por TAGPMA.

4.3.2 Notificación al suscriptor por la CA acerca de la emisión del certificado

El sistema de la UNLP PKIGrid enviará entonces un e-mail a la parte solicitante con la URL de la página de descarga del certificado. También le enviará un reconocimiento de la emisión a la RA correspondiente.

Un certificado (personal, de servicio o de host) será válido por 13 meses desde la fecha de emisión o menos de un año en casos específicos (por Ej., si se prevee que la afiliación del solicitante con la organización / unidad terminará en menos de un año).

4.4 Aceptación de certificados

4.4.1 Conducta constitutiva de la aceptación de un certificado

La parte demandante deberá notificar a la CA sobre el rechazo de un certificado, explicando a la CA y la RA las razones de ese rechazo. Los certificados cuyo rechazo no haya sido recibido por la CA dentro de una semana serán considerados aceptados.

4.4.2 Publicación del certificado por la CA

La CA de la UNLP PKIGrid publicará en su servidor web los certificados tan pronto como sean emitidos.

4.4.3 Notificación de emisión de certificado por la CA a otras entidades

No hay estipulación.

4.5 Par de claves y uso del certificado

4.5.1 Clave privada del suscriptor y uso del certificado

Los certificados emitidos por la CA de la UNLP PKIGrid y sus claves privadas asociadas deben ser usados solo de acuerdo con los permisos y prohibiciones establecidos en la sección 1.4. Deben ser usados solo de acuerdo a los campos de uso de clave del certificado. Cuando un certificado es revocado o ha expirado la clave privada asociada no deberá ser usada nunca más.

Los suscriptores no DEBEN compartir certificados.

4.5.2 Clave pública y uso del certificado de la parte solicitante

Una parte dependiente debe, luego de obtener un certificado emitido por la CA de la UNLP PKIGrid, chequear su validez:

- chequeando que confíe en la CA que emitió el certificado,

- chequeando que el certificado no haya expirado
- usándolo apropiadamente como descrito en la CP apuntada por el certificado en las claves de uso incluidas en el certificado

4.6 Renovación del certificado

4.6.1 Circunstancias de renovación del certificado

La renovación del certificado es el proceso por el cual un nuevo certificado con un periodo de validez extendido es creado para un par de claves existente. Los usuarios pueden renovar su certificado mientras no haya sido revocado o expirado. La renovación del certificado DEBE estar respaldada por la RA correspondiente, que deberá constatar que no hay riesgos en la reutilización de la contraseña. La CA de la UNLP PKIGrid puede decidir rechazar esa renovación por motivos de seguridad, para evitar riesgos derivados de largas exposiciones de claves privadas.

4.6.2 Quién puede pedir renovación

El dueño de un certificado puede pedir la renovación de un certificado antes de que expire usando una interfaz web segura.

4.6.3 Procesamiento de solicitudes de renovación de certificados

Tras el arribo de la solicitud respaldada por la RA correspondiente, la CA deberá procesar la renovación como procesa una petición de certificado inicial.

Los usuarios pueden hacer nuevas solicitudes de certificados, pero DEBEN probar su identidad usando su certificado actual. La solicitud DEBE tener el mismo DN que el certificado usado para probar la identidad.

Luego de la recepción de la solicitud constatada por la RA correspondiente, la UNLP PKIGrid CA deberá procesar la renovación como procesa una solicitud de certificación inicial. La RA deberá validar que el solicitante todavía esté trabajando en el proyecto original. El solicitante de la renovación debe preguntar al líder de proyecto que originariamente confirmó la necesidad del usuario de un certificado, para informar a la RA que el usuario todavía tiene derecho a un certificado

4.6.4 Notificación de nueva emisión de certificado a suscriptor

La CA de la UNLP PKIGrid deberá notificar al suscriptor de la emisión como descrito para la emisión de certificado inicial en 4.3.2.

4.6.5 Conducta constituyendo aceptación de un certificado de renovación

El mismo procedimiento será seguido, como descrito en 4.4.1

4.6.6 Publicación del certificado de renovación por parte de la CA

Véase 4.4.2

4.7 Cambio de contraseña de certificados

4.7.1 Circunstancias para el cambio de contraseñas de certificados

Por razones de seguridad, el cambio de contraseña en los certificados es el método preferido para emitir un nuevo certificado a un suscriptor cuyo certificado está a punto de expirar o que quiere un cambio en los parámetros del certificado.

4.7.2 Quién puede solicitar certificación de una nueva contraseña pública

El dueño de un certificado válido puede pedir la certificación de una nueva clave pública en un CSR también firmado con su clave privada vigente y válida.

Si el certificado ya ha expirado, un procedimiento de solicitud de certificado como descrito para una solicitud de certificación inicial debe ser seguido.

4.7.3 Procesamiento de solicitudes de cambio de contraseña de certificados

Los usuarios pueden usar la interfaz web de la UNLP PKIGrid para solicitar un cambio de contraseña. Tras la recepción de la solicitud acreditada por la RA correspondiente, la CA de la UNLP PKIGrid procesará la renovación como procesaría una solicitud de certificación inicial.

4.7.4 Notificación de emisión de nuevos certificados a suscriptores

La CA de la UNLP PKIGrid notificará a los suscriptores sobre la emisión como se describe en 4.3.2. para la emisión de certificado inicial.

4.7.5 Conducta constituyente de aceptación de un certificado con contraseña nueva

El mismo procedimiento descrito en 4.4.1 deberá ser seguido

4.7.6 Publicación del certificado con nueva contraseña por la CA

Véase 4.4.2.

4.7.7 Notificación de emisión de certificado de CA a otras entidades

Véase 4.4.3

4.8 Modificación de certificado

4.8.1 Circunstancias de modificación de certificado

Los certificados no DEBEN ser modificados. Los certificados viejos deberán ser revocados, y un nuevo par de claves deberá ser generado así como también una nueva solicitud para los contenidos del certificado modificado con la nueva contraseña. La revocación puede ser condicional a la emisión y aceptación del nuevo certificado, y así el viejo certificado será revocado solo luego de que el nuevo sea aceptado.

4.8.2 Quién puede solicitar modificación de un certificado

No es pertinente.

4.8.3 Procesamiento de solicitudes de modificación de un certificado

No es pertinente.

4.8.4 Notificación de emisión de un nuevo certificado al suscriptor

No es pertinente.

4.8.5 Conducta constituyente de la aceptación del certificado modificado

No es pertinente.

4.8.6 Publicación del certificado modificado por la CA

No es pertinente.

4.8.7 Notificación de emisión del certificado de parte de la CA a otras entidades

No es pertinente.

4.9 Revocación y suspensión de un certificado

4.9.1 Circunstancias de revocación

Un certificado será revocado cuando puede asegurase o sospecharse que la información que contiene o las afirmaciones implicadas son incorrectas o están comprometidas. Esto incluye situaciones donde:

- Se informa a la CA que el suscriptor ha dejado de ser un miembro o asociado de un programa o actividad de UNLP PKIGrid,
- La clave privada del suscriptor se extravía o se sospecha comprometida,
- No se necesita más,
- La información en el certificado del suscriptor es incorrecta o imprecisa, o se sospecha en ese estado,
- La clave privada de la CA se ha extraviado o se encuentra comprometida

4.9.2 Quién puede solicitar revocación

Una revocación certificada puede ser pedida por:

- el dueño de la clave certificada;
- La CA de la UNLP PKIGrid o cualquier RA que tenga prueba de compromiso;
- La organización que desea revocar su consentimiento a estar incluida en un certificado;
- La RA que autenticó al propietario del certificado;
- El propietario del certificado;
- Cualquier persona que presente prueba de conocimiento de que la contraseña del suscriptor está comprometida o que los datos del suscriptor han cambiado.

4.9.3 Procedimiento para solicitud de revocación

A menos que la CA de la UNLP PKIGrid actúe sola, la solicitud de revocación debe ser efectuada por:

- el propietario del certificado, debidamente autenticado, usando las funciones de revocación dispuestas en la página web. En caso de emergencia, el propietario del certificado deberá ir a la RA tan pronto como sea posible y pedirle a la RA correspondiente que solicite la revocación.
- el administrador de RAs usando una interfaz web segura

Antes de revocar un certificado la CA de la UNLP PKIGrid deberá autenticar la fuente de la solicitud de acuerdo con los procedimientos para el registro inicial.

4.9.4 Período de gracia para solicitudes de revocación.

No hay ningún período de gracia definido para la solicitud de revocación.

4.9.5 Tiempo dentro del cual la CA deberá procesar la solicitud de revocación

La CA de la UNLP PKIGrid procesará las solicitudes autenticadas con prioridad y publicará la revocación dentro de dos días laborales de la CA determinando la necesidad de revocación.

4.9.6 Requerimientos de chequeo de revocaciones en partes dependientes

Se recomienda que las partes dependientes verifiquen un certificado contra la CRL más actualizada publicada por la CA para validar el uso del certificado.

4.9.7 Frecuencia de emisión de CRLs (si fuera pertinente)

Las CRLs se actualizan y vuelven a emitirse luego de cada revocación o por lo menos 7 días antes de la expiración de la CRL anterior.

4.9.8 Latencia máxima de CRLs (si fuera pertinente)

La CRL será copiada a un dispositivo removible inmediatamente después de haber sido creada en el sistema off-line de la CA y luego transferido sin demoras al repositorio on-line.

4.9.9 Posibilidad de chequeo online de status / revocaciones

La última CRL está siempre disponible en el sitio Web de la UNLP PKIGrid. La CA de la UNLP PKIGrid publicará la CRL en efecto en su repositorio (véase 2.1.). Ningún otro chequeo on-line está disponible por el momento.

4.9.10 Requerimientos para el chequeo online de las revocaciones

No hay estipulación.

4.9.11 Otras formas de publicación de las revocaciones disponibles

A excepción de la comunicación de la efectiva revocación de un certificado al dueño de tal y a la RA correspondiente, no se deberá publicar una nueva CRL que no sea la del repositorio de la CA de la UNLP PKIGrid.

4.9.12 Requisitos especiales compromiso de contraseña ya cambiada

No hay estipulación.

4.9.13 Circunstancias para suspensión

No hay estipulación.

4.9.14 Quién puede solicitar suspensión

No hay estipulación.

4.9.15 Procedimiento para solicitud de suspensión

No hay estipulación.

4.9.16 Límites del período de suspensión

No hay estipulación.

4.10 Servicios de estado del certificado

4.10.1 Características operativas

La CA de la UNLP PKIGrid CA deberá guardar en su repositorio público y hacer disponibles a través de su web site:

- El certificado de raíz de la CA
- Todos los certificados válidos
- La CRL más actualizada

4.10.2 Disponibilidad del servicio

La CA de la UNLP PKIGrid deberá hacer este servicio disponible de forma continua, en un esfuerzo razonable, salvo por actividades inevitables. Por la misma naturaleza de Internet este servicio no puede estar garantizado como siempre disponible. El downtime estipulado será anunciado en el sitio web de la CA con un mínimo de 48 horas de adelanto.

4.10.3 Características opcionales

No hay estipulación.

4.11 Fin de la suscripción

La suscripción finaliza con la expiración del certificado si no es renovado o cambiadas sus claves (re-key) antes de esa fecha. Una suscripción puede finalizar si el suscriptor solicita una revocación de su certificado.

4.12 Preservación de contraseña y recuperación

4.12.1 Políticas y prácticas de preservación y recuperación de claves

No se proveen políticas al respecto. El dueño de la clave deberá tomar sus propias precauciones para prevenir la pérdida de su contraseña.

4.12.2 Políticas y prácticas de encapsulamiento y recuperación de claves de sesión

Véase 4.12.1

5 Controles de lugar físico, administración y operación

5.1 Controles físicos

La máquina que firma de la UNLP PKIGrid está off-line todo el tiempo y en una caja fuerte cuando no se usa. Se encuentra en el CeSPI en La Plata. La CA mantiene un procedimiento de control de acceso limitado al sistema. Todos los accesos al servidor están limitados al staff de la CA de la UNLP PKIGrid o la CA misma. La CA corre en un sistema GNU Linux.

5.1.1 Localización y construcción

La CA de la UNLP PKIGrid se encuentra en la siguiente dirección: UNLP PKIGrid CA

Calle 115 y 50 S/N

B1900AYB La Plata

Argentina

Teléfono: 542214236609

Fax: 542214236610

5.1.2 Acceso físico

La CA opera en un ambiente controlado, donde el acceso está restringido a las personas autorizadas. La máquina que la aloja se mantiene bajo llave en una caja fuerte y la llave está en una caja fuerte diferente.

5.1.3 Electricidad y aire acondicionado

La(s) máquina(s) online opera(n) en un ambiente con aire acondicionado y no se la(s) reiniciadas ni se recicla energía salvo por tareas de mantenimiento esencial

La máquina off line se apaga entre operaciones de firma de certificados. La máquina opera en un ambiente con aire acondicionado.

5.1.4 Exposición al agua

El edificio está en una zona no sujeta a inundaciones.

5.1.5 Prevención y protección del fuego

La CA está almacenada en una caja de seguridad no inflamable

5.1.6 Medios de Almacenamiento

Medios removibles (USB sticks y disks) son almacenados en lugares seguros bajo llave, a los que solo el personal autorizado tiene acceso.

5.1.7 Eliminación de residuos

Los residuos que contengan datos que requieran protección (datos criptográficamente relevantes como contraseñas o claves privadas, o datos personales) deberán ser desechados de manera que se garantice que la información no pueda volver a utilizarse.

5.1.8 Backup fuera de la CA

Un backup mensual será almacenado en otro edificio de la Universidad. El medio de backup deberá ser almacenado en un cuarto asegurado a prueba de fuego con acceso restringido.

5.2 Controles de Procedimiento

5.2.1 Roles confiados

No hay estipulación al respecto.

5.2.2 Número de personas requeridas por tarea

Por lo menos dos personas deberán realizar las tareas de operador de la CA, en una forma no exclusiva.

5.2.3 Identificación y autenticación para cada rol

No hay estipulación al respecto.

5.2.4 Roles que requieran separación de funciones

Salvo por la dirección, ningún tipo de rol en la CA de la UNLP PKIGrid CA requiere separación de funciones.

La información sobre un suscriptor almacenada en el sitio físico de la CA de la UNLP PKIGrid que deba ser considerada privada (véase 9.4.2) será solo accesible para los operadores de la RA que administre la solicitud de ese suscriptor.

5.3 Controles de personal

5.3.1 Calificaciones, experiencia y requerimientos de entrada

Todo el personal de la CA de la UNLP PKIGrid deberá tener experiencia como analista o administrador de sistemas.

5.3.2 Procedimientos de chequeo de antecedentes

- Todo acceso a los servidores y aplicaciones pertenecientes al servicio de la UNLP PKIGrid está limitado al staff de soporte del sistema de la CA.
- El administrador de la RA debe ser un empleado con sueldo de la Organización Física que aloje la Autoridad de Registro y debe ser nombrado por una Autoridad responsable de un Departamento dentro de esa organización física.
- El administrador de la RA debe ser un miembro de este departamento. La Autoridad hará una declaración escrita al administrador de la CA escribiendo en papel con membrete de la organización. La información que deberá contener esta carta será definida por el administrador de la CA.
- El operador de la RA debe ser un empleado con sueldo del sitio que aloje la Autoridad de Registro y deberá ser nombrado por el administrador de RAs pertinente.
- El administrador de la RA hará una declaración escrita al administrador de la CA escribiendo en el papel personalizado de la organización. Si la RA es nombrada en un departamento diferente de aquel del Administrador de RAs, la carta deberá ser autenticada por una autoridad del departamento en el que el Operador es nombrado. La información que deberá contener esta carta será definida por el administrador de la CA.

Los Operadores RA deben tener certificados que adhieran también a las obligaciones de los suscriptores.

- Un administrador de RA puede nombrarse a sí mismo como un operador RA.
- Un administrador de RA puede nombrar cualquier número de operadores RA.

5.3.3 Requerimientos de Entrenamiento

Toda persona que actúe como un operador CA deberá ser entrenada para el trabajo por el staff de UNLP PKIGrid que desarrolló la interfaz de la CA.

5.3.4 Requerimientos y frecuencia de repetición de entrenamiento

La repetición del entrenamiento es obligatoria cuando se introduzcan nuevo software o características, así como también procedimientos organizacionales.

5.3.5 Frecuencia y secuencia de rotación de trabajo

No hay estipulación al respecto.

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.

5.3.7 Requerimientos de contra tante independiente

No hay estipulaciones.

5.3.8 Documentación facilitada al personal

Toda documentación necesaria para cumplir las tareas correspondientes deberá ser facilitada al personal de la UNLP PKIGrid CA .

- Es responsabilidad del administrador de la CA suministrar a los operadores de la CA una copia de los Procedimientos del Operador UNLP PKIGrid CA..

- Es responsabilidad del administrador de CA suministrar al administrador de la RA una copia de los Procedimientos del Administrador UNLP PKIGrid RA..
- Es responsabilidad del administrador de la RA suministrar a los operadores de la RA una copia de los Procedimientos del Operador UNLP PKIGrid RA..

5.4 Procedimientos de historial (log) para auditoría

5.4.1 Tipos de eventos registrados

Los siguientes eventos deberán ser registrados:

UNLP PKIGrid CA host

- login / logout / reinicio
- creación y firma de certificados
- revocación de certificados
- temas relacionados con la CRL

UNLP PKIGrid web/LDAP online server

- recepción de solicitud de revocación de certificado
- validación de solicitud de certificado de la RA
- exportación de CSR desde RA
- emisión e importación de certificado a LDAP
- revocación de certificado
- temas relacionados con la CRL

5.4.2 Frecuencia de procesamiento de historial (log)

Los archivos de historial (log) deberán ser analizados una vez al mes o luego de que una potencial brecha de seguridad sea sospechada o conocida; lo que ocurra primero.

5.4.3 Período de retención del historial (log)

El período de retención mínimo de los historiaes (log´s) es de 3 años para archivos de historial (log) y datos LDAP.

5.4.4 Protección del historial (log) para auditoría

Los historiales (log´s) para auditoría deberán ser accesibles solo para los operadores y administradores CA UNLP PKIGrid y personal de auditoría autorizado. La CA deberá hacer el mejor esfuerzo para protege los logs.

5.4.5 Procedimientos de backup del historial (log) para auditoría

Deberá hacerse un backup de los historiales (log´s) cada noche en un medio removible no-reescribible (WORM) para auditoría.

El medio de backup deberá ser almacenado en un cuarto a prueba de fuego con acceso restringido.

El procedimiento de backup del historial (log) para auditoría está detallado en el documento "CA_Obligaciones&Estructura&Operaciones" publicado en el sitio de la CA.

5.4.6 Sistema de colección de auditoría (interno vs. externo)

Interno

5.4.7 Notificación a sujeto que cause evento

No hay estipulaciones

5.4.8 Medición de vulnerabilidad

No hay estipulaciones

5.5 Archivo de Registros

5.5.1 Tipos de registros archivados

Véase 5.4.1

5.5.2 Período de retención de archivo

El período mínimo de retención es de 3 años.

5.5.3 Protección del archivo

El archivo deberá ser accesible sólo para el personal de operación y administración de CA UNLP PKIGrid.

5.5.4 Procedimiento de backup del archivo

Deberá hacerse un backup del registro en un medio removible, que deberá ser almacenado en un cuarto a prueba de fuego con acceso restringido.

5.5.5 Requerimientos para fechar los registros

Todos los registros de eventos deberán contar con su fecha.

5.5.6 Sistema de colección de archivo (interno o externo)

Interno.

5.5.7 Procedimientos para obtener y verificar información del archivo

No hay estipulaciones.

5.6 Cambio de clave

El cambio de clave es el proceso por el cual se asigna una nueva clave pública al usuario de una CA. Cuando los datos criptográficos de la CA necesiten ser cambiados la transición será hecha; desde el momento de distribución de los nuevos datos criptográficos, solo la nueva clave será usada para firma de certificados. La superposición de la clave vieja y nueva debe ser al menos el mayor tiempo en el cual un certificado de entidad final sea valido.. El certificado viejo pero aún vigente debe estar disponible para verificar firmas viejas – y la clave secreta para firmar CRLs – hasta que todos los certificados firmados usando la clave privada asociada hayan expirado.

La CA generará un nuevo par de claves raíz por lo menos un año antes de que expire el certificado de la CA. En el último año el certificado viejo de la CA estará disponible para

propósitos de validación solamente, mientras que los nuevos certificados y CRLs serán firmados con la nueva clave CA.

5.7 Compromiso y recuperación en caso de desastre

5.7.1 Procedimientos de manejo de incidentes y compromiso

- Si la clave privada de un operador RA está comprometida o se sospecha en tal estado, el operador o administrador de RA deberá informar a la CA y solicitar la revocación del certificado del operador de RA.
- Si la clave privada de la CA se encuentra o se sospecha comprometida, la CA deberá:
  - ✓ Hacer todo esfuerzo razonable para notificar a los suscriptores y RAs,
  - ✓ Detener la emisión y distribución de certificados y CRLs,
  - ✓ Solicitar revocación del certificado comprometido,
  - ✓ Generar un Nuevo par de claves y certificado CA y publicar el certificado en el repositorio,
  - ✓ Revocar todos los certificados firmados usando la clave comprometida, y publicar la nueva CRL en el repositorio CA UNLP PKIGrid.

5.7.2 Recursos de computación, software y/o datos corruptos

La CA tomará precauciones en base al mejor esfuerzo para lograr la recuperación.

Para poder retomar la operación lo más pronto posible luego de que la base computacional de la CA está corrupta los siguientes pasos deberán ser tomados:

- Deberá hacerse un backup de todo el software CA en medios removibles luego de que una nueva versión de cualquiera de sus componentes sea instalado.
- Deberá hacerse un backup de todos los archivos de datos de la CA off line en un medio removible luego de cada cambio, antes de que se cierre la sesión.

En caso de corrupción de alguna parte del sistema corriente, un hardware funcional deberá ser cargado con un backup del último estado del software y datos en un medio de sólo lectura y deberán considerarse como no – corruptos. Si no todas las copias encriptadas de las claves privadas de la CA UNLP PKIGrid son destruidas o perdidas, y no se hallan comprometidas, la operación deberá ser restaurada cuanto antes posible sin necesidad de revocar todos los certificados emitidos.

5.7.3 Procedimientos de compromiso de clave privada de entidad

En caso de que la clave de una entidad destino se halle comprometida, el certificado correspondiente DEBE ser revocado. Todas las partes dependientes cuya aceptación de la clave sea conocida deberán ser informadas por el dueño de la clave.

5.7.4 Capacidad de continuidad luego de un desastre

La CA UNLP PKIGrid está localizada dentro de un edificio que es parte de establecimientos gubernamentales para investigación y educación superior. Los planes de continuidad de trabajo y recuperación luego de un desastre para actividades gubernamentales relacionadas con investigación y educación son relevantes.

5.8 Terminación de CA o RA

Antes de que la CA UNLP PKIGrid termine sus servicios, deberá:

- Informar a las Autoridades de Registro, suscriptores y partes dependientes que la CA conozca;
- Hacer a la información sobre su terminación altamente disponible;
- Dejar de emitir certificados;
- Revocar todos los certificados;
- Emitir y publicar una CRL;
- Destruir sus claves privadas y copias de éstas;
- Informar a TAGPMA

En el caso de una terminación normal (programada), el tiempo de notificación mínimo debe ser de 90 días.

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; esto hará que los certificados de los suscriptores puedan usarse hasta que expiren. En este caso la notificación de terminación se dará a no menos de un año y 60 días de la terminación, por ejemplo, no menos de 60 días antes de que la CA deje de emitir nuevos certificados.

6 Controles de seguridad técnica

6.1 Generación e instalación del par de claves

6.1.1 Generación del par de claves

El par de claves para la CA UNLP PKIGrid es generado por personal CA autorizado en una computadora que no esté conectada a la red. Las claves son generadas por software confiable usando OpenSSL. Los pares de claves para certificados de personas naturales (incluyendo agentes RA), Hosts o servicios son generadas por las partes solicitantes en persona en su sistema (interfaz web).

6.1.2 Entrega de claves privadas a un suscriptor

Cada suscriptor DEBE generar su propio par de claves usando la interfaz web UNLP PKIGrid. La CA no genera claves privadas para sus suscriptores.

6.1.3 Entrega de claves privadas a un emisor de certificados

Las claves públicas de los suscriptores son entregadas a la CA emisora por el protocolo HTTP vía interfaz web UNLP PKIGrid.

6.1.4 Entrega de claves públicas de CA a partes dependientes

El certificado de la CA (conteniendo su clave pública) es entregado a suscriptores por transacción on line desde el servidor web online de UNLP PKIGrid. Puede ser bajado desde el repositorio (Véase 2.1).

6.1.5 Tamaño de claves

Claves de longitud menor a 1024 bits no serán aceptadas. La clave de la CA UNLP PKIGrid es de 2048 bits de longitud.

6.1.6 Generación de parámetros de claves públicas y control de calidad

No hay estipulaciones.

6.1.7 Propósitos de uso de las claves (para el campo de uso de clave X.509 v3)

Las claves deberán ser usadas de acuerdo al tipo de certificado:

Con un certificado de entidad destino para

- autenticación
- no-rechazo
- cifrado de datos y claves
- integridad del mensaje
- establecimiento de sesión
- creación de proxy

Con el certificado firmado por la CA

- firma de certificados
- firma de CRL

La firma privada de la CA es la única clave que puede ser usada para firmar certificados y CRLs.

6.2 Controles de Ingeniería de Módulo Criptográfico y Protección de Clave Privada

6.2.1 Estándares y controles de modulo criptográfico

Las entidades destino deberán usar la planilla web disponible en el sitio de la UNLP PKIGrid para generación de claves y CSR.

La clave privada de la CA UNLP PKIGrid es generada usando OpenSSL.

Una instancia extra de la clave privada encriptada con una contraseña generada al azar de por lo menos 15 caracteres deberá ser almacenada en un medio removible, que deberá ser depositado en un lugar seguro y bajo llave; la contraseña deberá ser almacenada en otro

medio removible o escrita, y el medio o papel deberá ser colocado en un sobre sellado y almacenado en un lugar seguro.

Ninguna instancia de la clave privada de la CA (normal o encriptada) deberá residir en el disco permanente de cualquier computadora que esté en línea.

6.2.2 Control multi-persona de clave privada (n de m)

Este tipo de control no se halla instalado todavía

6.2.3 Recuperación de clave privada

Las claves privadas no deben ser recuperadas.

6.2.4 Backup de la clave privada

Todas las copias backup de la clave privada de la CA se mantienen por lo menos tan seguras como la que se utiliza para firmar (por ejemplo, encriptadas y en medios asegurados en una caja fuerte). La contraseña para activar el backup está asegurada dentro de una caja fuerte diferente de la que contiene la clave encriptada.

6.2.5 Archivo de claves privadas

No hay estipulación.

6.2.6 Transferencia de clave privada desde o hacia un módulo criptográfico

No hay estipulación.

6.2.7 Almacenamiento de clave privada en un modulo criptográfico

La clave privada de la CA es activada por una contraseña que, para emergencias, se conserva en un sobre sellado en una caja fuerte. La caja fuerte que contiene la contraseña no contiene ninguna copia de la clave privada.

6.2.8 Método para activar la clave privada

La clave privada de la CA es activada teniendo que entrar en el operador de CA su passphrase (palabra de paso) personal y después la passphrase de la clave privada de la CA

6.2.9 Método para desactivar la clave privada

La clave privada sin encriptar solo deberá almacenarse en la RAM y borrarse cuando la actividad para la cual se necesitaba finalice.

6.2.10 Método de destrucción de clave privada

Véase 6.2.9.

6.2.11 Tasación del Módulo Criptográfico

No hay estipulación.

6.3 Otros aspectos de administración de pares de claves

6.3.1 Archivo de clave pública

La CA archivará todos los certificados emitidos en un medio removible que será almacenado off line en una bóveda de seguridad.

6.3.2 Períodos operativos de certificados y períodos de uso de pares de claves

No hay estipulación en cuanto a la validez del par de claves generado. Solo la validez del certificado emitido por la CA UNLP PKIGrid es definida por este documento CP/CPS.

Los certificados de los suscriptores tienen un período de validez de 13 meses (un año y un mes) o menos si la afiliación de la parte solicitante con el grupo participante en la UNLP Grid es de menos que un año.

El certificado de CA tiene una vida útil de 10 años.

6.4 Datos de activación

6.4.1 Generación e instalación de datos de activación

La clave privada de la CA es protegida por una passphrase sólida que consiste al menos de 15 caracteres.

6.4.2 Protección de datos de activación

Todos los operadores CA UNLP PKIGrid conocen los datos de activación para la clave privada de la CA. Ninguna otra persona conoce los datos de activación. Sin embargo, los datos de activación de la clave privada de la CA también son conservados en un sobre sellado en una caja fuerte separada de las cajas fuertes conteniendo la clave privada y sus copias de backup.

6.4.3 Otros aspectos de datos de activación

No hay estipulación.

6.5 Controles de seguridad computacional

6.5.1 Requerimientos técnicos específicos de seguridad computacional

El servidor que aloje el producto CA corre e un sistema GNU Linux de origen razonable.

No hay otros servicios o software cargados u operados en el servidor de la CA. El servidor recibe parches y otros ajustes ocasionales si lo requiere el riesgo de seguridad, o si el juicio del personal de la CA UNLP PKIGrid lo indica.

6.5.2 Medición de seguridad computacional

No hay estipulación.

6.6 Controles técnicos de vida útil

6.6.1 Controles de desarrollo de sistemas

No hay estipulación.

6.6.2 Controles de administración de seguridad

No hay estipulación.

6.6.3 Controles de seguridad de vida útil

No hay estipulación.

6.7 Controles de seguridad en redes

La máquina firmante de la CA nunca estará conectada a una red de computadoras bajo ninguna circunstancia (no tiene un adaptador para red). Los certificados son firmados en una máquina no conectada a ningún tipo de red, localizada en un ambiente seguro y manejada por una persona entrenada especialmente.

La máquina pública es protegida por un firewall adecuadamente configurado.

6.8 Fecha

Todos los fechados de entradas creadas en los servidores online en la CA UNLP PKIGrid están basados en el tiempo de red provisto por el servidor de tiempo de la CA UNLP PKIGrid, sincronizado con el tiempo oficial provisto por el Observatorio Astronómico de la Facultad de Ciencias Astronómicas y Geofísicas de la UNLP.

El reloj de hardware del sistema off line para firma de certificados y CRL, que determina el fechado de los certificados y CRLs, será sincronizado por el operador en cualquier momento que el host se inicie.

7 Perfiles de Certificado, CRL y OSCP

7.1 Perfil de certificado

Todos los certificados emitidos por la CA UNLP PKIGrid entran en el perfil Internet PKI (PKIX) para certificados X.509 como definido por RFC 3280.

7.1.1 Número(s) de Versión

Solo los certificados X.509 versión 3 son emitidos por la CA UNLP PKIGrid.

7.1.2 Extensiones del certificado

Las extensiones al certificado X.509 v3 que deben estar presentes en los certificados CA de la UNLP PKIGrid son:

Certificados para persona natural:

▪ Basic Constraints:	critical, ca: false
▪ Subject Key Identifier:	hash
▪ Authority Key Identifier:	keyid
▪ Subject Alternative Name:	Email
▪ Key Usage:	critical, digitalSignature, nonRepudiation, KeyEncipherment, dataEncipherment
▪ Extended Key Usage	clientAuth, emailProtection, codeSigning timeStamping
▪ Netscape Cert Type:	SSL Client, S/MIME, Object Signing
▪ Netscape Comment:	STRING
▪ CRL Distribution Points:	URI
▪ Certificate Policies:	OID
▪ Issuer alternative Name:	Email
▪ nsRevocationUrl	URI
▪ nsCaPolicyUrl	URI

Certificados para servidor/servicios:

▪ Basic Constraints:	critical, ca: false
▪ Subject Key Identifier:	Hash
▪ Authority Key Identifier:	Keyid
▪ Subject Alternative Name:	DNS, Email
▪ Key Usage:	critical, digitalSignature, KeyEncipherment, dataEncipherment
▪ Extended Key Usage	serverAuth, clientAuth, timeStamping
▪ Netscape Cert Type:	SSL Server, SSL Client
▪ Netscape Comment:	STRING
▪ CRL Distribution Points:	URI (CRL)
▪ Certificate Policies:	OID
▪ Issuer alternative Name:	Email
▪ nsRevocationUrl	URI
▪ NsCaPolicyUrl	URI

Certificados para la CA:

▪ Basic Constraints:	critical, ca: true
▪ Subject Key Identifier:	hash
▪ Authority Key Identifier:	keyid
▪ Key Usage:	Critical, KeyCertSign, CRLSign
▪ Netscape Comment:	STRING
▪ CRL Distribution Points:	URI
▪ nsRevocationUrl	URI
▪ NsCaPolicyUrl	URI

7.1.3 Algoritmos Identificadores de Objetos

Los OID para algoritmos usados para firma de certificados emitidos por la CA UNLP PKIGrid son:

- Función hash: id-sha1 1.3.14.3.2.26
- Encriptación: rsaEncryption 1.2.840.113612.1.1.1
- Firma: sha1WithRSAEncryption 1.2.840.113612.1.1.5

7.1.4 Formas del nombre

Cada entidad tiene Nombre Distinguido (DN) único e inequívoco en todos los certificados emitidos a la misma entidad por la CA UNLP PKIGrid. El DN debe estar estructurado como definido en ITUT Standards Recommendation X.501.

Issuer:

C=AR, O=e-Ciencia, OU=UNLP, L=CeSPI, CN=PKIGrid,

Subject EE:

C=AR, O=e-Ciencia, OU=UNLP CN=Javier Diaz

L indicará el nombre de la RA. La lista válida de RAs estará disponible en el sitio público.

7.1.5 Restricciones de Nombre

No hay ninguna restricción de nombre salvo las derivadas de las estipulaciones en 7.1.4, 3.1.2 y 3.1.1.

7.1.6 Identificador de objeto de Política de Certificado

El OID de este CP/CPS es 1.2.840.113612.5.4.2.3.1.0.2.7S (versión en español)

7.1.7 Uso de la extensión de Restricciones de Política

No hay estipulaciones.

7.1.8 Sintáctica y semántica de calificadores de política

No hay estipulaciones.

7.1.9 Procesamiento de semántica para la extensión de Políticas de Certificado críticas

No hay estipulaciones.

7.2 Perfil CRL

7.2.1 Número(s) de Versión

La CA UNLP PKIGrid crea y publica CRLs X.509 v2.

7.2.2 Extensiones de CRL y campos de CRL

La CA de UNLP PKIGrid deberá emitir CRLs completas para todos los certificados emitidos por ella independientemente de la razón de la revocación. La razón de la revocación no deberá estar incluida en la CRL.

La CRL deberá incluir la fecha para la cual la próxima CRL deberá ser emitida. Una nueva CRL deberá ser emitida antes de esa fecha si nuevas revocaciones son emitidas.

Las extensiones de CRL que deberán estar incluidas son:

- El Identificador de Clave de Autoridad
- El número de CRL

No se usarán extensiones de campos de CRL.

7.3 Perfil OCSP

No se usa.

7.3.1 Número(s) de versión

No hay estipulaciones.

7.3.2 extensiones OCSP

No hay estipulaciones.

7.3.3 Restricciones de nombre

No hay ninguna restricción de nombre salvo las derivadas de las estipulaciones en 7.1.4, 3.1.2 y 3.1.1.

7.3.4 Identificador de objeto de Política de Certificado

El OID de este CP/CPS es 1.2.840.113612.5.4.2.3.1.0.2.7S (versión en español)

7.3.5 Uso de la extensión de Restricciones de Política

No hay estipulaciones.

7.3.6 Sintáctica y semántica de calificadores de política

No hay estipulaciones.

7.3.7 Procesamiento de semántica para la extensión de Políticas de Certificado críticas

No hay estipulaciones.

8 Auditoría de desempeño y otras inspecciones

8.1 Frecuencia o circunstancias de la inspección

La CA de la UNLP PKIGrid deberá hacer por lo menos una auto-inspección al año para asegurarse de que el desempeño de las operaciones sea acorde al documento CP/CPS.

La CA deberá inspeccionar el desempeño de las RA de acuerdo al documento CP/CPS en vigencia por lo menos una vez al año.

Las auditorías operacionales internas deberán ser realizadas por personas no relacionadas al staff de la CA/RA.. Las auditorías internas deben realizarse por lo menos una vez al año.

8.2 Identidad/calificaciones del inspector

No hay estipulaciones.

8.3 Relación del inspector con la entidad inspeccionada

Las inspecciones serán hechas por personal de la CA UNLP PKIGrid o miembros de la comunidad UNLP Grid.

Una auditoría externa puede ser realizada por el departamento argentino de gobierno o la institución académica.

En el caso de que otras CAs confiables o partes dependientes pidieran una inspección externa, el costo de la inspección será cubierto por la parte demandante, exceptuando el costo del personal e infraestructura de la CA UNLP PKIGrid.

8.4 Temas incluidos por la inspección

La auditoría verificará que los servicios provistos por la CA se rijan por la última versión aprobada del CP/CPS.

8.5 Acciones como resultado de deficiencia

En caso de una deficiencia, el administrador de la CA UNLP PKIGrid anunciará los pasos que deberán seguirse para remediar esta deficiencia. Este anuncio deberá incluir un horario programado.

Si una deficiencia descubierta tuviera consecuencias directas en la confiabilidad del proceso de certificación, los certificados (sospechados de haber sido) emitidos bajo la influencia de este problema deberán ser revocados cuanto antes.

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.

9 Otros aspectos legales y comerciales

9.1 Tarifas

No se cobrarán tarifas para el servicio de certificación de la CA de la UNLP PKIGrid y por lo tanto no habrá encumbramientos financieros.

9.1.1 Tarifas de emisión o renovación de certificados

Véase 9.1.

9.1.2 Tarifas de acceso al certificado

Véase 9.1.

9.1.3 Tarifas de acceso a información de estado o revocación

Véase 9.1.

9.1.4 Tarifas por otros servicios

No se cobrarán tarifas por acceder a la CP y CPS u otra información de estado de CA.

9.1.5 Política de reembolso

Véase 9.1.

9.2 Responsabilidad financiera

No se aceptará responsabilidad financiera alguna por certificados emitidos bajo esta política.

9.2.1 Cobertura de seguro

No hay estipulaciones.

9.2.2 Otros aspectos

No hay estipulaciones.

9.2.3 Cobertura de garantía o seguro para entidades de destino

No hay estipulaciones.

9.3 Confidencialidad de información comercial

9.3.1 Alcance de información confidencial

No hay estipulaciones.

9.3.2 Information fuera del alcance de la información confidencial

No hay estipulaciones.

9.3.3 Responsabilidad de protección de información confidencial

No hay estipulaciones.

9.4 Información privada o personal

El servicio de la CA UNLP PKIGrid recolecta información sobre sus suscriptores. La información incluida en certificados y CRLs emitidos no es considerada confidencial.

La CA UNLP PKIGrid recolectará el nombre del suscriptor, los números telefónicos del lugar de trabajo y dirección de correo electrónico. Adicionalmente, para administradores y operadores RA, la información personal de contacto será guardada por la CA (número telefónico y dirección del lugar de trabajo).

Bajo ninguna circunstancia la CA de la UNLP PKIGrid tendrá acceso a las claves privadas de suscriptor alguno para el cual emita un certificado.

9.4.1 Plan de privacidad

No definido por el momento.

9.4.2 Información considerada privada

La información provista por el suscriptor para verificar su identidad será tomada como confidencial, exceptuando la incluida en el certificado.

9.4.3 Información considerada no privada

La información incluida en certificados y CRLs emitidos no es considerada confidencial. La información de contacto de una RA no es considerada confidencial ya que es información que generalmente está disponible en las páginas Web de los empleadores de la RA.

Las estadísticas referidas a emisión y revocación de certificados contiene información no personal y no es considerada confidencial.

9.4.4 Responsabilidad de protección de información privada

La responsabilidad de proteger la información privada descansa en la CA de la UNLP PKIGrid y sus RAs acreditadas.

9.4.5 Aviso y consentimiento del uso de información privada

En caso de que la CA UNLP PKIGrid o cualquiera de sus RAs acreditadas deba usar información privada deberá pedir al suscriptor que exprese su consentimiento escrito. Ningún suscriptor deberá estar bajo la impresión de que es su obligación brindar su consentimiento.

9.4.6 Revelación de información confidencial por procesos administrativos-o judiciales

La CA no deberá revelar información confidencial a ninguna tercera persona o parte excepto por expresa autorización del suscriptor o cuando se requiera por oficiales de seguridad pública que exhiban la apropiada documentación legal.

9.4.7 Otras circunstancias de revelación de información

Revelación a pedido del dueño de acuerdo con las Leyes de Protección de Datos. Específicamente, la información será revelada al suscriptor si la CA ha recibido un e-mail firmado del suscriptor pidiendo la información. La CA no pedirá remuneración monetaria por este servicio.

La CA reconocerá pedidos escritos para la revelación de información personal de un suscriptor solo si el suscriptor puede ser autenticado apropiadamente.

9.5 Derechos de propiedad intelectual

La CA de la UNLP PKIGrid no reclamará ningún Derecho de Propiedad Intelectual (DPI) sobre certificados que haya emitido.

Partes de este documento están inspiradas o incluso copiadas (en ningún orden particular) de AUSTRIANGRID, CERN, CNRS, German Grid, UK e-Science, IRISGrid, GRID Canada, y puede estar indirectamente como parte de documentos en los que los anteriores se inspiran.

Cualquier persona podrá copiar cualquier versión de la CP/CPS de la CA UNLP PKIGrid, siempre y cuando incluyan un reconocimiento de la fuente.

La CA UNLP PKIGrid debe otorgar a TAGPMA e IGTF el derecho de redistribución ilimitada de su información.

9.6 Representaciones y garantías

9.6.1 Representaciones y garantías de la CA

La CA de la UNLP PKIGrid garantiza la emisión de certificados solo a suscriptores identificados por solicitudes recibidas de RAs por vías seguras. La CA de la UNLP PKIGrid revocará un certificado solo en respuesta a una solicitud autenticada del suscriptor o la RA que aprobó la solicitud del suscriptor, o si lleva consigo prueba razonable de que las circunstancias de revocación están presentes.

La CA UNLP PKIGrid no garantiza sus procedimientos ni se responsabiliza de problemas que surjan de su operación o el uso de los certificados que provee, y no da garantías de la seguridad o idoneidad del servicio.

La CA solo garantiza verificar las identidades de los suscriptores de acuerdo a los procedimientos descritos en este documento.

La CA no acepta responsabilidad por pérdidas financieras o de otra índole originadas por daños o impedimentos accidentales resultantes de su operación. Ninguna otra responsabilidad, implícita o explícita, es aceptada.

9.6.2 Representaciones y garantías de la RA

Todas las RAs acreditadas deberán realizar las tareas de identificación de las partes solicitantes como descrito en 3.2.3. y 3.2.2. en base al mejor esfuerzo. No se aceptan otras garantías.

Una RA puede concluir, a su propio riesgo estrictamente, un acuerdo mas estricto con sus suscriptores, pero esto nunca deberá comprometer a la CA UNLP PKIGrid ni a ninguna otra RA acreditada.

Es responsabilidad de la RA solicitar la revocación de un certificado si la RA considera que las circunstancias de revocación están presentes.

9.6.3 Representaciones y garantías del suscriptor

Al solicitar un certificado a la CA UNLP PKIGrid se compromete a usar y proteger el certificado y las claves certificadas de acuerdo a las estipulaciones del documento CP/CPS en efecto a la fecha de emisión de dicho certificado. El suscriptor podrá, sin embargo, aplicar observaciones más estrictas.

Los suscriptores deben:

- Leer y adherir a los procedimientos publicados en este documento
- Usar el certificado para los propósitos permitidos solamente
- 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;
    - (Certificados personales) protegiendo la Contraseña de otros;
- Notificar inmediatamente a la CA de la UNLP PKIGrid y otras partes dependientes si la clave privada se pierde o se halla comprometida;
- Solicitar 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.

En caso de un incumplimiento de las estipulaciones en el documento CP/CPS al cual el suscriptor ha adherido al solicitar un certificado de la CA UNLP PKIGrid, dicho certificado deberá ser revocado inmediatamente. No se requieren mayores garantías del suscriptor.

9.6.4 Representaciones y garantías de las parte dependiente

Una parte dependiente deberá aceptar el certificado del suscriptor para propósitos de autenticación si:

- La parte dependiente conoce las CP y CPS de la CA que generaron el certificado antes de llegar a conclusiones sobre si confiar en el certificado del suscriptor; y
- La dependencia es razonable y de buena fe en vista de todas las circunstancias conocidas por la parte dependiente en el momento de dependencia; y

- El certificado es usado para propósitos permitidos solamente; y
- La parte dependiente ha verificado el estado del certificado para su propia satisfacción antes de la dependencia.

La CRL debe estar convalidada por la parte dependiente y el certificado del suscriptor debe estar verificado contra la CRL.

9.6.5 Representaciones y garantías de otros participantes

No hay estipulaciones.

9.7 Renuncia de garantías

La CA de la UNLP PKIGrid utiliza software y procedimientos para la autenticación de entidades que, para su mejor conocimiento, corren de acuerdo a este documento CP/CPS. Sin embargo, declina cualquier garantía de su completa exactitud.

Además, la CA de la pkUNLGrid no puede hacerse responsable de cualquier uso incorrecto de su certificado por un suscriptor o cualquier otra parte que deba encontrarse en posesión de la clave privada correspondiente, y de cualquier aceptación sin previo estudio de cualquiera de sus certificados por una parte dependiente.

Cualquier parte dependiente que acepte un certificado para cualquier uso para el cual este no había sido emitido lo hace a su propio riesgo y responsabilidad.

9.8 Limitaciones de responsabilidad

Excepto que se exprese lo contrario por la ley argentina la CA UNLP PKIGrid declina cualquier responsabilidad por daños sufridos por una parte dependiente que haya aceptado uno de sus certificados, o un suscriptor cuyo certificado válido sea rechazado o cuyo certificado revocado sea aceptado sin problemas por una parte dependiente.

También declina cualquier responsabilidad por daños causados por la no-emisión de un certificado solicitado, o por la revocación de un certificado iniciado por la CA o la RA apropiada en conformidad con este documento CP/CPS.

9.9 Indemnizaciones

La CA UNLP PKIGrid declina cualquier pago de indemnizaciones por daños ocasionados por el uso o rechazo de certificados que emite.

Las entidades destino deberán indemnizar y eximir de responsabilidad a la CA UNLP PKIGrid y todas las RAs apropiadas operando bajo este CP/CPS de todas las afirmaciones y acuerdos resultantes de información fraudulenta proveída con el formulario de certificación, y el uso y aceptación de un certificado que viole las provisiones de este documento CP/CPS.

9.10 Período y terminación

9.10.1 Período

Este documento es efectivo luego de su publicación en el web site de la CA UNLP PKIGrid con la fecha de comienzo especificada en el sitio.

No se estipula un período para su expiración.

9.10.2 Terminación

Este CP/CPS permanece efectivo hasta ser suplantado por una nueva versión.

9.10.3 Efecto de terminación y supervivencia

Su texto deberá permanecer disponible por lo menos 5 años luego de que el ultimo certificado emitido bajo este CP/CPS expire o sea revocado.

9.11 Notificación individual y comunicación con participantes

Todas las comunicaciones por e-mail entre la CA y sus RAs acreditadas DEBEN ser firmadas con una clave certificada.

Todas las comunicaciones por e-mail entre la CA o una RA y un suscriptor DEBEN ser firmadas con una clave certificada para poder tener validez de prueba.

9.12 Enmiendas

9.12.1 Procedimiento de enmienda

Las enmiendas a este CP/CPS deben pasar el mismo procedimiento que la aprobación inicial (véase 1.5.4). La reformulación de provisiones para mejorar su entendimiento y correcciones puramente gramáticas no son consideradas enmiendas.

9.12.2 Período y mecanismo de notificación

El documento CP/CPS enmendado será publicado en las páginas web de la CA UNLP PKIGrid por lo menos dos semanas antes de hacerse efectivo.

La CA UNLP PKIGrid informará de esto a sus suscriptores y todas las partes dependientes que conozca por medio de un e-mail.

9.12.3 Circunstancias bajo las cuales el OID deberá ser cambiado

En cada nueva versión del CP/CPS DEBE cambiar el OID. Cambios sustanciales pueden causar el cambio de OID. Esta decisión es tomada por el administrador de la CA UNLP PKIGrid y enviada a TAGPMA para su aprobación.

9.13 Provisiones sobre resolución de disputas

Disputas originadas por el CP/CPS deberán ser resueltas por el administrador de la CA UNLP PKIGrid.

9.14 Ley gobernante

La CA UNLP PKIGrid y su operación están sujetas a la ley argentina. Todas las disputas legales que surjan del contento de este documento CP/CPS, la operación de la CA UNLP PKIGrid y sus RAs acreditadas, el uso de sus servicios, la aceptación y uso de cualquier certificado emitido por la CA UNLP PKIGrid deberá ser tratada de acuerdo con la ley argentina.

9.15 Cumplimiento de la ley

Todas las actividades relacionadas a la solicitud, emisión, uso o acepto de un certificado de la CA UNLP PKIGrid debe cumplir con la ley Argentina.

Todas las actividades iniciadas en o destinadas a otro país que Argentina también deberán cumplir la ley de éste país.

9.16 Provisiones misceláneas

9.16.1 Acuerdo entero

Este documento CP/CPS suplanta a cualquier acuerdo, escrito u oral, entre las partes cubiertas por el presente documento.

9.16.2 Asignaciones

No hay provisiones.

9.16.3 Separabilidad

Si una cláusula del presente documento CP/CPS se volviera nulo porque ha sido declarado no válido o no ejecutable por una corte u otra entidad del cumplimiento de la ley, esta cláusula se tornará nula (y debería ser reemplazada lo más pronto posible por una cláusula pertinente), pero el resto del documento seguirá siendo aplicable.

9.16.4 Cumplimiento (tarifas de abogados y dispensa de derechos)

No hay estipulaciones.

9.16.5 Fuerza mayor

Todos los eventos que comprometan a los servicios de la CA UNLP y estén fuera del control razonable de la UNLP serán tratados inmediatamente por TAGPMA e IGTF.

9.17 Otras provisiones

No hay estipulaciones.

10 Referencias

- Certification Authority AustrianGrid CA Certificate Policy (CP) and Certification Practices Statement (CPS), Version 1.0.0, Marzo 2005 https://ca.austriangridca.at/CP_CPS/AustrianGridCA_CP_CPS_1_0_0.pdf.
- SWITCH (the Swiss Education & Research Network) Certificate Policy and Certification Practice Statement (CP/CPS) ver:1.1.6 http://www.switch.ch/pki/SWITCH_CP-CPS.pdf
- DOEGrids Certificate Policy And Certification Practice Statement. Version 2.6. http://www.doegrids.org/Docs/CP-CPS.pdf
- Esnet Root CA Certificate Policy And Certification Practice Statement, Version 1.3, September 2003 http://www.ar.net/CA/d1b603c3/Certificate%20Policy.pdf
- Eugridpma. European Policy Management Authority for Grid Authentication http://www.eugridpma.org/
- Grid Canada Certification Authority Certificate Policy and Certification Practices Statement. http://www.gridcanada.ca/ca/gc-ca-cp-cps-1.1.htm
- 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, Enero 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, Abril 2002 http://www.ietf.org/rfc/rfc3280.txt
- RedIris Certification Authority Certificate Policy and Certification Practices Statement http://www.irisgrid.es/pki/policy/1.3.6.1.4.1.7547.2.2.4.1.0.0/
- S. Chokani and W. Ford, " Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework" , RFC 2527, Marzo 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, Noviembre 2003 [reemplaza a 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. Septiembre 20, 2005

- UK eScience Certification Authority Certificate Policy and Certification Practices Statement, Version 1.1, Marzo 2005 http://www.grid-support.ac.uk/files/cps/cps-1.1.pdf