Universidad Nacional de La Plata

UNLP PKIGrid CA

Obtener un Certificado

de Usuario/Host/Servicio

Staff:

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

OID Document 1.2.840.113612.5.4.2.3.4.0.1.0S.
Noviembre 16, 2006

Obtener un Certificado de Usuario/Host/Servicio

Objetivo: Delinear los pasos a seguir para obtener un certificado de usuario/host/servicio utilizando un navegador.

El procedimiento consta de tres (3) pasos básicos:

a) *Obtener el certificado de la autoridad de certificación CA*
b) *Requerir un certificado de usuario/host/servicio*
c) *Obtener el certificado de usuario firmado por la CA*

Se recomienda leer el documento *"Obligaciones de los Suscriptores*"
Si necesita una guía mas detallada del procedimiento leer el documento paso a paso: *"Como obtener un certificado desde Internet Explorer*".
A continuación se detallan los ítems mencionados anteriormente:

Ante cualquier duda consulte al Operador de la RA raoperator@pkipgrid.unlp.edu.ar.

a) Obtener el certificado de la CA

Antes de poder solicitar un certificado de usuario/host/servicio es necesario confiar en la CA. Para ello es necesario descargar el certificado de la entidad raíz CA de confianza e instalarlo en su Browser.
A continuación se detallan los pasos necesarios para completar este procedimiento.

1. Conectarse al sitio público de la PKI: https://www.pkigrid.unlp.edu.ar
2. Seleccionar "CRL y certificado raíz"
3. Seleccionar "Certificado de la CA"
4. Seleccionar certificado de la CA en formato CRT. Los formatos disponibles son CRT[1], PEM[2], DER[3], CER[4] y TXT[5]. El mecanismo de importación puede variar de acuerdo al tipo de formato seleccionado y navegador utilizado. En algunos casos se importa directamente y en otros debe ser copiado el contenido en un archivo y posteriormente instalarlo desde el navegador.
5. Una vez instalado el certificado verifique que la importación fue satisfactoria.

b) Requerir un certificado de usuario/host/servicio

Una vez instalado el certificado de la autoridad de certificación emisora podrá solicitar un certificado de usuario/host/servicio conectándose al sitio público de la misma.
Recuerde que la clave privada cifrada quedará en la computadora desde la cual realizó la solicitud del certificado, a no ser que se este utilizando un dispositivo criptográfico

A continuación se detallan los pasos necesarios para completar el procedimiento.

[1] CRT para los navegadores Mozilla, Netscape e Internet Explorer.
[2] PEM para formato importable servidor.
[3] DER para otros Microsoft Internet Explorer
[4] CER para otros Microsoft Internet Explorer
[5] TXT para formato texto

1. Conectarse al sitio público de la PKI: https://www.pkigrid.unlp.edu.ar
2. Seleccionar “Obtener un certificado”
3. Seleccionar “Solicitar un Certificado”
4. Seleccionar el tipo de certificado a requerir (usuario/host/servicio)
5. Complete los datos requeridos:
    - el email que será utilizado para el envío de mails firmados digitalmente
    - Nombre completo siguiendo las reglas establecidas en el CP/CPS
    - La unidad organizacional OU
    - Seleccionar el tipo de certificado.
    - Seleccionar la RA correspondiente a la cual le esta solicitando el certificado
    - La palabra de paso utilizada para encriptar la clave privada. (La cual debe ser mantenida en secreto y segura)
    - Reingreso de la misma para verificación que el usuario no cometió un error de tipeo
    - Longitud de la clave que debe ser de 1024
6. Verificar que los datos ingresados sean correctos. Podrá especificar si la clave privada será almacenada en un dispositivo criptográfico o en el almacén de default de su navegador
7. Imprima o guarde una copia digital del comprobante de solicitud del certificado.
8. Dentro de los nueve (9) días deberá presentarse ante la RA para validar su identidad y aprobar el requerimiento, con documento de identidad y comprobante impreso de solicitud. El aval de la Relying Party deberá haber sido presentado a la RA. Pasado dicho lapso el requerimiento será dado de baja

c) Obtener el certificado de usuario firmado por la CA

Dentro de los tres (3) días de haberse presentado ante la RA deberá ser notificado de la emisión de su certificado. El mismo deberá ser descargado del sitio público de la CA. Desde la misma PC desde la que generó el requerimiento
A continuación se detallan los pasos necesarios para completar este procedimiento.

1. Conectarse al sitio público de la PKI: https://www.pkigrid.unlp.edu.ar
2. Seleccionar “Obtener un certificado”
3. Seleccionar “Obtener el Certificado solicitado”
4. Ingresar el ID del serial del certificado o el serial del requerimiento o su ID (ver comprobante impreso o seleccionar del menú “Certificados emitidos y verificar el ID desde el listado disponible)
5. Una vez seleccionado el tipo de formato (PEM) pulse “Install de certificate”, tras lo cual comenzará el proceso de instalación de su certificado en su navegador:
6. Debe verificar si la instalación se completó satisfactoriamente
7. Una vez completado el paso anterior quedará el certificado instalado en el navegador como propio. De allí puede ser exportado e importado en cualquier cliente de mail.
8. **Importante:** No olvide generar una copia de seguridad de su certificado en un medio removible y protegido.