FACULTAD DE INFORMÁTICA
UNIVERSIDAD NACIONAL DE LA PLATA

TESINA DE GRADO

AMPLIACIÓN Y MEJORA DE SERVICIOS EN LA INFRAESTRUCTURA DE CLAVE PÚBLICA PARA E-CIENCIA DE LA UNLP (PKIGRID UNLP)

GUIDO JOSÉ CELADA - JUAN MANUEL FILANDINI

ÍNDICE

ÍNDICE

MOTIVACIÓN

- La UNLP cuenta con un proyecto a cargo del CeSPI para la emisión de certificados digitales para su uso en aplicaciones de E-Ciencia en la comunidad académica argentina (PKIGrid UNLP).
- Es de interés para la UNLP mejorar los servicios brindados e incorporar nuevos servicios así como evaluar otras alternativas para su implementación.

OBJETIVO

- Presentar una alternativa a la tecnología que se utiliza actualmente en PKIGrid UNLP.
- Proponer mejoras a los servicios existentes y evaluar la posibilidad de incorporar nuevos servicios.
- Realizar una demostración de la migración tecnológica de la infraestructura presente a la alternativa propuesta.

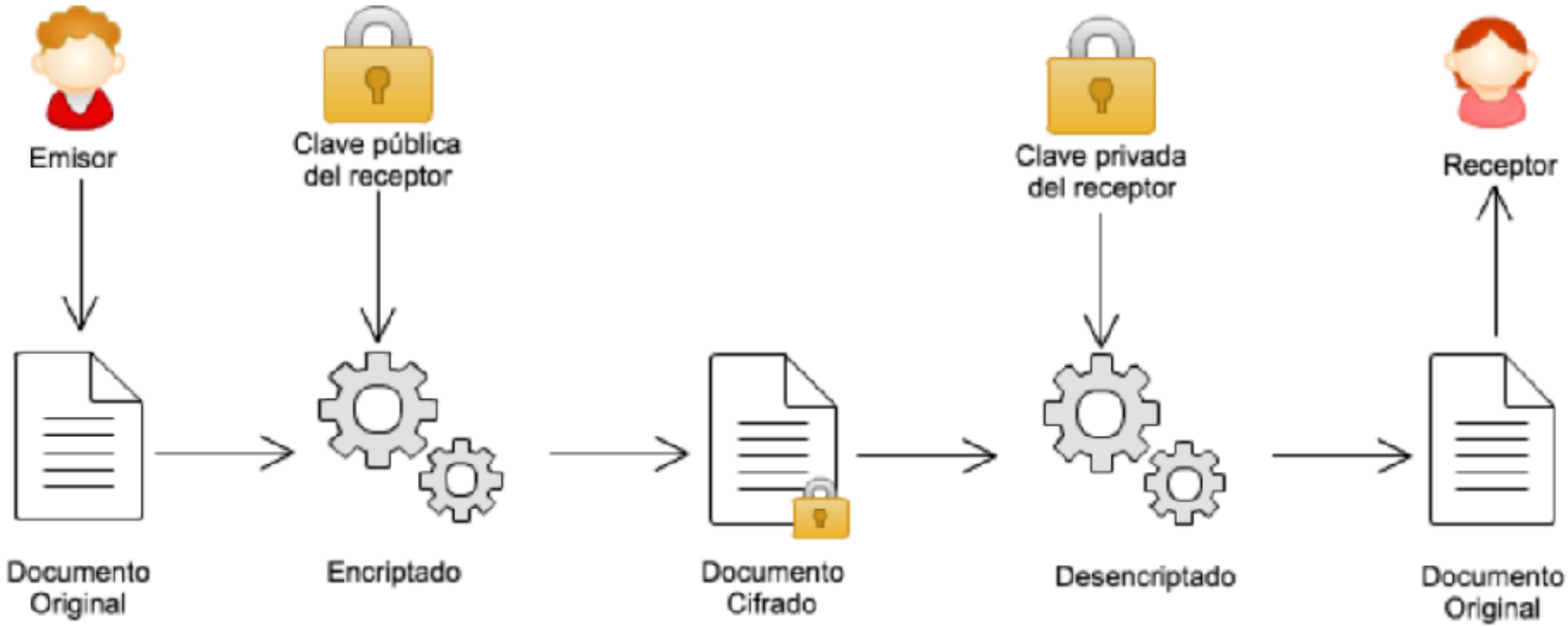
ÍNDICE

BASES DE LA CRIPTOGRAFÍA

- **Confidencialidad:** La información es accesible únicamente al personal autorizado
- **Integridad:** El mensaje es correcto y completo.
- **Vinculación:** El mensaje se puede vincular a una persona o a un sistema de gestión criptográfico automatizado.
- **Autenticación:** Se proporcionan mecanismos que permiten verificar la identidad del comunicador.

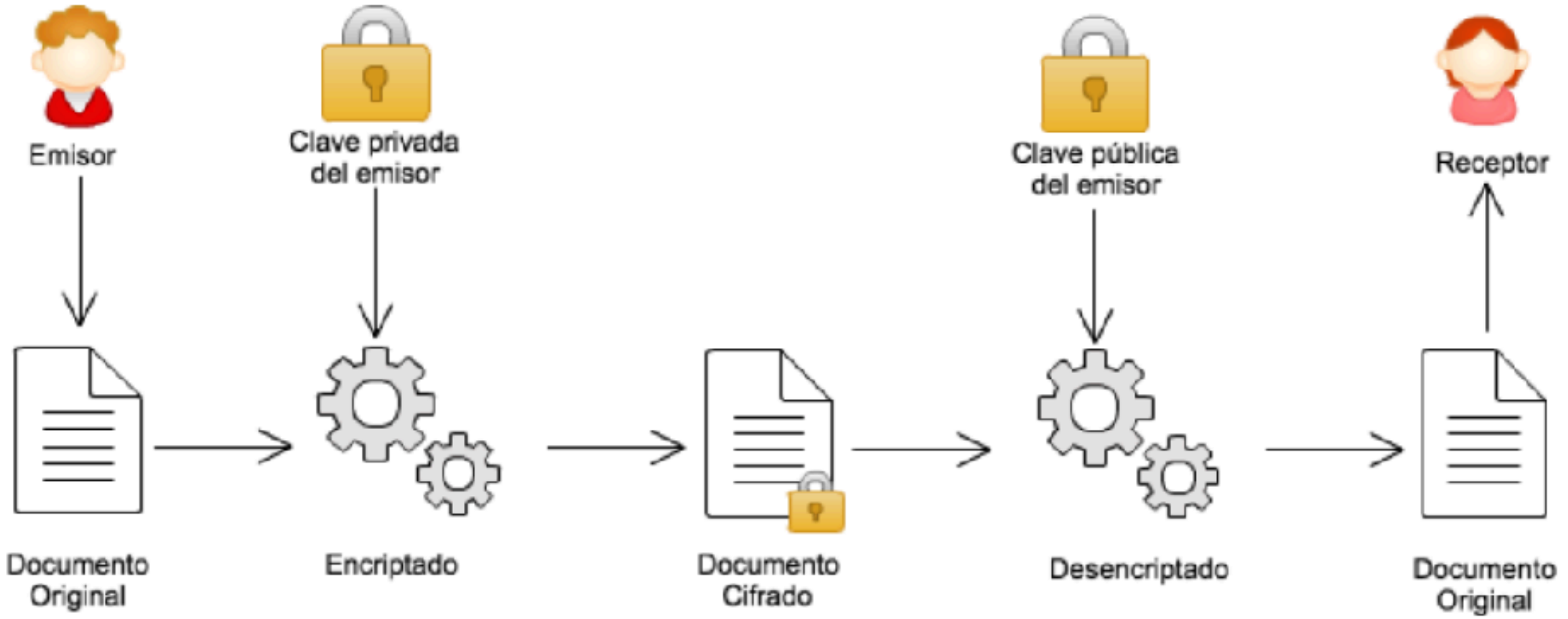
TIPOS DE SISTEMAS CRIPTOGRÁFICOS

- Criptografía de clave pública - Modo encriptación



TIPOS DE SISTEMAS CRIPTOGRÁFICOS

- Criptografía de clave pública - Modo autenticación



ÍNDICE

INFRAESTRUCTURA DE CLAVE PÚBLICA (PKI)

- Utiliza la criptografía de clave pública.
- Es básicamente una manera de relacionar las identidades de personas u organizaciones con sus respectivas claves públicas.
- Se encarga de la administración de los certificados digitales.

COMPONENTES

Certificados Digitales

Autoridad de Registro

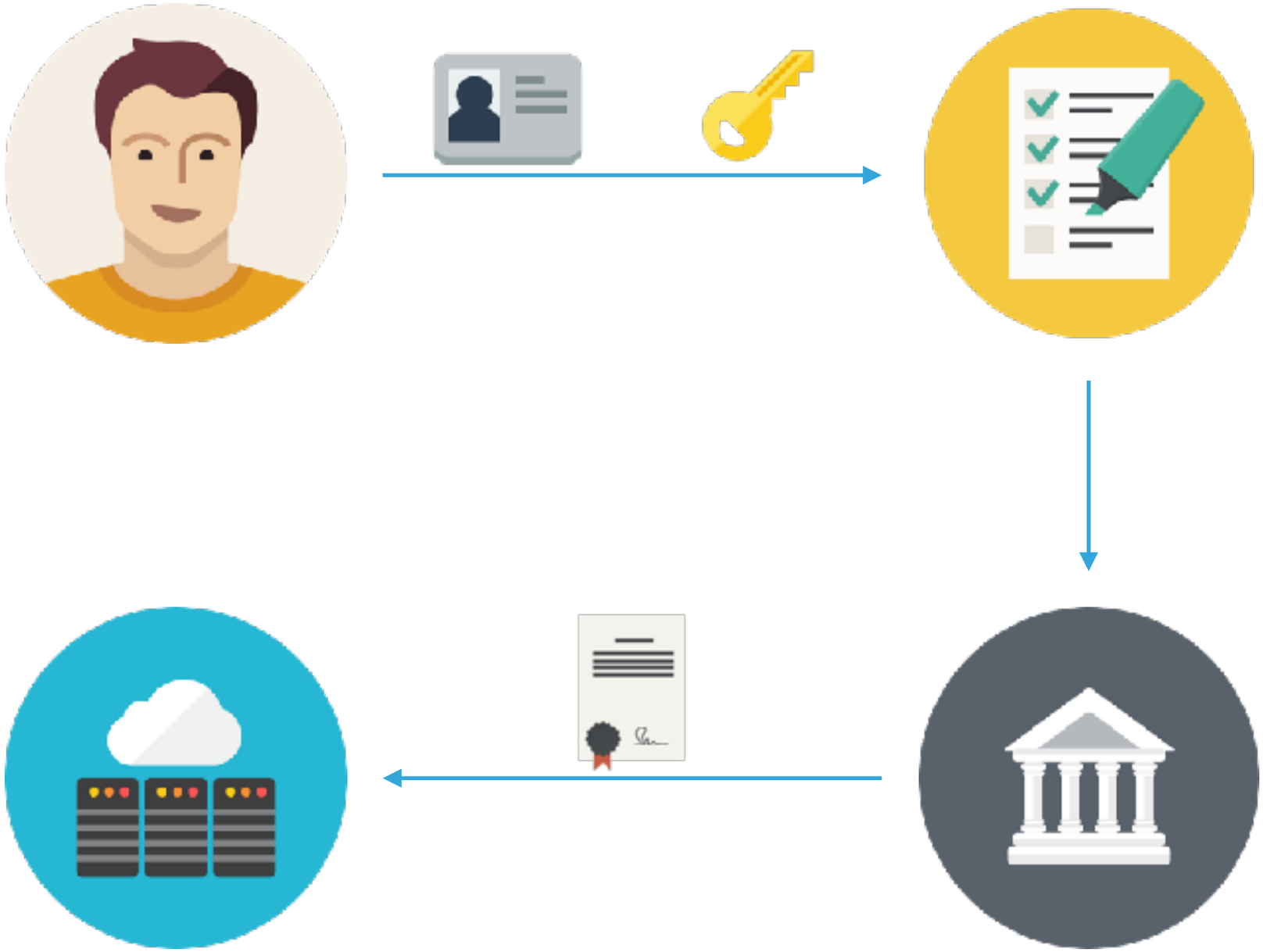
Autoridad Certificadora

CP & CPS

Repositorio de certificados

Listas de revocación

PROCESO DE EMISIÓN DE UN CERTIFICADO DIGITAL



TIPOS DE USO DE UN CERTIFICADO DIGITAL

Autenticación:

- Autenticación HTTPS.
- Firma digital de documentos.
- Firma digital de emails.
- Firma digital de software.

TIPOS DE USO DE UN CERTIFICADO DIGITAL

Encriptación:

- Navegación segura encriptada utilizando SSL.
- Encriptación de e-mail.
- Encriptación de documentos sensibles.
- Redes inalámbricas seguras utilizando PEAP & EAP-TLS.
- Encriptación de filesystem.

ÍNDICE

APLICACIONES GRID PARA E-CIENCIA

- Promueven adelantos en investigación a partir de la posibilidad de compartir recursos globalmente.
- Es importante fortalecer los mecanismos de seguridad subyacentes a fin de garantizar que los mismos sean usados únicamente por grupos autorizados y de una manera adecuada.
- Existen varias iniciativas de PKI mundialmente fortalecen la seguridad de estas aplicaciones.

PKIGRID UNLP

- La UNLP cuenta con una PKI para emisión de certificados para Argentina acreditada por TAGPMA la cual soporta las actividades de E-Ciencia de la comunidad académica Argentina.
- Esta PKI se encuentra implementada por el CeSPI utilizando OpenCA.

ÍNDICE

OPENCA

- Proyecto open source para implementar y administrar una PKI completa.
- Permite realizar muchas de las operaciones de la PKI a través de una interfaz web.
- Implementado en el lenguaje de programación **Perl**.

OPENCA

OpenCA
http://www.openca.org

Email | Print

PKI Info | My Certificates | Information | Help | Languages | Home

Request a Certificate

To request a certificate use one of this links. You will be asked to fill in a form and to confirm inserted data. After having completed the request you will have to go to the chosen RA for request approval.

Browser Certificate Request
Request form with automatic browser detection

Authenticated Browser Certificate Request
Request form with automatic browser detection

Server Certificate Request
PKCS#10 PEM formatted Request Upload Form

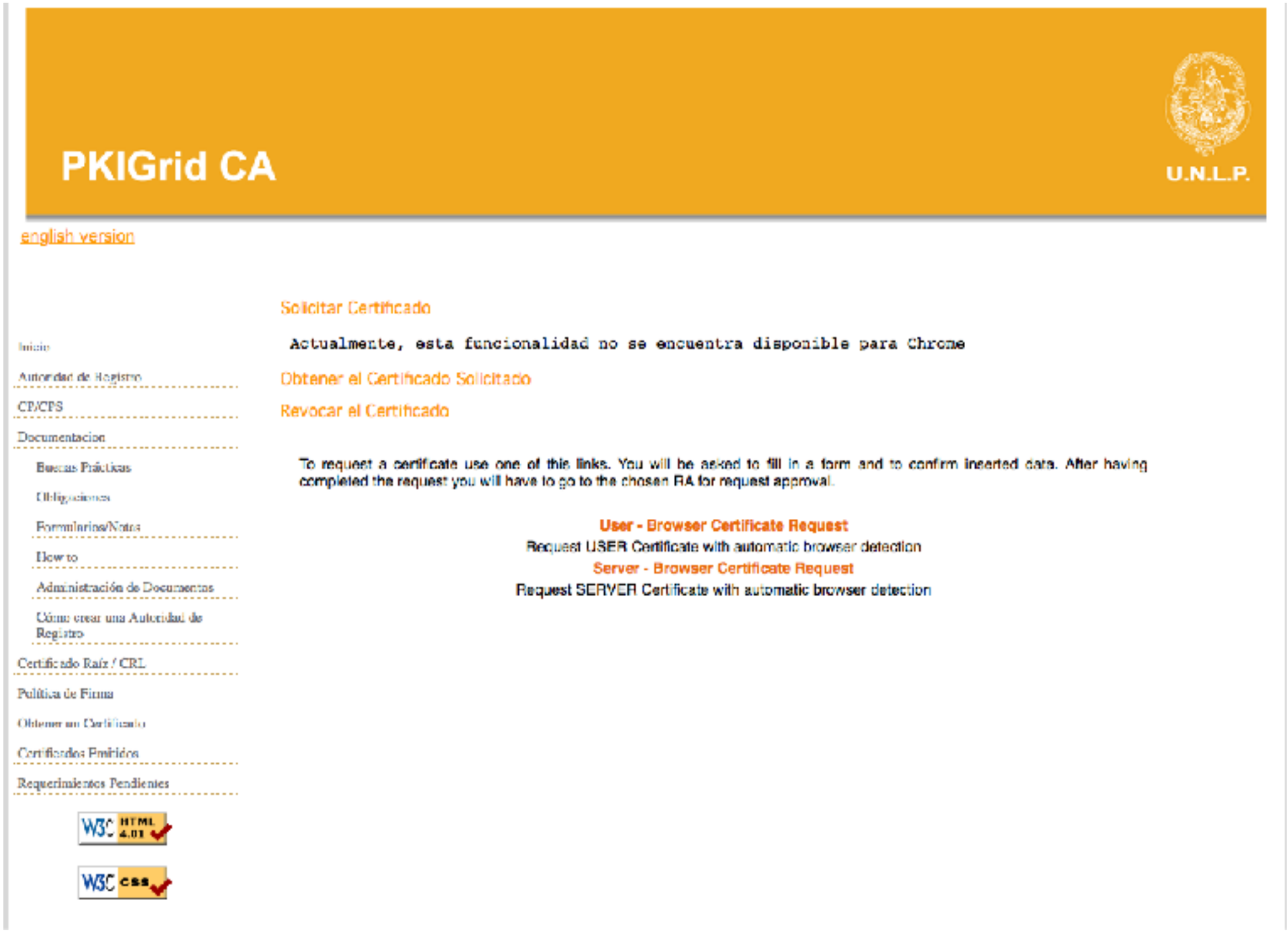
Search | My Certs | My Profile | Messages | Notices

OPENCA

- Este producto se ha adaptado para cumplir con las reglas definidas en las políticas de certificados y declaraciones de prácticas de certificación de la PKI a implementar, las cuales cumplen con las pautas definidas por TAGPMA.

- Algunas de estas adaptaciones fueron:
  - Perfiles de certificados (**.conf, *.ext*)
  - Adaptación de configuración y scripts del módulo *PUB*.

OPENCA



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

PROBLEMAS

- **Soporte**: OpenCA no tuvo más actualizaciones desde el año 2013, no provee soporte, la comunidad online es casi nula y la documentación oficial es sumamente escasa e incompleta.
- **Actualizaciones del software**: Las actualizaciones de OpenCA poseen una instalación compleja.
- **Problemas de encoding de acentos**: Las palabras con acentos y caracteres especiales no se muestran de una manera correcta en la web.
- **Soporte de exploradores**: OpenCA solo posee soporte para Mozilla Firefox para solicitar un certificado.
- **Falta de emails de vencimiento de certificados**: Se requiere que se envíen alertas por email cuando se aproxime la fecha de vencimiento del certificado.
- **OCSP no habilitado**.

ÍNDICE

EJBCA

- Es un paquete de software libre (Licencia GNU).
- Alternativa a OpenCA.
- Implementado en **Java EE**.
- Independiente de plataforma.
- Soporta el uso de HSM.
- Presenta una separación de la vista pública y la vista de administración.

SOLUCIÓN

- **Soporte:** EJBCA posee una mantenibilidad constante en su proyecto, presenta una documentación completa y actualizada.
- **Actualizaciones de software:** Cuando se realiza una actualización no es necesario re-instalar ni re-configurar EJBCA.
- **Problemas de encoding de acentos:** EJBCA no presenta este problema.
- **Soporte de exploradores:** EJBCA posee soporte para todos los exploradores modernos.
- **Falta de emails de vencimiento de certificados:** EJBCA presenta una interfaz intuitiva en donde se pueden configurar diversos eventos de emails.
- **OCSP:** EJBCA permite operar con OCSP.

ONLINE CERTIFICATE STATUS PROTOCOL (OCSP)

- Alternativa más eficiente a las CRL.
- Verifica la validez de un certificado en tiempo real.
- En EJBCA viene activado por defecto.
- La CA actúa como OCSP Responder.

ÍNDICE

MIGRACION DE CERTIFICADOS Y CRL EXISTENTES

- EJBCA soporta la importación de certificados de otro sistema.
- Provee comandos para importar certificados individualmente o por bloques.

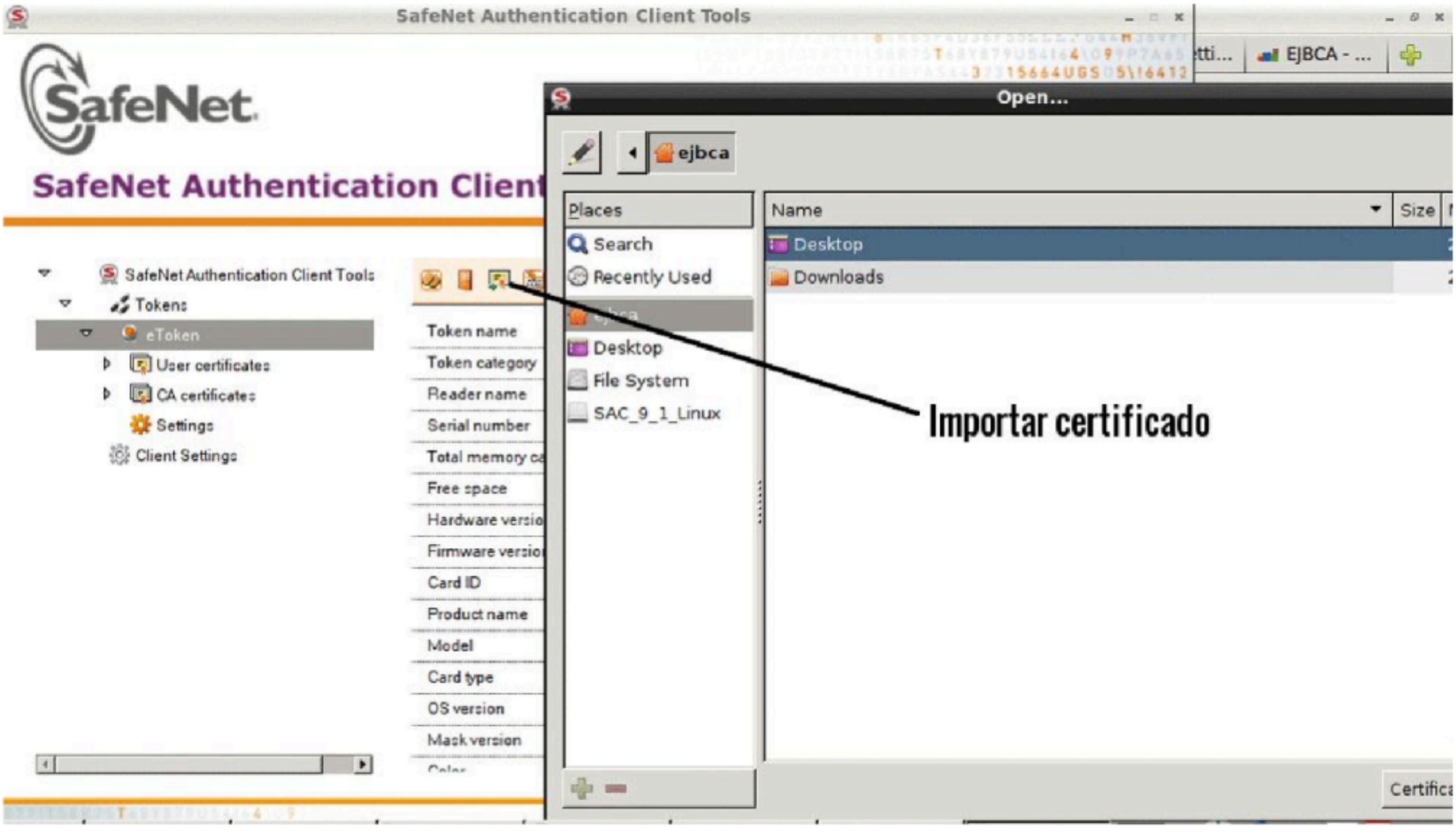
```
bin/ejbca.sh ca importcert <username> <password> <caname> <status> --email <email>
<certificate file> [--eeprofile <endentityprofile>] [--certprofile
<certificateprofile>] [--revocation-reason <reason>] [--revocation-time <time>]
```

```
bin/ejbca.sh ca importcertdir <username-source> <caname> <status> <certificate dir>
--eeprofile <endentityprofile> --certprofile <certificateprofile> [-resumeonerror]
[--revocation-reason <reason>] [--revocation-time <time>]
```

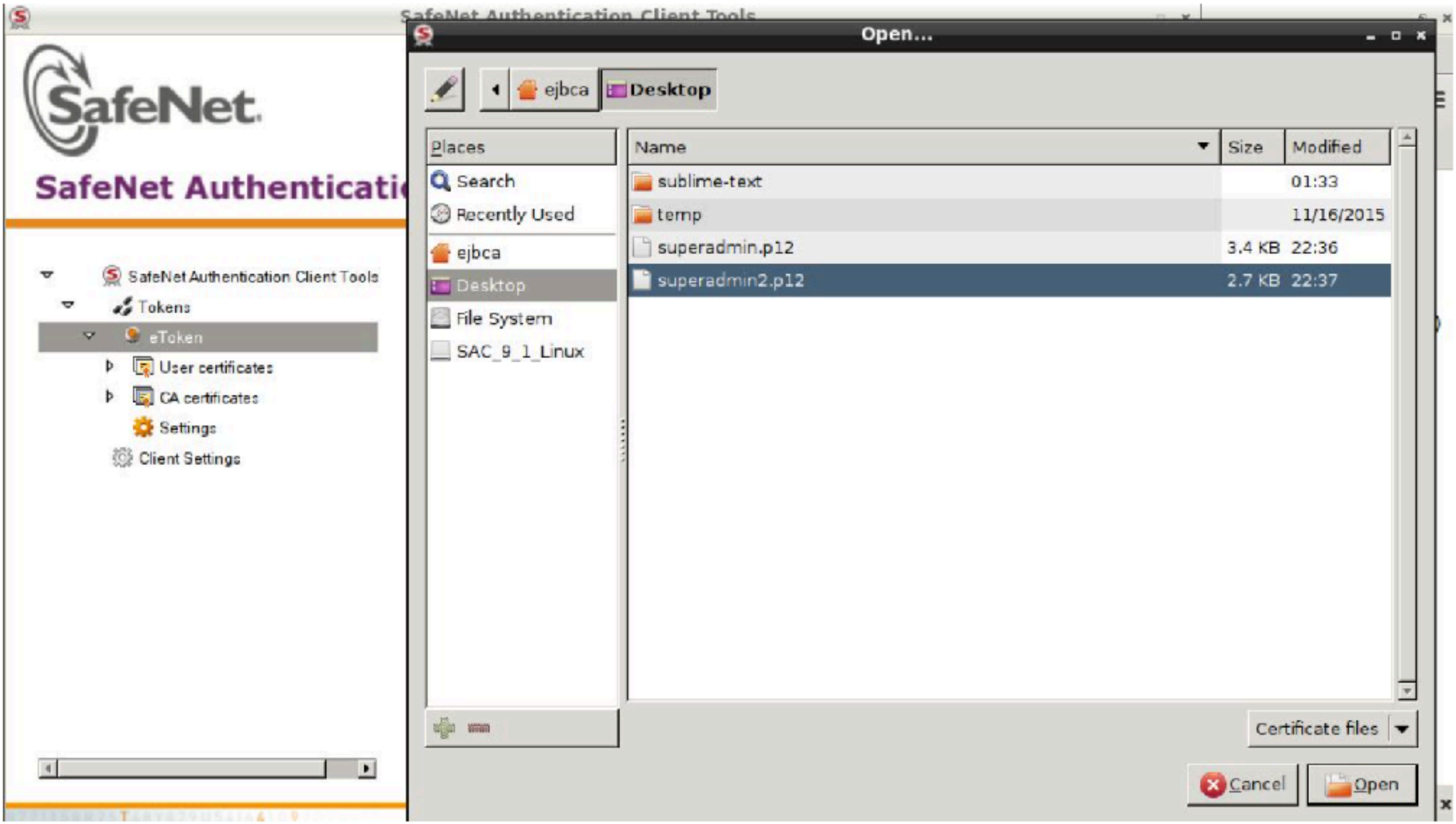
USO DE TOKEN DE AUTENTICACIÓN

- Se utiliza SafeNet Authentication Client para guardar el certificado del Administrador en el eToken SafePro64.
- Ante un intento de fuerza bruta, el eToken queda inutilizable.

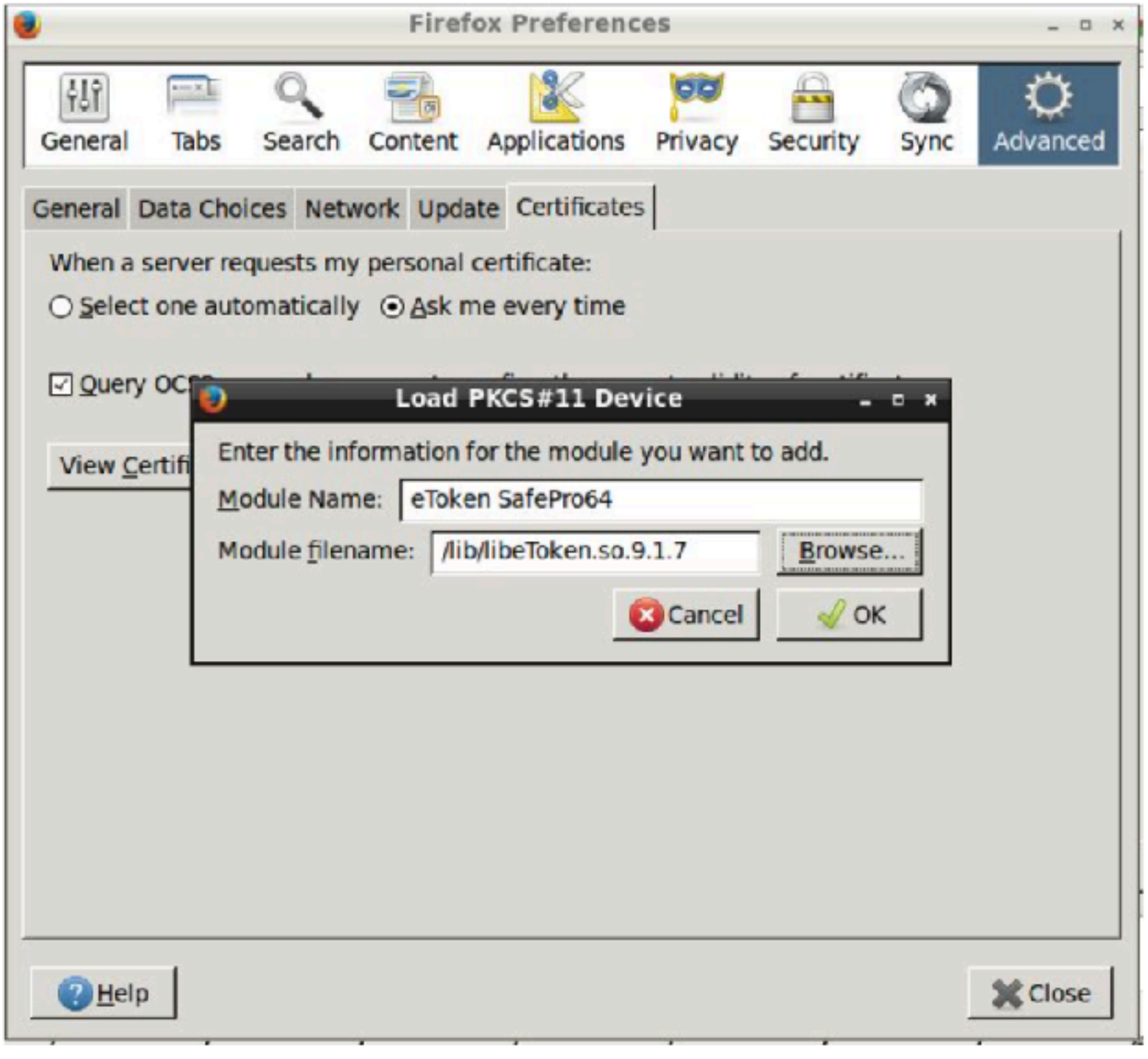
USO DE TOKEN DE AUTENTICACIÓN



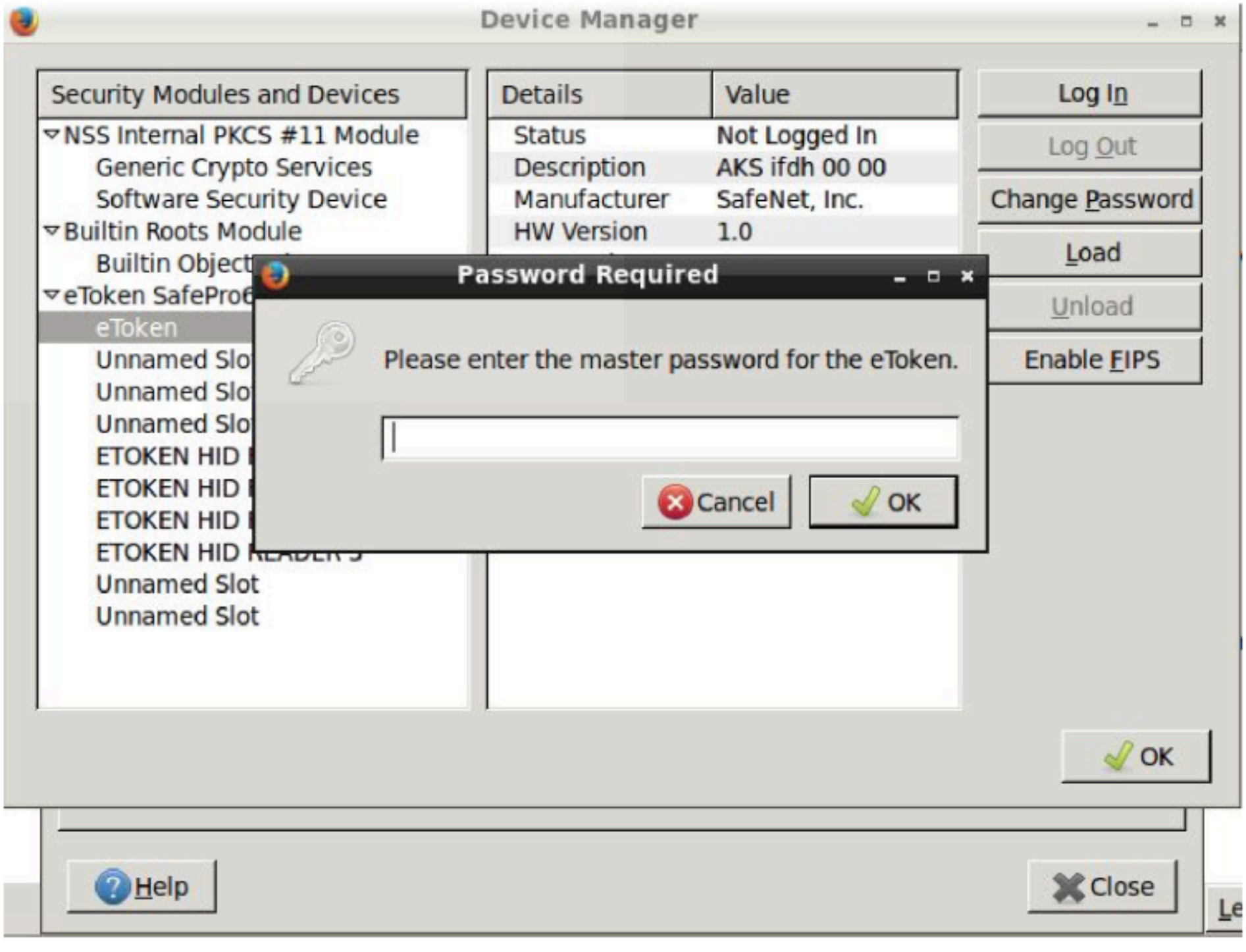
USO DE TOKEN DE AUTENTICACIÓN



USO DE TOKEN DE AUTENTICACIÓN



USO DE TOKEN DE AUTENTICACIÓN



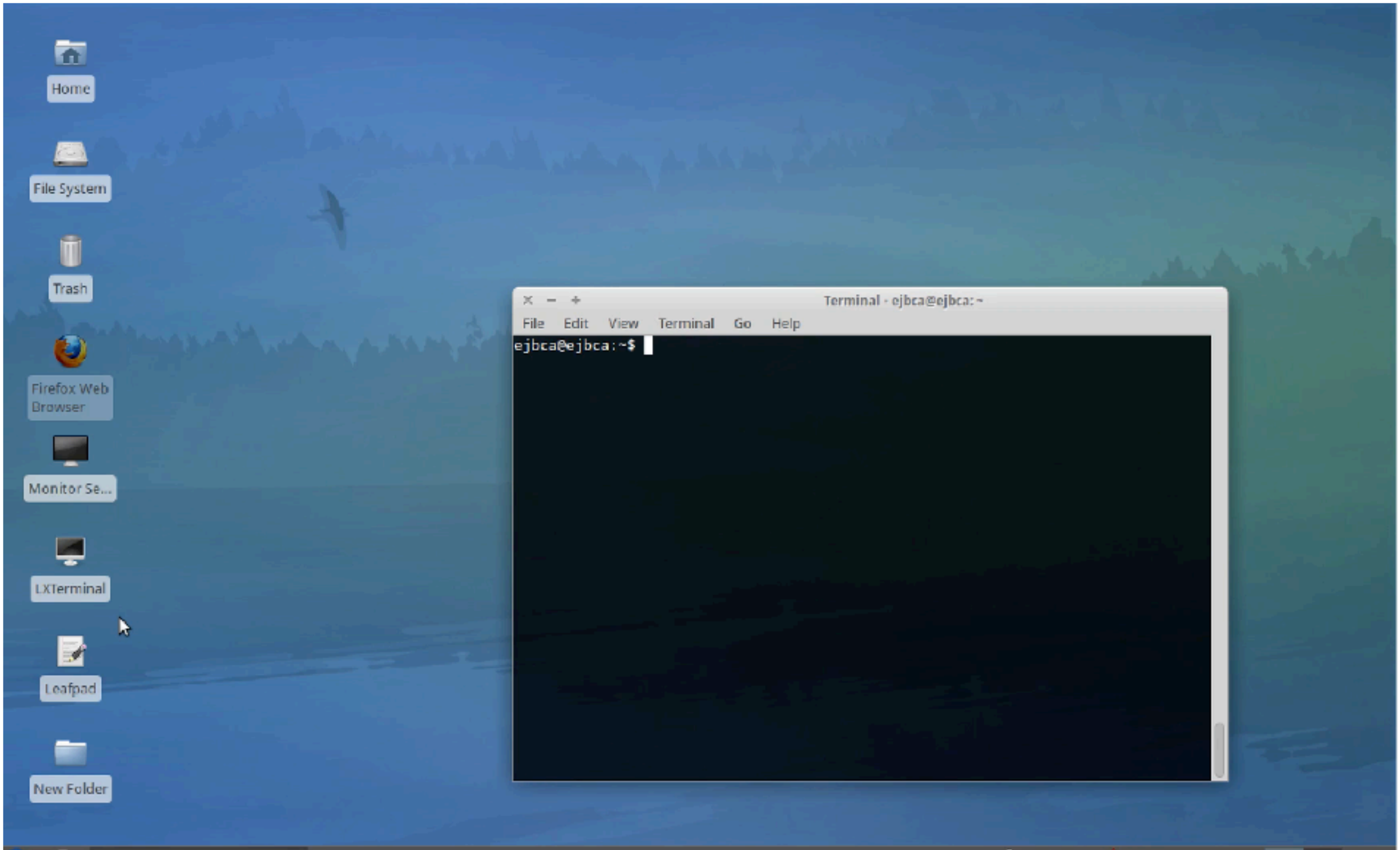
WEB PÚBLICA

- Reorganización de la información.
- Implementación de un diseño UX nuevo y moderno.
- Adaptación de las funciones de EJBCA al nuevo diseño.
- Configuración de EJBCA para la solicitud de registro de entidades finales desde la web pública.

WEB PÚBLICA

- Para hacer esto posible se utilizó el mecanismo de desarrollo de plugins.
- Se trabajó sobre:
  - Módulo de interfaz web pública y módulo de renovación de certificados.
  - Archivos **.properties*.

WEB PÚBLICA


Home
File System
Trash
Firefox Web Browser
Monitor Se...
LXTerminal
Leafpad
New Folder
Terminal - ejbca@ejbca: ~
File Edit View Terminal Go Help
ejbca@ejbca:~$
Terminal - ejbca@ejbca: ~
Thu, 15 Dec 23:25
ejbca

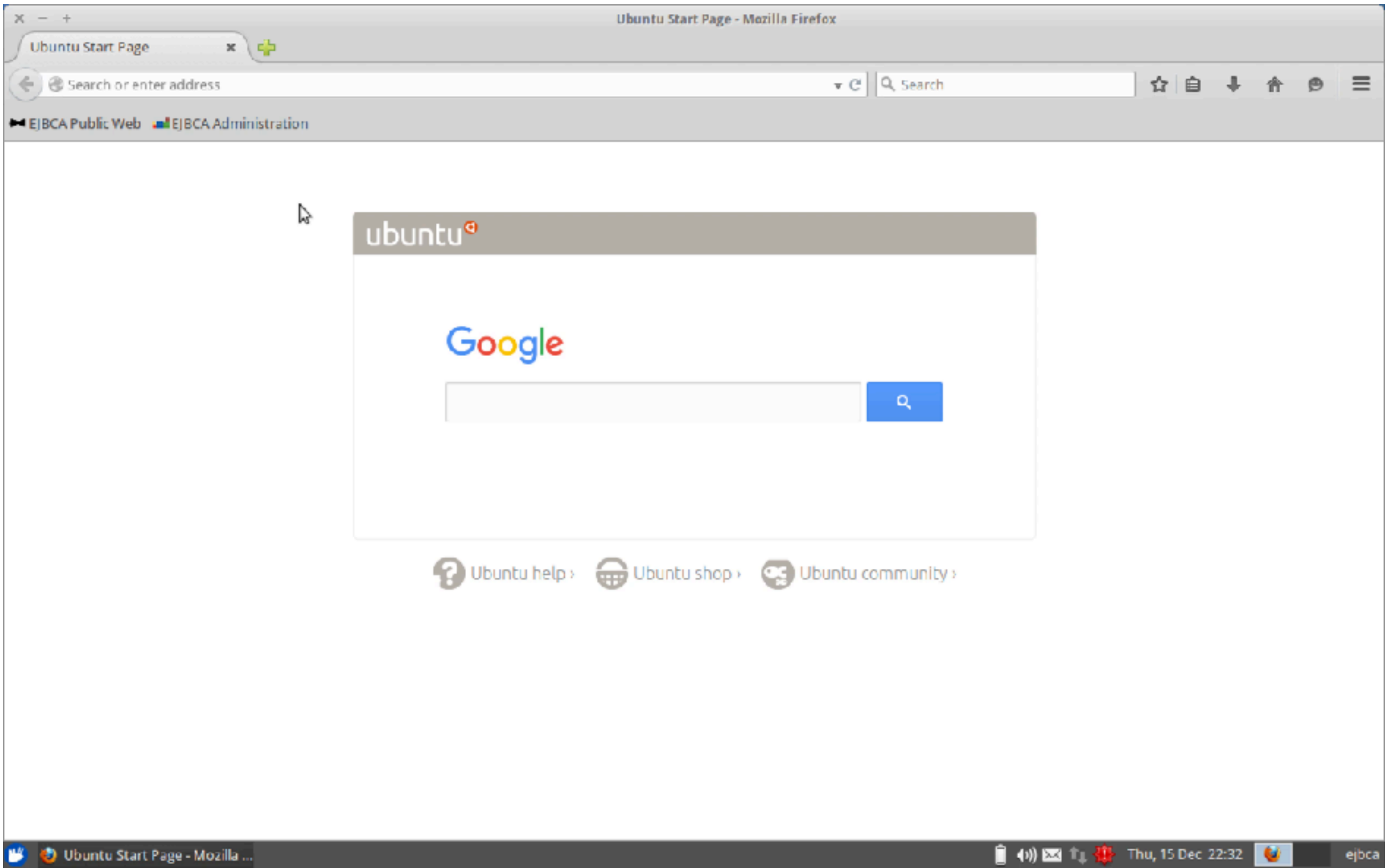
PERFILES DE CERTIFICADO Y DE ENTIDAD FINAL

- Las CP & CPS definen el formato de los certificados emitidos por la CA, en especifico, las extensiones y los tipos de certificados emitidos.
- PKIGrid UNLP emite certificados para persona natural y servidor/servicio.

PERFILES DE CERTIFICADO Y DE ENTIDAD FINAL

- Un perfil de certificado define las extensiones utilizadas en el mismo.
- Un perfil de entidad final determina cual es la información que puede o debe estar presente cuando una entidad final se registra bajo este perfil.
- Un perfil de entidad final especifica uno o más perfiles de certificados utilizados al momento de generar los certificados.

PERFILES DE CERTIFICADO Y DE ENTIDAD FINAL



ÍNDICE

CONCLUSIÓN

- EJBCA presenta ventajas al momento de adaptar y de configurar la PKI, haciendo de estas tareas un trabajo mucho menos tedioso para el encargado de mantener, y verificar el sistema.
- EJBCA tiene mucho potencial, es robusto, conciso y la documentación existente respecto a dicha tecnología es en comparación, abundante.
- Si bien es entendible que la migración puede llevar a traer problemas, tanto de inconsistencia como de tiempo, se puede observar que las mejoras que presenta EJBCA sobre OpenCA superan en amplio margen cualquier tipo de contingencia generada por el proceso de migración.

¿PREGUNTAS?

GRACIAS!