

Certificación Digital PKI

OpenSecure

Descripción General

La familia de productos PKI de Realsec proporciona soluciones que permiten disponer de certificados digitales reconocidos por parte de cualquier proveedor de servicios públicos o propios, en aquella combinación que resulte óptima para cada organización.

Así mismo y gracias al toolkit disponible permiten que cualquiera de sus aplicativos pueda tanto operar y gestionar los contenedores en que se almacenen los certificados como disponer gracias a ellos de los servicios de seguridad que sus aplicativos necesiten.

Los servicios de seguridad que para cualquier aplicativo puede ofrecer el uso de certificados digitales son:

- Confidencialidad.
- Firma digital del contenido del mensaje.
- Autenticación.



Es por ello por lo que las infraestructuras de certificación cobran especial relevancia en los siguientes entornos:

- **Ámbito interno a una organización**
 - Solución para la autenticación en aplicativos internos.
 - Solución para un workflow adaptado a los procedimientos de firma.
 - Solución para un teletrabajo "seguro".
 - Solución para la confidencialidad y política de encriptación de la organización.

- **Ámbito externo a una organización**
 - Solución para la autenticación.
 - Solución para la firma electrónica avanzada.
 - Solución para la confidencialidad.

OpenSecure CA

Especificaciones Técnicas:

- CA raíz e intermedias (soporte de jerarquías).
- Emite certificados x509v1/v3 y CRLs V2.
- Generación de claves RSA de 512, 1024 y 2048.
- Soporta PKCS#10, para generación de solicitudes de certificado (formatos PEM o DER).
- Permite configuración y una gestión a través de interfaz gráfico.
- Soporte de múltiples Ras distribuidas mediante protocolo estándar PKIX3.
- Soporte para extensiones de certificado privadas.
- Publicación de certificados y CRLs en cualquier directorio que soporte el estándar LDAP.
- Genera logs de información, tanto en ficheros como en bases de datos, sobre transacciones, estado de diferentes partes de la CA y de gestión en global.



OpenSecure RA

Los *componentes* en los que conceptualmente se divide la Autoridad de Registro son:

➤ **Servicio RA (dispatcher).**- Encargado de tramitar las peticiones(certificación, revocación, renovación, etc..) de los usuarios y del operador de la RA.

➤ **Páginas de Administración.**- Compuestas por páginas ASP y encargadas de todas las tareas de administración de la RA, gestión de políticas, prevalidaciones, informes, etc.

➤ **Páginas de Usuario.**- Este grupo lo componen las páginas ASP de petición de certificado: son el interfaz de la RA con el público.

➤ **Servicio de publicación X500.**- Está compuesto por un Spooler que permite recuperar regularmente los certificados y crl's gestionados por el Servicio RA y de publicarlos en el directorio público mediante LDAP.

➤ **Herramienta de configuración del dispatcher.**- Se trata de la aplicación encargada de configurar los datos necesarios para el funcionamiento del dispatcher de la RA.

Especificaciones Técnicas

➤ La Autoridad de Registro actúa como entidad intermedia entre el cliente y las Autoridades de Certificación.

➤ Permite una gestión robusta y de fácil manejo, de certificados(x509v1/v3), transacciones, políticas de certificación de usuarios, políticas de certificación de servidores, revocación, gestión de políticas distribuidas, control de acceso y autenticación de usuarios ... etc, a través de un entorno Web.

➤ Permite la administración de forma remota a través del entorno web seguro.

➤ Jerarquía de Operadores.

➤ Cumple el estándar de certificados X509v1/v3.

➤ Políticas de certificación que nos permiten crear certificados para diferentes tipos usos(certificados de servidor Web, certificados para firma y cifrado de mensajes S/MIME...)

➤ Permite la comunicación y políticas de certificación con varias CA's.

➤ Permite la generación de claves y almacenamiento de certificados en tarjetas inteligentes.

➤ Permite la publicación de certificados y CRL's sobre cualquier directorio que cumpla el estándar LDAP.

➤ Soporta longitudes de cifrado de 2048.

➤ Permite carga masiva de prevalidaciones de usuarios.

➤ Gestión y generación de informes sobre.

- Registro de Peticiones de Certificación online.
- Administración de certificados emitidos.
- Generación de claves y criptografía por hardware criptográfico CB2000



Realia Technologies, S.L.
info@realsec.com
www.realsec.com