PKI, implantación

Curso práctico de 4 días - 28h
Ref.: PKI - Precio 2025: 2 040€ sin IVA

Este curso le mostrará cómo llevar a cabo un proyecto PKI en las mejores condiciones posibles. Los ejercicios prácticos le enseñarán a desplegar una autoridad de certificación, generar certificados e implantar mensajería segura y una solución de inicio de sesión único (SSO).

OBJETIVOS PEDAGÓGICOS

Al término de la formación, el alumno podrá:

Conocimiento de los distintos algoritmos de cifrado simétrico y asimétrico

Implantación de una jerarquía de autoridades de certificación

Implantación de mensajería segura

Implantar la autenticación robusta mediante certificados X509

PROGRAMA

última actualización: 02/2024

1) Introducción

- Los puntos débiles de las soluciones tradicionales.
- ¿Por qué no es seguro el correo electrónico?
- ¿Podemos confiar en la autenticación mediante contraseña?
- Suplantación del remitente de un mensaje.

Trabajo práctico : Utilización de las lagunas del protocolo.

2) Criptografía

- Conceptos y vocabulario.
- Algoritmos de cifrado simétricos y asimétricos.
- Funciones hash: principio y utilidad.
- Técnicas de intercambio de claves.
- Instalación y configuración de un servidor SSH.
- SSH y Man in the Middle.
- SSH, el uso de cifrado asimétrico sin certificado.

3) Certificación digital

- Presentación de la norma X509 y X509v3.
- Autoridades de certificación.
- Delegación de confianza.
- Firma electrónica y autenticación.
- Certificados personales y claves privadas.
- Certificados de exportación e importación.

Trabajo práctico : Tiendas de certificados Microsoft.

4) Arquitectura PKI

- ¿Cómo se elabora una política de certificación?
- Autoridad de certificación. Publicación de certificados.
- Autoridad de Registro (AR).
- Modelos de confianza jerárquicos y distribuidos.

PARTICIPANTES

Ingenieros, administradores de sistemas y redes.

REQUISITOS PREVIOS

Buenos conocimientos de sistemas, redes y seguridad informática.

COMPETENCIAS DEL FORMADOR

Los expertos que imparten la formación son especialistas en las materias tratadas. Han sido validados por nuestros equipos pedagógicos, tanto en el plano de los conocimientos profesionales como en el de la pedagogía, para cada curso que imparten. Cuentan al menos con entre cinco y diez años de experiencia en su área y ocupan o han ocupado puestos de responsabilidad en empresas.

MODALIDADES DE EVALUACIÓN

El formador evalúa los progresos pedagógicos del participante a lo largo de toda la formación mediante preguntas de opción múltiple, escenificaciones de situaciones, trabajos prácticos, etc.
El participante también completará una prueba de posicionamiento previo y posterior para validar las competencias adquiridas.

MEDIOS PEDAGÓGICOS Y TÉCNICOS

• Los medios pedagógicos y los métodos de enseñanza utilizados son principalmente: ayudas audiovisuales, documentación y soporte de cursos, ejercicios prácticos de aplicación y ejercicios corregidos para los cursillos prácticos, estudios de casos o presentación de casos reales para los seminarios de formación.
• Al final de cada cursillo o seminario, ORSYS facilita a los participantes un cuestionario de evaluación del curso que analizarán luego nuestros equipos pedagógicos.
• Al final de la formación se entrega una hoja de presencia por cada media jornada de presencia, así como un certificado de fin de formación si el alumno ha asistido a la totalidad de la sesión.

MODALIDADES Y PLAZOS DE ACCESO

La inscripción debe estar finalizada 24 horas antes del inicio de la formación.

ACCESIBILIDAD DE LAS PERSONAS CON DISCAPACIDAD

¿Tiene alguna necesidad específica de accesibilidad? Póngase en contacto con la Sra. FOSSE, interlocutora sobre discapacidad, en la siguiente dirección psh-accueil@orsys.fr para estudiar de la mejor forma posible su solicitud y su viabilidad.

- Presentación del protocolo LDAP v3.
- Implantación de una autoridad de certificación raíz.
- Generación de certificados de usuario y servidor.

Trabajo práctico : Implantación de una jerarquía de autoridades de certificación.

5) Gestión de proyectos PKI: ¿por qué aplicaciones empezar?

- Los diferentes componentes de un proyecto PKI.
- Elección de tecnologías.
- Legislación.

6) Panorama de las ofertas del mercado

- El enfoque de Microsoft.
- Ofertas comerciales dedicadas: Betrusted (ex Baltimore) y Entrust.
- OpenPKI: la comunidad de código abierto.
- IdealX, entre una solución comercial y el código abierto.
- Servicios externalizados de Certplus, Versign...

Trabajo práctico : Autenticación SSL v3 Web-SSO con cortafuegos de aplicaciones. Autenticación fuerte mediante certificados X509. Implementación de un servidor de correo seguro y un directorio para certificados.

FECHAS

Contacto