Certificaciones técnicas de DigiCert
Guía de formación en SSL/TLS

Introducción

Esta guía de formación está diseñada para ayudarle a preparar el examen **DigiCert Technical Certification: SSL/TLS.** El examen consistirá en 50 preguntas de opción múltiple y tendrá una duración máxima de 1 hora.

Este examen está destinado a cualquier persona que trabaje con la tecnología SSL/TLS desempeñando un cargo técnico (asistencia técnica, administración de SSL/TLS, etc.).

Objetivos

Antes de presentarse al examen **DigiCert Technical Certification**: **SSL/TLS,** asegúrese de saber realizar las siguientes tareas:

- Describir el propósito y las funciones principales de SSL y TLS.
- Describir la historia y las versiones de SSL y TLS.
- Describir los modelos de criptografía simétrica y asimétrica.
- Describir el funcionamiento de las firmas digitales.
- Describir la información que contiene un certificado SSL/TLS, incluidas las extensiones y los formatos de archivo.
- Describir los certificados con validación de dominio (DV), con validación de empresa (OV), con validación extendida (EV) y SSL privados.
- Describir las ventajas de los certificados con EV.
- Describir los certificados SAN y comodín.
- Describir los métodos de validación de empresas y del control de dominios.
- Describir en detalle cómo funciona el protocolo de enlace (*handshake*) de SSL/TLS y para qué sirven los certificados raíz, de autoridades certificadoras intermedias (ICA), de entidad final (EE) y raíz cruzados.
- Describir los métodos de validación de revocación CRL (lista de revocación de certificados) y OCSP (protocolo de estado de certificados en línea), incluido el grapado de OCSP.
- Enumerar los algoritmos que más se suelen utilizar en TLS para el intercambio de claves, el cifrado, las firmas digitales y los hash.
- Describir la confidencialidad directa total (*forward secrecy*).
- Enumerar las ventajas de la criptografía de curva elíptica (ECC) para TLS.
- Explicar los peligros de que algún certificado de su entorno esté caducado, mal configurado, autofirmado o proceda de un proveedor.
- Identificar vulnerabilidades habituales de los protocolos desfasados (Heartbleed, etc.).

- Describir el funcionamiento de los sitios web de *phishing*.
- Describir la indicación del nombre del servidor (SNI).
- Describir la Transparencia de certificados (CT).
- Describir la autorización de la autoridad de certificación (CAA).
- Describir el concepto de asignación de certificados o *certificate pinning*.
- Describir el sistema HTTP Strict Transport Security (HSTS).
- Describir el protocolo HTTP/2.
- Explicar el término «Always-on SSL».
- Explicar la función del CA/B Forum.
- Enumerar y describir las prácticas recomendadas para garantizar la seguridad y el adecuado rendimiento de la tecnología SSL.
- Describir el protocolo ACME.
- Describir Google AMP (Accelerated Mobile Pages), los intercambios firmados de HTTP (SXG) y las credenciales delegadas.
- Describir las herramientas de certificados y generación de solicitudes de firma de certificados SSL/TLS, como Java Keystore y OpenSSL.

Guía de formación

Antes de presentarse al examen de certificación, repase los objetivos anteriores.

Si considera que es capaz de cumplir todos los objetivos enumerados en la lista, le invitamos a reservar su plaza para presentarse al examen; de lo contrario, le sugerimos que antes de hacerlo investigue un poco más sobre los temas que no domine aún.

A continuación encontrará enlaces, descargas y sitios web útiles para aprender por su cuenta. Recuerde que estos recursos no son más que un punto de partida. Le recomendamos encarecidamente que los complemente con otros para prepararse bien todos los objetivos del examen. Con otros recursos nos referimos a que busque en Internet (p. ej., Wikipedia) y utilice los productos y herramientas de DigiCert relacionados con estos temas para practicar.

Además de las opciones de autoaprendizaje descritas anteriormente, le ofrecemos la posibilidad de asistir a un taller de DigiCert en el que un instructor le dará información detallada sobre muchos de los objetivos del examen. Si desea más información, póngase en contacto con su gestor de cuentas de DigiCert.

Recursos de autoaprendizaje recomendados

SSL Best Practice Workshop Student Guide	https://www.digicert.com/digicert-tls-ssl-certified-expert/#downloads
NIST SP 1800-16: Securing Web Transactions: TLS Server Certificate Management	https://csrc.nist.gov/publications/detail/sp/1800-16/final
TLS Best Practice eBook	https://www.digicert.com/resources/tls-best-practices.pdf
SSL/TLS and PKI History	https://www.feistyduck.com/ssl-tls-and-pki-history/

Recursos en línea

CA/Browser Forum Baseline Requirements	https://cabforum.org/baseline-requirements-documents/
CA/Browser Forum Guidelines for EV Certificates	https://cabforum.org/extended-validation/
TLS 1.2 (RFC 5246)	https://tools.ietf.org/html/rfc5246
TLS 1.3 (RFC 8446)	https://tools.ietf.org/html/rfc8446
OCSP (RFC 6960)	https://tools.ietf.org/html/rfc6960
SNI (RFC 6066)	https://tools.ietf.org/html/rfc6066#section-3
CAA (RFC 6844)	https://tools.ietf.org/html/rfc6844 https://www.digicert.com/blog/new-caa-requirement-2/
HSTS (RFC 6797)	https://tools.ietf.org/html/rfc6797
HTTP/2 (RFC 7540)	https://tools.ietf.org/html/rfc7540
ACME (RFC 8555)	https://tools.ietf.org/html/rfc8555
AMP & SXG	https://www.digicert.com/google-amp-security-solutions/ https://www.digicert.com/blog/googles-signed-http-exchange-solution-displays-publisher-urls-for-amp-pages-via-tls/
Delegated Credentials	https://blog.cloudflare.com/keyless-delegation/
Transparencia de certificados	https://www.certificate-transparency.org/
US Government Compliance Guide	https://https.cio.gov/guide/#compliance-and-best-practice-checklist
“Always-on” SSL	https://otalliance.org/resources/always-ssl-aossl https://casecurity.org/2016/09/30/always-on-ssl/ https://www.digicert.com/always-on-ssl.htm
OpenSSL	www.openssl.org https://www.feistyduck.com/books/openssl-cookbook/
General CSR Creation Guidelines	https://www.digicert.com/csr-creation.htm
How to Install an SSL Certificate	https://www.digicert.com/ssl-certificate-installation.htm
Certificate file formats	https://knowledge.digicert.com/generalinformation/INFO4448.html

Aprendizaje virtual (YouTube)

Cryptography Overview (8:31)
Symmetric vs. Asymmetric Encryption (4:18)
Public Keys and Private Keys (4:10)
Session Keys (4:22)
Block vs. Stream Ciphers (3:13)
Hashing (3:30)
Perfect Forward Secrecy (3:38)
Cryptographic Hash Functions (7:04)
Symmetric Encryption Ciphers (6:42)

Asymmetric Cryptography Algorithms (2:36)
Certificate Authorities (2:52)
Key Revocation (3:31)
Digital Certificates (3:01)
Public Key Infrastructure (3:33)