DigiCert Technical Certifications SSL/TLS Training Guide

Introduction

This training guide is designed to help you prepare for the **DigiCert Technical Certification: SSL/TLS** assessment exam. The exam will consist of 50 multiple-choice questions with a maximum time allowed of 1 hour.

The intended audience for this assessment is anybody who works with SSL/TLS technology in a technical role (technical support, SSL/TLS administrator, etc).

Objectives

Before attempting the **DigiCert Technical Certification: SSL/TLS** assessment exam, you should be able to do the following:

- Describe the main purpose and functions of SSL & TLS
- Describe the history and versions of SSL & TLS
- Describe symmetric and asymmetric encryption models
- Describe how digital signatures work
- Describe the details of an SSL/TLS certificate, including extensions and file formats
- Describe DV, OV, EV and private SSL certificates
- Describe the benefits of EV certificates
- Describe SAN and wildcard certificates
- Describe domain control and organisation validation methods
- Describe how the SSL/TLS "handshake" works in detail, Including the role of root, intermediate (ICA), end-entity and cross-root certificates
- Describe the CRL and OCSP methods for revocation checking (including OCSP Stapling)
- List common algorithms used in TLS for key agreement, encryption, digital signatures, and hashing
- Describe "Forward Secrecy"
- List the benefits of Elliptic Curve Cryptography for TLS
- Explain the dangers of expired, misconfigured, self-signed and "vendor" certificates
- Identify common vulnerabilities of outdated protocols (Heartbleed, etc)
- Describe how phishing websites work
- Describe Server Name Indication (SNI)
- Describe Certificate Transparency (CT)
- Describe Certificate Authority Authorisation (CAA)
- Describe Certificate Pinning
- Describe HTTP Strict Transport Security (HSTS)
- Describe HTTP/2
- Explain the term "Always-on SSL"
- Explain the role of the CA/B Forum
- List and describe best practices for SSL security and performance

- Describe the ACME protocol
- Describe Google AMP (Accelerated Mobile Pages), Signed HTTP Exchange (SXG) and delegated credentials
- Describe commonly-used SSL/TLS CSR generation and certificate tools, e.g. OpenSSL, Java Keystore

Training Guide

Before attempting a certification assessment, you should review the objectives above.

If you believe that you are already able to meet all the objectives listed, you are welcome to schedule an assessment. However, if there are any objectives listed where you may need additional preparation, you should plan to research these topics in detail prior to scheduling an assessment.

Below you will find links for e-learning, downloads and relevant websites. Please note – these resources are just a starting point! It is strongly recommended that you do further research in order to be fully prepared for an assessment on all the objectives. This could include research on the internet (e.g. Wikipedia) and/or hands-on experience using relevant DigiCert products and tools.

In addition to the self-directed learning options described above, it may be possible to attend a DigiCert instructor-based workshop which will give in-depth information on many of the assessment objectives. Please contact your DigiCert account manager if you would like to find out more.

Recommended Self-paced Training Content

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/

Additional Resources

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/
Certificate Transparency	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

E-learning (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)