

Zertifikate & PKI

Verschlüsselung, Authentisierung & Integrität

Egal ob TLS-Verschlüsselung, Token-Authentisierung, Signatur von Firmware oder Excel Macros, oder Verschlüsselung von Sprache und E-Mails – überall kommen Zertifikate zum Einsatz. Dieser Kurs führt in die Grundlagen der Kryptographie ein, klärt über die Notwendigkeit von Zertifikaten auf und erläutert deren Inhalte und Einsatzzwecke. Ferner zeigt der Kurs die Bestandteile einer Public Key Infrastructure auf und diskutiert Herausforderungen, wie beispielsweise die Hochverfügbarkeit und das Versions-Management. Abgerundet wird das Thema durch die Veranschaulichung mit Hilfe von OpenSSL, den Active Directory Certificate Services, sowie dem Tool XCA. Jene Teilnehmer und Teilnehmerinnen, die ihr Wissen rund um das Thema Verschlüsselung, Authentisierung & Daten-Integrität erweitern wollen, werden mit diesem Kurs auf ihre Kosten kommen!

Kursinhalt

- Asymmetrische und symmetrische Verschlüsselung
- Hash-Werte und Digitale Signaturen
- Zertifikats-Inhalte und deren Bedeutung sowie Zertifikats-Formate
- Einsatzzwecke wie TLS-Verbindungen, Mutual-Authentication und Code Signing
- Anforderungen an Zertifikatsinhalte
- Bestandteile einer PKI
- Nutzung von privaten und öffentlichen Zertifizierungsstellen sowie Let's Encrypt
- Erstellen eines Certificate Signing Requests und Ausstellen von Zertifikaten
- Klassische Sperrlisten und OCSP
- Verwalten der Lebenszyklen von Zertifikaten und Zertifizierungsstellen
- Einsatzmöglichkeiten am Beispiel von Active Directory Certificate Services, OpenSSL und XCA

E-Book Sie erhalten das ausführliche deutschsprachige Unterlagenpaket von ExperTeach – Print, E-Book und personalisiertes PDF! Bei Online-Teilnahme erhalten Sie das E-Book sowie das personalisierte PDF.

Zielgruppe

Dieser Kurs richtet sich an Administratoren, die sich tiefgründig mit dem Thema Zertifikate und Certification Authorities beschäftigen möchten.

Voraussetzungen

Kenntnisse zu Netzwerksicherheit hilfreich; eine gute Vorbereitung ist ein Besuch des Kurses Security-Konzepte und Technologien – Verschlüsselung, Authentisierung und Datenintegrität.

Dieser Kurs im Web



Alle tagesaktuellen Informationen und Möglichkeiten zur Bestellung finden Sie unter dem folgenden Link: www.experteach.ch/go/WPCA

Vormerkung

Sie können auf unserer Website einen Platz kostenlos und unverbindlich für 7 Tage reservieren. Dies geht auch telefonisch unter 06074 4868-0.

Garantierte Kurstermine

Für Ihre Planungssicherheit bieten wir stets eine große Auswahl garantierter Kurstermine an.

Ihr Kurs maßgeschneidert

Diesen Kurs können wir für Ihr Projekt exakt an Ihre Anforderungen anpassen.

Training		Preise zzgl. MwSt.	
Termine in Deutschland		2 Tage CHF 1.975,-	
Termine in Österreich		2 Tage CHF 1.975,-	
Online Training		2 Tage CHF 1.975,-	
Termin/Kursort		Kurssprache Deutsch	
13.05.-14.05.24	Frankfurt	26.08.-27.08.24	Online
13.05.-14.05.24	Online	23.09.-24.09.24	Düsseldorf
17.06.-18.06.24	Online	23.09.-24.09.24	Online
17.06.-18.06.24	Wien	04.11.-05.11.24	Hamburg
22.07.-23.07.24	Frankfurt	04.11.-05.11.24	Online
22.07.-23.07.24	Online	09.12.-10.12.24	Online
26.08.-27.08.24	München	09.12.-10.12.24	Wien

Stand 21.04.2024



EXPERTeach



Inhaltsverzeichnis

Zertifikate & PKI – Verschlüsselung, Authentisierung & Integrität

<p>1 Grundkonzepte der Kryptographie</p> <p>1.1 Einleitung</p> <p>1.2 Grundlegendes Wissen zur Verschlüsselung und Signatur</p> <p>1.2.1 Symmetrische Verschlüsselung</p> <p>1.2.2 Asymmetrische Verschlüsselung</p> <p>1.2.3 Hash-Algorithmen</p> <p>1.3 Einsatz von symmetrischen und asymmetrischen Schlüsseln</p> <p>1.3.1 Symmetrische Verschlüsselung</p> <p>1.3.2 Hybride Verschlüsselung</p> <p>1.3.3 Digitale Signatur</p> <p>1.3.4 Integrität des Schlüssels</p> <p>1.4 Zertifikate</p> <p>1.4.1 Signatur mit S/MIME</p> <p>1.4.2 Verschlüsselung mit S/MIME</p> <p>2 Digitale Zertifikate</p> <p>2.1 X.509 Zertifikat</p> <p>2.2 Version 1 Felder</p> <p>2.2.1 Signatur</p> <p>2.2.2 Issuer</p> <p>2.2.3 Validity</p> <p>2.2.4 Subject</p> <p>2.2.5 Public Key</p> <p>2.3 Version 3 Extensions</p> <p>2.3.1 Key Usage</p> <p>2.3.2 Extended Key Usage</p> <p>2.3.3 Critical Flag</p> <p>2.3.4 Subject Alternative Name</p> <p>2.3.5 Subject & Authority Key Identifier</p> <p>2.3.6 CRL Distribution Point</p> <p>2.3.7 Authority Information Access</p> <p>2.3.8 Basic Constraints</p> <p>2.3.9 Properties</p> <p>2.3.10 Thumbprint</p> <p>2.4 Validierungs-Beispiel</p> <p>2.5 Formate</p> <p>3 Einsatzgebiete</p> <p>3.1 Transport Layer Security</p> <p>3.2 Perfect Forward Secrecy</p> <p>3.3 Proxy Server</p> <p>3.4 Client Authentication</p> <p>3.5 Mutual Authentication</p> <p>3.6 S/MIME</p>	<p>3.7 Code Signatur</p> <p>4 Public Key Infrastructure</p> <p>4.1 Bestandteile einer PKI</p> <p>4.1.1 Öffentliche und private Zertifizierungsstellen</p> <p>4.1.2 Enterprise PKIs</p> <p>4.1.3 Let's Encrypt</p> <p>4.2 Zertifikate ausstellen</p> <p>4.2.1 Certificate Signing Request</p> <p>4.2.2 Zertifikate ohne CSR beantragen</p> <p>4.3 Certificate Revocation List</p> <p>4.3.1 Hochverfügbarkeit</p> <p>4.3.2 Base CRL</p> <p>4.3.3 Delta CRL</p> <p>4.3.4 Overlap Period</p> <p>4.3.5 Online Certificate Status Protocol</p> <p>4.3.6 OCSP Stapling</p> <p>4.4 Certificate Chain</p> <p>4.4.1 Sperren von End Entity Zertifikaten</p> <p>4.4.2 Sperren von CA Zertifikaten</p> <p>4.4.3 Zurückziehen des Root Zertifikats</p> <p>4.4.4 Policy CAs</p> <p>4.4.5 Authority Information Access</p> <p>4.5 Hardware Security Module</p> <p>4.6 Laufzeiten</p> <p>4.6.1 End Entity Zertifikate</p> <p>4.6.2 Issuing CA Zertifikate</p> <p>4.6.3 Root CA Zertifikate</p> <p>4.6.4 Beispiel mit 3 Generationen der Root CA</p> <p>4.7 Cross Signing</p> <p>4.7.1 Root Zertifikat im Trusted Store aufnehmen</p> <p>4.7.2 Cross Certificate</p> <p>5 Certification Authorities und Tools</p> <p>5.1 Microsoft Windows und ADCS</p> <p>5.1.1 Root Zertifikat hinzufügen</p> <p>5.1.2 Zertifikats-Vorlage erstellen</p> <p>5.1.3 Zertifikats-Vorlage veröffentlichen</p> <p>5.1.4 Signing Request erstellen</p> <p>5.1.5 Signing Request einreichen</p> <p>5.1.6 Zertifikat signieren</p> <p>5.1.7 Sperrliste prüfen</p> <p>5.2 OpenSSL</p> <p>5.2.1 CA erstellen, End Entity Zertifikat signieren und umwandeln</p> <p>5.2.2 Erweiterter Zertifikats Request</p>	<p>erzeugen/anzeigen</p> <p>5.3 XCA</p> <p>5.3.1 Datenbank anlegen</p> <p>5.3.2 Private Key erzeugen</p> <p>5.3.3 Self-Signed Root Zertifikat erzeugen</p> <p>5.3.4 CSR für ein Server-Zertifikat erzeugen</p> <p>5.3.5 Server-Zertifikat signieren</p> <p>5.3.6 Server-Zertifikat signieren</p>
--	--	---

