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 sowie die Lebenszyklen der Zertifikate. Auch die Herausforderungen hinsichtlich des Quantencomputings wird thematisiert. Abgerundet wird das Thema durch Übungen mit 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
- Einsatzzecke 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
- Auswirkung des Quantencomputer auf die Kryptographie

E-Book Das ausführliche deutschsprachige digitale Unterlagenpaket, bestehend aus PDF und E-Book, ist im Kurspreis enthalten.

Zielgruppe

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

Voraussetzungen

Kenntnisse zu Netzwerksicherheit sind hilfreich; eine gute Vorbereitung ist der 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.de/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	**3 Tage**	**€ 2.195,-**
Termine in Österreich	**3 Tage**	**€ 2.195,-**
Online Training	**3 Tage**	**€ 2.195,-**

Termin/Kursort — Kurssprache Deutsch

19.05.-21.05.25	HY Frankfurt	08.09.-10.09.25	HY Online
19.05.-21.05.25	HY Online	06.10.-08.10.25	HY Düsseldorf
23.06.-25.06.25	HY Düsseldorf	06.10.-08.10.25	HY Online
23.06.-25.06.25	HY Online	10.11.-12.11.25	HY Frankfurt
28.07.-30.07.25	HY Frankfurt	10.11.-12.11.25	HY Online
28.07.-30.07.25	HY Online	10.12.-12.12.25	HY Online
08.09.-10.09.25	HY Hamburg	10.12.-12.12.25	HY Wien

Stand 01.05.2025

ExperTeach

Inhaltsverzeichnis

Zertifikate & PKI – Verschlüsselung, Authentisierung & Integrität

1 Grundkonzepte der Kryptographie
1.1 Einleitung
1.2 Grundlegendes Wissen zur Verschlüsselung
1.2.1 Symmetrische Verschlüsselung
1.2.2 Zufallszahlen
1.2.3 Asymmetrische Verschlüsselung
1.2.4 Hash-Algorithmen
1.3 Symmetrische Verschlüsselung
1.3.1 Substitution
1.3.2 Entschlüsselung
1.3.3 Permutation
1.3.4 Umkehren
1.3.5 Wiederholen
1.3.6 Adavanced Encryption Standard
1.3.7 Algorithmen im Vergleich
1.4 Diffie-Hellman
1.4.1 Primzahl und Generator
1.4.2 Geheimnis
1.4.3 Theorie
1.4.4 Potenz
1.4.5 Symmetrischer Schlüssel
1.4.6 Logarithmus
1.4.7 Modulo
1.4.8 Trapdoor
1.4.9 Öffentlicher Schlüssel
1.4.10 Symmetrischer Schlüssel
1.4.11 Angreifer
1.5 Rivest Shamir Adleman
1.5.1 Primzahlen
1.5.2 Eulersche Phi-Funktion
1.5.3 Öffentlicher Schlüssel
1.5.4 Multiplikative Inverse
1.5.5 Euklidischer Algorithmus
1.5.6 Erweiterter Euklidischer Algorithmus
1.5.7 Private Key
1.5.8 Verschlüsselung
1.5.9 Entschlüsseln
1.6 Einsatz der Schlüssel
1.6.1 Öffentlicher und privater Schlüssel
1.6.2 Eigener Private Key
1.6.3 Eigener Public Key
1.6.4 Public Key des Empfängers
1.6.5 Symmetrische Schlüssel
1.6.6 Hybride Verschlüsselung
1.6.7 Digitale Signatur
1.7 Digital Signature Algorithm
1.8 Signatur erzeugen
1.8.1 Signatur validieren
1.8.2 Gefahr
1.8.3 Deterministische Signaturen
1.9 Elliptic Curve Cryptography
1.9.1 Punktaddition
1.9.2 Punktmultiplikation
1.9.3 Schlüsselgenerierung
1.10 Asymmetrische Algorithmen
1.10.1 Elliptic Curve
1.10.2 Unterschiede

2 Digitale Zertifikate
2.1 Legende
2.2 Integrität
2.3 Zertifikate
2.3.1 Public Key und Subject
2.3.2 Gültigkeitszeitraum
2.3.3 Weitere Inhalte
2.3.4 Signatur
2.4 Validierung
2.4.1 Verändern der Zertifikatsinhalte
2.4.2 Austausch des Zertifikats
2.4.3 Kompromittierter Schlüssel
2.5 Beispiele
2.5.1 Signatur mit S/MIME
2.5.2 Verschlüsselung mit S/MIME
2.6 X.509 Standard
2.7 Signature Algorithm
2.8 Issuer
2.9 Validity
2.9.1 Generalized Time Format
2.10 Public Key
2.10.1 Public Key Parameters
2.11 Subject
2.12 Subject Alternative Name
2.12.1 IP-Adressen
2.12.2 Wildcard Zertifikate
2.13 Thumbprint

3 Verwendung von Zertifikaten
3.1 Transport Layer Security
3.2 Festlegen des Verwendungszecks
3.2.1 Key Usage
3.2.2 Extended Key Usage
3.3 Perfect Forward Secrecy
3.4 Client Authentication
3.4.1 802.1X
3.5 Modern Authentication
3.6 Mutual Authentication
3.7 S/MIME
3.7.1 Gruppenpostfächer

4 Public Key Infrastructure
4.1 Trusted Store
4.2 Bestandteile einer PKI
4.2.1 Öffentliche und private Zertifizierungstellen
4.2.2 Enterprise PKIs
4.2.3 Protokolle
4.3 Hardware Security Module
4.3.1 Let's Encrypt
4.4 Zertifikate ausstellen
4.4.1 Certificate Signing Request
4.4.2 Zertifikate ohne CSR beantragen
4.4.3 CAA Record
4.4.4 SCT-List
4.5 Zertifikatskette
4.5.1 Basic Constraints
4.5.2 Subject & Authority Key Identifier
4.5.3 Authority Information Access
4.5.4 Certificate Chain
4.6 Policy CAs
4.6.1 Name Constraints
4.6.2 Certificate Policy
4.7 Formate
4.8 Praxisbeispiele
4.8.1 Proxy Server
4.8.2 DNSSEC
4.8.3 DNS-Based Authentication of Named Entities
4.8.4 Cross Signing

5 Sperrung und Laufzeiten
5.1 Certificate Revocation List
5.1.1 CRL Distribution Point
5.1.2 Hochverfügbarkeit
5.1.3 Base CRL
5.1.4 Delta CRL
5.1.5 Overlap Period
5.2 Gültigkeit von Zertifikaten
5.2.1 Entschlüsseln
5.2.2 Gültigkeit von Signaturen
5.2.3 Gültigkeit von gesperrten Zertifikaten
5.2.4 Bereinigung der Sperrliste
5.3 Code Signatur
5.4 Online Certificate Status Protocol
5.4.1 Ablauf
5.4.2 OCSP Stapling
5.5 Sperren von Zertifikaten
5.5.1 End Entity Zertifikate
5.5.2 CA Zertifikate
5.5.3 Root Zertifikat
5.6 Laufzeiten
5.6.1 End Entity Zertifikate
5.6.2 Issuing CA Zertifikate
5.6.3 Sperrlisten signieren
5.6.4 Root CA
5.6.5 Neue Root CA
5.6.6 Karenzzeit
5.6.7 Bundesamt für Sicherheit

6 Certification Authorities und Tools
6.1 Microsoft Windows und ADCS
6.1.1 Root Zertifikat hinzufügen
6.1.2 Zertifikats-Vorlage erstellen
6.1.3 Zertifikats-Vorlage veröffentlichen
6.1.4 Signing Request erstellen
6.1.5 Signing Request einreichen
6.1.6 Zertifikat signieren
6.1.7 Sperrliste prüfen
6.2 OpenSSL
6.2.1 CA erstellen, End Entity Zertifikat signieren und umwandeln
6.2.2 Erweiterter Zertifikats Request erzeugen/anzeigen
6.3 XCA
6.3.1 Datenbank anlegen
6.3.2 Private Key erzeugen
6.3.3 Self-Signed Root Zertifikat erzeugen
6.3.4 CSR für ein Server-Zertifikat erzeugen
6.3.5 Server-Zertifikat signieren
6.3.6 Server-Zertifikat signieren

ExperTeach Gesellschaft für Netzwerkkompetenz mbH
Waldstr. 94 · 63128 Dietzenbach · Telefon: +49 6074 4868-0 · Fax: +49 6074 4868-109 · info@experteach.de · www.experteach.de