Master Class: Public Key Infrastructure (PKI) Deep Dive (PKIDD)

ID PKIDD **Preis** 5.800,– € (exkl. MwSt.) **Dauer** 5 Tage

Kursüberblick

Für viele ist das Thema PKI ein Buch mit (mindestens) sieben Siegeln.

Zertifikate sind aus der heutigen Welt nicht mehr wegzudenken – gerade im Thema Sicherheit ist das Thema PKI tief verwurzelt.

Wir haben diesen Kurs komplett neu aufgebaut mit dem Wissen aus unseren PKI-Trainings der letzten Jahrzehnte.

In fünf Tagen werden Sie zu einem PKI-Fachmann.

Angefangen bei den Grundlagen (private & öffentliche Schlüssel, digitale Signatur und TLS) bis zu High-End-Themen wie mehrstufige PKIs, Algorithmen, virtuelle SmartCards und vieles mehr:

Public Key Infrastructure – nach diesem Kurs jonglieren Sie mit allen Themen rund um das Thema PKI!

Zielgruppe

Dieser Kurs wendet sich an ***erfahrene*** System-Administratoren, Consultants und Active-Directory-Designer.

Nach diesem Seminar werden Sie in der Lage sein, Public Key Infrastrukturen zu designen, zu erstellen und hochsicher zu betreiben.

Voraussetzungen

Mindestens 5 Jahre Erfahrung mit Servern und Client-Systemen, mindestens 3 Jahre Erfahrung im Active Directory.

Kursinhalt

- Windows Server 2016 / 2019 / 2022 PKI
- Design und Implementierung einer mehrstufigen 2019 PKI
- PKI-Administration mit Rollenseparation
- Zertifikatsvorlagen Typ 1, 2, 3 und 4
- Key Archivierung und Recovery
- Windows 10 & Windows Server 2019 Enrollment
- Smart Cards
- Virtual Smart Card (VSC) – SCAMA – TPM Key Attestation
- EFS Encrypted File System
- Certificate Revocation List – CRLOverlap
- Online Certificate Status Protocol (OCSP)
- Certificate Erneuerung
- Auditing & Troubleshooting
- Network Device Enrollment Service (NDES)
- Backup / Recovery von PKI-Database
- Certificate Lifecycle Notification (Optional)

Schulungsumgebung:

In der Schulungsumgebung wird komplett mit Hyper-V gearbeitet. Für den proaktiven Aufbau der Schulungsumgebung nutzen wir ein Powershell-Skript, mit dem Sie in Sekunden neue virtuelle Maschinen erstellen können. Das Skript wurde von Ihrem Trainer selber entwickelt und ermöglicht den Schulungsaufbau nach Wunsch des Kunden in extremer Schnelligkeit mit geringem Aufwand.

Hardware:

Jedem Teilnehmer steht ein dedizierter Server in einem Rechenzentrum mit insgesamt 1 Gbit-Anschluss ins Internet zur Verfügung.

Jeder Teilnehmer-Server ist folgendermaßen ausgestattet:

- Mind. 256 GB RAM bis 768 GB RAM (!)
- mind. 40 vCores
- 2 NVME-SSDs mit mind. 3.000 MB/s schreibend und mind. 2.000 MB/s lesend
- 1 Gbit ins Internet Gesamt-Bandbreite

Ihr Trainer:

Die Advanced Master Class wurde von Andy Wendel entwickelt und wird von ihm selbst und seinem erfahrenen Team durchgeführt.

Andy Wendel ist seit über 20 Jahren Trainer mit tiefer Erfahrung in Active Directory, Public Key Infrastruktur, Gruppenrichtlinien, WSUS sowie HyperV und der System-Center -Suite. Neben seiner Arbeit als Senior Cloud-Architect & Consultant in großen Rechenzentren war Andy Wendel auch bei Microsoft in Redmond zum Troubleshooten von Storage-Spaces für einen großen Rechenzentrums-Betreiber.

Andy Wendel ist MCLC (einer von 46 weltweit), sowie MCSE und MCT.

Im Jahr 2016 erwarb Andy Wendel durch Paula Januszkiewicz (einer der besten 20 Security-Experten weltweit) den **Certified Security Master Specilization: Advanced Windows Security 2017**.

Zu diesem Kurs wurden nur 100 Teilnehmer weltweit zugelassen und nur 4 deutsche Teilnehmer schafften auch die Prüfung. Andy Wendel schloss diese mit Auszeichnung ab.

Dieses Training wurde erneut 2018, 2019, 2020 und 2021 und 2022 besucht.

Detaillierter Kursinhalt

Windows Server 2016 / 2019 / 2022 PKI

- Notwendigkeit von Public Key Infrastructure » Securing Public Key Infrastructure
- Anwendungen durch PKI
- Mehrstufige PKI (2-stufig, 3-stufig)
- Krytographische Verfahren: Symmetric, Asymmetric (Public Key), Hash (One-Way Function)
- Kryptographische Algorithmen: Symmetric Key (AES-128, AES-256), Hash (SHA-256), Public Key (RSA, Elliptic Curve ECDSA, ECDH)
- NIST, NSA Suite-B Cryptography
- Kryptographische Standards: X509v3, PKCS etc.
- CryptoAPI (CAPI) und CNG (Cryptography Next Generation) sowie CAPI2
- CSP (Cryptographic Service Provider) und KSP (Key Service Provider)
- Digital Certificate X.509v3 und die Felder
- Windows Cipher Suite
- PKI-Anwendungen: Smartcard, SSL/TLS, S/MIME, EFS, Authenticode, IPSec

Block 2 Aufbau der 2019 PKI – RSA 4096 und KSP:

Design und Implementierung einer mehrstufigen 2019 PKI:

- Design einer PKI (einstufig, zweistufig und dreistufig)
- Stammzertifizierungsstelle (Standalone und Enterprise Certificate Authority = CA); SubCA und Ausstellende CA
- Implementieren einer dreistufigen PKI mit einer Offline RootCA, Offline Policy CA und Online Enterprise SubCA
- Alle Zertifizierungsstellen werden nach dem strengeren ISIS-MTT (Europa Standard) eingerichtet!
- Konfigurieren von CAPOLICY.INF für die CA-Installation (Key-Länge, Lebensdauer, etc.)
- Postinstallation durch ConfigMe.cmd: Automatisierte Konfiguration der CA-Registry, CDP und AIA, Basis- und Delta-CRL
- Publizieren CDP und AIA in Active Directory und auf dem Webserver
- Konfigurieren einer Offline RootCA: Zertifikatslebensdauer, Key-Länge, Registry-Einstellungen mit Certutil -setreg
- Implementieren von mehreren Offline Policy CAs mit CPS (Certification Practice Statemnents) und mehreren ausstellenden Online Enterprise SubCAs (Issue)
- Gezieltes Publizieren von Certificate Templates, z.B. Kerberos Authentication, Smartcard Enrollment Agent, etc.
- Zertifikatsprüfung: Certificate Discovery, Path Validation (Vertrauenspfad) und Revocation Checking (Sperrung)

Block 3 Administration:

PKI-Administration mit Rollenseparation

- Verwaltungsaufgaben in einer PKI; Installieren und Konfigurieren einer CA; Erneuern von CA-Zertifikaten; Key Archivierung
- Publizieren von Zertifikatsvorlagen; Einschränken der Zertifikatsverwaltung
- Rollenseparation: PKI-Admin, PKI-CertManager, PKI-Auditor und Key Recovery Agenten
- Auditing von Zertifizierungsstellen: Dienst Starten/Stoppen, Veröffentlichen von CRL
- Zertifikat registrieren und verweigern, Sicherheitseinstellungen, Datenbank-Sicherung und -Wiederherstellung
- CA-Ereignisse senden per E-Mail
- Zertifikatsvorlagen Typ 1, 2, 3 und 4
- Unterschiede zwischen Zertifikatsvorlagen Typ 1, 2, 3 (2008 R2) und 4 (ab 2012)
- Kopieren von Zertifikatsvorlagen
- Die wichtigsten Zertifikatsvorlagen-Einstellungen:
- Anforderungsverarbeitung
- Anwendungs- und Ausstellungsrichtlinien
- Ausstellungsvoraussetzungen
- Delegieren der Zertifikatsvorlagenverwaltung
- Gültigkeitsdauer und Erweiterungszeitraum

- Festlegung der Zertifikatszwecke bzw. Schlüsselverwendung
- Key Archivierung und Recovery
- Manuelle und Automatische Registrierung (Enrollment) für Benutzer und Computer
- Publizieren von Zertifikat
- Änderung bestehender Zertifikatsvorlage und Erneuern von Zertifikat

Key Archivierung und Recovery

- Windows CA mit Private Key Archivierung
- Vorbereitung der Zertifikatsvorlage für Key Recovery, Key Recovery Agent (KRA) und KRA-Zertifikat
- Verschlüsselung von Privatkeys und Zertifikat PKCS#12
- Export und Import von Zertifikat und Privat Keys
- Archivieren von EFS-Private Key
- Wiederherstellen von archivierten Private Keys

Windows 10 & Windows Server 2019 Enrollment

- Neue Features von Windows 10 und Server 2019
- Einfachere Auswahl von Zertifikat im Certificate Store
- Neues HTTP/HTTPS-Enrollment (wird im Kurs nur Besprechen) vs. RPC/DCOM

Block 4 PKI-Anwendungen:

Smart Cards

- Kerberos Authentication Zertifikat für alle Domain Controller
- Installieren SmartCard-Reader
- SmartCard Registrierungsagent, Ausstellen von Smartcard-Zertifikaten
- Konfigurieren von Gruppenrichtlinien für SmartCard-Benutzer und Computer

Virtual Smart Card (VSC) – SCAMA – TPM Key Attestation

- Virtual Smart Card ist ab Windows 8.1 möglich, setzt TPM 1.2 oder höher voraus
- TPM und Smart Card Zertifikatsvorlage für Windows 10 Clients
- Arbeiten mit TPMVSCMgr und Mini-Driver manager
- TPM Key Attestation ab 2012 R2 CA
- Einrichten SCAMA – Smart Card Vorlage mit Issuance Policy (High, Medium, Low Assurance)

EFS Encrypted File System

- Funktionsweise von EFS
- Selbstsigniertes und CA signiertes EFS-Zertifikat
- Sperren von EFS-Einsatz in einer Active Directory Umgebung ohne PKI
- Erstellen von EFS-Zertifikat Typ 4 mit Key Recovery und Auto Enrollment
- Verschlüsseln von lokalen Dateien

Block 5 Erneuerung von Zertifikat und CRL

Certificate Revocation List – CRLOverlap

- Lebensdauer einer Base CRL und Delta CRL
- Verlängerung der Lebensdauer durch CRLOverlap (Überhang)
- Standardwerte von CRLOverlap und CRLDeltaOverlap
- Wie soll ein CRLOverlap eingestellt werden?

Online Certificate Status Protocol (OCSP)

- OCSP-Vorlage erstellen
- OCSP-Array erstellen und einrichten.
- CA Revocation Konfiguration mit CRL Refresh Time einrichten
- OCSP Response optimieren
- OCSP Stapling
- Lokal CRL – On-Demand Sperrung

Certificate Erneuerung

- Erneuerung eines CA Zertifikats mit demselben Schlüsselpaar
- Verändern der PKI-Struktur (2-Stufig in 3-Stufig und umgekehrt) durch CA-Zertifikatserneuerung
- CA in eine neue PKI-Struktur umhängen
- Einschränkung des Wirkungsbereichs eines CA durch Constraints (Path, Application, Name)
- Erneuerung eines CA Zertifikats mit neuem Schlüsselpaar
- Cross RootCA Zertifikat
- Migration oder Konsolidierung in eine neue PKI-Struktur

Block 6 Auditing & Troubleshooting

Auditing & Troubleshooting

- Audit von PKI konfigurieren
- Auswerten der Ereignisse
- Troubleshooting von Zertifikatsenrollment
- E-Mail Benachrichtigung

Network Device Enrollment Service (NDES)

- Einrichtung und Konfiguration
- Kerberos Delegation
- Anfordern eines Zertifikates

Backup / Recovery von PKI-Database

- Die PKI-Datenbank *.edb, Transaktionsdateien *.log und

Prüfpunktdatei
- „Kleine“ und „große“ Datenbank-Sicherung
- Wiederherstellen von CA-Keys und Datenbank
- Datenbank aufräumen durch das Löschen von abgelaufenen Zertifikaten

Certificate Lifecycle Notification (Optional)

- Konfigurieren von Task Scheduler
- Event 1001 bis 1007
- PowerShell Script um E-Mail zu versenden, wenn 1003 erscheint
- SCOM Monitor

Über Fast Lane

Fast Lane ist weltweiter, mehrfach ausgezeichneter Spezialist für Technologie und Business-Trainings sowie Beratungsleistungen zur digitalen Transformation. Als einziger globaler Partner der drei Cloud-Hyperscaler Microsoft, AWS und Google und Partner von 30 weiteren führenden IT-Herstellern bietet Fast Lane beliebig skalierbare Qualifizierungslösungen und Professional Services an. Mehr als 4.000 erfahrene Fast Lane Experten trainieren und beraten Kunden jeder Größenordnung in 90 Ländern weltweit in den Bereichen Cloud, künstliche Intelligenz, Cybersecurity, Software Development, Wireless und Mobility, Modern Workplace sowie Management und Leadership Skills, IT- und Projektmanagement.

Fast Lane Services

- ✓ Highend-Technologietraining
- ✓ Business- & Softskill-Training
- ✓ Consulting Services
- ✓ Managed Training Services
- ✓ Digitale Lernlösungen
- ✓ Content-Entwicklung
- ✓ Remote Labs
- ✓ Talentprogramme
- ✓ Eventmanagement-Services

Trainingsmethoden

- ✓ Klassenraumtraining
- ✓ Instructor-Led Online Training
- ✓ FLEX Classroom – Klassenraum und ILO kombiniert
- ✓ Onsite & Customized Training
- ✓ E-Learning
- ✓ Blended & Hybrid Learning
- ✓ Mobiles Lernen

Technologien und Lösungen

- ✓ Digitale Transformation
- ✓ Artificial Intelligence (AI)
- ✓ Cloud
- ✓ Networking
- ✓ Cyber Security
- ✓ Wireless & Mobility
- ✓ Modern Workplace
- ✓ Data Center

Weltweit vertreten
mit High-End-Trainingszentren rund um den Globus

Mehrfach ausgezeichnet
von Herstellern wie AWS, Microsoft, Cisco, Google, NetApp, VMware

Praxiserfahrene Experten
mit insgesamt mehr als 19.000 Zertifizierungen

Deutschland
Fast Lane Institute for Knowledge Transfer GmbH
Tel. +49 40 25334610
info@flane.de / www.flane.de

Österreich
ITLS GmbH
(ITLS ist ein Partner von Fast Lane)
Tel. +43 1 6000 8800
info@itls.at / www.itls.at

Schweiz
Fast Lane Institute for Knowledge Transfer (Switzerland) AG
Tel. +41 44 8325080
info@flane.ch / www.flane.ch