VIRTUAL & ONSITE

PKI TRAINING

Class Audience > Beginners | Intermediate | Advanced

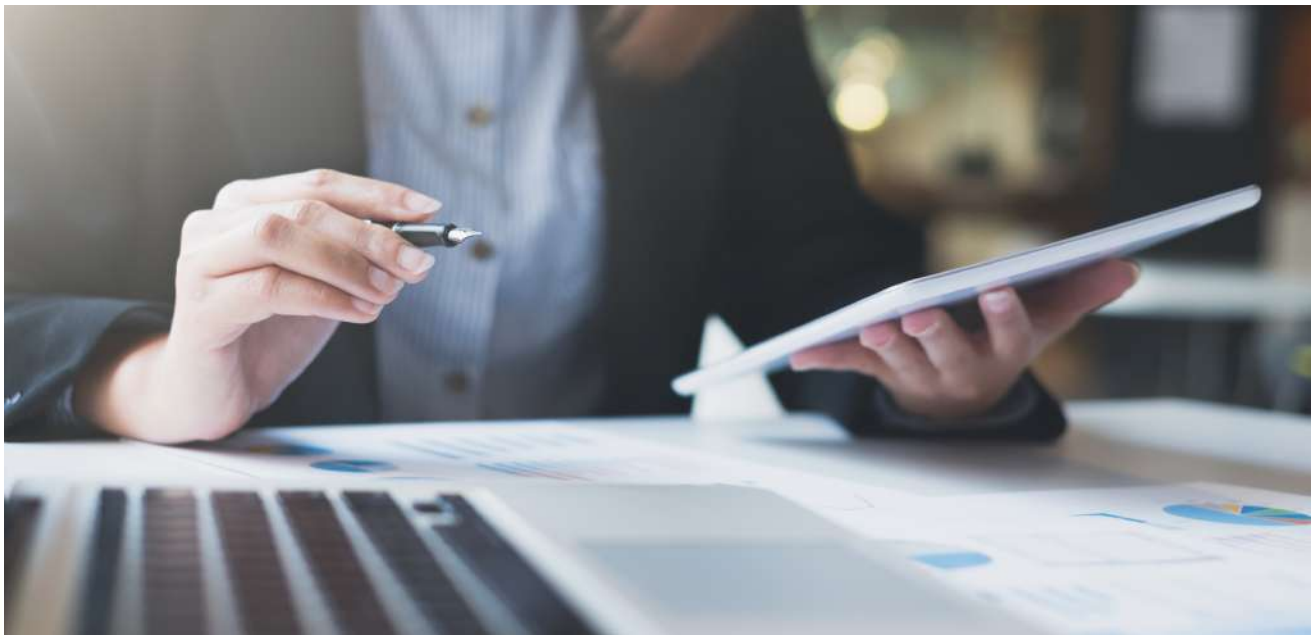
Upgrade Your
Public Key Infrastructure (PKI)
Skills With A Training From
Encryption Consulting LLC

ENCRYPTION CONSULTING

Planning a Public Key Infrastructure (PKI) can have a significant skill ceiling, as an organization's authentication, encryption, and digital signing can depend on how the PKI is built. An organization needs a robust and secure PKI infrastructure to ensure security and privacy and meet regulations and compliance. Creating and managing a PKI requires ample knowledge about it, which Encryption Consulting brings along with the experience needed for organizations to have a custom solution for their needs.
In our three days, PKI Training delivered online, In-person focusing on Microsoft Active Directory Certificate Service (ADCS) Training, customers will learn how to deploy or design PKI solutions in the enterprise.
You will learn how to build a PKI on Windows Server 2019, focusing on areas such as integration with HSM, Two-tier PKI, Cloud PKI, and more.
There is a strong emphasis on:

- PKI Governance
- PKI Design best practices
- Certificate Lifecycle Management process
- PKI operations
- Hands-on skills lab

Syllabus



DAY 01

Module 01: Introduction to PKI

- Introduction to Cryptography
- Symmetric Encryption
- Asymmetric Encryption
- Hash Functions and Digital Signatures
- Introduction to HSM
- Introduction to PKI

Module 02: Certificate Revocation and Chain Building

This module will give you a vital understanding of

- Certificate Verification and Chain Building
- Certificate Revocation Lists (CRLs)
    - Functionality
    - Design considerations
    - How to deal with revocation cache
    - Lab 1: Deploying 2 tier PKI
- Online Certificate Status Protocol (OCSP)
- Troubleshooting

DAY 02

Module 03: Deploy a Two-Tier PKI Hierarchy

In this module, you will learn:

- Define CAPolicy.inf for root Certification Authority (CA) and subordinate CA
- Active Directory Certificate Services (AD CS) PowerShell cmdlets
- Install and configure offline root CA
- Publish root CA certificate and CRL to CDP and AIA URLs
- Install and configure subordinate CA
- Post-install health checks
- CA Security
- Lab 2: Deploying OCSP

Module 04: Certificate Templates and Enrollment Methods

This module covers the purpose of certificate templates. Configuration and management will be explained in addition to different enrollment methods. This module will give you an overview of:

- Certificate Templates
- Template Versions
- Configuration of Templates
- Enrollment methods

DAY 03

Module 05: Enhancements in Windows Server 2012 R2

Windows Server 2019 and Windows 8 introduce a lot of new PKI-related features:

- New installation and deployment features
- New Server Core features
- Enhanced RPC Security
- ADCS Site Awareness for ADCS and PKI Clients
- Support for Internationalized Domain Names (IDNs)
- Template management and Version 4 templates
- Group Protected PFX
- Certificate Lifecycle Notification
- Key-based renewal
- Certificate renewal with same key
- TPM Key Attestation
- Policy module for NDES

Module 06: Public Key Infrastructure (PKI) Maintenance & Availability Operations

CA Operations

- Offline CA Maintenance
- CA Backup
- Private Key Backup & Storage
- CA Renewal
- Maintenance Tasks on a Clustered CA

Module 07: Cloud PKI Hierarchy

In this module, you will learn:

- Different PKI Hierarchy in Cloud PKI deployment
- AWS Certificate Manager (ACM)
- AWS Private Certificate Authority (CA)
- CA Security considerations in Cloud

Certificate of Completion

Every student that attends and completes the full training scoring 70% in the PKI exam will receive a certificate of completion.
The certificate will allow student to qualify for ISC2 continuing education credit for annual CPE commitments.

Why Encryption Consulting LLC?

ENCRYPTION CONSULTING
www.encryptionconsulting.com

Encryption Advisory Services

Encryption is used for securely protecting data from unauthorized access. Data encrypted can only be seen by those that possess the key to change the data back to plain text. Encryption is now one of the oldest yet still most effective technology solutions able to have data security

Public Key Infrastructure

PKI is a security ecosystem that has stood the test of time for achieving secure Internet-based transactions by the use of digital certificates. Digital certificates have provided security to servers and routers from the very early stages of the Internet through Public Key Infrastructure

Hardware Security Module – HSM

Hardware Security Modules provides protection and strong authentication with cryptographic processing by the use of digital keys inside a physical computing device. This device offers an isolated tamperproof environment which can create and secure cryptographic keys, protecting critical cryptographic operations, all while enforcing self-implemented policies over the keys.

Certificate Lifecycle

Certificates typically have a 4-phase lifecycle - Discovery, Enrollment, Provisioning, and End-of-life. To make your PKI mature and reliable, you must have more control over all the phases

Enterprise Encryption Platforms

Does your business have the need to encrypt large amounts of data-at-rest found in structured databases or in unstructured files across physical, cloud, or both types of environments? Do you want to protect data without disruptive changes to applications or business practices?

Cloud Data Protection Services

The transition towards uploading data on the public cloud is now becoming the normal standard. With relying on the cloud for data storage, cloud security must now become the number one priority for organizations

Encryption Consulting LLC.
130 N Preston Rd, Prosper, TX 75078, USA |
+1- 469-815-4136 | info@encryptionconsulting.com
www.encryptionconsulting.com

Find us:
"EncryptionConsulting" on

CONFIDENTIALITY. INTEGRITY. AVAILABILITY.