ATC-PUBLIC-KEY-INFRA: Public Key Infrastructure (PKI)

Course Code: ATC-PUBLIC-KEY-INFRA
Duration: 5 days
Instructor-led Training (ILT) | Virtual Instructor-led Training (VILT)

OVERVIEW

This Public Key Infrastructure – Implement and Manage course helps any individual to gain knowledge in managing robust PKI and having better understanding of topics surrounding public key infrastructure. Moreover, the PKI course is a preparation for the increasingly critical component – which ensures confidentiality, integrity, and authentication in an enterprise. Our PKI course provides the knowledge and skills necessary to select, design and deploy PKI, to secure existing and future applications within your organization. It also gives a deeper look into the foundations of cryptography and the working principles of the algorithms being used.

Throughout the whole course, participants will gain in-depth knowledge on the following topics:

- Legal aspects of a PKI
- Elements of a PKI
- PKI management
- Trust in a digital world
- Digital signature implementation
- Trust models
- Smart Cards
- NDES, CEP/CES
- SSL
- OCSP

After completing the PKI course, every individual will be able to successfully design, setup, deploy, Troubleshoot and manage a public key infrastructure (PKI). This is a 5-day course is considered essential for anyone who needs to understand Public Key Infrastructure (PKI) and the issues surrounding its implementation. It covers the issues and technologies involved in PKI in-depth and gives hands-on practical experience of setting up and maintaining a variety of PKI solutions. Detailed knowledge of issues surrounding PKI helps to put recent attacks which have appeared in the news headlines into context and enable valid decisions to be made about their relevance to your organization.

SKILLS COVERED

- To introduce the student to the theoretical aspects of the foundations and benefits of Public Key Infrastructure (PKI), including different types of encryption, digital signatures, digital certificates and Certificate Authorities.
- To give students hands on experience of implementing and using PKI solutions with a variety of applications.
- To give students an understanding of the concepts of evaluating and selecting PKI technologies

WHO SHOULD ATTEND?

This course is recommended for anyone using, managing, deploying or designing PKI solutions with ADCS components.

PREREQUISITES

- An Ideal candidate must have basic knowledge of Windows Servers and Networking
- For practical revision, students require windows server 2012 R2 machines

MODULES

Module 1: Introduction to PKI

- Basic Security Concepts
- Public Key Infrastructure Defined
- Digital Certificates and Signatures
- Smart Cards
- PKI Standards
- Basic cryptography
- Uses of Cryptography
- History of Cryptography including early methods
- Symmetric and Asymmetric Encryption plus Algorithms
- Diffie-Hellman Key Generation
- Hashing for Integrity plus Algorithms
- Cryptographic Functions
- Hashing
- Cryptographic Keys
- Key Types
- Key Lengths

Module 2: Practical Uses for Encryption and Associated Issues

- Signed and Encrypted Email using S/MIME and PGP Secure connections to websites Digitally signing PDFs Encrypting files Encrypting hard drives Encrypting “containers” SSL, VPN and Wireless PKI and Cloud Computing Attacks on Encryption Certificate Authorities Public v Private CAs Regulations governing CAs CA Certificate Policies Types of Certificates Provided CA Hierarchies Certificate Authority Operations Certificate expiration Certificate revocation

Module 3: Certificate Revocation Lists (CRL)

- Base and Delta CRL Overview
- CRL Overlap
- Design Principles

Module 4: Online Certificate Status Protocol (OCSP)

- Key recovery
- Installing a CA and issuing certificates

Module 5: Smart Card Logon

- Smart Card Concept
- Working and Logon Process in Detail

Module 6: SSL in Detail

- Working of SSL using Network Traces
- Troubleshooting of SSL issues
- Discuss some common error codes

Module 7: Certificates & Certificate Stores

- Digital Certificates
- Keypairs
- Windows Certificate Stores

Module 8: Lab : Deploy a 2-tier PKI

- Certificate Validation
- Chain Building
- Revocation checking
- Troubleshooting Tools and Techniques

Module 9: Lab : Online Certificate Status Protocol

- Overview
- OCSP Process
- Limitations
- Design Configurations
- Weaknesses

Module 10: Enterprise Templates

- Overview
- Template Schema Versions
- Template Properties
- Template Configuration Versioning

Module 11: Certificate Enrollment Types

- Enrollment Overview
- Certificate Authority Web Enrollment (CAWE)
- Cross Forest Enrollment

Module 12: Automated Certificate Enrollment

- Certificate Autoenrollment Overview
- Group Policy Settings
- Autoenrollment Processes
- Troubleshooting

Module 13: Certificate Enrollment Web Services (CES/CEP) and NDES (SCEP)

- Overview
- Infrastructure Requirements
- Installation & Configuration
- Troubleshooting
- Common ADCS Mistakes
- ADCS Known Issues
- Troubleshooting CA Issues
- ADCS Debug Logs
- ADCS Configuration
- Certutil
- Hands on with OpenSSL
- Summary and Closing

END OF PAGE