
Designing and Managing a Windows Public Key Infrastructure

Duration: 4 Days **Course Code: M2821**

Overview:

This five-day instructor-led course is designed to provide functional skills in planning and implementing infrastructure security. The primary product focus is on Microsoft Windows Server™ 2003 based infrastructure solutions but will include some client-focused content where appropriate.

Target Audience:

The course is designed for system administrators or system engineers who have the foundation implementation skills and knowledge for the deployment of secure Microsoft Windows Server 2003 based solutions. This course will cover planning skills at a level sufficient to enable decision making for the implementation process.

Objectives:

- Plan and configure an authorization and authentication strategy in a multi-forest organization.
 - Install, configure, and manage a certification authority (CA).
 - Configure, deploy, and manage certificates.
 - Plan, implement, and troubleshoot smart card certificates.
 - Plan, implement, and troubleshoot Encrypting File System (EFS).
 - Plan, configure, and deploy a secure member server baseline.
 - Plan, configure, and implement secure baselines for server roles.
 - Plan, configure, implement, and deploy a secure client computer baseline.
 - Plan and implement Software Update Services.
 - Plan, implement, and troubleshoot data transmission security.
 - Plan and implement security for wireless networks.
 - Plan and implement perimeter security with Internet Security and Acceleration Server (ISA) 2000.
 - Secure remote access.
-

Prerequisites:

Delegates are required to meet the following prerequisites:

- Completed Course M2810 Fundamentals of Network Security or equivalent knowledge.
- Experience implementing a Windows® 2000 or Windows Server 2003 Active Directory® environment.
- Experience with organizational resources such as Web, FTP and Exchange servers, (not expected to have detailed knowledge) shared resources and network services such as DHCP, DNS and WINS also helpful.

Testing and Certification

Recommended as preparation for exam(s):

- Exam 70-299: Implementing and Administering Security in a Microsoft Windows Server 2003 Network
-

Content:

Planning and Configuring an Authorization and Authentication Strategy

- Groups and Basic Group Strategy in Windows Server 2003
- Creating Trusts in Windows Server 2003
- Planning, Implementing, and Maintaining an Authorization Strategy Using Groups
- Components of an Authentication Model ; Planning and Implementing an Authentication Strategy
- Installing, Configuring, and Managing Certification Authorities
- Installing ; Managing a Certification Authority
- Backing Up and Restoring a Certification Authority
- Configuring, Deploying and Managing Certificates
- Configuring Certificate Templates
- Deploying and Revoking User and Computer Certificates
- Managing Certificates
- Planning, Implementing, and Troubleshooting SmartCard Certificates
- Introduction to Multifactor
- Authentication Planning, Implementing, Managing and troubleshooting a Smart Card Infrastructure
- Planning, Implementing, and Troubleshooting Encrypting File System
- Implementing EFS in a Standalone Microsoft WindowsXP Environment
- Planning and Implementing EFS in a Domain Environment with a PKI
- Troubleshooting EFS
- Planning, Configuring, and Deploying a Secure Member Server Baseline
- Planning a Secure Member Server Baseline
- Configuring Additional Security Settings
- Deploying Security Templates
- Planning, Configuring, and Implementing Secure Baselines for Server Roles
- Planning and Configuring a Secure Baseline for Domain Controllers and DNS Servers
- Planning and Configuring a Secure Baseline for Infrastructure Servers
- Planning a Secure Baseline for File and Print Servers and IIS Servers
- Planning, Configuring, Implementing, and Deploying a Secure Client Computer Baseline
- Planning and Implementing a Secure Client Computer Baseline
- Configuring and Deploying a Client Computer Baseline
- Planning and Implementing a Software Restriction Policy
- Implementing Security for Mobile Clients
- Planning and Implementing Software Update Services
- Planning an Update Management Strategy
- Implementing an SUS Infrastructure
- Planning, Deploying, and Troubleshooting Data Transmission Security
- Secure Data Transmission Methods
- Introducing IPSec
- Planning Data Transmission Security

- Implementing Secure Data Transmission Methods
- Troubleshooting IPSec Communications
- Planning and Implementing Security for Wireless Networks
- Implementing 802.1x Authentication
- Planning a Secure WLAN Strategy
- Implementing a Secure WLAN
- Troubleshooting Wireless Networks
- Planning and Implementing Perimeter Security with Internet Security and Acceleration Server2000
- Installing ISA Server2000
- Securing a Perimeter Network with ISA Server2000
- Publishing Servers on a Perimeter Network
- Securing ISA Server Computers
- Securing Remote Access
- Planning a Remote Access Strategy
- Deploying Network Access
- Quarantine Control Components

Further Information:

For More information, or to book your course, please call us on 00 20 (0) 2 2269 1982 or 16142

training@globalknowledge.com.eg

www.globalknowledge.com.eg

Global Knowledge, 16 Moustafa Refaat St. Block 1137, Sheraton Buildings, Heliopolis, Cairo, Egypt