Implement Security in Azure Development Solutions

Duration: 1 Day **Course Code: M-AZ-200T04**

Overview:

This course is part of a series of four courses to help you prepare for Microsoft's Azure Developer certification exam AZ-200: Develop Core Microsoft Azure Cloud Solutions. These courses are designed for developers who already know how to code in at least one of the Azure-supported languages.
The coursework covers how authentication and authorization work in Azure, and how to implement secure data solutions with: encryption; Azure Key Vault; and SSL and TLS communications.

Target Audience:

These courses are for experienced programmers who want to develop and host solutions in Azure. Learners should have some experience with Azure and must be able to program in at least one Azure-supported language. These course focus on C#, Node.js, Azure CLI, Azure PowerShell, and JavaScript.

Objectives:

- After completing this course, students will be able to:
- Learn about the different authentication options, including multi-factor, available in Azure and how they operate
- Learn about implementing access control in your solution including claims- and role-based authorization
- Implement secure data solutions by using encryption, Azure confidential computing, and SSL/TLS communications
- Manage cryptographic keys in Azure Key Vault

Content:

Module 1: Implementing authentication

Lessons

- Implement authentication in applications
- Implement multi-factor authentication
- Claims-based authorization
- Role-based access control (RBAC) authorization
- Encryption options
- End-to-end encryption
- Implement Azure confidential computing
- Manage cryptographic keys in Azure Key Vault

After completing this module, students will be able to:

- Learn about the different authentication options, including multi-factor, available in Azure and how they operate
- Learn about implementing access control in your solution including claims- and role-based authorization
- Implement secure data solutions by using encryption, Azure confidential computing, and SSL/TLS communications

Module 2: Implementing access control

Lessons

- Implement authentication in applications
- Implement multi-factor authentication
- Claims-based authorization
- Role-based access control (RBAC) authorization
- Encryption options
- End-to-end encryption
- Implement Azure confidential computing
- Manage cryptographic keys in Azure Key Vault

After completing this module, students will be able to:

- Learn about the different authentication options, including multi-factor, available in Azure and how they operate
- Learn about implementing access control in your solution including claims- and role-based authorization
- Implement secure data solutions by using encryption, Azure confidential computing, and SSL/TLS communications

Module 3: Implementing secure data solutions

Lessons

- Implement authentication in applications
- Implement multi-factor authentication
- Claims-based authorization
- Role-based access control (RBAC) authorization
- Encryption options
- End-to-end encryption
- Implement Azure confidential computing
- Manage cryptographic keys in Azure Key Vault

After completing this module, students will be able to:

- Learn about the different authentication options, including multi-factor, available in Azure and how they operate
- Learn about implementing access control in your solution including claims- and role-based authorization
- Implement secure data solutions by using encryption, Azure confidential computing, and SSL/TLS communications

Further Information:

For More information, or to book your course, please call us on 353-1-814 8200

info@globalknowledge.ie

www.globalknowledge.com/en-ie/

Global Knowledge, 3rd Floor Jervis House, Millennium Walkway, Dublin 1