**Module Title : AZ-300T05-A: Implementing Authentication and Secure Data**
**Duration : 0.5 day**

## Overview

Learn how to Implement authentication in applications (certificates, Azure AD, Azure AD Connect, token-based), implement secure data (SSL and TLS), and manage cryptographic keys in Azure Key Vault.

## Audience profile

Successful Cloud Solutions Architects begin this role with practical experience with operating systems, virtualization, cloud infrastructure, storage structures, billing, and networking.

## At course completion

After completing this course, students will be able to:

- Understand how to Implement authentication using certificates, Azure AD, Azure AD Connect, and tokens.
- Implement Role-aBsed Access Control (RBAC) authorization.
- Implement secure data for end-to-end encryption.
- Implement secure data for implementing SSL and TLS communications.
- Use Azure Key Vault to manage cryptographic keys.

## Course Outline

**Module 1: Implementing Authentication Topics for this module include:**

**Lessons**

- Implementing authentication in applications (certificates, Azure AD, Azure AD Connect, token-based)
- Implementing multi-factor authentication
- Claims-based authorization
- Role-based access control (RBAC) authorization

After completing this module, students will be able to:

- Understand how to Implement authentication using certificates, Azure AD, Azure AD Connect, and tokens
- Implement Role-Based Access Control (RBAC) authorization

**Module 2: Implementing Secure Data**

**Lessons**

- End-to-end encryption
- Implementing Azure confidential computing
- Implementing SSL and TLS communications
- Managing cryptographic keys in Azure Key Vault

After completing this module, students will be able to:

- Implement secure data for end-to-end encryption
- Implement secure data for implementing SSL and TLS communications.
- Use Azure Key Vault to manage cryptographic keys