Filename: microsoft-ms101-10-9-1-implement-aip-tenant-key
ShowName: Microsoft 365 Mobility and Security
SubTitle: Exam MS-101
Topic: Implement Azure Information Protection (AIP)
EpisodeName: Implement AIP Tenant Key
Description: Adam and Wes discuss the steps necessary to help you successfully implement the AIP tenant key.

Implement AIP Tenant Key

Manage Microsoft 365 Governance and Compliance (35-40%)

Implement Azure Information Protection (AIP)
• Plan AIP Solution
• Plan for Deployment On-Prem Rights Management Connector
• Plan for Windows Information Protection (WIP) Implementation
• Plan for Classification Labeling
• Configure Information Rights Management (IRM) for Workloads
• Configure Super User
• Deploy AIP Clients
• Implement Azure Information Protection Policies
• Implement AIP Tenant Key

==========

Implement AIP Tenant Key

NOTE: Operations for your Azure Information Protection tenant key:
https://docs.microsoft.com/en-us/azure/information-protection/operations-tenant-key

Planning and implementing your Azure Information Protection tenant key:
https://docs.microsoft.com/en-us/azure/information-protection/plan-implement-tenant-key

What is the Azure Information Protection tenant key?

```
• The Azure Information Protection tenant key is a root key for your
```

organization. Other keys can be derived from this root key, such as user keys, computer keys, and document encryption keys. Whenever Azure Information Protection uses these keys for your organization, they cryptographically chain to your Azure Information Protection tenant key.

```
• The Azure Information Protection tenant key is the online equivalent of the
```

Server Licensor Certificate (SLC) key from Active Directory Rights Management Services (AD RMS).

Decide which tenant key topology is best for your organization:

```
• Managed by Microsoft: Microsoft automatically generates a tenant key for your
```

organization and this key is used exclusively for Azure Information Protection. By default, Microsoft uses this key for your tenant and manages most aspects of your tenant key life cycle.

This is the simplest option with the lowest administrative overheads. In most cases, you do not even need to know that you have a tenant key. You just sign up for Azure Information Protection and the rest of the key management process is handled by Microsoft.

```
• Managed by you (BYOK): For complete control over your tenant key, use Azure
```

Key Vault with Azure Information Protection. For this tenant key topology, you create the key, either directly in Key Vault, or create it on-premises. If you create it on-premises, you next transfer or import this key into Key Vault. You then configure Azure Information Protection to use this key, and you manage it in Azure Key Vault.

NOTE: If required, you can change your tenant key topology after deployment, by using the Set-AipServiceKeyProperties cmdlet.

To create your own key, you have the following options -

• A key that you create on-premises and transfer or import to Key Vault:

```
• An HSM-protected key that you create on-premises and transfer to Key Vault
```

as an HSM-protected key.

```
• A software-protected key that you create on-premises, convert, and then
```

transfer to Key Vault as an HSM-protected key. This option is supported only when you migrate from Active Directory Rights Management Services (AD RMS).

```
• A software-protected key that you create on-premises and import to Key Vault
```

as a software-protected key. This option requires a .PFX certificate file.

• A key that you create in Key Vault:

```
• An HSM-protected key that you create in Key Vault.

• A software-protected key that you create in Key Vault.
```