Implementing the AIP Tenant key

The Azure Information Protection (AIP) 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.

Depending on your tenant key topology for Azure Information Protection, you have different levels of control and responsibility for your AIP tenant key. The AIP key topologies that are available include a “Microsoft-managed” key, a “customer-managed” key, and a third key type that is a mix of these two.

Differences between key types

The major difference between these three types of keys are the place where they are created.

- **The Microsoft-managed key is generated directly in the Azure RMS environment and stored in the Azure Key Vault.**
- **The customer-managed key is generated in the on-premises AD RMS environment and then uploaded to the same Azure Key Vault. This is also called “Bring-your-own-key” (BYOK).**
- **The third key type utilizes both the Microsoft-managed and customer-managed keys to differentiate on-premises and cloud encrypted documents and files. This is called “Hold-your-own-key” (HYOK).**

The following table identifies when each key topology should be used.

Microsoft-managed	**Customer-managed – “Bring your own key” (BYOK)**	**Mix of both – “Hold-your-own-key” (HYOK)**
If you don’t have an AD RMS environment in place and you do not have special business requirements that disallow the source of authority of your key in the cloud, you can safely generate the key in Azure. The backup is then managed by Microsoft and fewer additional administrative effort is required within the key-lifecycle.	If you already have an on-premise AD RMS environment, you need to integrate both environments to preserve access to all content protected with the on-premises AD RMS key. This can be achieved by migrating the key you have used on-premises into the cloud and continue working with the same key for protection. In that topology you are responsible for the backup and all renewal procedures of the key.	The third way of managing the keys is the “Hold-your-own-Key” solution. In this case the key from the on-premise AD RMS environment is not migrated and a second key is generated in Azure. In this case it is possible to use different labels that use one of the keys to protect content, that will not be accessible from the other premises side. This solution is not a way of migration and only required if very high security and compliance requirements must be fulfilled. This solution requires the most administration and is limited in flexibility.

Given the fact that HYOK types require the most administration and are limited in flexibility, the remainder of this topic will focus on the Microsoft-managed and Customer-managed keys, which are the two key types most commonly implemented.

Life cycle operations for Microsoft-managed and Customer-managed keys

Within the life-cycle of a key, you must consider different management actions with your tenant's key.

The following table identifies the operations that you can do, depending on the topology that you've chosen for your Azure Information Protection tenant key.

Operation	**Microsoft-managed (default)**	**Customer-managed**
Revoke your tenant key	No (automatic)	Yes
Rekey your tenant key	Yes	Yes
Back up and recover your tenant key	No	Yes
Export your tenant key	Yes	No
Respond to a breach	Yes	Yes

Operational considerations for each key type

You need to consider the following operational tasks when implementing an AIP tenant key:

- **Revoke your tenant key**. Remove the specific key from RMS completely.

- **Rekey your tenant key**. Rekeying is also known as rolling your key. When you perform this operation, Azure Information Protection stops using the existing tenant key to protect documents and emails and starts to use a different key.
- **Back up and recover your tenant key.** Back up the Azure Information Protection key for emergency situations.
- **Export your tenant key.** Export the key from the Azure Key Vault.
- **Respond to a breach.** No security system, no matter how strong, is complete without a breach response process. Your tenant key might be compromised or stolen. Even when it's protected well, vulnerabilities might be found in current generation key technology or in current key lengths and algorithms.

There are important differences in your key life-cycle to consider when deciding for a key topology.

Microsoft-managed	**Customer-managed**
Revoke your tenantkey: When you cancel your subscription for Azure Information Protection, Azure Information Protection stops using your tenant key and no action is needed from you.	**Revoke your tenant key:** In Azure Key Vault, you can change the permissions on the key vault that contains your Azure Information Protection tenant key so that the Azure RMS can no longer access the key. However, when you do this, nobody will be able to open documents and emails that you

	previously protected.
Rekey your tenant key: To rekey, you can select a different Microsoft-managed key to become your tenant key, but you cannot create a new Microsoft-managed key. To create a new key, you must change your key topology to be customer-managed (BYOK).	**Rekey your tenant key:** To rekey to another key that you manage, you can either create a new key in Azure Key Vault or use a different key that is already in Azure Key Vault.
Back up and recover your tenant key: Microsoft is responsible for backing up your tenant key and no action is required from you.	**Back up and recover your tenant key:** Because you are managing your tenant key, you are responsible for backing up the key that Azure Information Protection uses.
Export your tenant key: You can export your Azure Information Protection configuration and tenant key.	**Export your tenant key:** If you use BYOK, you cannot export your tenant key from Azure Key Vault or Azure Information Protection. The copy in Azure Key Vault is non-recoverable.
Respond to a breach: If a security related problem with the key generation algorithms is detected, Microsoft will update the HSM and instruct all customers to rekey their	**Respond to a breach:** You must secure and maintain your HSM and react yourself on security related issues regarding the key generation algorithms.

tenant keys.	

Additional reading. For more information about the HYOK solution, see the following article on Hold your own key (HYOK) protection for Azure Information Protection.