Arctera™ Insight Archiving Key Management

(BYOK vs. MYOK)

White Paper | February 2025

Contents

BYOK vs. MYOK

"Manage Your Own Key" (MYOK) and "Bring Your Own Key" (BYOK) are techniques used in SaaS products to implement encryption. Each has its advantages and disadvantages, depending on the organization's needs.

By using BYOK, customers can bring their encryption keys to the SaaS provider's infrastructure. This reduces customers' burdens but does not provide the same level of security as MYOK. This is because the keys are managed in the SaaS provider's infrastructure.

With MYOK, customers can manage their encryption keys within the SaaS provider's infrastructure. A customer's ability to revoke their encryption keys at any time provides higher security levels. Therefore, managing these keys may require additional customer resources and expertise, as well as additional costs.

We know customers value security, so MYOK lets them manage their encryption keys within its own infrastructure providing a higher level of security. By doing this, customers have full control over their keys and can revoke them at any time.

By supporting MYOK over BYOK, we demonstrate our commitment to providing our customers with the highest level of security and control over their data.

Arctera Insight Archiving - Default Key management

- Historically, customer keys are not used.
- Arctera Insight Archiving generates a key for every tenant.
  - Tenant keys are stored in the Azure Key Vault.
  - The tenant key encrypts/decrypts data.
  - Customer keys are deleted upon leaving Arctera Insight Archiving.

Arctera Insight Archiving - Manage your own key

Customers manage keys throughout their life cycle, from creation to destruction. The following chart illustrates the customer's complete control over the key life cycle. This also illustrates the types of resources they want to encrypt, and key storage options.

Key management parameter	Microsoft-managed keys	Customer-managed keys (MYOK)	Customer-provided keys (BYOK)
Encryption/decryption operations	Azure	Azure	Azure
Azure Storage services supported	All	Blob Storage, Azure Files 1,2	Blob Storage
Key storage	Microsoft key store	Azure Key Vault or Azure Key Vault HSM*	Customer's key store
Key rotation responsibility	Microsoft	Customer	Customer
Key control	Microsoft	Customer	Customer
Key scope	Account (default), container, or blob	Account (default), container, or blob	N/A

Figure 1 - Customer key management

Note: By default, Arctera Insight Archiving encryption uses the approach defined in the first column (Microsoft-managed keys). The second column is enabled for customers who choose the MYOK encryption option.

Azure Data Encryption at rest with CMK + Federated identity

The following illustration demonstrates how the federated identity can encrypt data at rest when MYOK is enabled (a cross-tenant MYOK workflow).

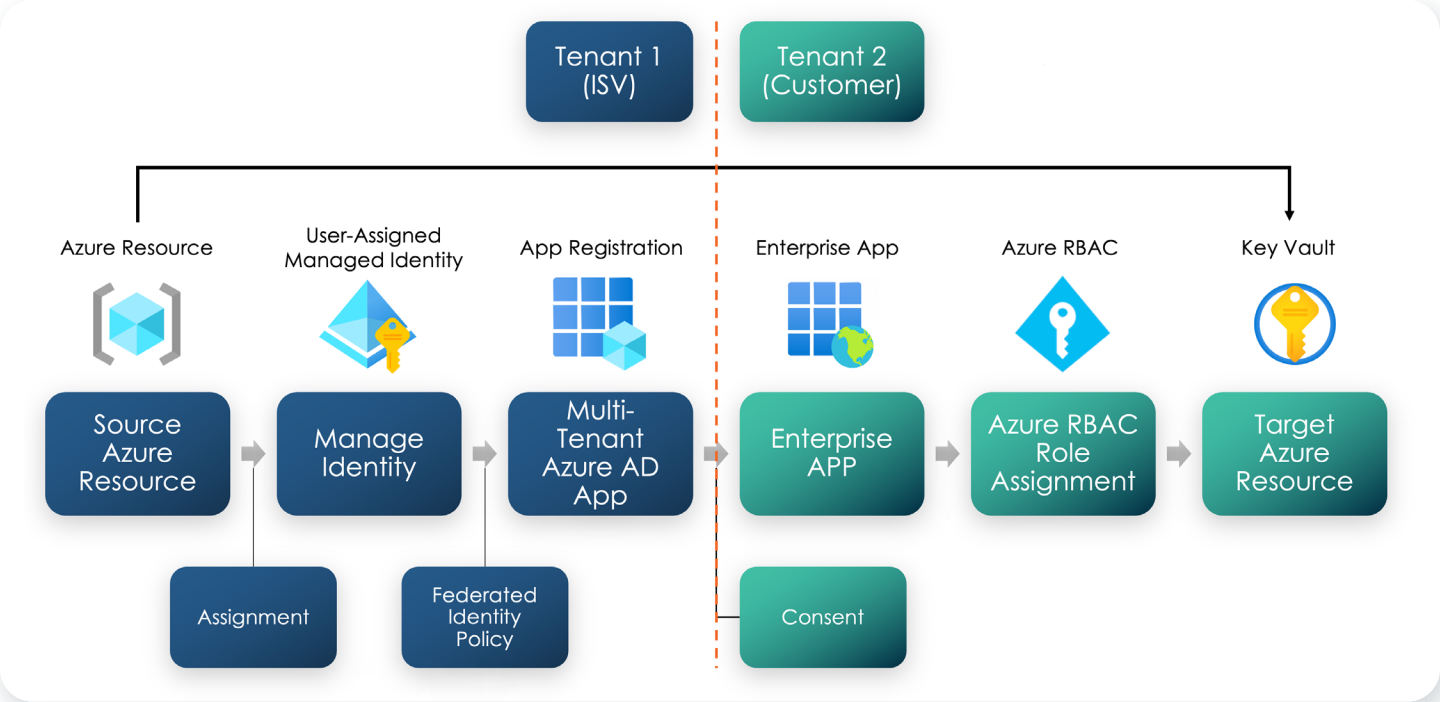

Figure 2 – Cross-A MYOK workflow involving a service provider and its customer.

Manage Your Own Key Flow

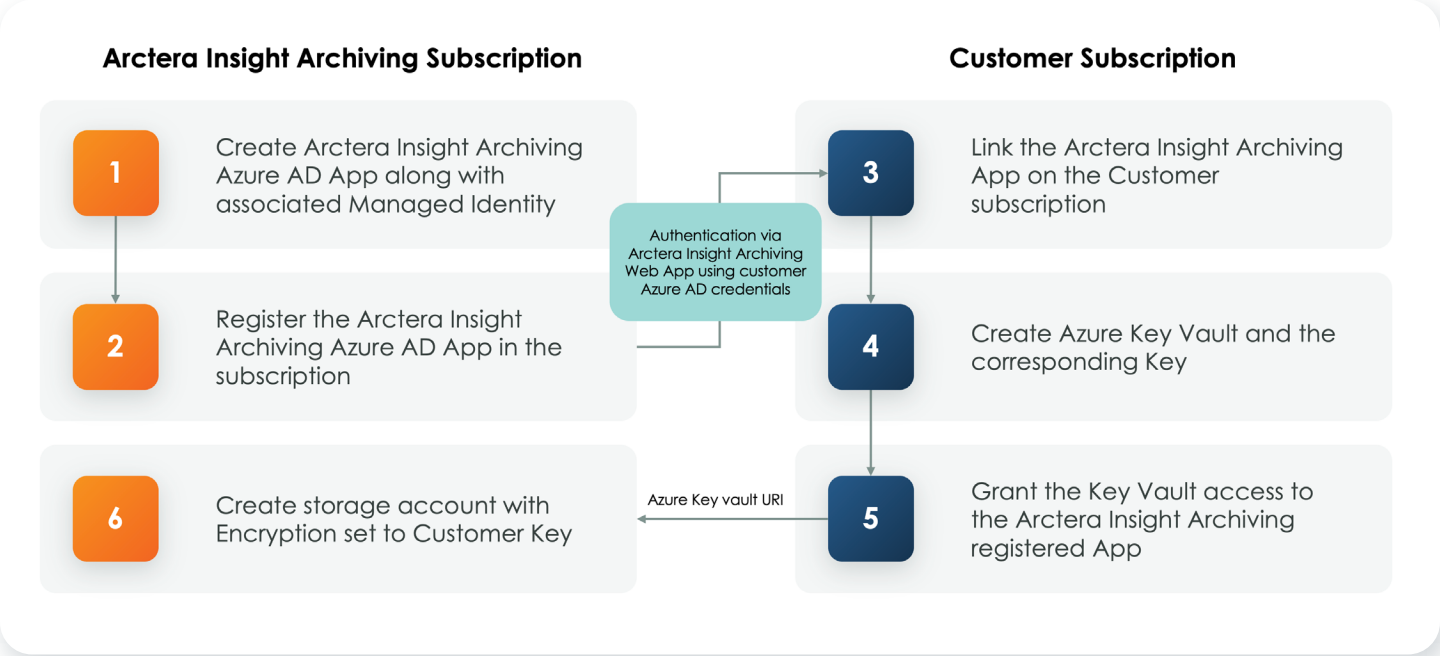

Figure 3 - Customer key flow management

- Customers can add Azure subscriptions directly.
  - Key policies are set by customers, such as:
    - Rotation
    - Expiration
    - Enabled
  - Permitted operations.
- Customers and Arctera Insight Archiving provide keys used to encrypt/decrypt data stored in Arctera Insight Archiving Blob storage.
- To provide service to customers, the customer's data must be encrypted/decrypted using Arctera Insight Archiving tenant keys.

For example:

- Arctera_Insight_Archiving_Key* » Created and stored in Azure Key Vault.
- Customer_Key » Created and stored in Azure Key Vault.
- Accessing Customer data from blob storage requires a Customer_Key.
- Arctera Insight Archiving Blob API (2nd layer of encryption) uses Arctera_Insight_Archiving_Key for encryption and decryption.

Customer keys usually open the door, while Arctera Insight Archiving Tenant keys allow data access. A master key (owned by the customer) is required to access data on Arctera Insight Archiving.

Arctera Insight Archiving MYOK High-Level End-To-End Flow

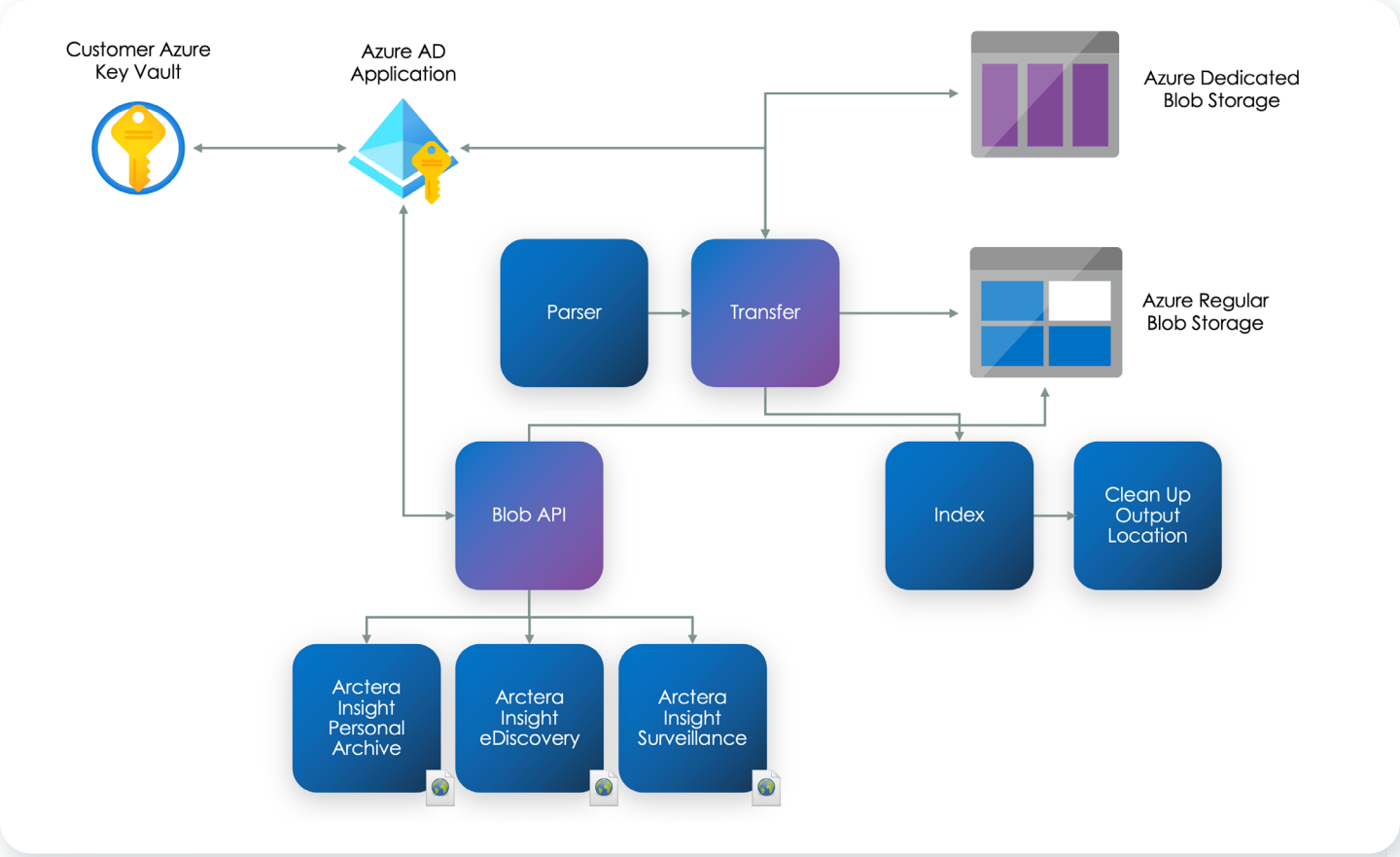

Figure 4 - Master key process

- By creating a blob storage with Arctera Insight Archiving, encrypted code can be reused with customer keys.
- A customer-specific blob storage account must be created by triggering the backend change in Arctera Insight Management Console "MYOK".
- The Customer Storage data account can be encrypted/decrypted using a key provided by the customer using Azure Key Vault.
- The customer is responsible for establishing a key rotation policy.
- Use an Azure AD application to connect to the customer's Azure Key Vault for setting up cross-tenant customer-managed keys on an existing storage account.
- Only new customers can benefit from this new encryption approach since existing customers already have their storage provisioned and encrypted.
- The customer needs an Azure Key Vault subscription.
- Existing customers must create a new archive to use this encryption feature. Paid migration services would be required to move the existing archives to a new archive, then delete them.
- Arctera Insight Archiving cannot decrypt customer data if the key is changed or deleted by the customer.

* Existing customers who wish to enable MYOK are charged a migration fee. Each case is handled by a sales representative.

What content is encrypted?

- Only Azure Blob customer data is covered.
- Arctera manages a separate encryption key for data stored outside of Azure Blob. This includes metadata in the database or Elastic index.

Safeguarding lost keys

- Customer-managed keys cannot be set without "Purge Protection" enabled.
- Deleted keys can be retrieved within 90 days of deletion before they become irrecoverable.
- The customer can restore the key by downloading a backup.

About Arctera

Arctera, a business unit of Cloud Software Group, is the leading global provider of compliance and governance solutions that enable firms to unleash game-changing technologies into their organizations while minimizing risk. Created in 2024 from Veritas Technologies, Arctera helps the biggest companies in the world monitor and control exactly how their information is being accessed, used and shared. The Arctera Insight Platform is able to capture data from over 130+ different content sources, and more than 280 AI policies help firms streamline compliance and adapt to evolving regulations.

Learn more: arctera.com

Connect:

Contact: press@arctera.com

A0163 11/25