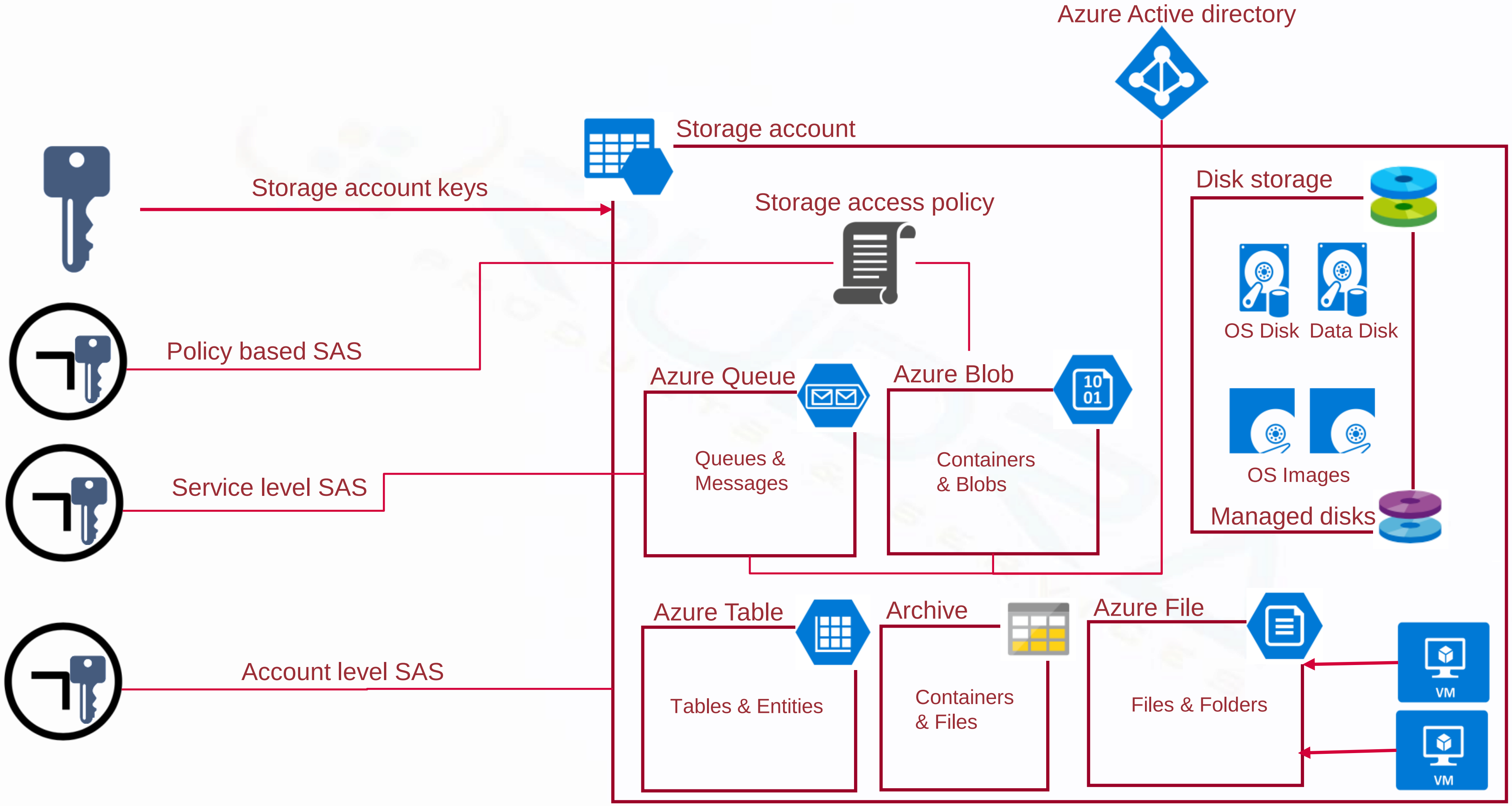
Azure Storage services – Data plane security deep dive

Data plane security options



Storage account keys

- **Storage account keys** – These are 512-bit strings created by Azure, along with the storage account name, can be used to access the data objects stored in storage account.

- For example, you can read blobs, write to queues, create tables, and modify files.

- Access to the storage keys for a storage account using the Azure Resource Manager model can be controlled through Role-Based Access Control (RBAC).

Shared Access Signatures

- A **Shared Access Signature** is a string containing a security token that can be attached to a URI that allows you to delegate access to storage objects and specify constraints such as permissions and date/time range of access
  - With tables, you can actually grant permissions to access a range of entities in the table by specifying the partition and row key ranges that you want user to access.
  - For queues, you can grant permission to a web role to put the messages into queue and a worker role to read messages from the queues.
  - With blobs, you can give somebody to upload videos into the container and an web application to read the videos.

- **Why SAS**
  - Storage account keys gives complete access to data objects in storage account whereas with SAS you can be selective.
  - Give permissions for a limited amount of time
  - Restrict requests made using SAS to a certain IP address or range external to Azure
  - Restrict requests to be made using a specific protocol

Types of SAS

- A **service level SAS** can be used to access specific resources in the storage account. For e.g.
  - Retrieving list of blobs in a container
  - Add messages into a queue

- An **account-level SAS** can be used to grant permissions that are not permitted using a service level SAS. For e.g.
  - Permission to create containers, tables, queues and file shares.
  - Access to multiple services at once

Controlling a SAS with a stored access policy

A shared access signature can take one of two forms:

Adhoc SAS: When you create an adhoc SAS, the start time, expiry time, and permissions for the SAS are all specified in the SAS URI. This type of SAS can be created as an account SAS or a service SAS.

SAS with stored access policy: A stored access policy is defined on a resource container--a blob container, table, queue, or file share--and can be used to manage constraints for one or more shared access signatures. When you associate a SAS with a stored access policy, the SAS inherits the constraints--the start time, expiry time, and permissions--defined for the stored access policy.