70-532 Exam Prep Session 3 of 5

Manage Application, Messaging and Identity Services

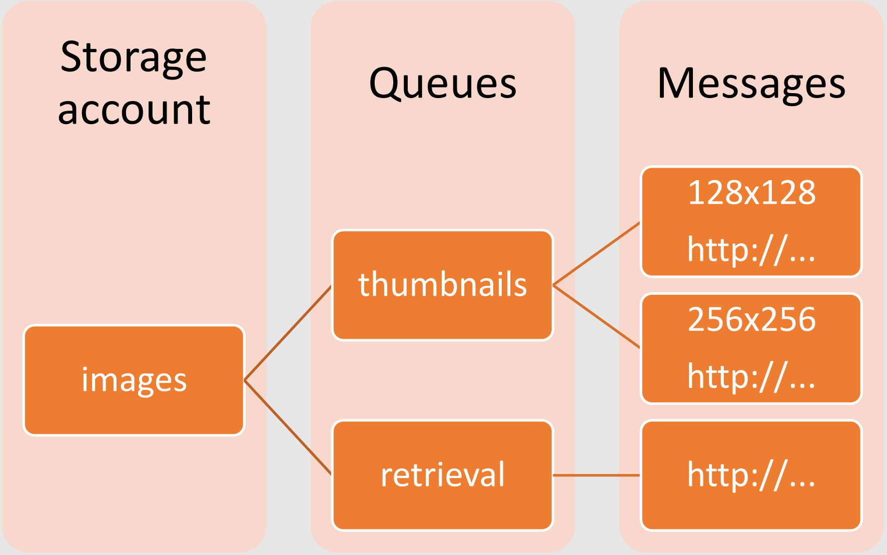
Agenda

- Azure Storage Queues
- Azure Service Bus
- Azure Service Bus Queues
- Azure Service Bus Relay
- Azure Service Bus Notification Hubs

- Azure Active Directory
- Azure AD Directories
- Azure AD Multi-Factor Authentication

Storage Queues Overview

- Storage queues provide a method for storing messages that might be accessed by any number of clients
  - Provide reliable messaging between role instances
  - Built for massive scale and multiple messages



Storage Queues Overview (cont.)

Azure Storage Queues allows you to store large quantities of small messages that can be consumed by a scalable number of consumers

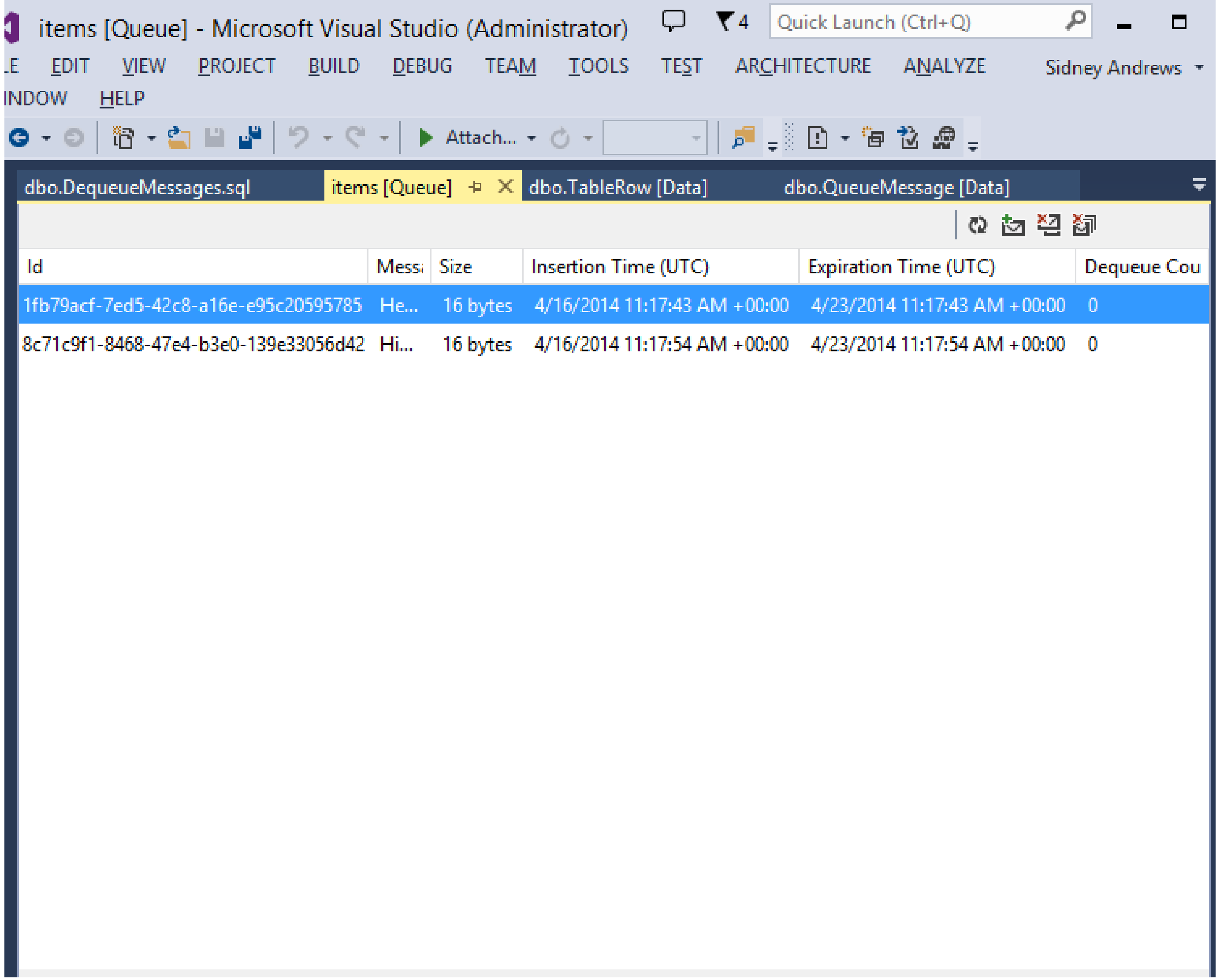
Queue messages have flexible leasing and can be processed again by a different consumer/worker if there is a failure with the initial consumer

Queues can take advantage of the built-in Azure Storage logging and metrics

Queues can have a concept of “state” across workers/consumers

Viewing Queue Storage Data

- Visual Studio Server Explorer provides a view for Storage queue items in the emulator or in a live Azure storage account.

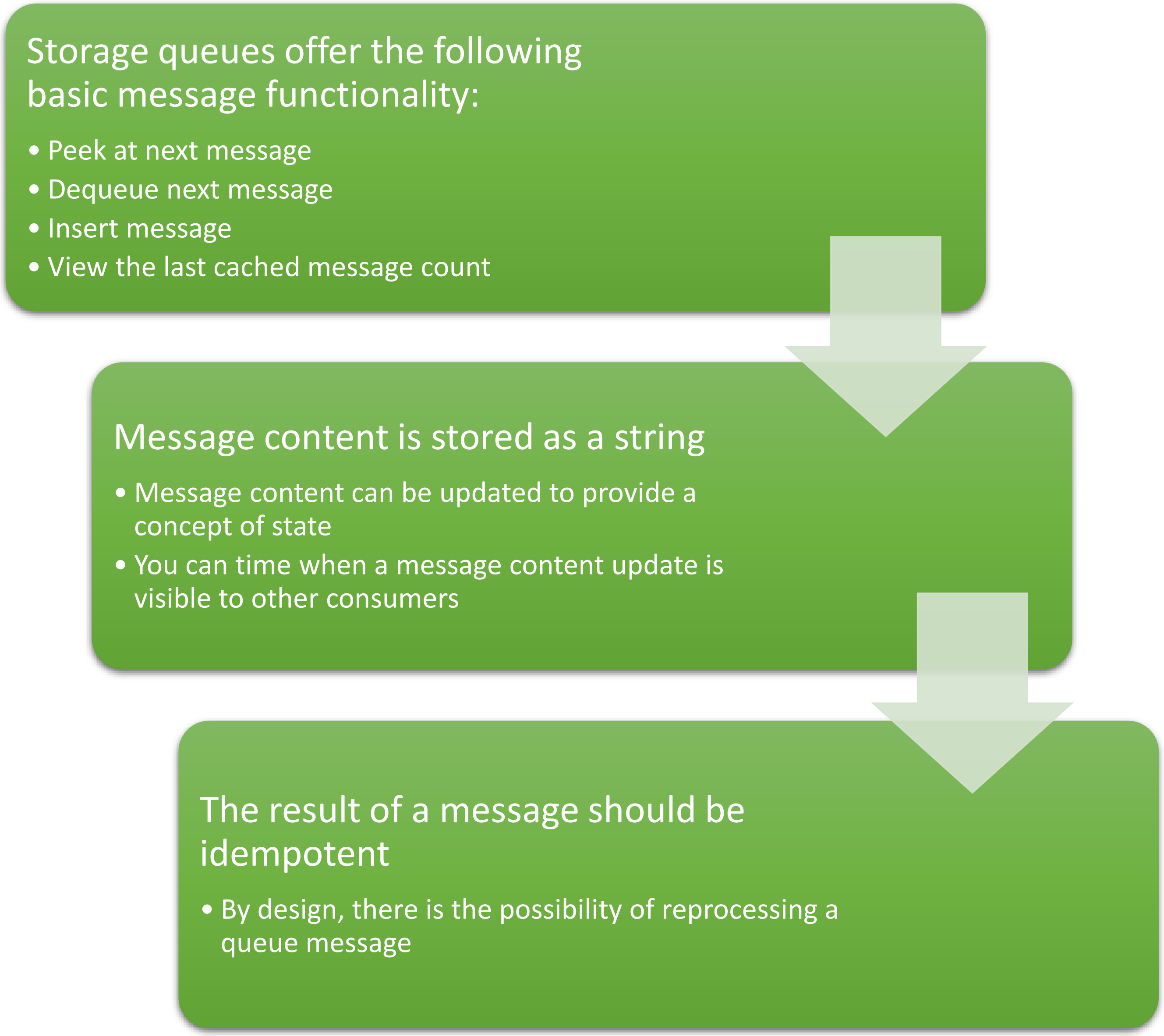


Id	Messi	Size	Insertion Time (UTC)	Expiration Time (UTC)	Dequeue Cou
1fb79acf-7ed5-42c8-a16e-e95c20595785	He...	16 bytes	4/16/2014 11:17:43 AM +00:00	4/23/2014 11:17:43 AM +00:00	0
8c71c9f1-8468-47e4-b3e0-139e33056d42	Hi...	16 bytes	4/16/2014 11:17:54 AM +00:00	4/23/2014 11:17:54 AM +00:00	0

DEMO: Storage Queues in VS

- Storage Queues content (messages) in VS2017

Storage Queue Messages



Storage queues offer the following basic message functionality:

- Peek at next message
- Dequeue next message
- Insert message
- View the last cached message count

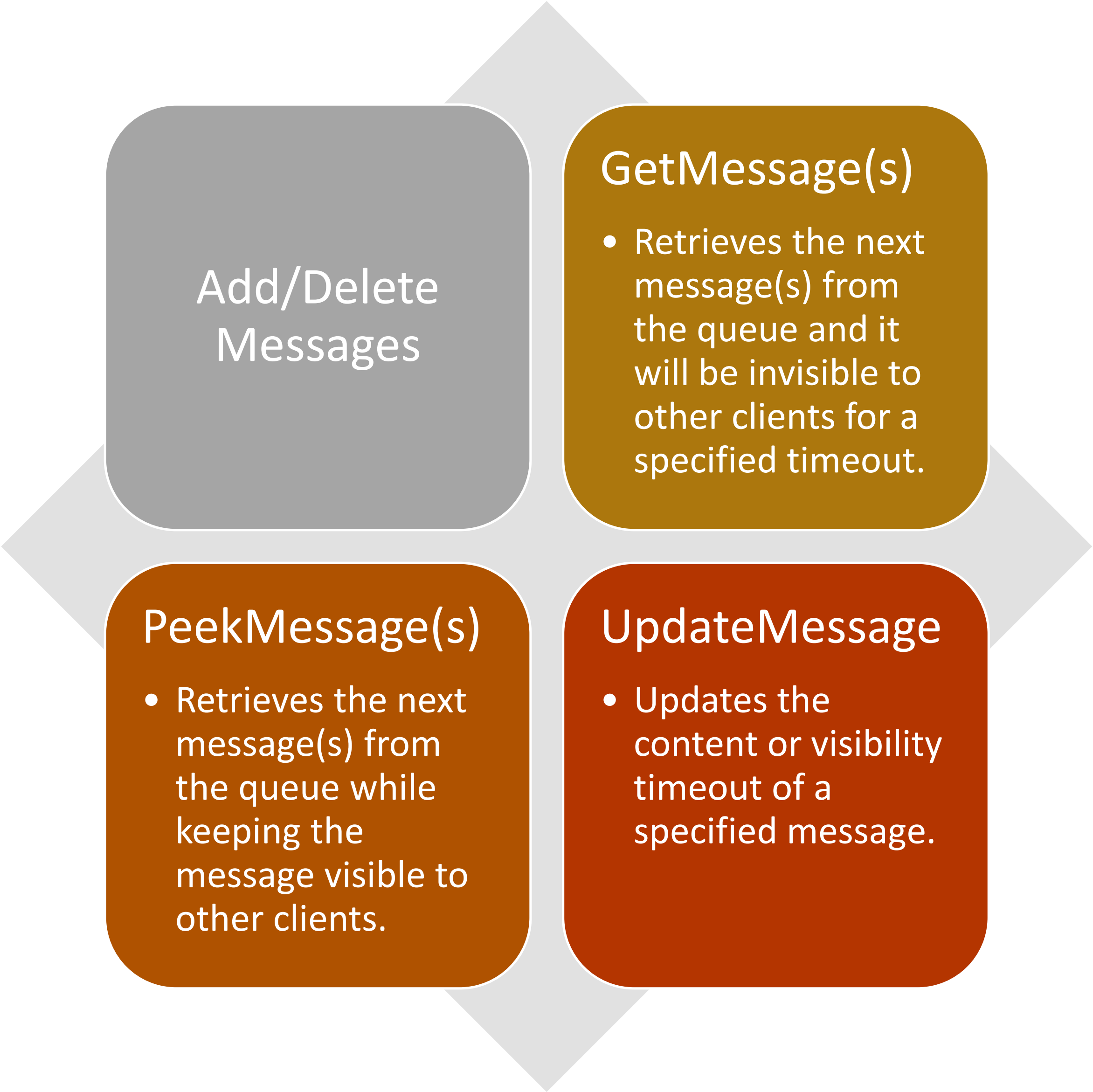
Message content is stored as a string

- Message content can be updated to provide a concept of state
- You can time when a message content update is visible to other consumers

The result of a message should be idempotent

- By design, there is the possibility of reprocessing a queue message

Storage Queue Messages (cont.)



Add/Delete Messages

GetMessage(s)

- Retrieves the next message(s) from the queue and it will be invisible to other clients for a specified timeout.

PeekMessage(s)

- Retrieves the next message(s) from the queue while keeping the message visible to other clients.

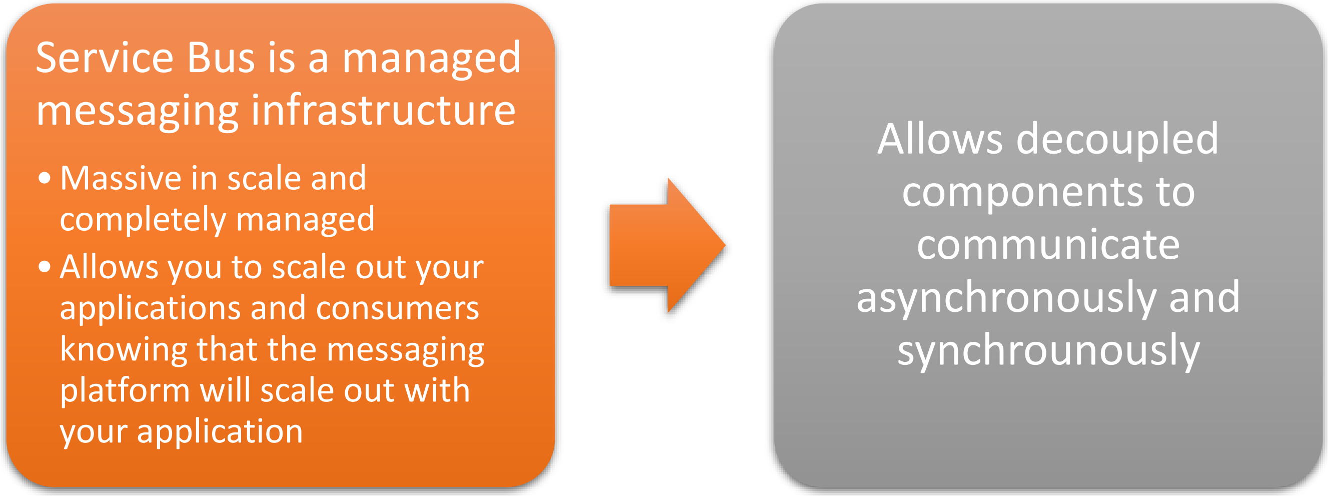
UpdateMessage

- Updates the content or visibility timeout of a specified message.

DEMO: Storage Queues

- Storage Queue configuration in Azure
- Integration Storage Queue processing

Service Bus Overview



Service Bus is a managed messaging infrastructure

- Massive in scale and completely managed
- Allows you to scale out your applications and consumers knowing that the messaging platform will scale out with your application

Allows decoupled components to communicate asynchronously and synchrounously

Service Bus Features

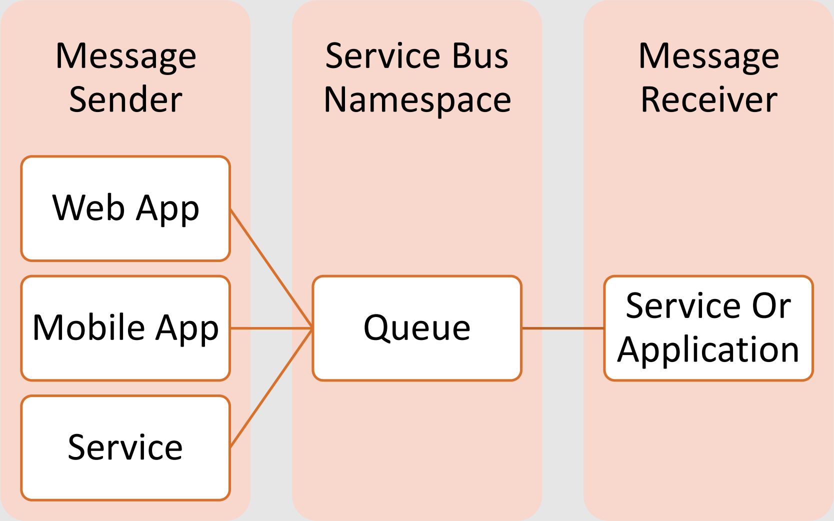
- Relayed Messaging
- Publish-Subscribe Topics
- Queues
- Notification Hubs

Namespaces

- A Service Bus namespace is a logical grouping of Service Bus service instances
  - It scopes your resources to provide a common and predictable address
  - It provides management credentials to use for operations

Service Bus Queues Overview

- Service Bus queues offer a brokered messaging communication model
  - Distributed applications can share messages in a First In First Out (FIFO) pattern
  - Individual messages are only received by one message consumer



Message Sender

Web App

Mobile App

Service

Service Bus Namespace

Queue

Message Receiver

Service Or Application

Queue Message Delivery

- Service Bus queues provide a queuing mechanism with tight control on the order and delivery of messages
  - Messages will appear only once
  - Messages are processed using the FIFO pattern
  - Message locks can be renewed
  - Supports transactions

Characteristics of Service Bus Queue Messages

- Service Bus queue messages consist of few major parts
  - Body
    - The body can be any serializable object or a stream
    - The DataContractSerializer is used to serialize the complex object
  - Label
    - Simple text label
  - TimeToLive
  - Properties
    - Dictionary of properties that can be used by your specific consumers.

DEMO: ServiceBus Queues

- ServiceBus Queue configuration in Azure
- Integration ServiceBus Queue processing

Service Bus Queues vs. Storage Queues

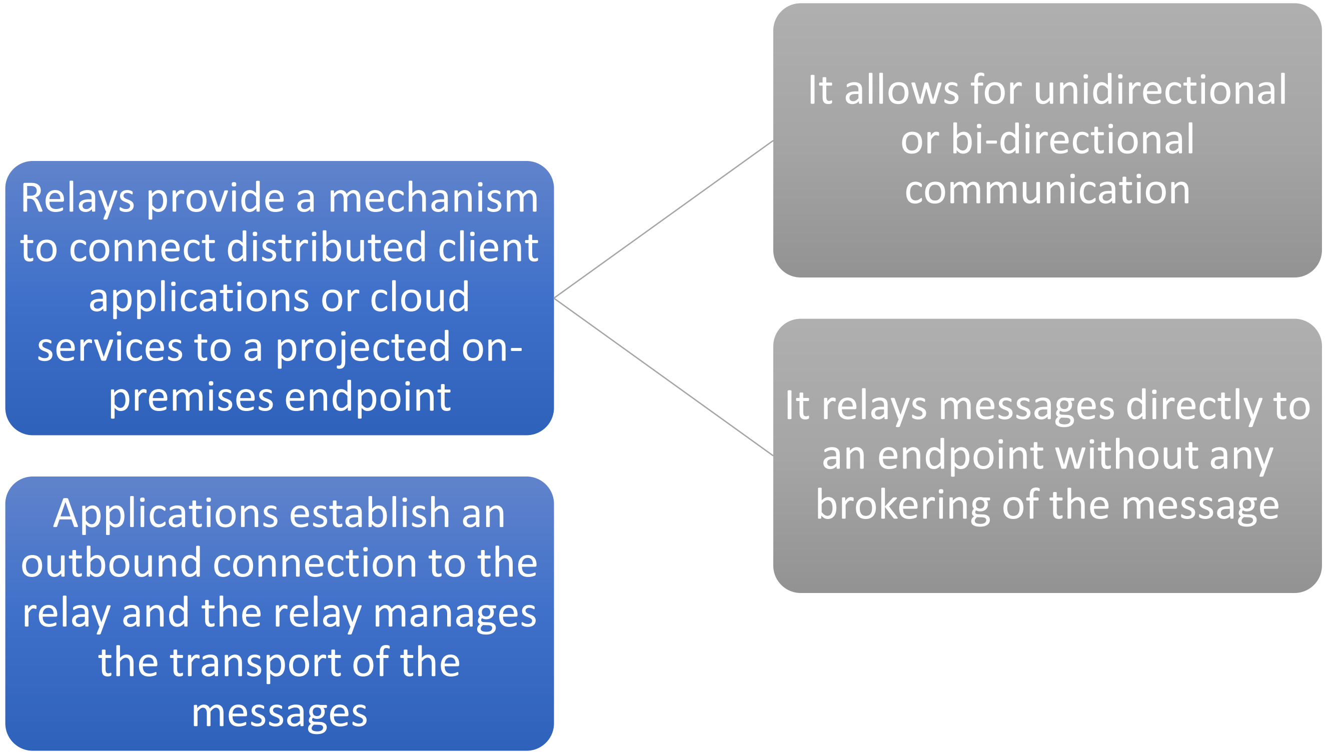
Storage Queues

- Arbitrary ordering
- Delivery at least once, possibly multiple times
- 30 second default locks can be extended to 7 days
- Supports in-place updates of the message content
- Can integrate with WF through a custom activity

Service Bus Queues

- FIFO guaranteed ordering
- Delivery at least once and at most once
- 60 second default locks can be renewed
- Messages are finalized once consumed
- Native integration with WCF and WF

Service Bus Relay Overview



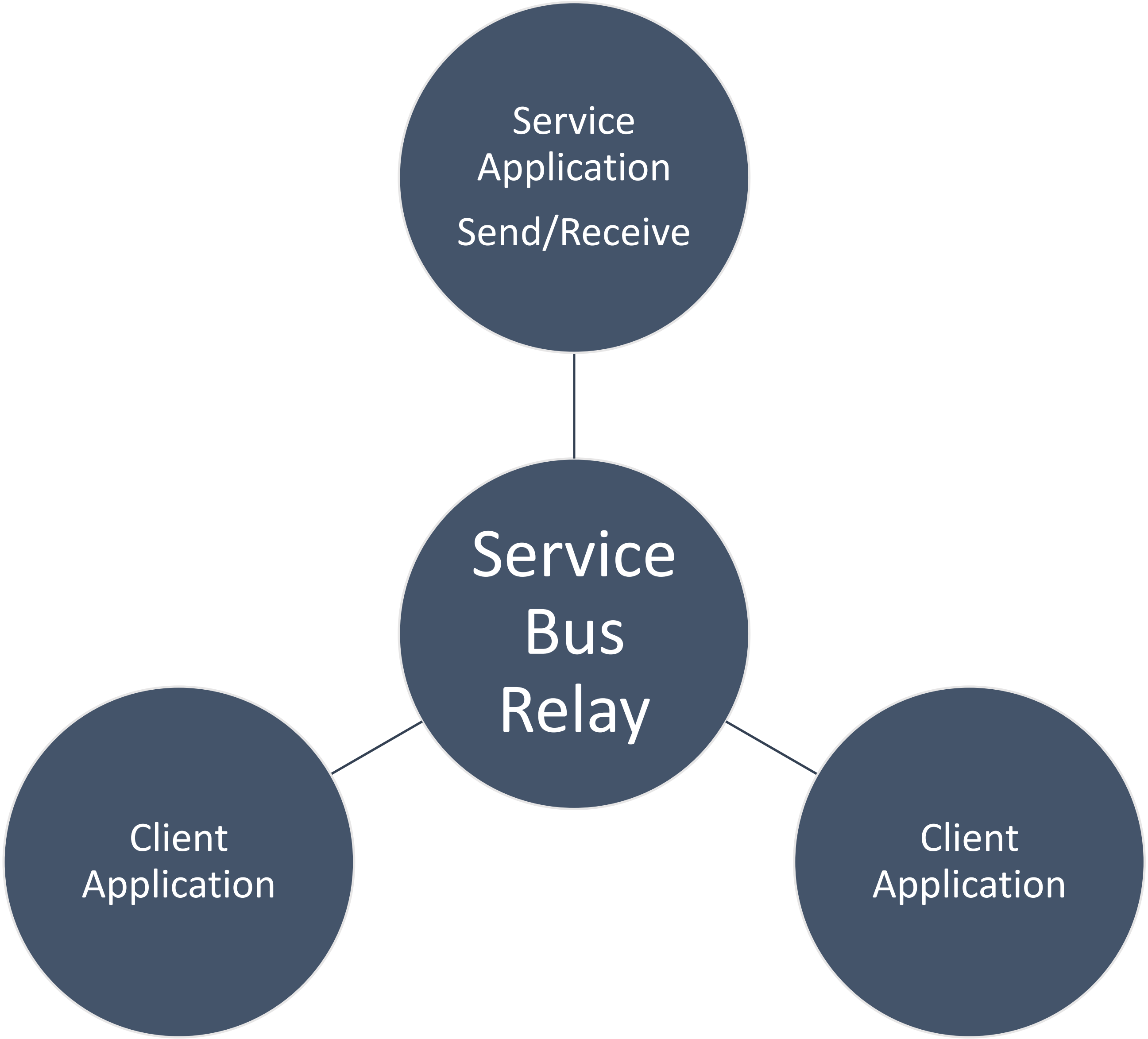
Relays provide a mechanism to connect distributed client applications or cloud services to a projected on-premises endpoint

It allows for unidirectional or bi-directional communication

It relays messages directly to an endpoint without any brokering of the message

Applications establish an outbound connection to the relay and the relay manages the transport of the messages

Service Bus Relay Architecture



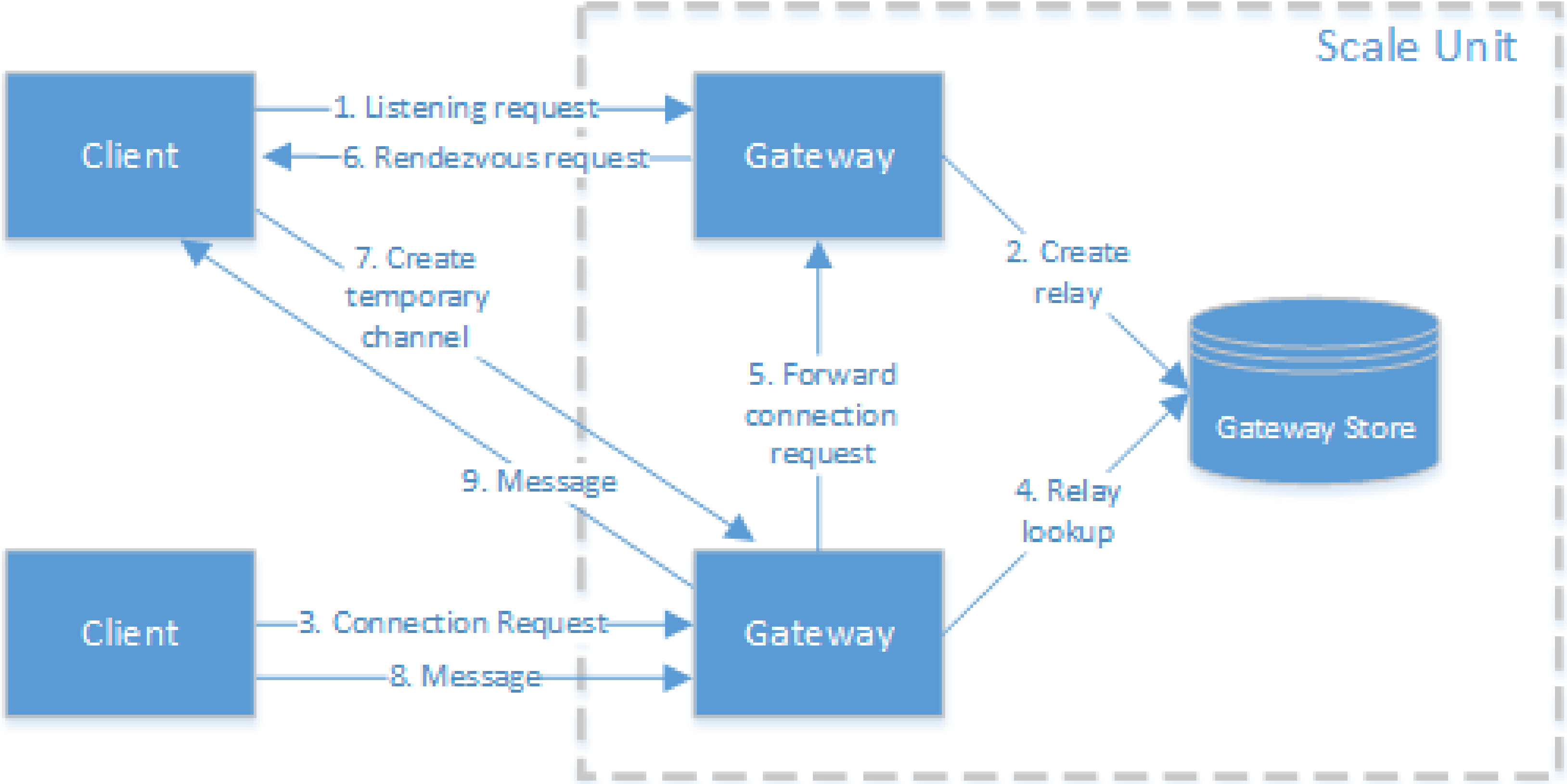
Service Application

Send/Receive

Service Bus Relay

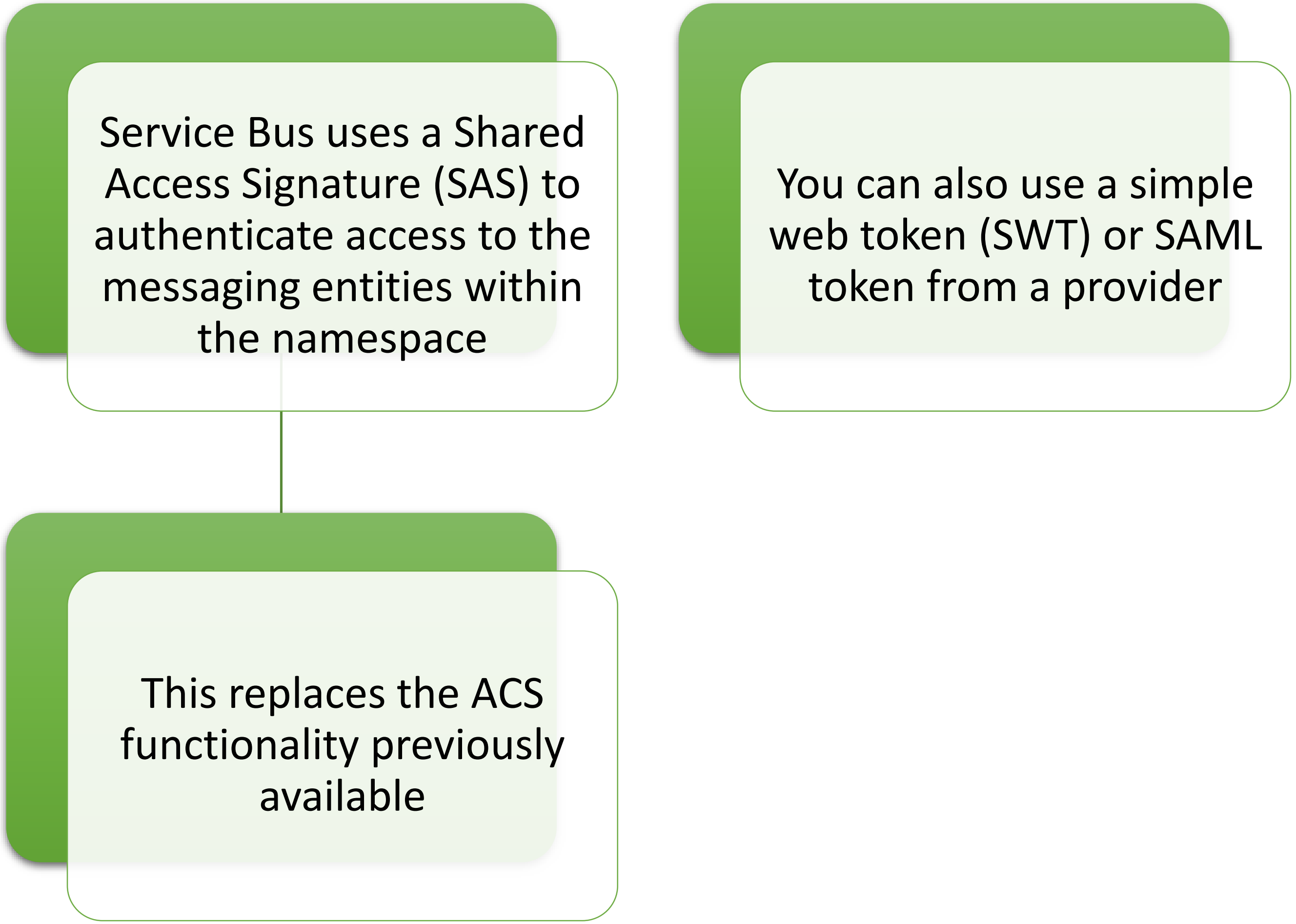
Client Application

Client Application



Service Bus Relay Architecture (cont.)

Management Credentials = how to access



Service Bus uses a Shared Access Signature (SAS) to authenticate access to the messaging entities within the namespace

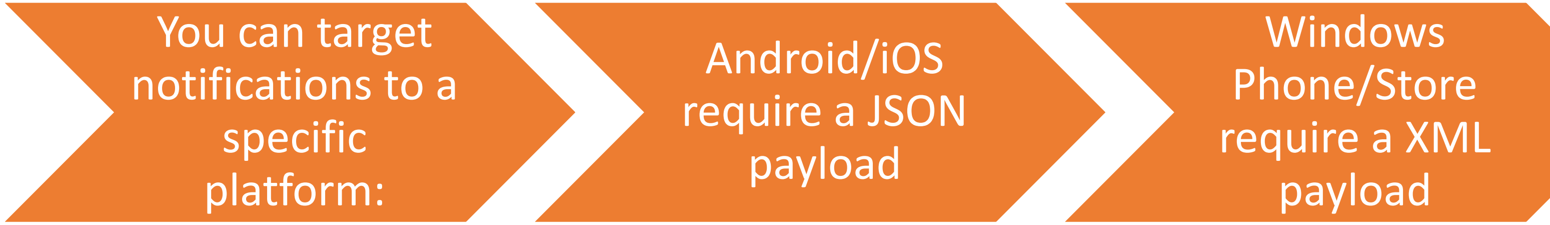
You can also use a simple web token (SWT) or SAML token from a provider

This replaces the ACS functionality previously available

Service Bus Notification Hubs - Overview

- Managed infrastructure for sending push notifications to mobile devices
  - Multiplatform
  - Scalable
  - Simple SDK
    - Available on many major mobile platforms
- Broadcast to many users or target specific users

Target Platforms



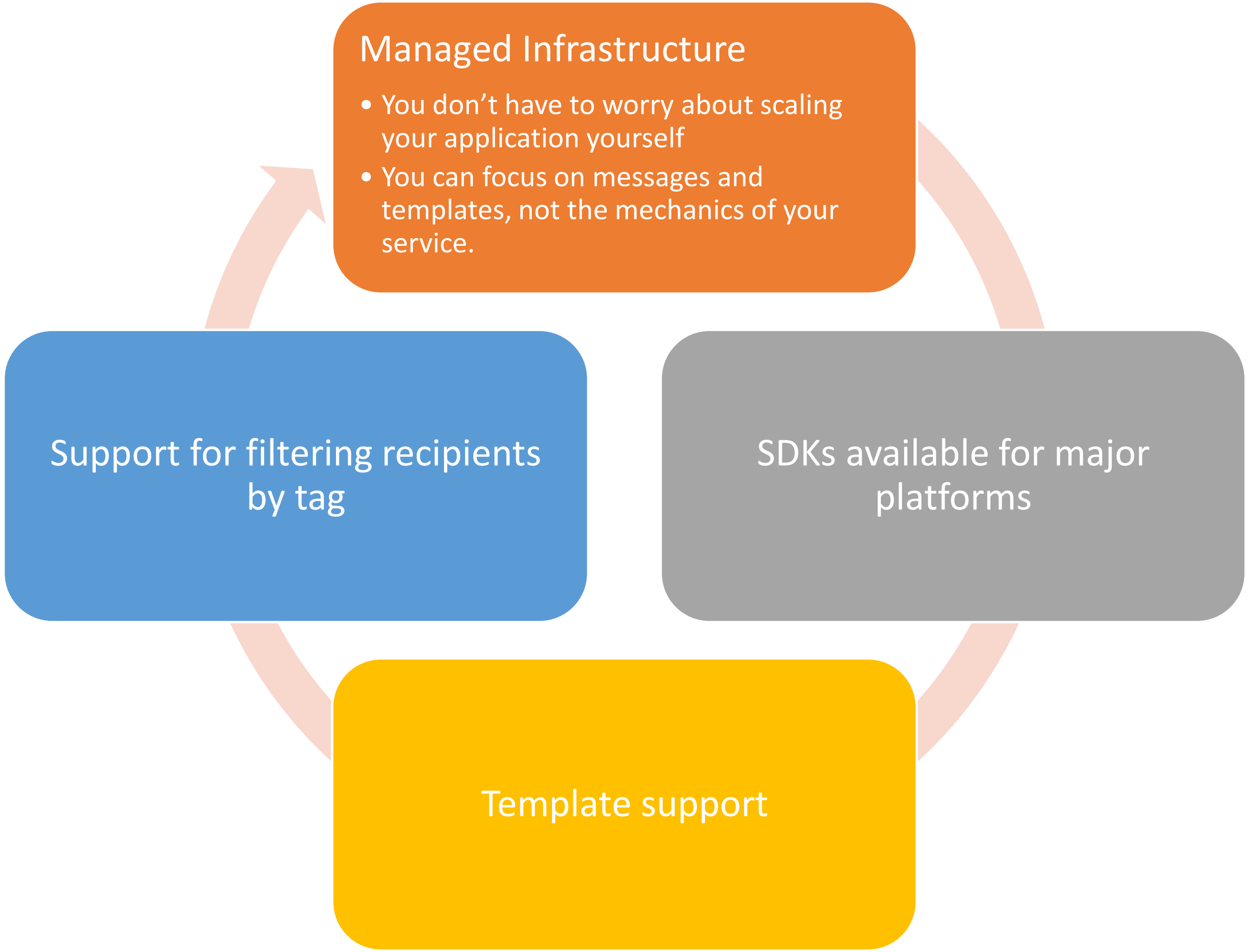
You can target notifications to a specific platform:

Android/iOS require a JSON payload

Windows Phone/Store require a XML payload

- Android
  - GcmService object
- iOS
  - ApnsService object
- Windows Phone
  - MpnsService object
- Windows Store
  - WnsService object

Benefits of using Notification Hubs



Managed Infrastructure

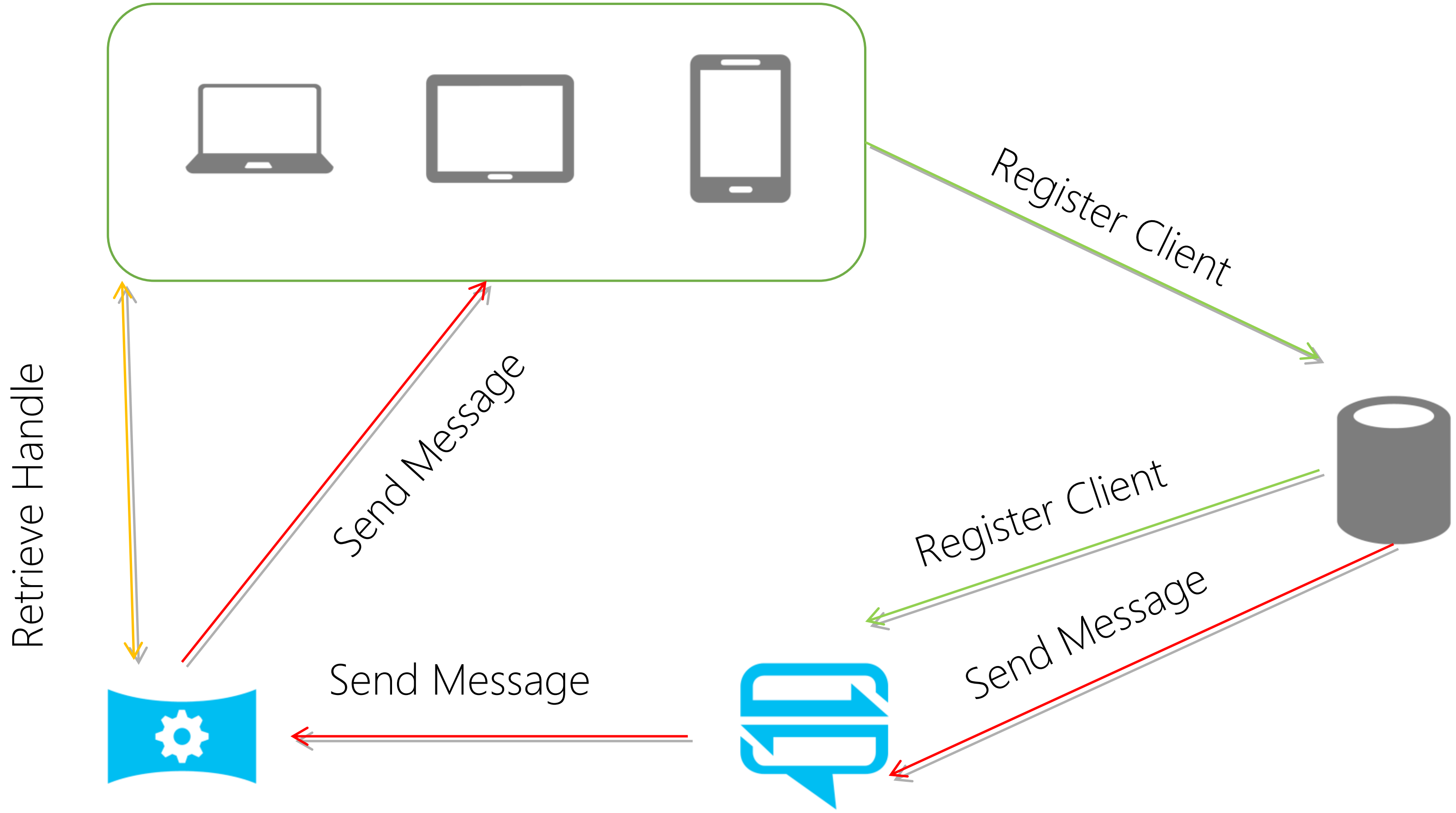
- You don’t have to worry about scaling your application yourself
- You can focus on messages and templates, not the mechanics of your service.

SDKs available for major platforms

Template support

Support for filtering recipients by tag

Notification Hubs Architecture



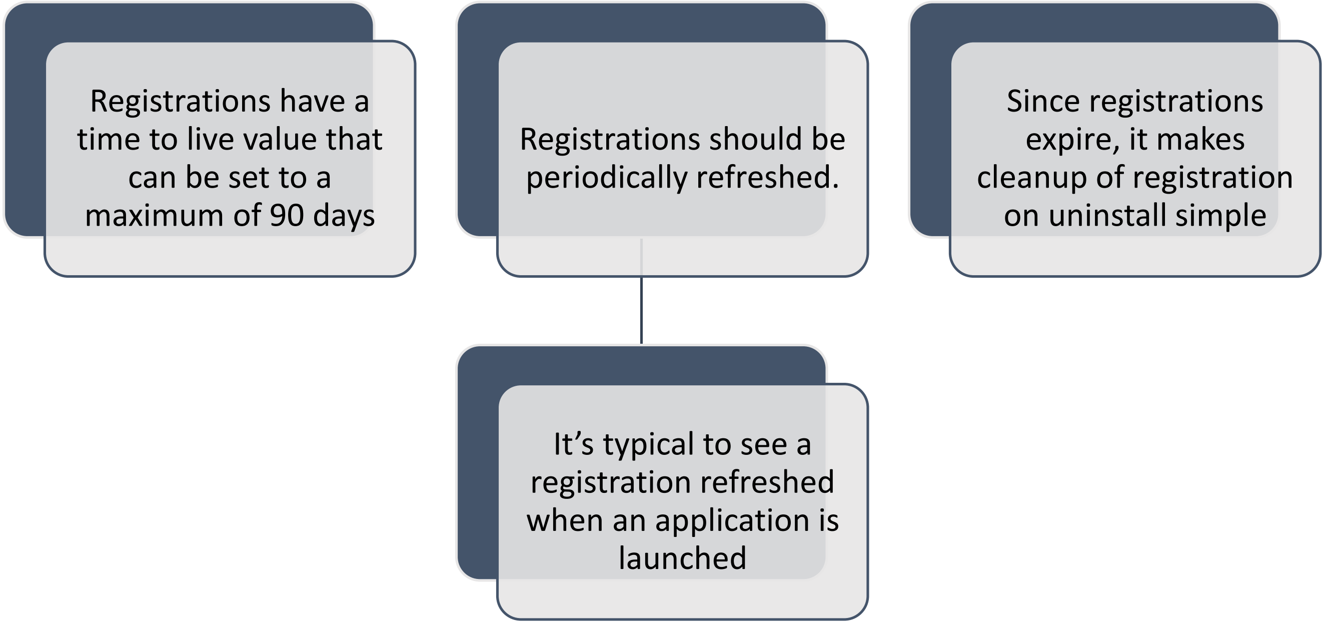
Registrations

- Each SDK provides a unique mechanism to register for remote notifications
- You must register with the Notification Hub using the name of the hub and your unique connection string from the connection information panel
  - Two connection strings are available by default:
    - DefaultFullSharedAccessSignature
    - DefaultListenSharedAccessSignature
  - You can opt to use the DefaultListenSharedAccessSignature as a restricted listen-only connection string for your application

Registering from the Service Application

- Registrations can occur from the application back-end instead of the client app
  - Use NotificationHubClient.CreateClientFromConnectionString to get the hub client.
  - Use the appropriate method on the hub client class
    - CreateWindowsNativeRegistrationAsync
    - CreateAppleNativeRegistrationAsync
  - Use the channelUri, installationId and a unique user names

Transient Registrations



Registrations have a time to live value that can be set to a maximum of 90 days

Registrations should be periodically refreshed.

It’s typical to see a registration refreshed when an application is launched

Since registrations expire, it makes cleanup of registration on uninstall simple

Message Templates and Tags

Templates allow you to send a single message from a back-end and have it transformed into the correctly structured message for each platform

Templates use a binding format where you can specify where the message will appear in the XML or JSON content

Custom properties can be used in the template

Clients can create multiple registrations to leverage different templates

Message Templates and Tags (cont.)

- Tags can be used to uniquely identify a client registration
- When sending messages, tags can be leveraged to target the message to a specific set of devices:
  - Broadcast – send message to all registrations
  - Tag – send message to registrations that contain the specific tag
  - Tag expression – send message to registrations whose set of tags match the specified expression

Identity

Securing Azure Web Applications

Azure Active Directory Overview

01

Managed identity and access management solution in Azure

- Focus on managing your domain, users and applications

02

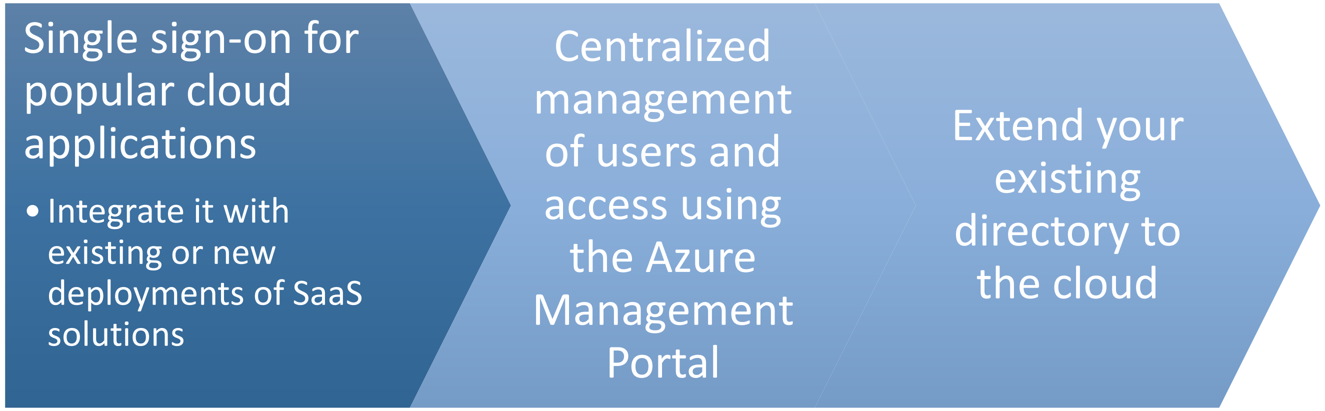
Rich single sign-on solution

03

Supports existing standard protocols such as:

- SAML 2.0
- WS-Federation
- OpenID Connect
- OAuth 2.0

Azure Active Directory Overview (continued)



Single sign-on for popular cloud applications

- Integrate it with existing or new deployments of SaaS solutions

Centralized management of users and access using the Azure Management Portal

Extend your existing directory to the cloud

Azure Active Directory Overview (continued)

- Azure Active Directory Premium
  - Self-Service group management and password reset
  - SSO portal branding
  - Group-based access to SaaS applications
  - Advanced reports and alerts

DEMO:
Azure Active Directory

- Azure Active Directory

Azure AD Services

Directory Services

Multi-Factor Authentication Provider

Managing Directories

You can manage your organization’s tenant data using either of these three tools:

- Microsoft Azure AD Portal
- Microsoft Azure Management Portal
- Office 365 Account Portal

In the Management Portal, you can perform tasks such as:

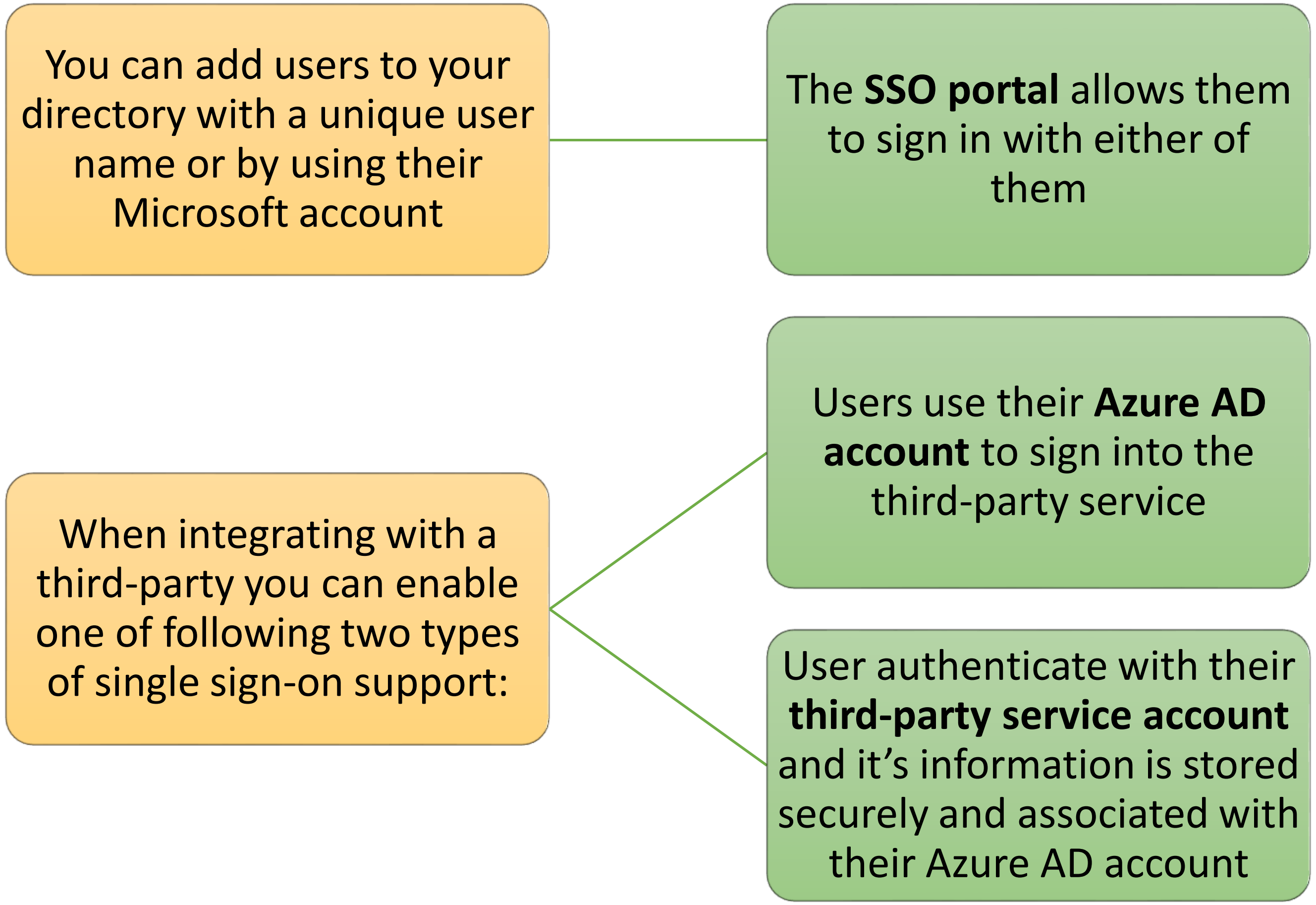
- Create, modify ,and dispose user accounts
- Manage passwords

Managing Directories (cont.)

Options for syncing an existing directory with Azure AD

Whiteboard Session

Directory Users



You can add users to your directory with a unique user name or by using their Microsoft account

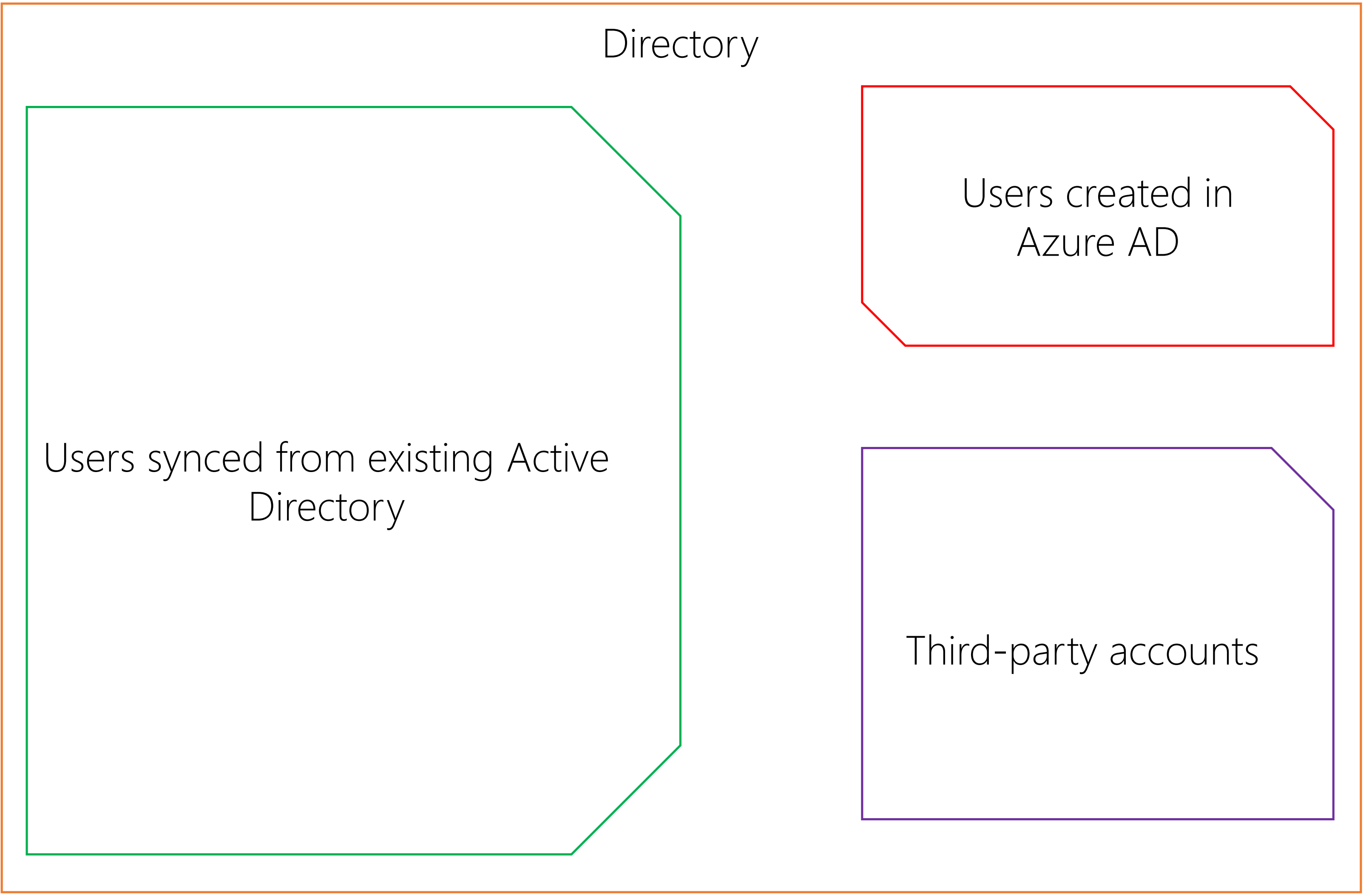
The **SSO portal** allows them to sign in with either of them

When integrating with a third-party you can enable one of following two types of single sign-on support:

Users use their **Azure AD account** to sign into the third-party service

User authenticate with their **third-party service account** and it's information is stored securely and associated with their Azure AD account

Directory Users (cont.)



Directory

Users synced from existing Active Directory

Users created in Azure AD

Third-party accounts

Applications in Azure AD

- Your organization’s application can be integrated to your Azure AD instance to support the following features:
  - Single Sign-On (SSO) for your organizational users to have immediate access to the application without extra credentials
  - User Provisioning so your application’s accounts can be synced with your organization’s accounts.
  - Access Panel for your users to be able to discover your SSO supported applications.

DEMO:
Azure Active Directory

- Azure Active Directory Application Integration

Azure AD Graph

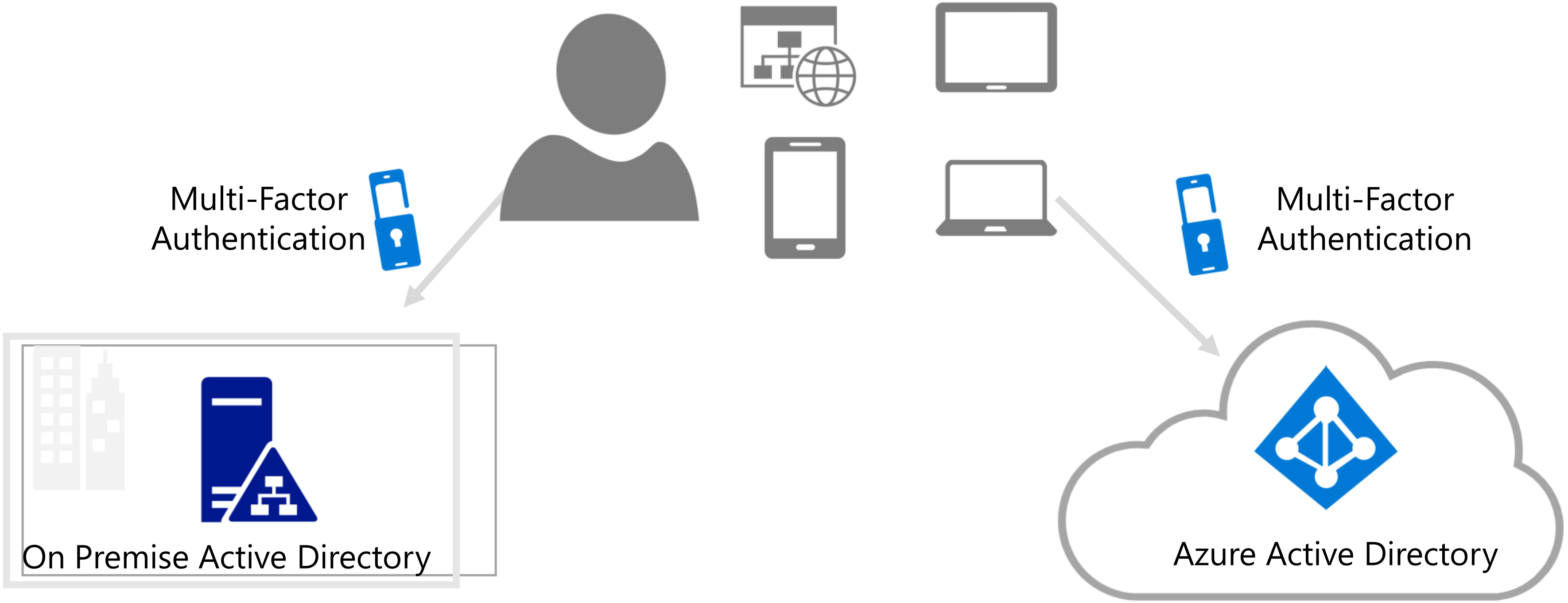
- Azure AD Graph provides programmatic access to your directory through REST API endpoints
  - Perform CRUD operations on Azure AD objects:
    - Users
    - Groups
  - Alternative to ADSI or ADO.NET libraries for accessing AD on premise
- The Azure AD Graph API allows you to extend the existing objects with custom properties that may be necessary for your Line of Business (LOB) application

DEMO: Azure Active Directory

- Azure Active Directory Graph API

Multi-Factor Authentication

- Azure Multi-Factor Authentication is an extra layer of authentication along with your credentials.
  - Multi-Factor Authentication can be used for both on-premises applications and cloud applications


Multi-Factor Authentication
Multi-Factor Authentication
On Premise Active Directory
Azure Active Directory

Multi-Factor Authentication Providers

- There are three authentication options available:
  - Multi-Factor Authentication apps
    - Target Windows Phone, Android, and iOS
    - Apps can send a notification to the end user and the user can then authenticate or deny a request to login
    - Apps can also provide a one-time passcode that must be used with the user name and password for each login attempt
  - Automated phone calls
  - Text messages

DEMO: Azure Active Directory

- Azure Active Directory MFA in action

Collaborate with partners: B2B collaboration

Share without complex configuration or duplicate users

- Partners use their own credentials to access your org
- Users lose access when leaving the partner org
- No external directories
- No per partner federation

You manage access

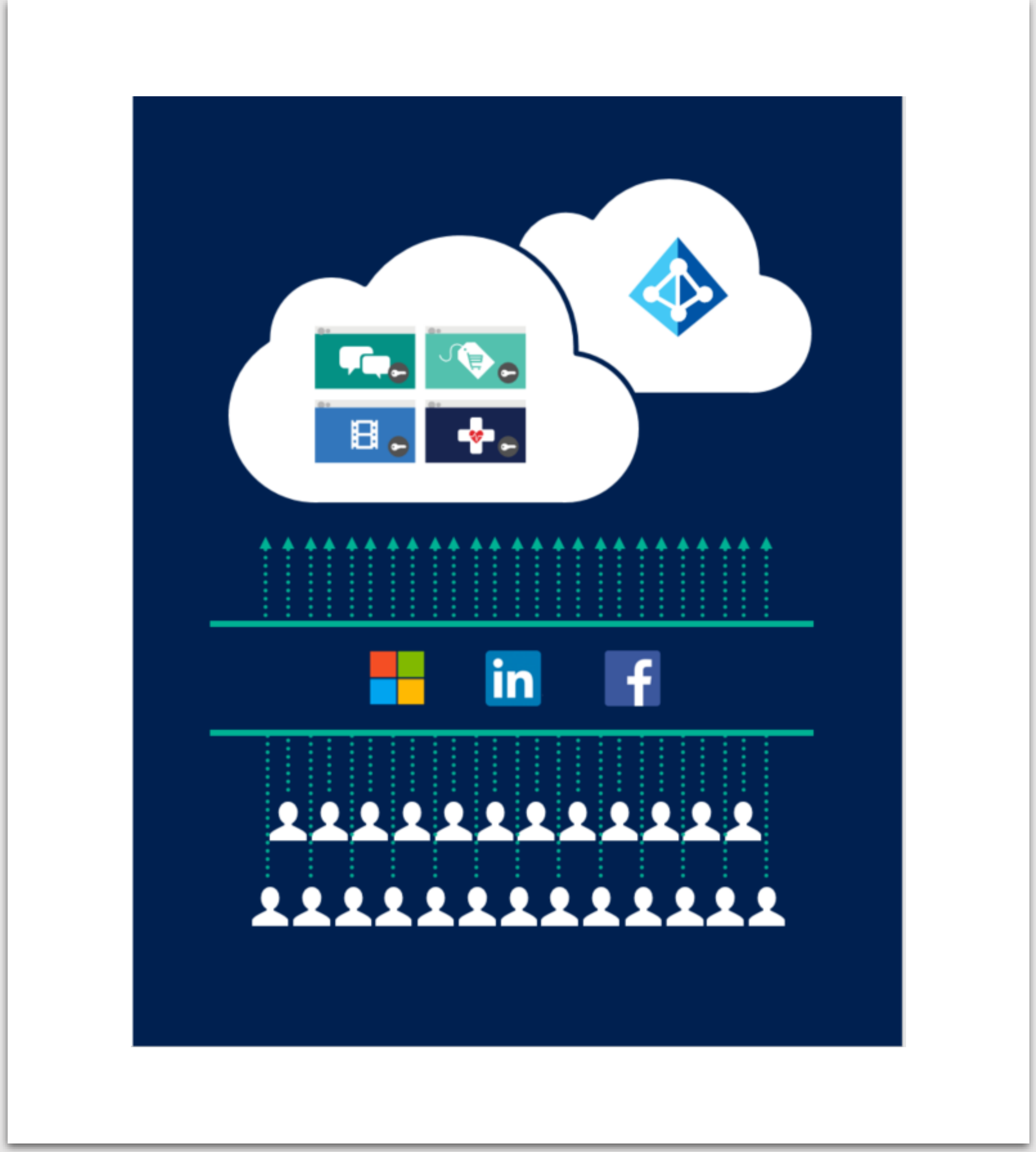
- You control partner access in your directory:
- app assignment
- group membership
- custom attributes

Partners of all sizes

- Bulk invite 1000s at a time
- Partners with Azure Active Directory sign in to accept invite
- Other partners simply sign up to accept invite

Connecting with consumers: Azure Active Directory B2C

- Consumer identity and access management in the cloud
  - Cross-platform
  - Identity management for consumers
  - Superior economics
  - Identity experience engine



DEMO: Azure Active Directory

- Azure Active Directory B2B / B2C

Secret management asks from our customers

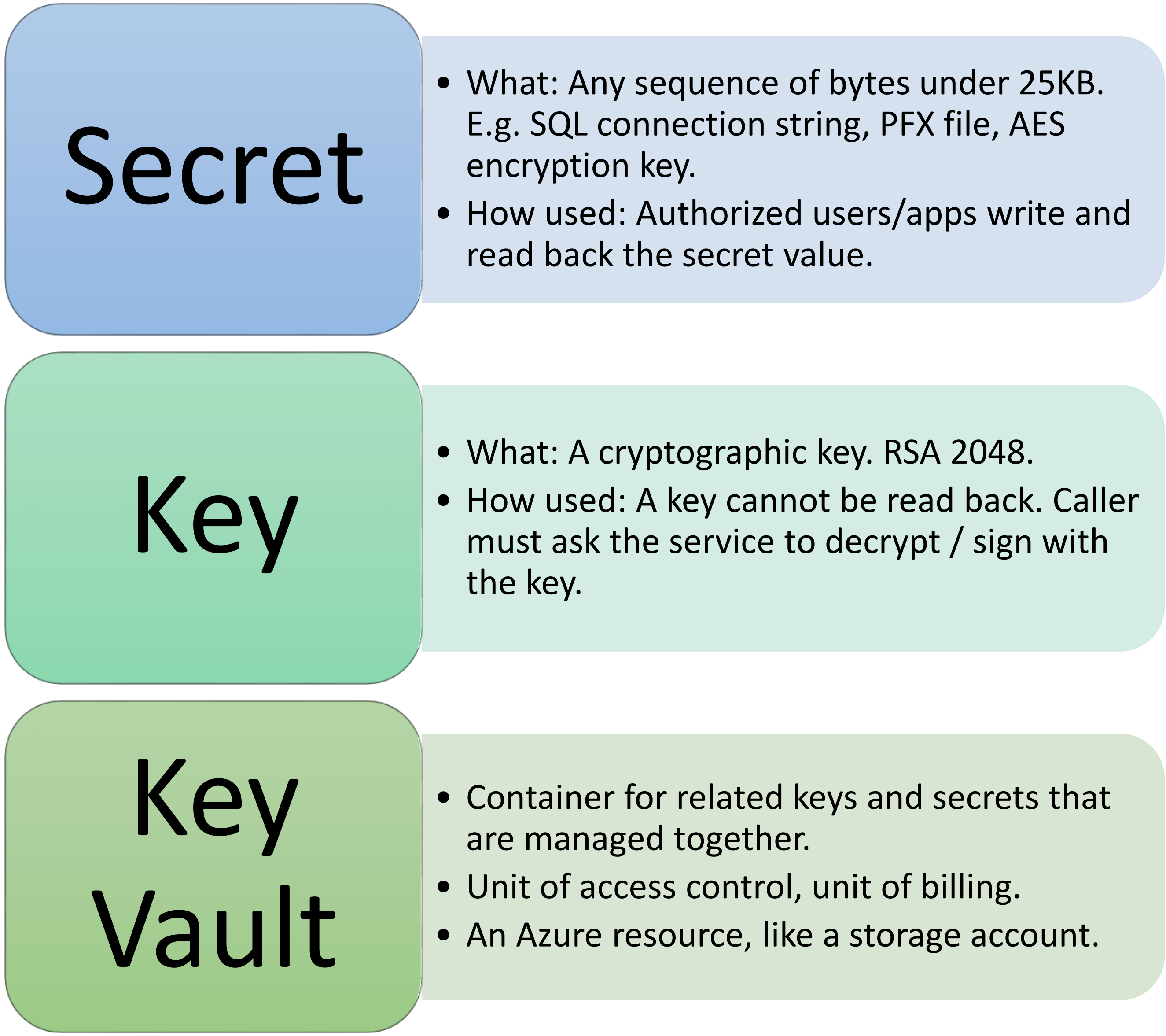
- “My app on Azure has passwords and cryptographic keys…”
- “I need a safe place to save these in Azure.”
- “I need to (re)use AD users and groups to manage access to secrets.”
- “I do NOT want to be in the news for a silly mistake”

Solution: Azure Key Vault

Your ORG is in control via Active Directory

- Users and apps authenticate to your key vaults using your organization’s Azure AD
- Benefits for organizations:
  - Organizations can centrally revoke access to ALL key vaults in their organization.
  - If a user leaves, they instantly lose access to ALL key vaults in the organization.
  - Organizations can customize authentication via the options in Azure AD.

Azure Key Vault Components



Secret

- What: Any sequence of bytes under 25KB. E.g. SQL connection string, PFX file, AES encryption key.
- How used: Authorized users/apps write and read back the secret value.

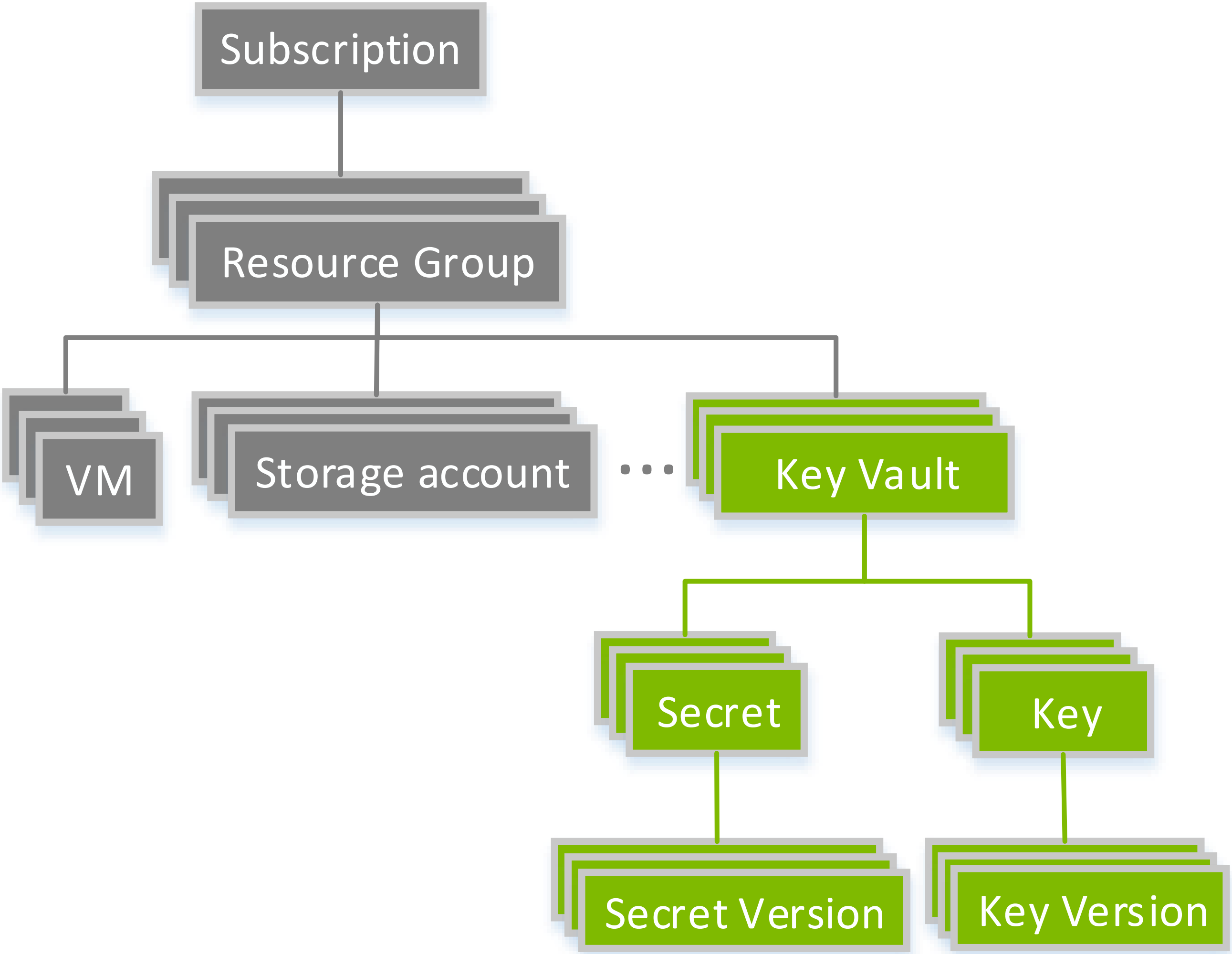
Key

- What: A cryptographic key. RSA 2048.
- How used: A key cannot be read back. Caller must ask the service to decrypt / sign with the key.

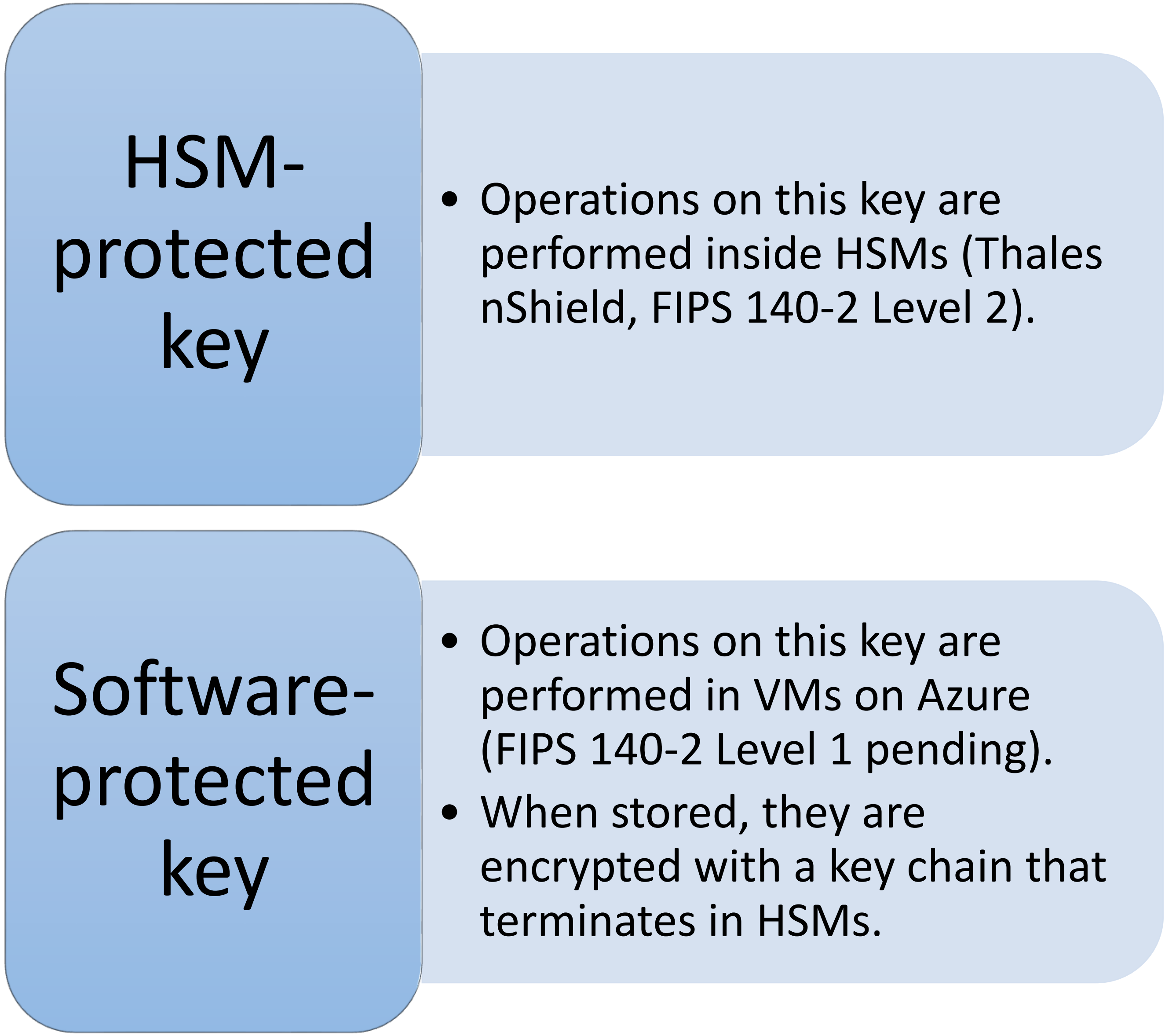
Key Vault

- Container for related keys and secrets that are managed together.
- Unit of access control, unit of billing.
- An Azure resource, like a storage account.

Azure Key Vault Object Model



Types of Keys Supported



HSM-protected key

- Operations on this key are performed inside HSMs (Thales nShield, FIPS 140-2 Level 2).

Software-protected key

- Operations on this key are performed in VMs on Azure (FIPS 140-2 Level 1 pending).
- When stored, they are encrypted with a key chain that terminates in HSMs.

Authorization into Azure Key Vault

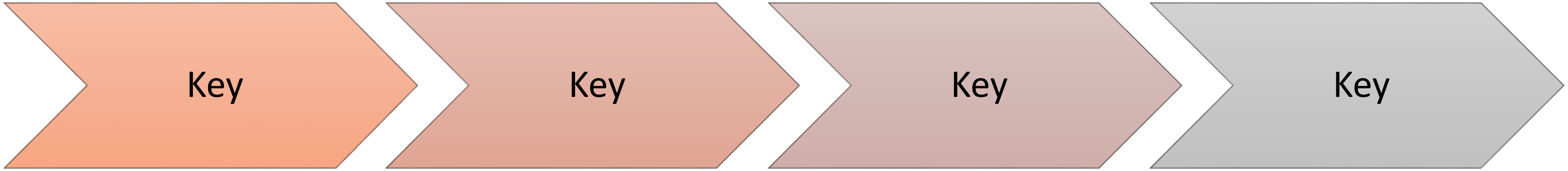
Offline

- Key Vault owner sets ACL on key vault that specifies WHO can do WHICH operations.
- Each entry is the pair : {Azure AD identity, operations}.
- Key Operations: Create Key, Import Key, Delete Key, Encrypt, Decrypt, Wrap, Unwrap, Backup, Restore.
- Secret Operations: Get, Set, Delete, List.

At runtime

- Key Vault service checks caller’s Azure AD token against permissions on the key vault, before performing operation.

Why Azure Key Vault?



Key

- Key Vault enables you to stay in control your keys and secrets.
  - Anchored to your Active Directory
  - Protected by HSMs

Key

- Key Vault does this while retaining “cloud expectations”
  - Quick to deploy and scale.
  - Pay only for what you use.
  - Scales with your cloud app.

Key

- Key Vault enables segregation of duty between managing keys and managing apps/data.

Key

- Key Vault makes it easy to move your application from development to pilot to production.

DEMO: Azure Key Vault

- Azure Key Vault

Student Reference

https://tinyurl.com/532S03Idnt