# Securing Service Bus Entities

**Alan Smith**
Active Solution

youtube.com/user/CloudCasts

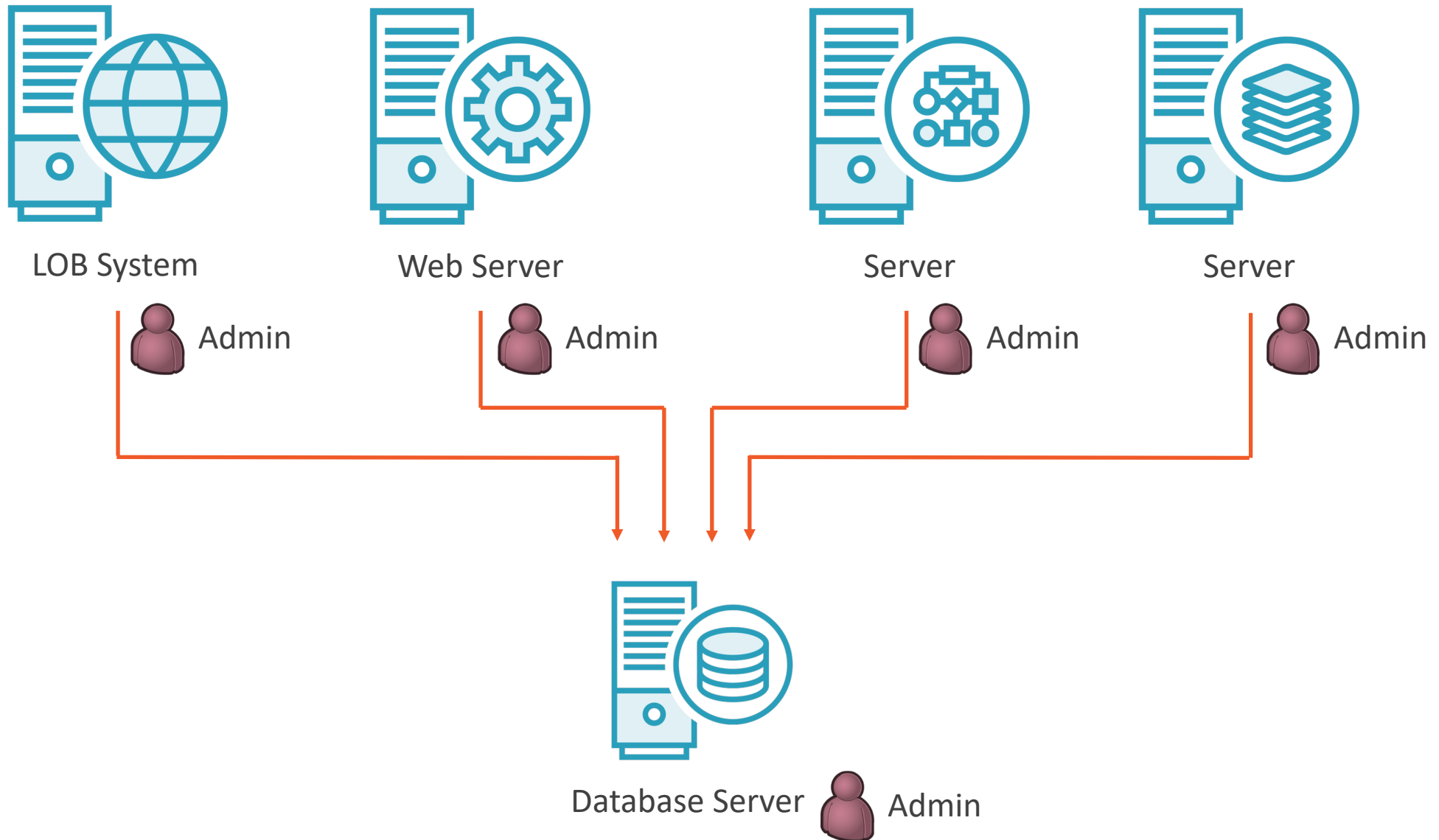# Overview

**Security Requirements**

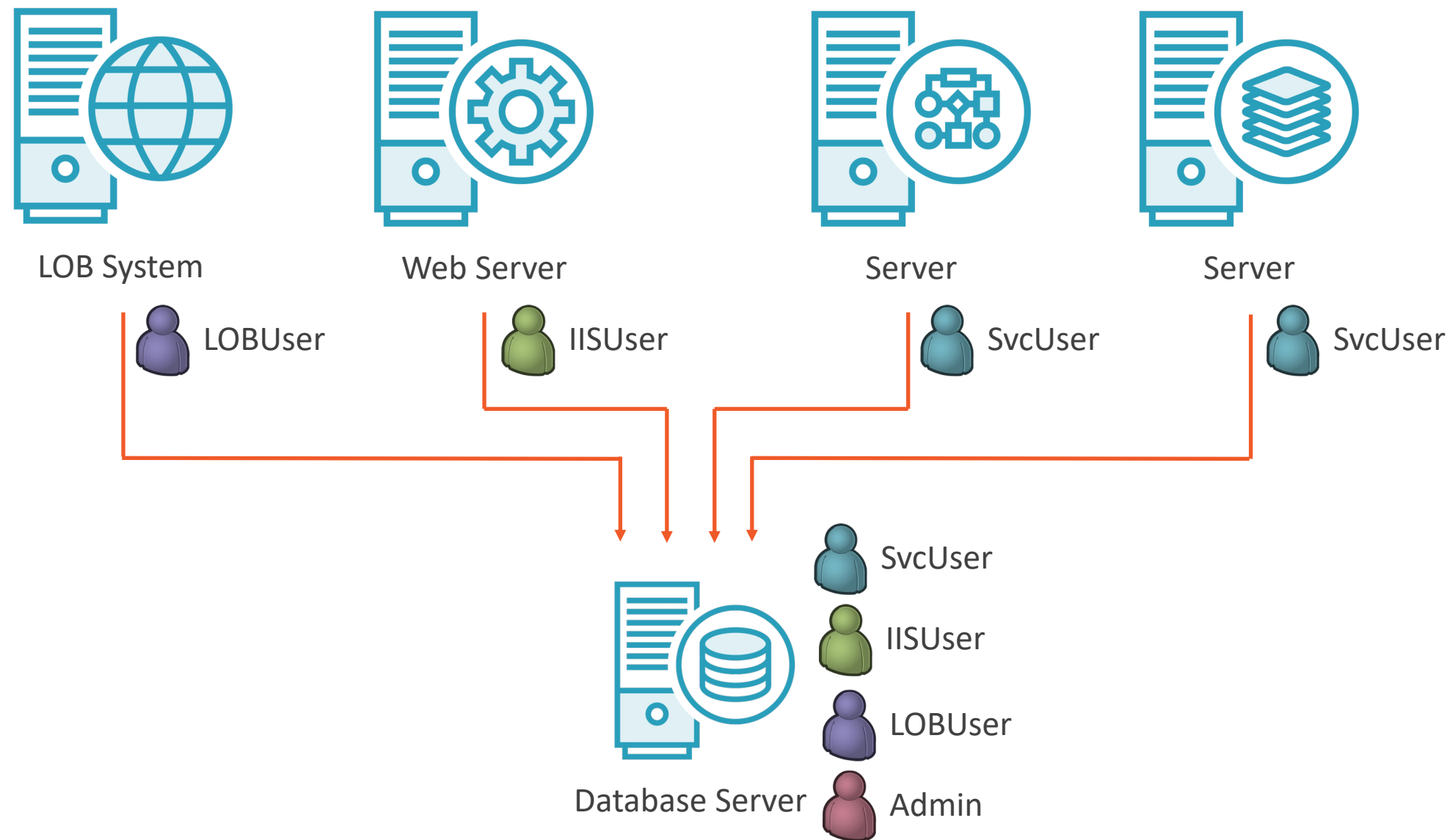**Working with Shared Access Signatures**

**Demo: Securing Service Bus Artifacts using Shared Access Signatures**
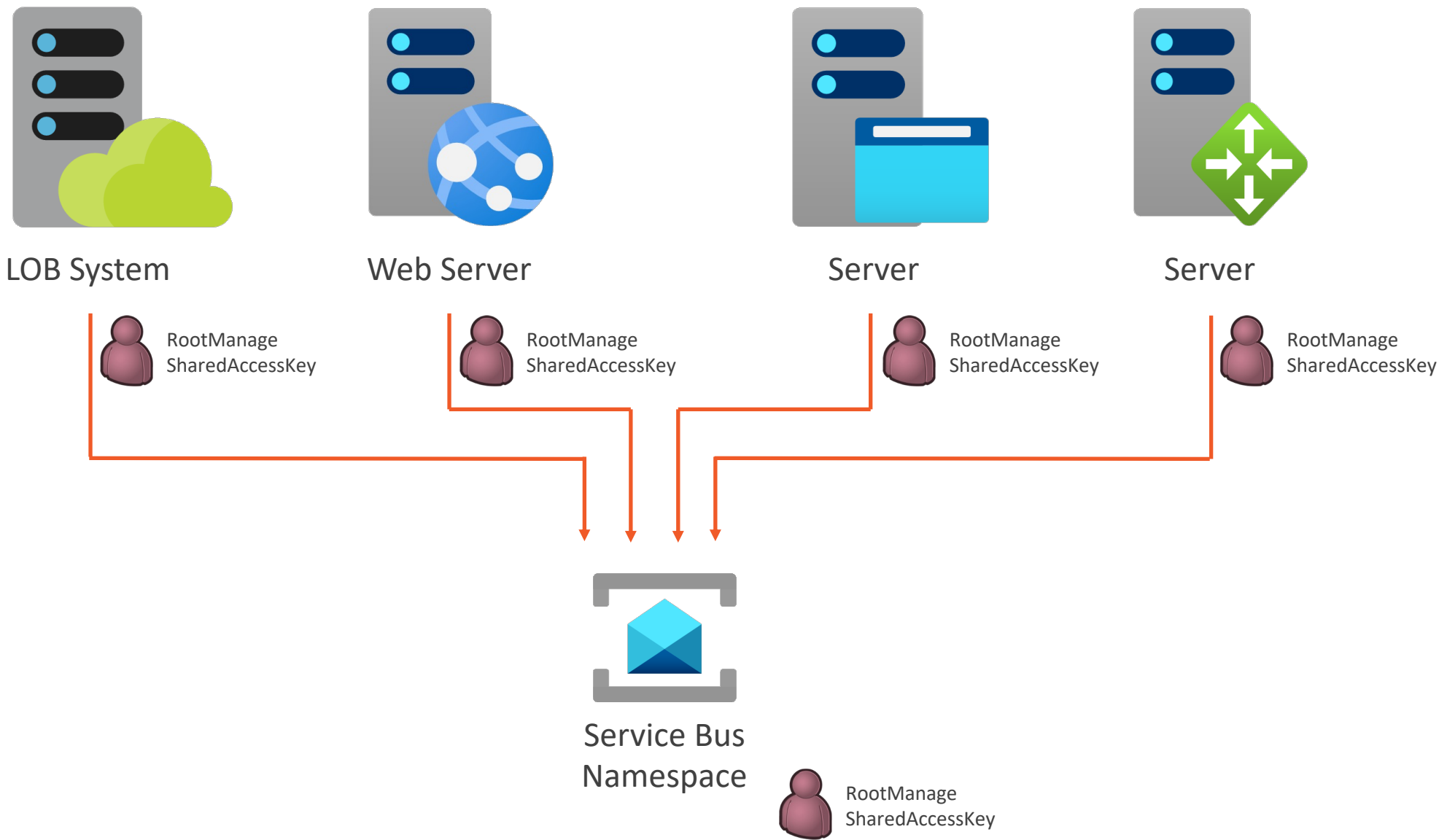
# Security Requirements
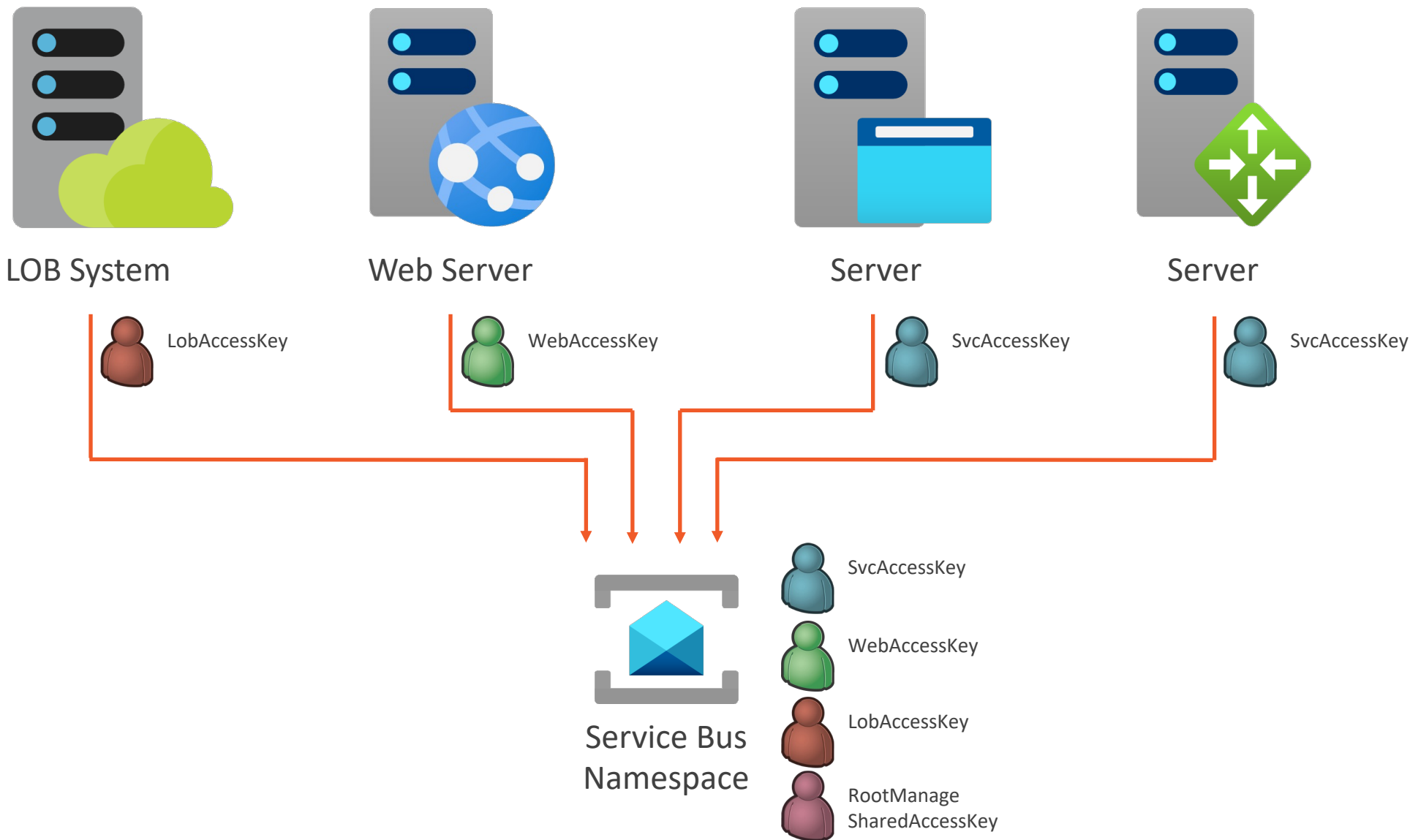
# Database Security

# Database Security

# Azure Service Bus

# Azure Service Bus

# Working with Shared Access Signatures

# Shared Access Signatures (SAS)

- Provides delegated and granular access to resources

# Shared Access Signatures (SAS)

- Provides delegated and granular access to resources

- Credentials to authenticate with Service Bus namespaces and entities
  - Policy name
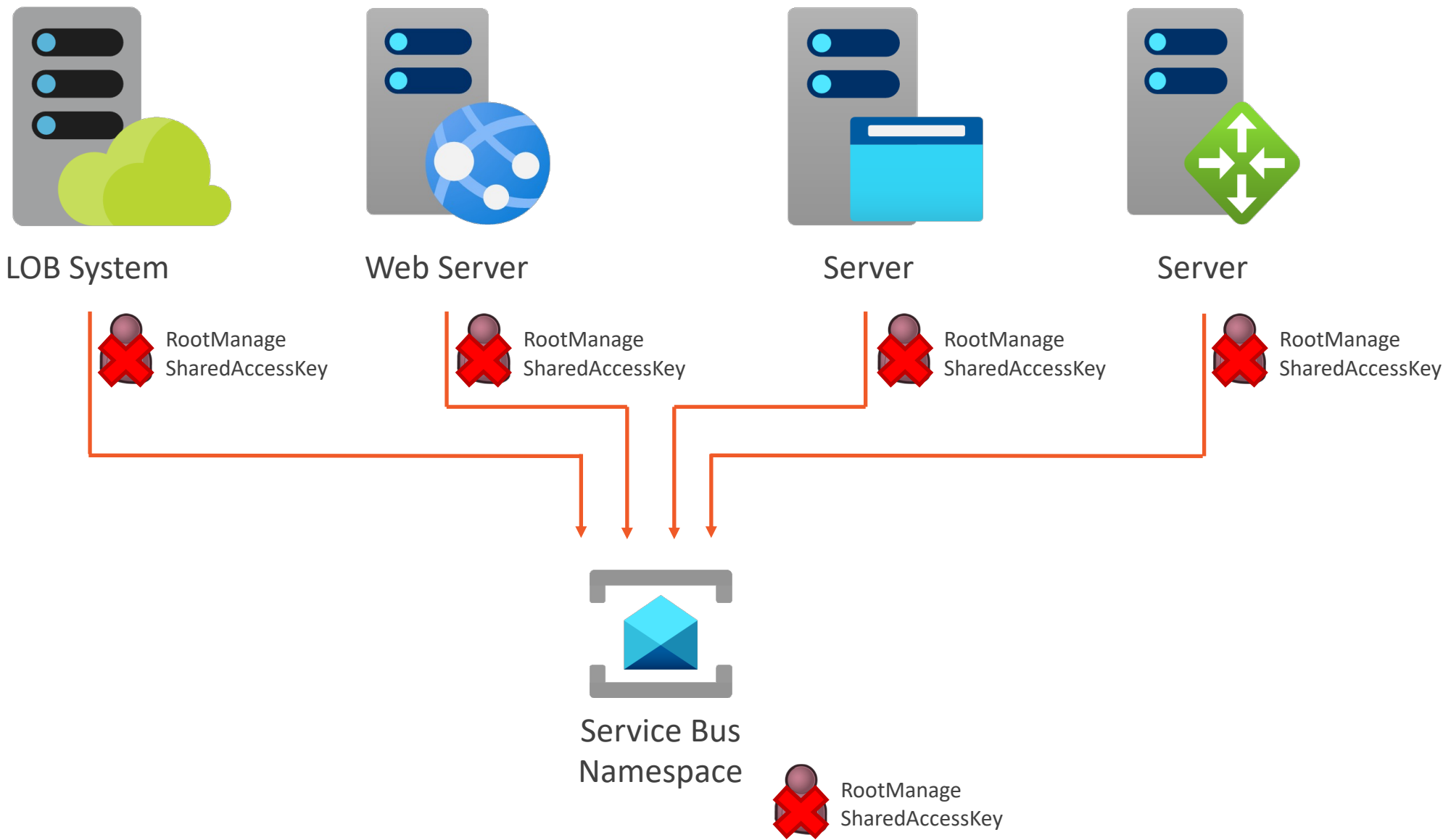  - Primary key
  - Secondary key

# Shared Access Signatures (SAS)

- Provides delegated and granular access to resources

- Credentials to authenticate with Service Bus namespaces and entities
  - Policy name
  - Primary key
  - Secondary key

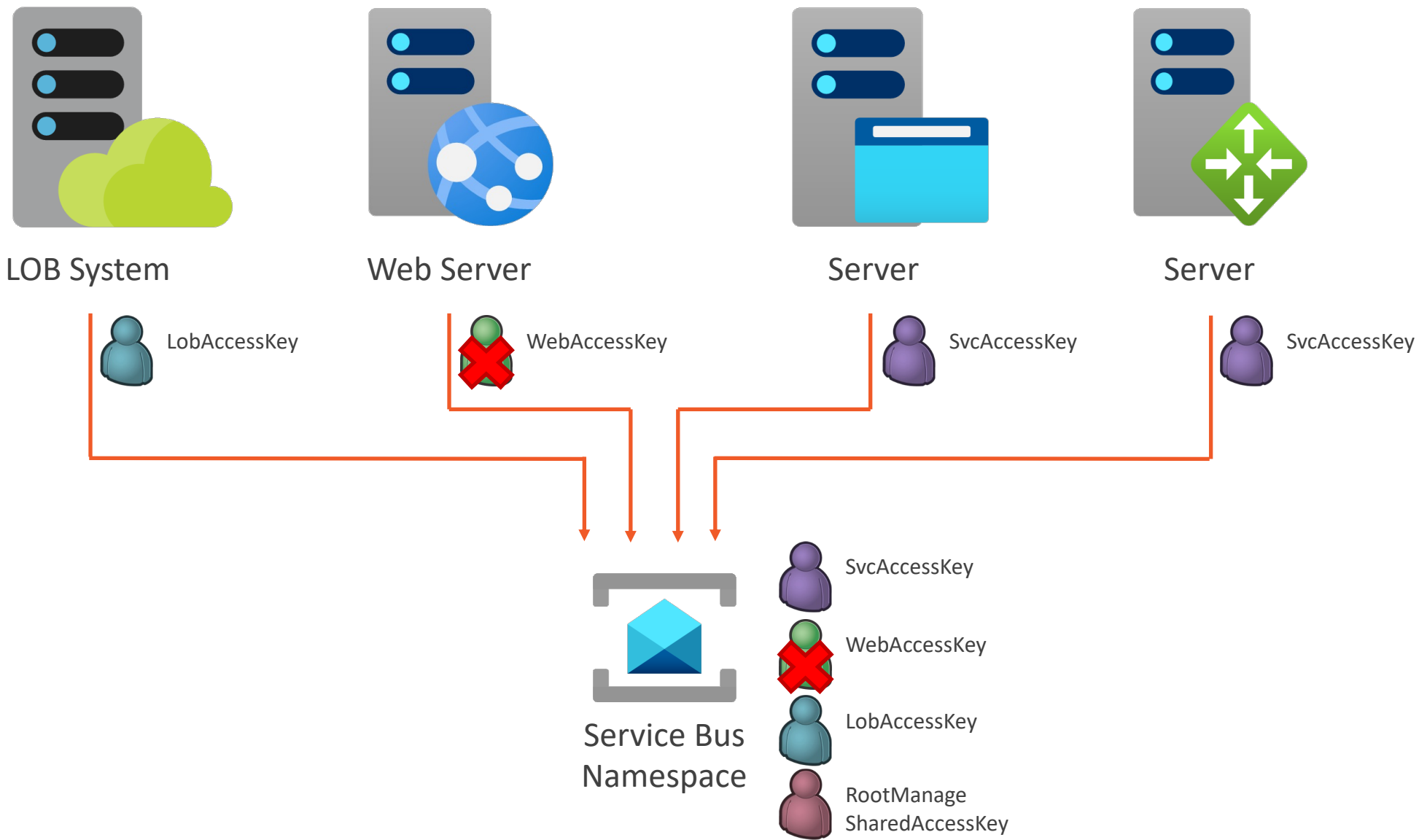- Credentials can be assigned to namespaces, queues, topics and subscriptions

# Service Bus Claims

| Claim | Brokered Messaging |
|-------|-------------------|
| Manage | Manage artifacts |
| Send | Send messages to queues and topics |
| Listen | Receive messages from queues and subscriptions |

# Azure Service Bus



LOB System

Web Server

Server

Server

RootManage
SharedAccessKey

RootManage
SharedAccessKey

RootManage
SharedAccessKey

RootManage
SharedAccessKey

Service Bus
Namespace

RootManage
SharedAccessKey

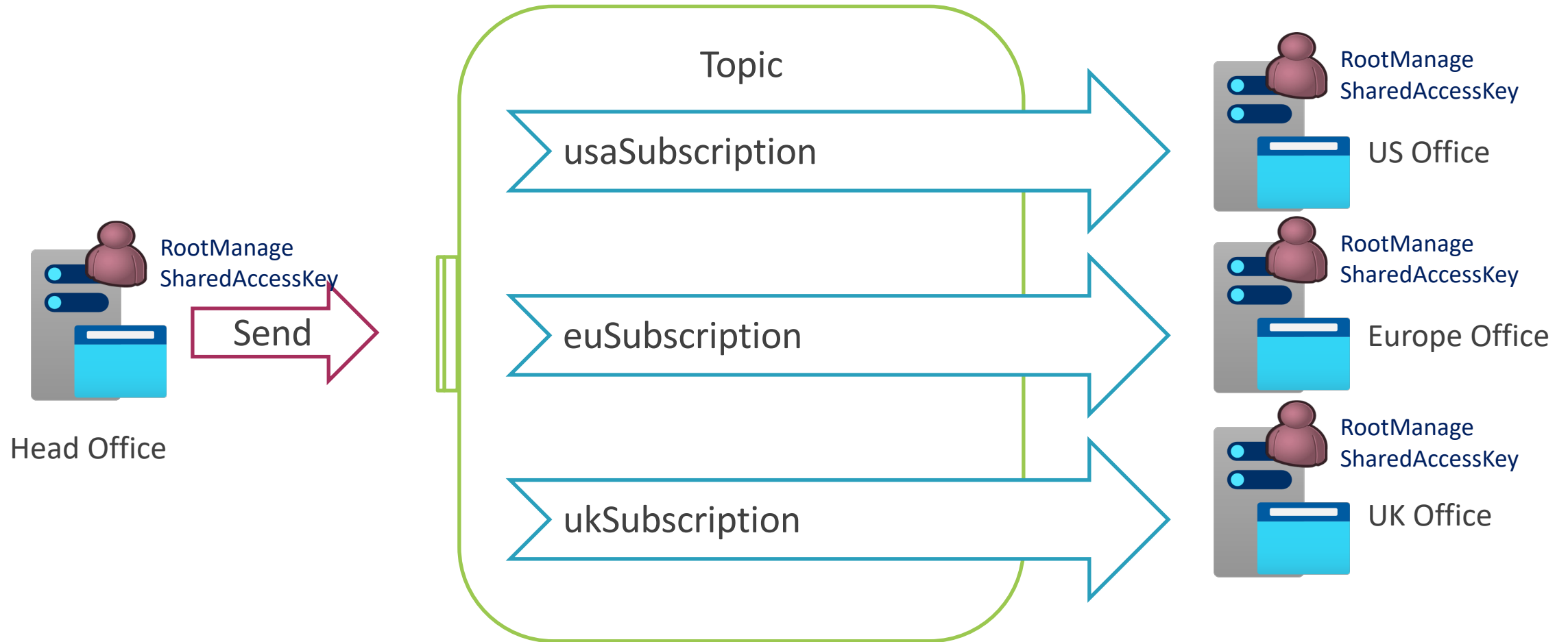# Azure Service Bus

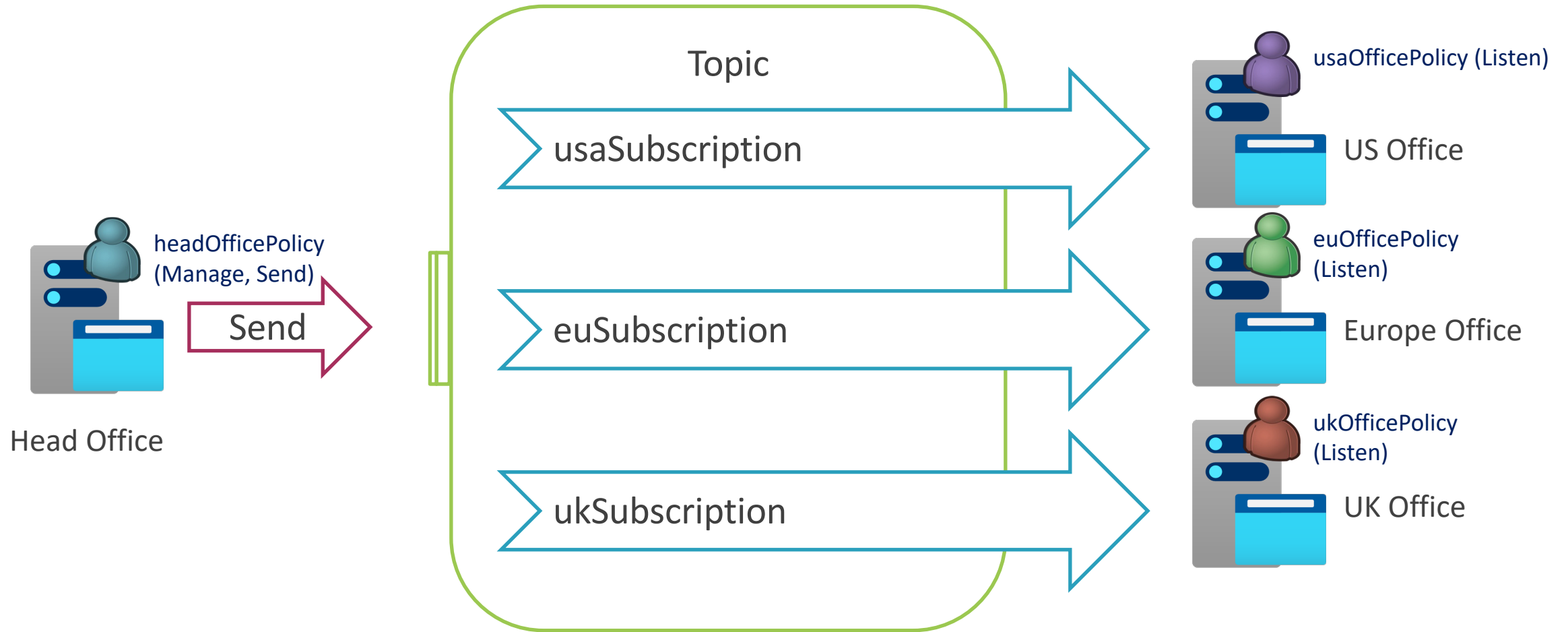# Shared Access Signatures (SAS)

# Demo

**Demo: Securing Service Bus Artifacts using Shared Access Signatures**

- Using RootManageSharedAccessKey

- Regenerating keys

- Creating shared access signatures

- Using shared access signatures

# Demo Scenario

# Demo Scenario

# Summary

Shared Access Signatures (SAS) are used for authentication in the service bus

The RootManageSharedAccessKey SAS is created with the service bus namespace

Has Manage, Send and Listen credentials on the service bus namespace

Controlling granular access on the service bus is similar to a database server

Create identities

Grant access

Issue credentials to applications

Using RootManageSharedAccessKey should be avoided in production applications