Microsoft

Reactor

STOCKHOLM

This session will commence shortly

We are constantly striving to create excellent content
and would appreciate if you could take this brief survey.

Survey Link: https://aka.ms/Reactor/Survey

Please enter the event code 12454 at the start of survey

Speaker Slide:

Massimo Bonanni

Azure Technical Trainer @ Microsoft

I spend my time to help customers to empower their Azure skills to achieve more and leverage the power of Azure in their solutions.
I'm also a technical speaker both for local and international events and a user-group guy.
I founded Aa couple of communities in Italy and collaborated with most of the Italian communities.
Finally, I is also passionate about biking, reading, and dogs!!

Secrets safe with Azure KeyVault

Massimo Bonanni

Azure Technical Trainer @ Microsoft

meetup.com/Microsoft-Reactor-Stockholm/

https://www.businessinsider.com/hawaii-emergency-agency-password-discovered-in-photo-sparks-security-criticism-2018-1?IR=T

Azure Key Vault is a service that enables you to store & manage cryptographic keys and secrets in one central secure vault!!

What Devs and IT Pros thinks!!

I want customers to **own and manage** their keys so that I can concentrate on doing what I do best, which is providing the core software features.

I don't want the **responsibility** or potential liability for my customers' tenant keys and secrets.

I want to make sure that my organization **is in control** of the key lifecycle and can monitor key usage.

I want to write an application for Azure that uses keys for **signing** and **encryption**. But I want these keys to be **external** from my application.

Azure KeyVault key features

Secrets Management

Azure Key Vault can be used to Securely store and tightly control access to tokens, passwords, certificates, API keys, and other secrets

Key Management

Azure Key Vault can also be used as a Key Management solution. Azure Key Vault makes it easy to create and control the encryption keys used to encrypt your data.

Certificate Management

Azure Key Vault lets you easily provision, manage, and deploy public and private Transport Layer Security/Secure Sockets Layer (TLS/SSL) certificates.

Store secrets backed by Hardware Security Modules

The secrets and keys can be protected either by software or FIPS 140-2 Level 2 validated HSMs

Azure KeyVault roles

Vault Owner

Can create a key vault and gain full access and control over it.

Can set up auditing to log who accesses secrets and keys.

Can control the key lifecycle.

Use RBAC for permissions.

Vault Consumer

A vault consumer can perform actions on the assets inside the key vault when the vault owner grants the consumer access.

The available actions depend on the permissions granted.

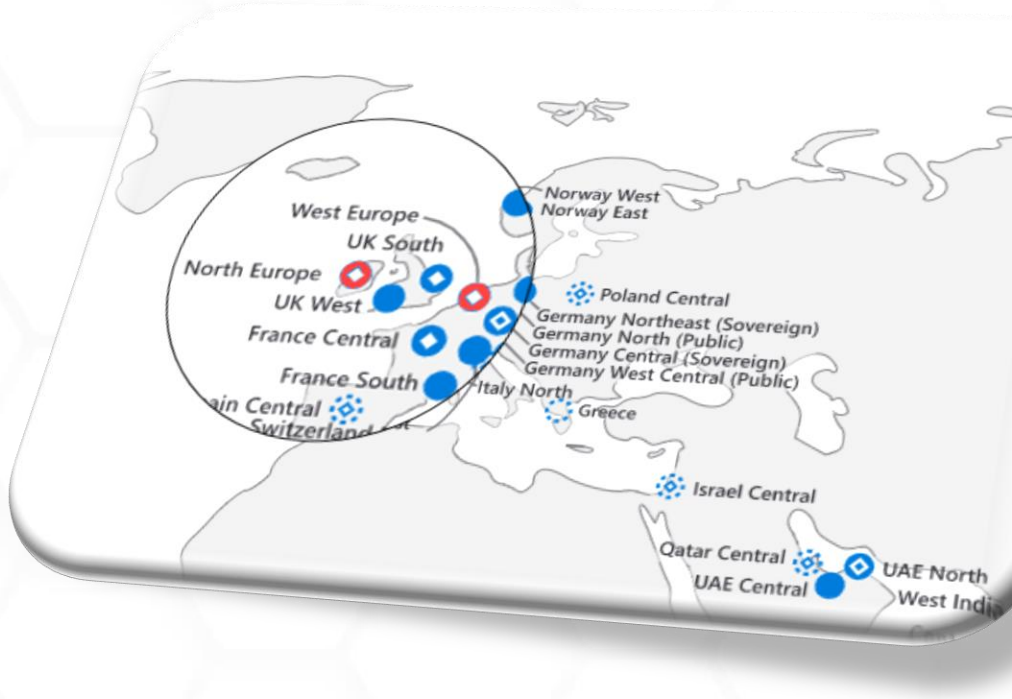
Use KeyVault Access Policy or RBAC (preview) for permissions.

Availability and redundancy

The contents of key vault are replicated within the region and to a pair region.

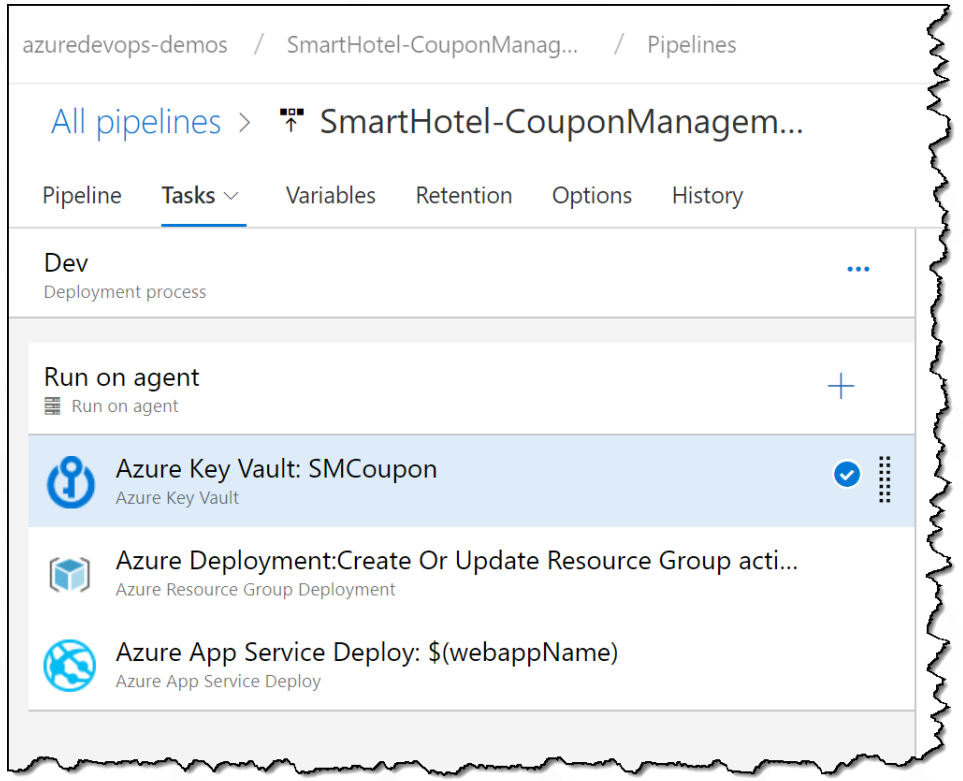
When the region is unavailable, the requests are automatically routed (***failed over***) to a secondary region (read only).

When the primary region is available again, requests are routed back (***failed back***) to the primary region.



Platform Integration

- Azure Disk Encryption
- Trasparent Data Encryption Azure SQL Database
- Azure App Service
- Storage Account
- ARM Template
- Azure DevOps pipelines
- …



How much?

Two different plans: Standard and Premium

Flat rate for transactions

Pay for renewal of certificates

Pay for HSM-protected keys

Photo by Markus Spiske on Unsplash

Platform Integration:

Storage Service Encryption & ARM Templates

AppService Integration

AppService Integration

Define Service Principal for AppService → Granting app access to KeyVault → Use secrets in your App

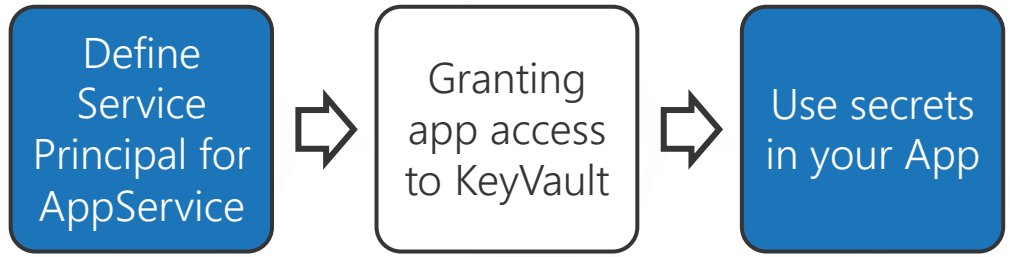
App Registration

- Registering your application establishes a trust relationship between your app and the Microsoft identity platform.
- The trust is unidirectional: your app trusts the Microsoft identity platform, and not the other way around.
- An App registration generates an ApplicationId and an ObjectId (Service Principal Id)

Managed Identity

- Managed identities eliminate the need for developers having to manage credentials by providing an identity for the Azure resource in Azure AD.
- You don't need to manage credentials. Credentials are not even accessible to you.
- You can use managed identities to authenticate to any Azure service that supports Azure AD authentication including Azure Key Vault.

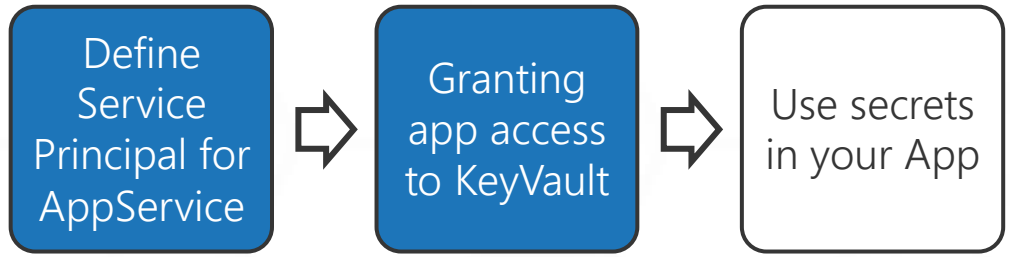
AppService Integration



- Key Vault access policies grant permissions separately to keys, secrets, or certificate.
- Access permissions for keys, secrets, and certificates are managed at the vault level.
- Key Vault access policies don't support granular, object-level permissions like a specific key, secret, or certificate.
- You can use KeyVault Access policies or RBAC (now in preview)

AppService Integration

No-code integration



Key Vault references can be used as values for Application Settings, allowing you to keep secrets in Key Vault instead of the site config.

Set the reference as the value of the setting:

```
@Microsoft.KeyVault(SecretUri=https://myvault.vault.azure.net/……f109c51a1f14cdb1931)
```

Your app can reference the secret through its key as normal. No code changes are required.

AppService Integration

Configuration Provider (ASP.NET Core)

Define Service Principal for AppService → Granting app access to KeyVault → Use secrets in your App

```
Install-Package Microsoft.Extensions.Configuration.AzureKeyVault
```

Configure the KeyVault Configuration Provider during the application startup:

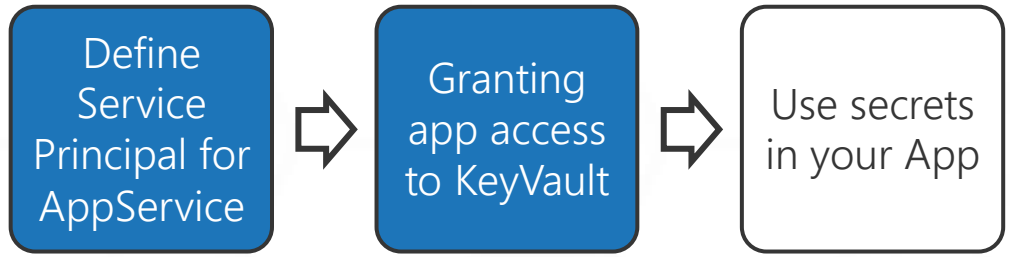
```
public static IHostBuilder CreateHostBuilder(string[] args) =>
    Host.CreateDefaultBuilder(args)
        .ConfigureAppConfiguration((context, config) =>
        {
            if (context.HostingEnvironment.IsProduction())
            {
                var builtConfig = config.Build();

                var azureServiceTokenProvider = new AzureServiceTokenProvider();
                var keyVaultClient = new KeyVaultClient(
                    new KeyVaultClient.AuthenticationCallback(
                        azureServiceTokenProvider.KeyVaultTokenCallback));

                config.AddAzureKeyVault(
                    $"https://myvault.vault.azure.net/",
                    keyVaultClient,
                    new DefaultKeyVaultSecretManager());
            }
        }).ConfigureWebHostDefaults(webBuilder =>
        {
```

AppService Integration

KeyVaultClient




```
Install-Package Azure.Security.KeyVault.Keys
```

Use the KeyVaultClient to manage the secrets

```
AzureServiceTokenProvider azureServiceTokenProvider = new AzureServiceTokenProvider();

KeyVaultClient keyVaultClient =
    new KeyVaultClient(
        new KeyVaultClient.AuthenticationCallback(azureServiceTokenProvider.KeyVaultTokenCallback));

var secret = await keyVaultClient
    .GetSecretAsync("https://myvault.vault.azure.net/secrets/DBConnectionString");
```

Platform Integration:

AppService Configuration & AzureKeyVault SDK

Takeaway


Encrypt your data
101
101
0101
0101
Platform integration
Simplifies administration
Audit your apps
Keep your secrets safe

Companies spend millions of dollars on firewalls and secure access devices, and it's money wasted because none of these measures address the weakest link in the security chain: the people who use, administer and operate computer systems!

Kevin Mitnic

Thanks for your attention!!!!!

Massimo Bonanni

Azure Technical Trainer

massimo.bonanni@microsoft.com
@massimobonanni

Connect with me on LinkedIn

linkedin.com/in/massimobonanni/

meetup.com/Microsoft-Reactor-Stockholm/

References

- Learning Path
  https://aka.ms/AzureKeyVault-7
- Azure Key Vault documentation
  https://docs.microsoft.com/en-us/azure/key-vault/
- Azure Key Vault Developer's Guide
  https://docs.microsoft.com/en-us/azure/key-vault/general/developers-guide
- Channel9 - Azure Key Vault with Sumedh Barde
  https://channel9.msdn.com/Shows/Cloud+Cover/Episode-169-Azure-Key-Vault-with-Sumedh-Barde
- Secret and Config GitHub Repo
  https://github.com/massimobonanni/azure-att-demo

Photo by Jaredd Craig on Unsplash

Join our community

meetup.com/Microsoft-Reactor-Stockholm/

@MSFTReactor

http://www.youtube.com/c/MicrosoftReactor

ReactorStockholm@microsoft.com

Microsoft Reactor at Epicenter,
Master Samuelsgatan 36, 5th floor,
111 57 Stockholm Sweden

Questions? ReactorStockholm@microsoft.com