Security research:

Hoe kan Azure keys gebruikt worden om gevoelige informatie te kunnen bewaren en gebruiken in mijn back-end gehost op Azure in een periode van 2 weken?



Contents

[Inleiding 3](#_Toc156388971)

[Wat is Azure 4](#_Toc156388972)

[Wat zijn Azure Keys? 5](#_Toc156388973)

[Hoe implementeer ik Azure keys in een gehoste applicatie? 6](#_Toc156388974)

[Proof of concept 8](#_Toc156388975)

[Conclusie 9](#_Toc156388976)

[Bronnenlijst 10](#_Toc156388977)

# Inleiding

Voor de C# back-end van mijn applicatie heb ik vanaf het begin de connectionstring naar de MongoDB database lokaal bewaard in een JSON string, zodat deze niet op Github bewaard hoeft te worden. Reden hiervoor is natuurlijk dat een connectionstring gevoelige informatie bevat die volledige toegang tot de database geeft.

Uiteindelijk heb ik mijn back-end gehost op Azure, zodat mijn back-end overal te gebruiken is en deze niet lokaal hoeft te draaien. Dit had natuurlijk als gevolg dat de lokale connectionstring niet meer beschikbaar was. En omdat de connectionstring in Github zetten geen optie is was er een alternatief nodig. Vanuit Azure zelf kwam de oplossing: Azure Keys.

Hieruit is de volgende hoofdvraagd ontstaan:

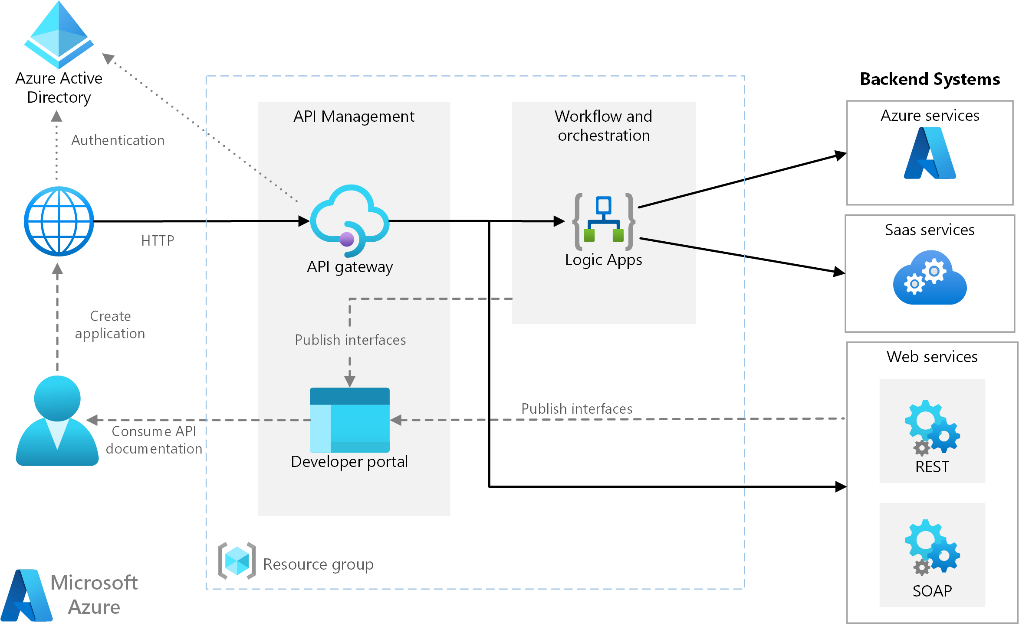
**Hoe kan Azure keys gebruikt worden om gevoelige informatie te kunnen bewaren en gebruiken in een back-end gehost op Azure?**

In dit document zal ik verder ingaan op wat Azure Keys is en hoe dit werkt. Vervolgens zal ik een proof of concept laten zien.

# Wat is Azure

Microsoft Azure is een cloud computing-platform, om verschillende soorten applicaties, websites en services online beschikbaar te stellen. Azure biedt een breed scala aan diensten die organisaties in staat stellen om hun digitale werklasten op een flexibele, schaalbare en veilige manier te hosten. Het hostingproces op Azure omvat het implementeren en beheren van virtuele machines, het gebruik van platformservices en het bieden van geavanceerde mogelijkheden voor schaalbaarheid, beveiliging en integratie.

Een fundamenteel aspect van hosten op Azure is het gebruik van virtuele machines (VM's). Deze VM's zijn virtuele instanties van computers die op de Azure-infrastructuur draaien. Organisaties kunnen verschillende besturingssystemen kiezen, zoals Windows of Linux, en deze op virtuele machines installeren. Deze VM's kunnen worden geconfigureerd met specifieke bronnen, zoals rekenkracht, geheugen en opslag, afhankelijk van de behoeften van de gehoste applicaties. (*What is Azure—Microsoft Cloud Services | Microsoft Azure*, z.d.)



Beveiliging is een belangrijk onderdeel van het hosten op Azure. Het platform biedt veel beveiligingsdiensten en -functies, zoals geavanceerde identiteits- en toegangsbeheer, versleuteling van gegevens en nalevingscertificeringen. developers kunnen gebruikmaken van deze ingebouwde beveiligingslagen om hun gegevens en applicaties te beschermen tegen bedreigingen

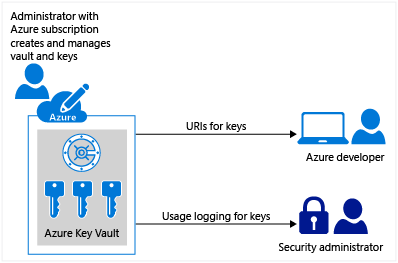
Azure biedt ook uitgebreide integratiemogelijkheden met andere Microsoft-producten en -diensten, en populaire tools en frameworks die door ontwikkelaars worden gebruikt. Dit vergemakkelijkt de samenwerking tussen verschillende componenten van een applicatie en bevordert een goede ontwikkelings- en implementatie-ervaring. (*Directory of Azure Cloud Services | Microsoft Azure*, z.d.)

.

# Wat zijn Azure Keys?

Azure Key Vault is een cloudservice van Microsoft Azure die is ontworpen om het beheer van gevoelige informatie, zoals wachtwoorden, geheime sleutels en certificaten, te vereenvoudigen en te beveiligen. Het functioneerd als een veilige kluis waarin applicaties hun geheimen kunnen opslaan en beheren, en biedt geavanceerde beveiligingsfuncties om ongeautoriseerde toegang te voorkomen. (Hanna & Holman, 2023)

Beveiliging staat centraal in Azure Key Vault. Het maakt gebruik van Hardware security modules (HSM's) om sleutels op te slaan en te beschermen tegen aanvallen. HSM's bieden een extra laag van fysieke beveiliging, waardoor het moeilijker wordt om toegang te krijgen tot de opgeslagen geheimen. Daarnaast biedt Azure Key Vault uitgebreide logging, waardoor organisaties inzicht krijgen in wie toegang heeft gehad tot welke sleutels en wanneer. (Msmbaldwin, 2023)



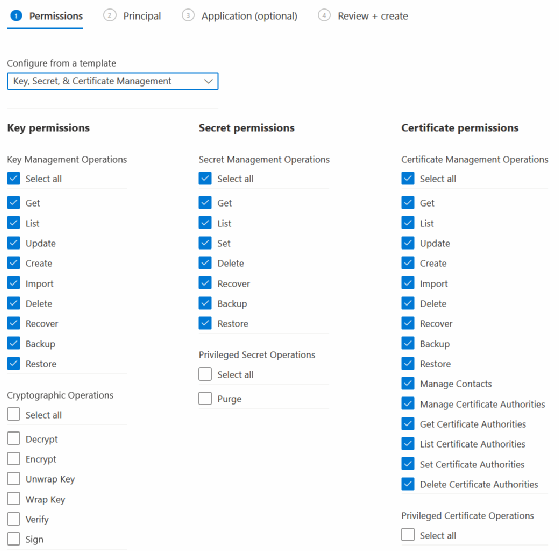
In conclusie biedt Azure Key Vault een betrouwbare en veilige oplossing voor het beheer van sleutels en geheimen in de cloud. Door gevoelige informatie te centraliseren, geavanceerde beveiligingsfuncties te bieden en goede integratie met andere Azure-services mogelijk te maken, draagt het bij aan het verhogen van de algehele beveiliging en naleving van organisaties die gebruikmaken van cloudtechnologieën.

# Hoe implementeer ik Azure keys in een gehoste applicatie?

In dit hoofdstuk zal ik stapsgewijs ingaan in hoe Azure Keys kan worden geconfigureerd in mijn .NET applicatie.

**Azure Key Vault Aanmaken**

Om te beginnen, maak je een Azure Key Vault aan via het Azure-portal. In de Key Vault voeg je de sleutels, geheimen of certificaten toe die je applicatie nodig heeft. Zorg ervoor dat je de juiste machtigingen instelt, zodat de applicatie toegang heeft tot de gegevens in de Key Vault. (Hanna & Holman, 2023b)



**Azure SDK Installeren**

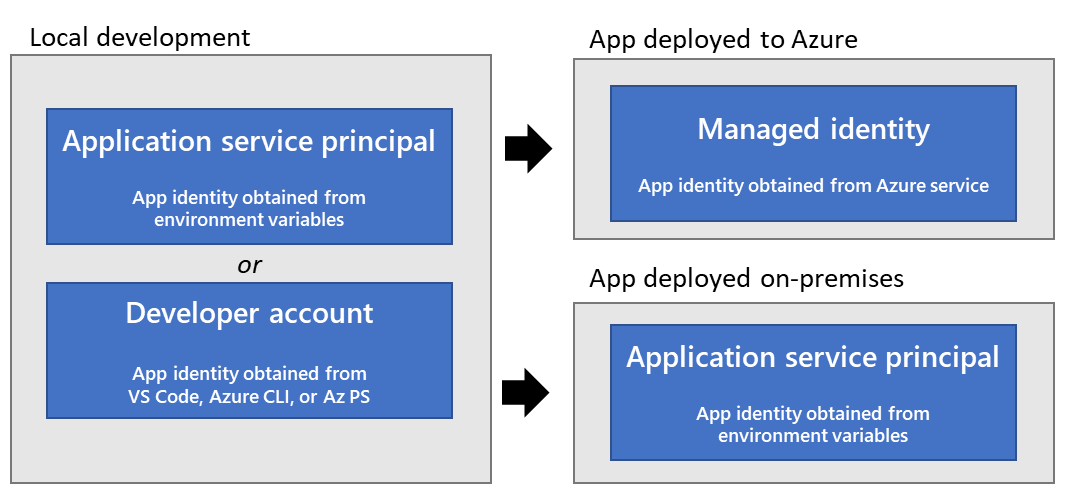
In de .NET-applicatie installeer je de Azure Key Vault SDK via NuGet-pakketbeheer. Dit SDK bevat de nodige klassen en methoden om verbinding te maken met en gegevens op te halen uit de Azure Key Vault. (Rick-Anderson, 2023)

Install-Package Microsoft.Azure.Services.AppAuthentication

Install-Package Microsoft.Azure.KeyVault

**Authenticatie Configureren**

Configureer de authenticatie van je applicatie. Afhankelijk van de omgeving waarin je app draait (bijv. lokaal, ontwikkeling, productie), kun je ervoor kiezen om gebruik te maken van bijvoorbeeld Managed Identity, Service Principal, of een specifiek account voor toegang tot Azure Key Vault.



**Code Implementeren**

In de .NET-code voeg je de logica toe om verbinding te maken met Azure Key Vault en gegevens op te halen. Hier is een voorbeeld in C#:

var keyVaultUri = "https://your-key-vault-name.vault.azure.net/";

var secretName = "your-secret-name";

var azureServiceTokenProvider = new AzureServiceTokenProvider();

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

var secret = await keyVaultClient.GetSecretAsync($"{keyVaultUri}secrets/{secretName}");

var secretValue = secret.Value;

Deze code maakt gebruik van AzureServiceTokenProvider voor tokenverstrekking en KeyVaultClient om de geheime waarde op te halen. (Azure-Sdk, z.d.)

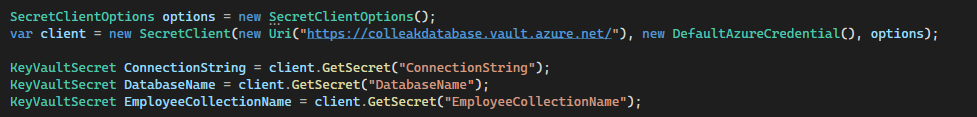
**Geheimen Gebruiken in de Applicatie**

Nu de secrets zijn opgehaald, kunnen ze gebruikt worden in de applicatie. Bijvoorbeeld, je kunt ze gebruiken als connectionstrings, wachtwoorden of andere configuratiegegevens.

# Proof of concept

In het groepsproject is Azure keys geïmplementeerd om de connectionstring te bewaren.

Nadat de applicatie toestemming heeft gekregen op de Azure portal, is de volgende code toegevoegd in de applicatie:

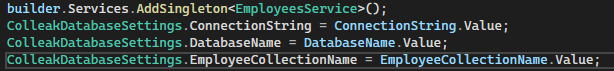


In dit deel van de code wordt een instantie van SecretClientOptions gemaakt. Deze klasse wordt gebruikt om opties te configureren voor de SecretClient.

Vervolgens wordt een SecretClient geïnstantieerd, die de communicatie met de Azure Key Vault-service mogelijk maakt. De eerste parameter is de URI van de Key Vault, de tweede parameter is een DefaultAzureCredential. Dit is een belangrijk onderdeel, omdat het aangeeft dat de applicatie probeert authenticatiegegevens op te halen op basis van de runtime-omgeving (bijv. Azure Managed Identity of ontwikkelingsreferenties). De derde parameter is de SecretClientOptions.

De laatste drie regels roepen de methode GetSecret aan op de SecretClient om specifieke geheime waarden op te halen uit de Key Vault. De argumenten zijn de namen van de geheime waarden zoals ze zijn opgeslagen in de Key Vault. Hier word de connectionstring, database naam en de naam van de database collection opgehaald.

Na het uitvoeren van deze code bevat elk KeyVaultSecret-object de opgehaalde geheime waarde, en je kunt deze waarden gebruiken in je applicatie. Dit helpt bij het scheiden van geheime informatie, waardoor het beheer van gevoelige gegevens wordt verbeterd en de beveiliging wordt verhoogd. Het gebruik van DefaultAzureCredential betekent dat de applicatie automatisch de juiste referenties gebruikt, afhankelijk van waar het wordt uitgevoerd. (Msmbaldwin, 2023a)



Vervolgens worden de waardes uit de Key Vault toegevoegd aan de bestaande database variabelen, zodat dit zonder problemen blijft functioneren in de bestaande code.

# Conclusie

Door het gebruiken van Azure Keys is het mogelijk om de connectionstring veilig te gebruiken op een gehoste Azure applicatie, waardoor de database nog steeds gebruikt kan worden. Hierdoor is de volledige back-end overal aan te roepen, wat handig is wanneer er in groepsverband met dezelfde api wordt gewerkt.

Het implenteren van Azure keys in de bestaande logica voor MongoDB is ook vrij soepel, nadat de waardes zijn opgehaald kunnen deze simpelweg gekoppeld worden aan de bestaande code voor de database.

Ondanks dat de implementatie niet heel ingewikkeld is, is dit onderzoek wel zeer handig geweest in het begrijpen van Azure keys en hosting in het algemeen.

# Bronnenlijst

Hanna, K. T., & Holman, T. (2023, 17 april). *Microsoft Azure Key Vault*. SearchWindowsServer. <https://www.techtarget.com/searchwindowsserver/definition/Microsoft-Azure-Key-Vault>

Msmbaldwin. (2023, 21 juli). *Azure Managed HSM Overview - Azure managed HSM*. Microsoft Learn. <https://learn.microsoft.com/en-us/azure/key-vault/managed-hsm/overview>

*What is Azure—Microsoft Cloud Services | Microsoft Azure*. (z.d.). <https://azure.microsoft.com/en-us/resources/cloud-computing-dictionary/what-is-azure>

*Directory of Azure Cloud Services | Microsoft Azure*. (z.d.). <https://azure.microsoft.com/en-us/products>

Rick-Anderson. (2023, 9 november). *Azure Key Vault configuration provider in ASP.NET core*. Microsoft Learn. <https://learn.microsoft.com/en-us/aspnet/core/security/key-vault-configuration?view=aspnetcore-8.0>

Azure-Sdk. (z.d.). *AzureServiceTokenProvider Class (Microsoft.Azure.Services.AppAuthentication) - Azure for .NET developers*. Microsoft Learn. <https://learn.microsoft.com/en-us/dotnet/api/microsoft.azure.services.appauthentication.azureservicetokenprovider?view=azure-dotnet-legacy>