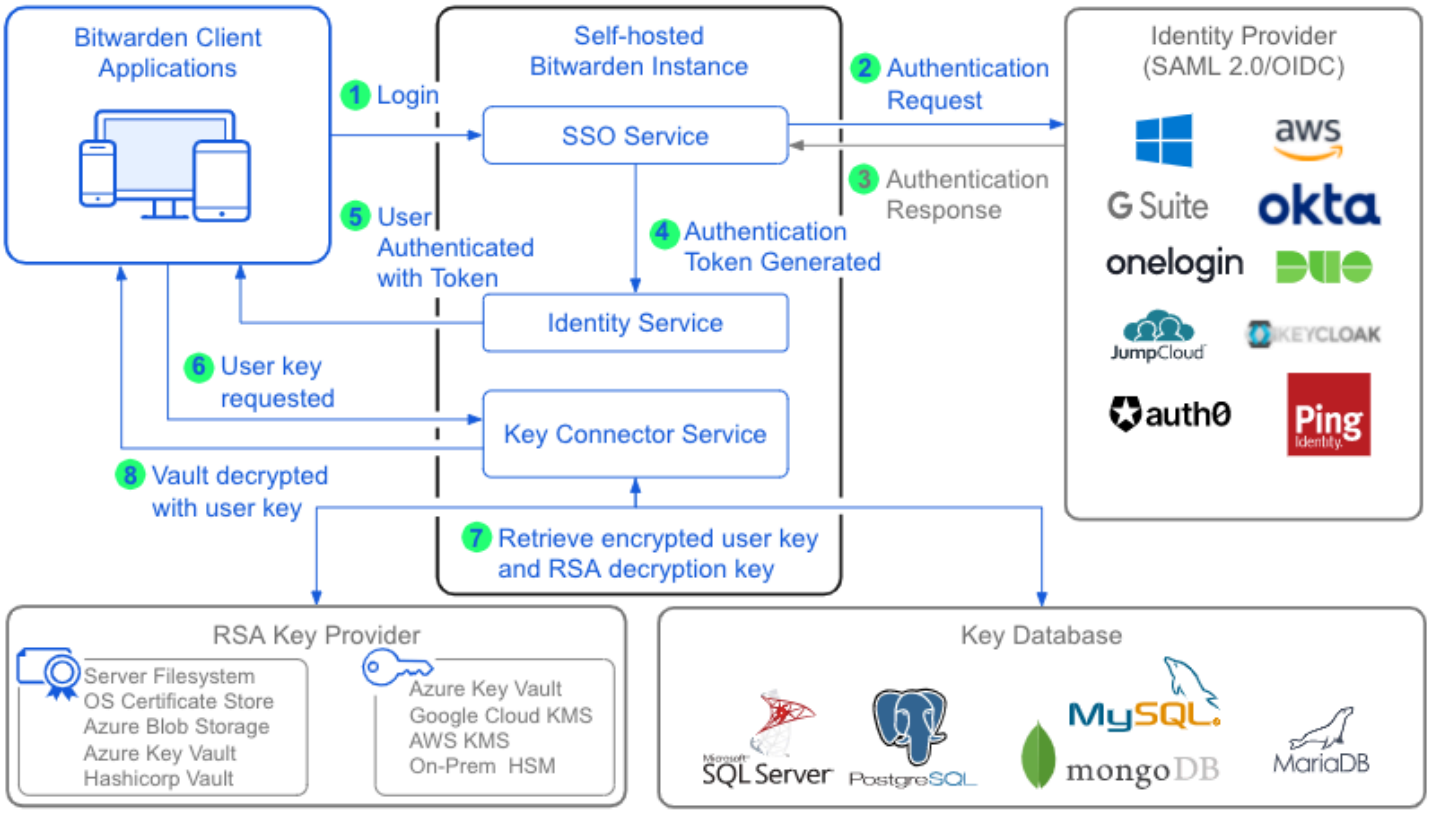
Over Key Connector

Over Key Connector

Key Connector is een zelf gehoste applicatie die klantgestuurde versleuteling (CMS) mogelijk maakt, waardoor een bedrijfsorganisatie cryptografische sleutels kan aanbieden aan Bitwarden-cliënten.

Key Connector draait als een docker-container op hetzelfde netwerk als bestaande services en kan worden gebruikt met login met SSO om cryptografische sleutels te serveren voor een organisatie als alternatief voor het vereisen van een hoofdwachtwoord voor kluisdecodering(meer informatie). Bitwarden ondersteunt de implementatie van één Key Connector voor gebruik door één organisatie voor een zelf gehoste instantie.

Key Connector vereist een verbinding met een **database waar versleutelde gebruikerssleutels zijn opgeslagen** en een **RSA sleutelpaar om opgeslagen gebruikerssleutels te versleutelen en te ontsleutelen**. Key Connector kan worden geconfigureerd met verschillende databaseproviders (bijvoorbeeld MSSQL, PostgreSQL, MySQL) en providers voor sleutelpaaropslag (bijvoorbeeld Hashicorp Vault, Cloud KMS-providers, On-prem HSM-apparaten) om te voldoen aan de infrastructuurvereisten van uw bedrijf.



Key Connector Architecture

Waarom Key Connector gebruiken?

Bij implementaties die master password decryption gebruiken, zorgt je identity provider voor authenticatie en is het master password van een lid nodig voor vault decryption. Deze scheiding van belangen is een belangrijke stap die ervoor zorgt dat alleen een lid van de organisatie toegang heeft tot de sleutel die nodig is om de gevoelige kluisgegevens van je organisatie te ontsleutelen.

In implementaties die gebruik maken van Key Connector voor ontsleuteling, zorgt je identity provider nog steeds voor authenticatie, maar wordt de ontsleuteling van de kluis afgehandeld door Key Connector. Door toegang te krijgen tot een versleutelde sleuteldatabase (zie het bovenstaande diagram), geeft Key Connector een gebruiker zijn ontcijferingssleutel wanneer hij inlogt, zonder dat er een hoofdwachtwoord nodig is.

We noemen Key Connector-implementaties vaak **Customer-Managed Encryption**, omdat uw bedrijf als enige verantwoordelijk is voor het beheer van de Key Connector-applicatie en van de ontcijferingssleutels van de kluis. Voor ondernemingen die een door de klant beheerde encryptieomgeving willen implementeren en onderhouden, maakt Key Connector een gestroomlijnde aanmeldervaring voor kluizen mogelijk.

Invloed op hoofdwachtwoorden

Omdat Key Connector op masterwachtwoord gebaseerde decodering vervangt door door de klant beheerde decoderingssleutels, moeten organisatieleden **het masterwachtwoord uit hun account verwijderen**. Eenmaal verwijderd, worden alle ontsleutelingsacties van de kluis uitgevoerd met de opgeslagen gebruikerssleutel. Naast het inloggen heeft dit ook gevolgen voor het offboarden en voor andere functies waar je rekening mee moet houden.

> ⚠ **Warning**
>
> Currently, there is not a way to re-create master passwords for accounts that have removed them.
>
> For this reason, organization owners and admins are not able to remove their master password and must continue using their master password even if using SSO. It is possible to elevate a user who has removed their master password to owner or admin, however we **strongly recommend** that your organization always have at least one owner with a master password.

Invloed op het lidmaatschap van de organisatie

Key Connector vereist dat gebruikers hun hoofdwachtwoorden verwijderen en gebruikt in plaats daarvan een eigen database met cryptografische sleutels om de kluizen van gebruikers te ontsleutelen. Omdat hoofdwachtwoorden niet opnieuw kunnen worden aangemaakt voor accounts die ze hebben verwijderd, betekent dit dat wanneer een account eenmaal gebruik maakt van Key Connector-decodering, het voor alle doeleinden **eigendom is van de organisatie**.

Deze accounts **mogen de organisatie niet verlaten**, omdat ze dan alle middelen verliezen om kluisgegevens te ontsleutelen. Ook als een organisatiebeheerder de account uit de organisatie verwijdert, verliest de account alle middelen om kluisgegevens te ontsleutelen.

Invloed op andere functies

Functie	Impact
Verificatie	Er zijn een aantal functies in Bitwarden-clienttoepassingen waarvoor normaal gesproken een hoofdwachtwoord moet worden ingevoerd om ze te kunnen gebruiken, zoals het exporteren van kluisgegevens, het wijzigen van de instellingen voor tweestapsaanmelding, het ophalen van API-sleutels en meer. **Al deze functies** zullen de bevestiging van het hoofdwachtwoord vervangen door TOTP-verificatie via e-mail.
Kluis vergrendelen/ontgrendelen	Onder normale omstandigheden kan een vergrendelde kluis worden ontgrendeld met een hoofdwachtwoord. Als je organisatie Key Connector gebruikt, kunnen vergrendelde clienttoepassingen alleen worden ontgrendeld met een PIN-code of met biometrische gegevens. Als noch PIN noch biometrie zijn ingeschakeld voor een clienttoepassing, zal de kluis altijd uitloggen in plaats van vergrendelen. In tegenstelling tot ontgrendelen, is voor inloggen **altijd** een internetverbinding nodig(meer informatie).

Functie	Impact
Hoofdwachtwoord opnieuw vragen	Wanneer Key Connector wordt gebruikt, wordt het opnieuw opvragen van het hoofdwachtwoord uitgeschakeld voor elke gebruiker die zijn hoofdwachtwoord heeft verwijderd als gevolg van de implementatie van Key Connector.
Admin-wachtwoord opnieuw instellen	Wanneer Key Connector wordt gebruikt, wordt het resetten van het beheerderswachtwoord uitgeschakeld voor elke gebruiker die zijn hoofdwachtwoord heeft verwijderd als gevolg van de implementatie van Key Connector.
Toegang voor noodgevallen	Wanneer Key Connector wordt gebruikt, wordt de optie voor accountovername in noodgevallen uitgeschakeld voor elke gebruiker die zijn hoofdwachtwoord heeft verwijderd als gevolg van de implementatie van Key Connector. Vertrouwde contactpersonen in noodsituaties kunnen nog steeds de individuele kluisgegevens van een verstrekker **bekijken** , met inachtneming van de vastgestelde workflow voor toegang in noodsituaties.

Hoe gebruik ik Key Connector?

Om aan de slag te gaan met Key Connector voor door de klant beheerde versleuteling, moet je de volgende vereisten bekijken:

> ⚠ **Warning**
>
> Management of cryptographic keys is incredibly sensitive and is **only recommended for enterprises with a team and infrastructure** that can securely support deploying and managing a key server.

Om Key Connector te kunnen gebruiken moet je ook:

- Een Enterprise-organisatie hebben.
- Een zelf gehoste Bitwarden-server hebben.
- Een actieve SSO-implementatie hebben.
- Activeer de beleidsregels voor één organisatie en vereisen één aanmelding.

Als jouw organisatie aan deze vereisten voldoet of kan voldoen, inclusief een team en infrastructuur die het beheer van een keyserver kan ondersteunen, neem dan contact met ons op en we zullen Key Connector activeren.