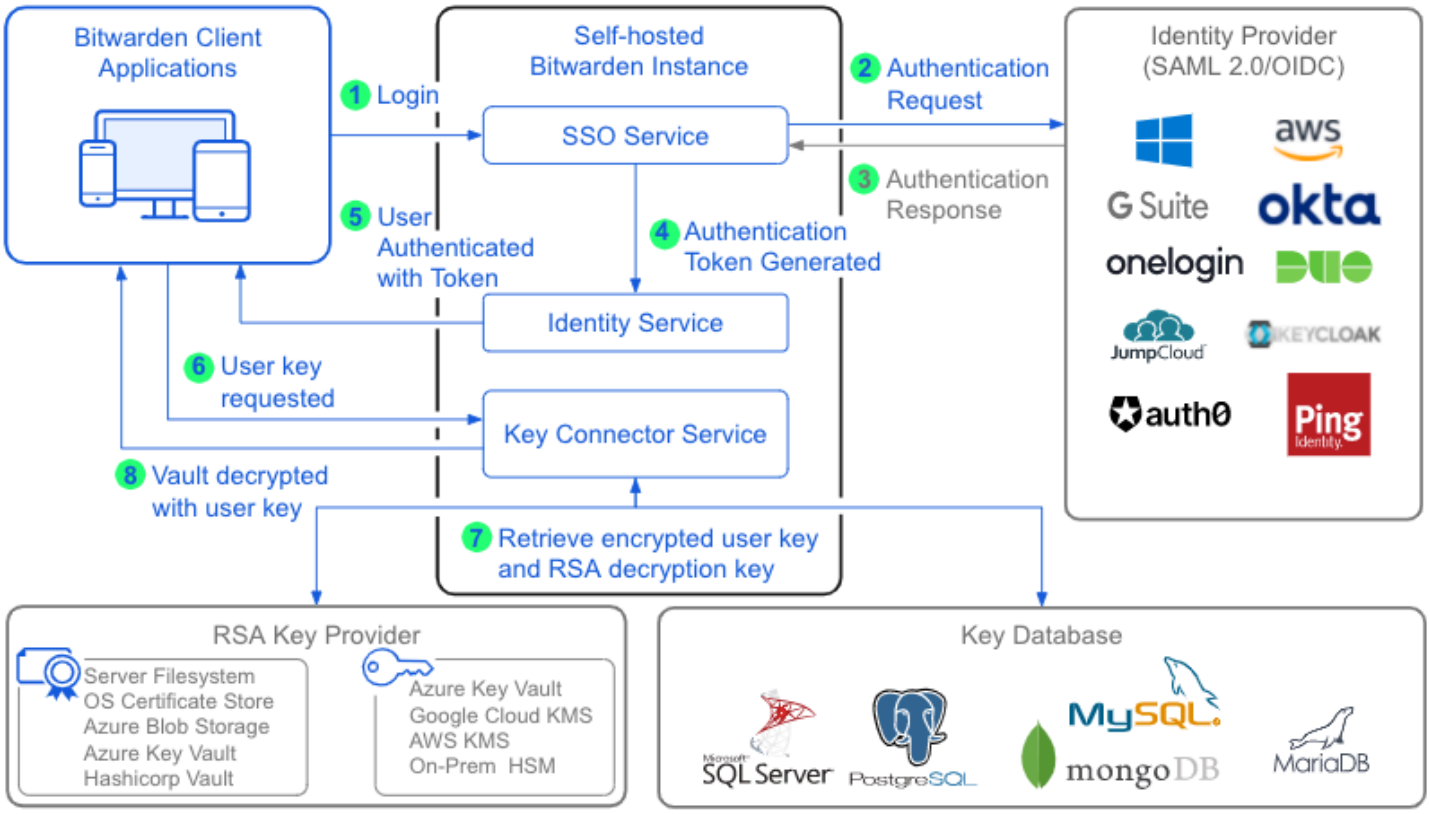
Über Key Connector

Über Key Connector

Key Connector ist eine selbst gehostete Anwendung, die kundengesteuerte Verschlüsselung (CMS) ermöglicht und es einer Enterprise-Organisation ermöglicht, kryptografische Schlüssel an Bitwarden-Clients zu liefern.

Key Connector läuft als Docker-Container im selben Netzwerk wie bestehende Dienste und kann mit Zugangsdaten mit SSO verwendet werden, um kryptografische Schlüssel für eine Organisation bereitzustellen, als Alternative zur Anforderung eines Master-Passworts für die Entschlüsselung des Tresors (mehr erfahren). Bitwarden unterstützt die Bereitstellung eines Key Connectors zur Nutzung durch eine Organisation für eine selbst gehostete Instanz.

Key Connector benötigt eine Verbindung zu einer **Datenbank, in der verschlüsselte Benutzerschlüssel gespeichert sind** und ein **RSA-Schlüsselpaar zum Verschlüsseln und Entschlüsseln gespeicherter Benutzerschlüssel**. Key Connector kann mit einer Vielzahl von Datenbankanbietern (z. B. MSSQL, PostgreSQL, MySQL) und Schlüsselpaar-Speicheranbietern (z. B. Hashicorp Vault, Cloud-KMS-Anbietern, lokalen HSM-Geräten) konfiguriert werden, um an die Infrastruktur Ihres Unternehmens angepasst zu werden Anforderungen.



Key Connector Architecture

Warum Key Connector verwenden?

Bei Implementierungen, die die Master-Passwort-Entschlüsselung nutzen , übernimmt Ihr Identitätsanbieter die Authentifizierung und für die Tresor-Entschlüsselung ist das Master-Passwort eines Mitglieds erforderlich. Diese Trennung von Zuständigkeiten ist ein wichtiger Schritt, der sicherstellt, dass nur ein Mitglied der Organisation Zugang zu dem Schlüssel hat, der zum Entschlüsseln der sensiblen Daten im Tresor Ihrer Organisation erforderlich ist.

In Implementierungen, die Key Connector für die Entschlüsselung nutzen , übernimmt Ihr Identitätsanbieter weiterhin die Authentifizierung, die Tresor-Entschlüsselung wird jedoch von Key Connector übernommen. Indem auf eine verschlüsselte Schlüsseldatenbank zugegriffen wird (siehe das obige Diagramm), stellt Key Connector einem Benutzer seinen Entschlüsselungsschlüssel zur Verfügung, wenn sie sich anmelden, ohne ein Master-Passwort zu benötigen.

Wir bezeichnen die Implementierungen des Key Connectors oft als Nutzung der **Kundenverwalteten Verschlüsselung**, weil Ihr Unternehmen die alleinige Verantwortung für die Verwaltung der Key Connector-Anwendung und der vom Tresor bereitgestellten Entschlüsselungsschlüssel hat. Für Unternehmen, die bereit sind, eine kundengesteuerte Verschlüsselungsumgebung zu implementieren und zu verwalten, erleichtert der Key Connector eine vereinfachte Zugangsdaten-Erfahrung für den Tresor.

Auswirkungen auf Master-Passwörter

Da der Key Connector die Entschlüsselung auf Basis des Master-Passworts durch vom Kunden verwaltete Entschlüsselungsschlüssel ersetzt, werden die Mitglieder der Organisation **dazu aufgefordert, das Master-Passwort von ihrem Konto zu entfernen**. Sobald entfernt, werden alle Entschlüsselungsaktionen des Tresors mit dem gespeicherten Benutzerschlüssel durchgeführt. Neben dem Anmelden wird dies einige Auswirkungen auf das Offboarding und auf andere Funktionen haben, dessen sollten Sie sich bewusst sein.

> ⚠ **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.

Auswirkungen auf die Mitgliedschaft in der Organisation

Key Connector verlangt von den Benutzern, ihr Master-Passwort zu entfernen und verwendet stattdessen eine firmeneigene Datenbank mit kryptographischen Schlüsseln, um die Tresore der Benutzer zu entschlüsseln. Da Master-Passwörter für Konten, die sie entfernt haben, nicht neu erstellt werden können, bedeutet dies, dass ein Konto, das die Key Connector Entschlüsselung verwendet, in jeder Hinsicht **im Besitz der Organisation ist**.

Diese Konten **dürfen die Organisation nicht verlassen**, da sie beim Verlassen jegliche Möglichkeit zur Entschlüsselung der Tresor-Daten verlieren würden. Ähnlich verhält es sich, wenn ein Organisationsadministrator das Konto aus der Organisation entfernt, verliert das Konto jegliche Möglichkeit, die Daten im Tresor zu entschlüsseln.

Auswirkungen auf andere Funktionen

Funktion	Aufprall
Überprüfung	Es gibt eine Reihe von Funktionen in Bitwarden Client-Anwendungen, die normalerweise die Eingabe eines Master-Passworts erfordern, um verwendet zu werden, einschließlich des Exports von Tresor-Daten, der Änderung der Zwei-Schritt-Zugangsdaten Einstellungen, dem Abrufen von API-Schlüsseln und mehr. **Alle diese Funktionen** ersetzen die Bestätigung des Master-Passworts durch eine E-Mail-basierte TOTP-Verifizierung.

Funktion	Aufprall
Tresor sperren/entsperren	Unter normalen Umständen kann ein gesperrter Tresor mit einem Master-Passwort entsperrt werden. Wenn Ihre Organisation den Key Connector verwendet, können gesperrte Client-Anwendungen nur mit einer PIN oder mit Biometrie entsperrt werden. Wenn weder PIN noch Biometrie für eine Client-Anwendung aktiviert sind, wird der Tresor immer abmelden statt sperren. Im Gegensatz zum Entsperren erfordert das Anmelden **immer** eine Internetverbindung (mehr erfahren).
Master-Passwort erneut abfragen	Wenn der Key Connector verwendet wird, wird die erneute Aufforderung des Master-Passworts für jeden Benutzer deaktiviert, der sein Master-Passwort aufgrund Ihrer Key Connector-Implementierung entfernt hat.
Administrator Passwort zurücksetzen	Wenn der Key Connector verwendet wird, wird das Zurücksetzen des Administrator-Passworts für jeden Benutzer deaktiviert, der sein Master-Passwort aufgrund Ihrer Key Connector-Implementierung entfernt hat.
Zugang im Notfall	Wenn der Key Connector verwendet wird, wird die Notzugriffsoption Kontoübernahme für jeden Benutzer deaktiviert, der sein Master-Passwort aufgrund Ihrer Key Connector-Implementierung entfernt hat. Vertrauenswürdige Notfallkontakte können immer noch die individuellen **Tresor Daten** eines Gewährleisters einsehen, vorbehaltlich des festgelegten Notfallzugriffsablaufs.

Wie fange ich an, Key Connector zu benutzen?

Um mit der Verwendung von Key Connector für kundengesteuerte Verschlüsselung zu beginnen, überprüfen Sie bitte die folgenden Anforderungen:

> ⚠ **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.

Um Key Connector zu verwenden, müssen Sie auch:

- Haben Sie eine Unternehmensorganisation .
- Verfügen Sie über einen selbst gehosteten Bitwarden-Server .
- Verfügen Sie über eine aktive SSO-Implementierung .
- Aktivieren Sie die einzelne Organisation und erfordern Sie Single-Sign-On-Richtlinien .

Wenn Ihre Organisation diese Anforderungen erfüllt oder erfüllen kann, einschließlich eines Teams und einer Infrastruktur, die die Verwaltung eines Schlüsselservers unterstützen kann, kontaktieren Sie uns und wir werden den Key Connector aktivieren.