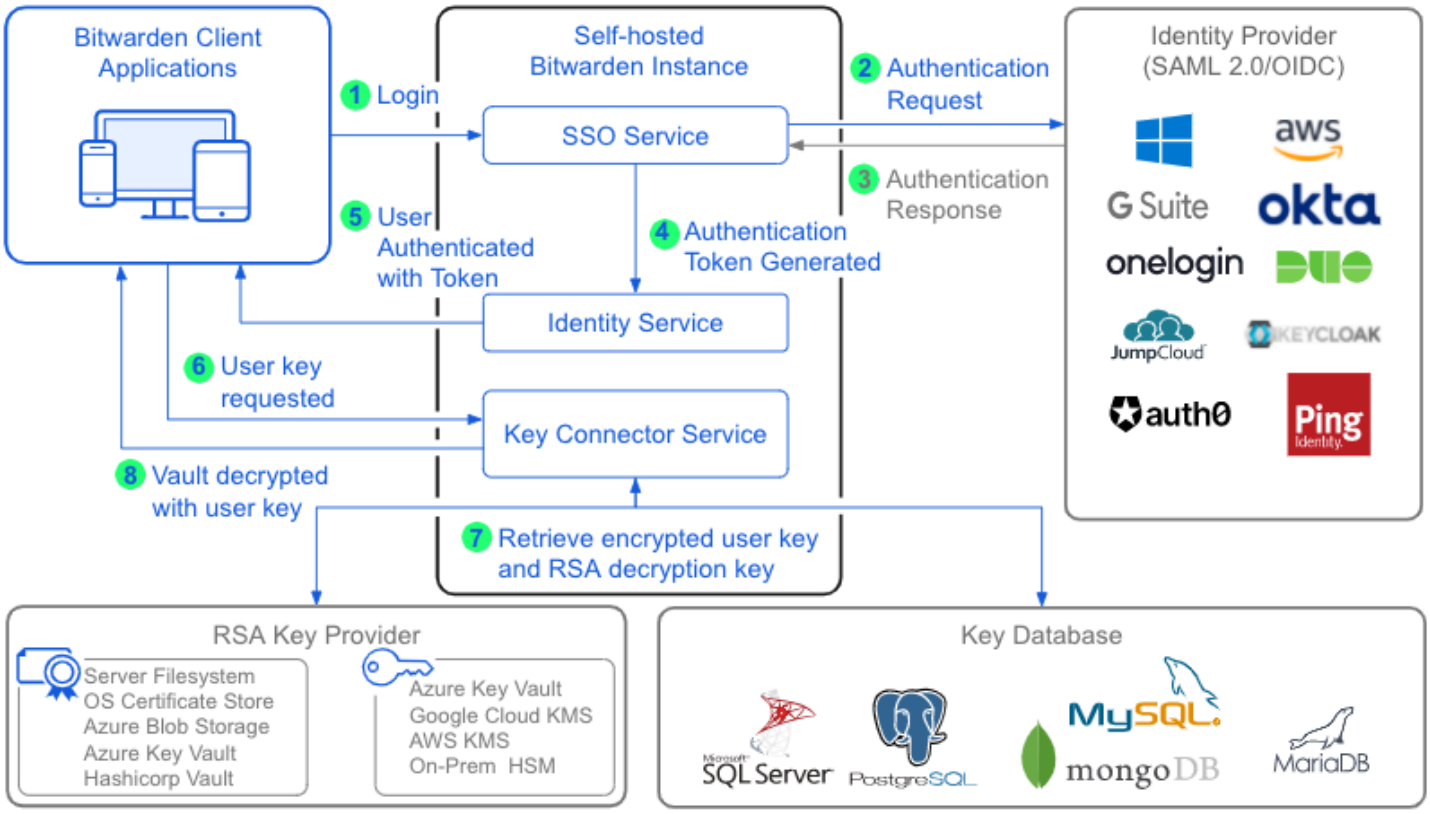
À propos de Key Connector

À propos de Key Connector

Key Connector est une application auto-hébergée qui facilite le chiffrement géré par le client (CMS), permettant à une organisation d'entreprise de fournir des clés cryptographiques aux clients Bitwarden.

Key Connector fonctionne comme un conteneur docker sur le même réseau que les services existants, et peut être utilisé avec identifiant avec SSO pour servir des clés cryptographiques pour une organisation comme une alternative à l'exigence d'un mot de passe principal pour le déchiffrement du coffre (en savoir plus). Bitwarden prend en charge le déploiement d'un Key Connector pour une utilisation par une organisation pour une instance auto-hébergée.

Key Connector nécessite une connexion à une **base de données où sont stockées les clés utilisateur cryptées** et une **paire de clés RSA pour crypter et décrypter les clés utilisateur stockées**. Key Connector peut être configuré avec une variété de fournisseurs de bases de données (par exemple, MSSQL, PostgreSQL, MySQL) et de fournisseurs de stockage de paires de clés (par exemple, Hashicorp Vault, fournisseurs Cloud KMS, appareils HSM sur site) afin de répondre aux exigences d'infrastructure de votre entreprise.



Key Connector Architecture

Pourquoi utiliser Key Connector ?

Dans les implémentations qui exploitent le déchiffrement du mot de passe principal , votre fournisseur d'identité gère l'authentification et le mot de passe principal d'un membre est requis pour le déchiffrement du coffre-fort. Cette séparation des préoccupations est une étape importante qui garantit que seul un membre de l'organisation a accès à la clé nécessaire pour déchiffrer les données sensibles du coffre de votre organisation.

Dans les implémentations qui exploitent Key Connector pour le déchiffrement , votre fournisseur d'identité gère toujours l'authentification, mais le déchiffrement du coffre-fort est géré par Key Connector. En accédant à une base de données de clés cryptées (voir le diagramme ci-dessus), Key Connector fournit à un utilisateur sa clé de déchiffrement lorsqu'il se connecte, sans nécessiter de mot de passe principal.

Nous faisons souvent référence aux mises en œuvre de Key Connector comme exploitant la **Chiffrement Géré par le Client**, car votre entreprise a la seule responsabilité de la gestion de l'application Key Connector et des clés de déchiffrement du coffre qu'elle sert. Pour les entreprises prêtes à déployer et à maintenir un environnement de chiffrement géré par le client, Key Connector facilite une expérience d'identifiant de coffre simplifiée.

Impact sur les mots de passe principaux

Parce que Key Connector remplace le déchiffrement basé sur le mot de passe principal par des clés de déchiffrement gérées par le client, les membres de l'organisation seront **obligés de supprimer le mot de passe principal de leur compte**. Une fois supprimé, toutes les actions de déchiffrement du coffre seront effectuées à l'aide de la clé utilisateur stockée. En plus de se connecter, cela aura des impacts sur la désinscription et sur d'autres fonctionnalités dont vous devriez être conscient.

> ⚠ **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.

Impact sur l'adhésion à l'organisation

Key Connector demande aux utilisateurs de supprimer leur mot de passe principal et utilise à la place une base de données appartenant à l'entreprise de clés cryptographiques pour décrypter les coffres des utilisateurs. Parce que les mots de passe principaux ne peuvent pas être recréés pour les comptes qui les ont supprimés, cela signifie qu'une fois qu'un compte utilise le déchiffrement Key Connector, il est à toutes fins utiles **possédé par l'organisation**.

Ces comptes **ne peuvent pas quitter l'organisation**, car en faisant cela, ils perdraient tout moyen de déchiffrer les données du coffre. De même, si un administrateur d'organisation supprime le compte de l'organisation, le compte perdra tout moyen de déchiffrer les données du coffre.

Impact sur d'autres fonctionnalités

Fonctionnalité	Impact
Vérification	Il existe un certain nombre de fonctionnalités dans les applications client Bitwarden qui nécessitent normalement la saisie d'un mot de passe principal pour être utilisées, y compris l'exportation des données du coffre, la modification des paramètres de l'identifiant en deux étapes, la récupération des clés API, et plus encore. **Toutes ces fonctionnalités** remplaceront la confirmation du mot de passe principal par une vérification TOTP par e-mail.

Fonctionnalité	Impact
Verrouillage/déverrouillage du coffre	Dans des circonstances ordinaires, un coffre verrouillé peut être déverrouillé à l'aide d'un mot de passe principal. Lorsque votre organisation utilise Key Connector, les applications client verrouillées ne peuvent être déverrouillées qu'avec un PIN ou avec la biométrie. Si ni le code PIN ni la biométrie ne sont activés pour une application client, le coffre se déconnectera toujours au lieu de verrouiller. Contrairement au déverrouillage, la connexion nécessite **toujours** une connexion Internet (en savoir plus).
Ressaisir le mot de passe principal	Lorsque Key Connector est utilisé, la demande de réintroduction du mot de passe principal sera désactivée pour tout utilisateur ayant supprimé son mot de passe principal suite à votre mise en œuvre de Key Connector.
Réinitialisation du mot de passe admin	Lorsque Key Connector est utilisé, la réinitialisation du mot de passe admin sera désactivée pour tout utilisateur ayant supprimé son mot de passe principal suite à votre mise en œuvre de Key Connector.
Accès d'urgence	Lorsque Key Connector est utilisé, l' option de prise de contrôle du compte d'accès d'urgence sera désactivée pour tout utilisateur ayant supprimé son mot de passe principal suite à la mise en œuvre de votre Key Connector. Les contacts d'urgence de confiance peuvent toujours **afficher** les données du coffre individuel du concédant, sous réserve du flux de travail d'accès d'urgence établi.

Comment commencer à utiliser Key Connector?

Pour commencer à utiliser Key Connector pour le chiffrement géré par le client, veuillez examiner les exigences suivantes :

> ⚠ **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.

Pour utiliser Key Connector, vous devez également :

- Avoir une organisation d'entreprise .
- Avoir un serveur Bitwarden auto-hébergé .
- Avoir une implémentation active du SSO .
- Activez l'organisation unique et exigez des stratégies d'authentification unique .

Si votre organisation répond ou peut répondre à ces exigences, y compris une équipe et une infrastructure qui peuvent gérer un serveur clé, contactez-nous et nous activerons Key Connector.