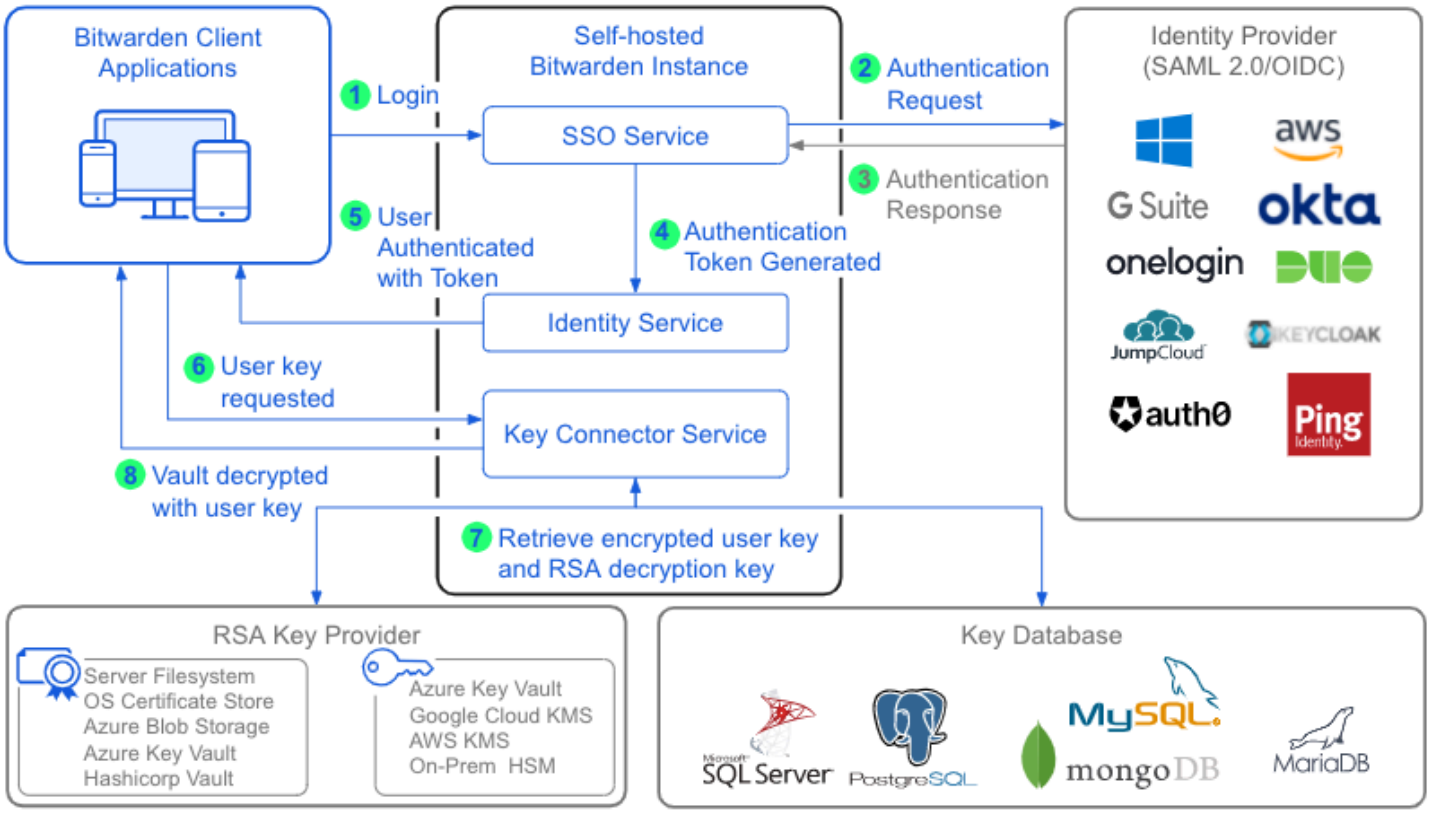
キーコネクターについて

キーコネクターについて

キーコネクターは、自己ホスト型のアプリケーションで、顧客管理型暗号化（CMS）を容易にし、
エンタープライズ組織がBitwardenクライアントに暗号鍵を提供することを可能にします。

キーコネクターは、既存のサービスと同じネットワーク上でDockerコンテナとして動作し、SSOでのログインと共に使用することで、
保管庫の復号化にマスターパスワードを必要とする代わりに、組織の暗号鍵を提供することができます(詳細はこちら)。Bitwardenは、
自己ホスト型インスタンスのための1つの組織が使用する1つのキーコネクターのデプロイメントをサポートします。

キーコネクターは、暗号化されたユーザーキーが保存されている**データベース**と、
保存されたユーザーキーを暗号化および復号化するための**RSAキーペア**に接続する必要があります。キーコネクターは、
様々なデータベースプロバイダー（例：MSSQL、PostgreSQL、MySQL）やキーペアストレージプロバイダー（例：Hashicorp 保管庫、Cloud KMS Providers、On-prem HSM デバイス）と設定することができ、
あなたのビジネスのインフラストラクチャ要件に合わせることができます。



Key Connector Architecture

なぜキーコネクターを使用するのですか？

マスター パスワードの復号化を利用する実装では、アイデンティティ プロバイダーが認証を処理し、ボールトの復号化にはメンバーのマスターパスワードが必要になります。この関心の分離は重要なステップであり、それにより組織のメンバーだけが、
組織の機密保管庫データを復号化するために必要なキーにアクセスできることを保証します。

復号化に Key Connector を利用する実装では、引き続き ID プロバイダーが認証を処理しますが、ボールトの復号化は Key Connector によって処理されます。暗号化されたキーデータベースにアクセスすることで（上記の図を参照）、
キーコネクターはユーザーがログインするときに、マスターパスワードを必要とせずに復号化キーを提供します。

私たちはしばしば、キーコネクターの実装を**顧客管理暗号化**を活用すると言及します。なぜなら、
あなたのビジネスがキーコネクターアプリケーションの管理と、それが提供する保管庫復号化キーの管理を単独で担当するからです。

エンタープライズが顧客管理の暗号化環境のデプロイと維持に準備ができている場合、
キーコネクターは保管庫へのログイン体験を効率化します。

マスターパスワードへの影響

キーコネクターはマスターパスワードによる復号化を顧客管理の復号化キーに置き換えるため、
組織のメンバーは**アカウントからマスターパスワードを削除する必要があります**。一度削除されると、
すべての保管庫復号化アクションは保存されたユーザーキーを使用して行われます。ログイン以外にも、
これはオフボーディングと他の機能に影響を与え、あなたが認識しておくべきです。

> ⚠ **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.

組織メンバーシップへの影響

Key Connector では、ユーザーはマスター パスワードを削除する必要があり、
代わりに会社所有の暗号キーのデータベースを使用してユーザーの保管庫を復号化します。マスターパスワードは、
それを削除したアカウントに対して再作成することができないため、一度アカウントがキーコネクターの復号化を使用すると、
それは事実上**組織が所有する**という意味になります。

これらのアカウントは**組亟から出ることはできません**、なぜならそうすると保管庫のデータを復号化する手段を失うからです。同様に、
組電の管理者が組織からアカウントを削除すると、アカウントは保管庫のデータを復号化する手段を失います。

他の機能への影響

機能	インパクト
確認	Bitwarden クライアント アプリケーションには、ボールト データのエクスポート、 2 段階ログイン設定の変更、 API キーの取得など、通常、使用するためにマスター パスワードの入力が必要な機能が多数あります。 **これらすべての機能は、**マスター パスワードの確認を電子メール ベースの TOTP 検証に置き換えます。
保管庫ロック/ロック解除	通常の状況下では、ロックされた保管庫はマスターパスワードを使用してロック解除できます。 あなたの組織がキーコネクターを使用している場合、 ロックされたクライアントアプリケーションは、PINまたは生体認証でのみロック解除できます。 クライアントアプリケーションにPINも生体認証も有効になっていない場合、 保管庫はロックする代わりに常にログアウトします。ロック解除とは異なり、 ログインは**常に**インターネット接続が必要です（詳細はこちら）。

機能	インパクト
マスターパスワードの再要求	キーコネクターが使用されているとき、 キーコネクターの実装の結果としてマスターパスワードを削除したユーザーに対しては、 マスターパスワードの再プロンプトが無効になります。
管理者パスワードリセット	キーコネクターが使用されているとき、 キーコネクターの実装の結果としてマスターパスワードを削除したユーザーに対して、 管理者パスワードのリセットは無効になります。
緊急アクセス	キーコネクターが使用されている場合、 キーコネクターの実装の結果としてマスターパスワードを削除したユーザーに対して、 緊急アクセスアカウントの乗っ取りオプションは無効になります。 信頼できる緊急連絡先は、設定された**緊急アクセスのワークフロー**に従って、 許可者の個々の保管庫のデータを表示することができます。

キーコネクターの使用をどのように開始しますか？

顧客管理の暗号化にキーコネクターを使用するために開始するには、以下の要件を確認してください：

> ⚠ **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.

キーコネクターを使用するためには、以下のことも必要です：

- エンタープライズ組織を持っている。
- 自己ホスト型の Bitwarden サーバーを用意します。
- アクティブな SSO 実装がある。
- 単一の組織をアクティブ化し、シングル サインオン ポリシーを要求します。

あなたの組織がこれらの要件を満たす、または満たすことができ、
キーサーバーの管理を支援できるチームとインフラストラクチャを含む場合、お問い合わせください。
私たちはキーコネクターを有効にします。