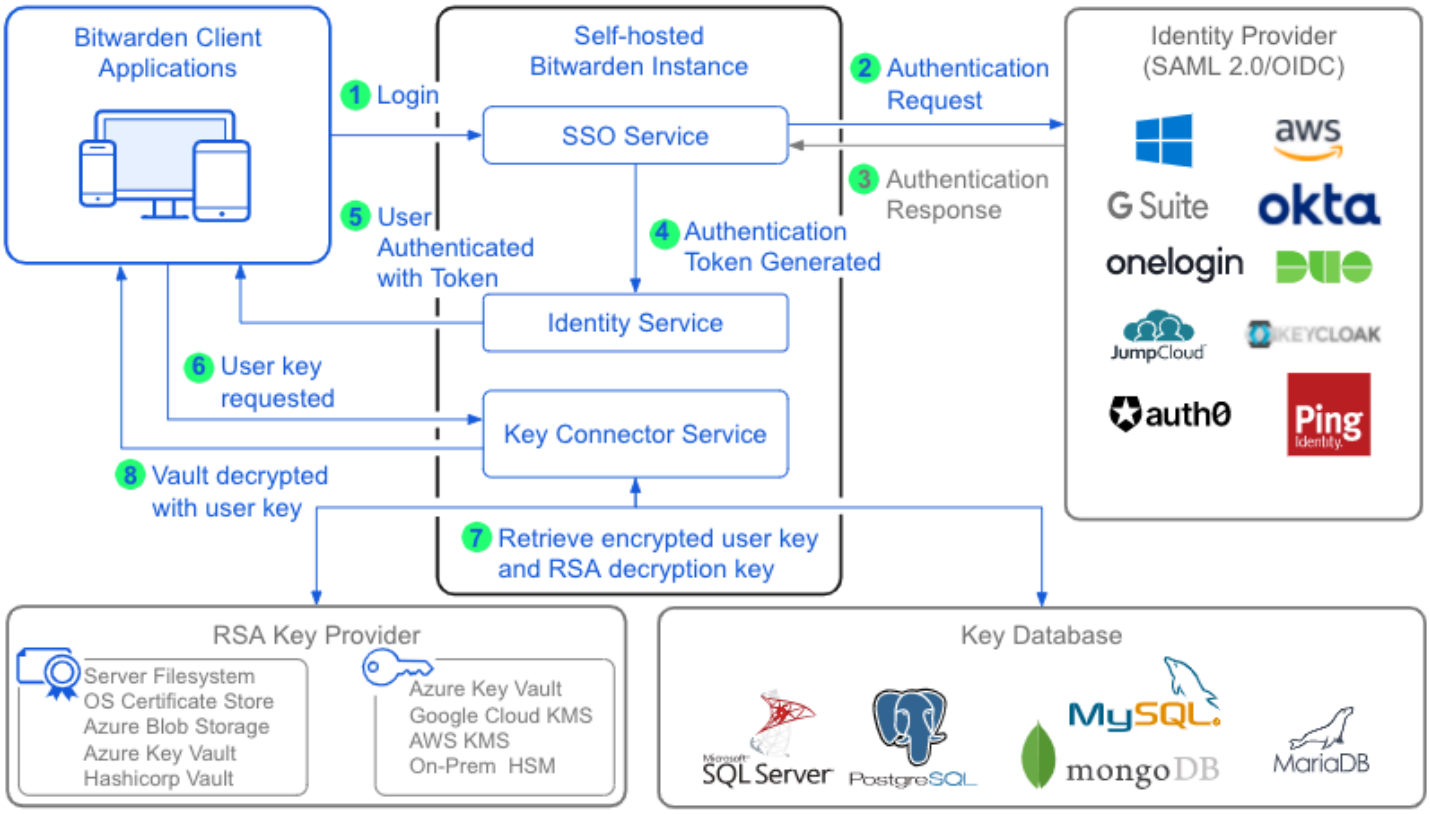
Acerca del Conector de clave

Acerca del Conector de clave

Conector de clave es una aplicación autoalojada que facilita la encriptación gestionada por el cliente (CMS), permitiendo a una organización de Empresa proporcionar claves criptográficas a los clientes de Bitwarden.

Conector de clave se ejecuta como un contenedor docker en la misma red que los servicios existentes, y se puede usar con inicio de sesión con SSO para servir claves criptográficas para una organización como una alternativa a requerir una contraseña maestra para la descifrado de la caja fuerte (aprende más). Bitwarden admite la implementación de un Conector de clave para su uso por una organización para una instancia autoalojada.

El Conector de clave requiere conexión a una **base de datos donde se almacenan las claves de usuario cifradas** y un **Par de claves RSA para cifrar y descifrar las claves de usuario almacenadas**. El Conector de clave puede ser configurado con una variedad de proveedores de bases de datos (por ejemplo, MSSQL, PostgreSQL, MySQL) y proveedores de almacenamiento de pares de claves (por ejemplo, caja fuerte de Hashicorp, Proveedores de Cloud KMS, dispositivos HSM locales) para adaptarse a los requisitos de infraestructura de su negocio.



Key Connector Architecture

¿Por qué usar el Conector de clave?

En implementaciones que aprovechan el descifrado de contraseña maestra , su proveedor de identidad maneja la autenticación y se requiere la contraseña maestra de un miembro para el descifrado de la bóveda. Esta separación de responsabilidades es un paso importante que garantiza que solo un miembro de la organización tiene acceso a la clave que se requiere para descifrar los Datos sensibles de la caja fuerte de su organización.

En las implementaciones que aprovechan Key Connector para el descifrado , su proveedor de identidad aún maneja la autenticación, pero el descifrado del almacén lo maneja Key Connector. Al acceder a una base de datos de claves cifradas (ver el diagrama anterior), el Conector de clave proporciona al usuario su clave de descifrado cuando inician sesión, sin requerir una contraseña maestra.

A menudo nos referimos a las implementaciones de Conector de Clave como el aprovechamiento de **Cifrado Gestionado por el Cliente**, porque su negocio tiene la única responsabilidad de gestionar la aplicación de Conector de Clave y las claves de descifrado de la caja fuerte que sirve. Para las empresas listas para implementar y mantener un entorno de cifrado gestionado por el cliente, el Conector de clave facilita una experiencia de inicio de sesión en la caja fuerte simplificada.

Impacto en las contraseñas maestras

Debido a que el Conector de clave reemplaza el descifrado basado en la contraseña maestra con las claves de descifrado gestionadas por el cliente, se requerirá que los miembros de la organización **eliminen la contraseña maestra de su cuenta**. Una vez eliminado, todas las acciones de descifrado de la caja fuerte se realizarán utilizando la clave de usuario almacenada. Además de iniciar sesión, esto tendrá algunos impactos en la desvinculación y en otras funcionalidades de las que deberías estar consciente.

> ⚠ **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.

Impacto en la membresía de la organización

El Conector de clave requiere que los usuarios eliminen sus contraseñas maestras y en su lugar utiliza una base de datos propiedad de la empresa de claves criptográficas para descifrar las cajas fuertes de los usuarios. Debido a que las contraseñas maestras no pueden ser recreadas para cuentas que las han eliminado, esto significa que una vez que una cuenta utiliza la desencriptación del Conector de clave, para todos los efectos y propósitos **es propiedad de la organización**.

Estas cuentas **no pueden abandonar la organización**, ya que al hacerlo perderían cualquier medio para descifrar los datos de la caja fuerte. De manera similar, si un administrador de la organización elimina la cuenta de la organización, la cuenta perderá cualquier medio para descifrar los datos de la caja fuerte.

Impacto en otras funcionalidades

Funcionalidad	Impacto
Verificación	Hay un número de funcionalidades en las aplicaciones cliente de Bitwarden que normalmente requieren la entrada de una contraseña maestra para ser utilizadas, incluyendo exportar los datos de la caja fuerte, cambiar los ajustes de inicio de sesión en dos pasos, recuperar las claves API, y más. **Todas estas funciones** reemplazarán la confirmación de la contraseña maestra con la verificación TOTP basada en correo electrónico.

Funcionalidad	Impacto
Bloquear/desbloquear caja fuerte	Bajo circunstancias ordinarias, una caja fuerte bloqueada puede ser desbloqueada utilizando una contraseña maestra. Cuando su organización está utilizando el Conector de clave, las aplicaciones de cliente bloqueadas solo pueden ser desbloqueadas con un PIN o con biométrica. Si ni el PIN ni la biométrica están habilitados para una aplicación de cliente, la caja fuerte siempre cerrará sesión en lugar de bloquear. A diferencia de desbloquear, iniciar sesión **siempre** requiere una conexión a internet (aprende más).
Volver a preguntar contraseña maestra	Cuando se utiliza el Conector de clave, se desactivará la solicitud de nuevo de la contraseña maestra para cualquier usuario que haya eliminado su contraseña maestra como resultado de su implementación del Conector de clave.
Restablecimiento de contraseña del administrador	Cuando se utiliza el Conector de clave, el restablecimiento de la contraseña del administrador se desactivará para cualquier usuario que haya eliminado su contraseña maestra como resultado de su implementación del Conector de clave.
Acceso de emergencia	Cuando se utiliza el Conector de clave, la opción de toma de control de la cuenta de acceso de emergencia se desactivará para cualquier usuario que haya eliminado su contraseña maestra como resultado de su implementación del Conector de clave. Los contactos de emergencia de confianza aún pueden **ver** los datos de la caja fuerte individual del otorgante, sujetos al flujo de trabajo de acceso de emergencia establecido.

¿Cómo empiezo a usar el Conector de clave?

Para comenzar a usar el Conector de clave para la encriptación gestionada por el cliente, por favor revise los siguientes requisitos:

> ⚠ **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.

Para usar el Conector de clave también debes:

- Tener una organización empresarial .
- Tener un servidor Bitwarden autohospedado .
- Tener una implementación SSO activa .
- Active la organización única y exija políticas de inicio de sesión único .

Si su organización cumple o puede cumplir con estos requisitos, incluyendo un equipo e infraestructura que pueden gestionar un servidor clave, contáctenos y activaremos el Conector de clave.