Über vertrauenswürdige Geräte

Über vertrauenswürdige Geräte

SSO mit vertrauenswürdigen Geräten ermöglicht es Benutzern, sich mit SSO zu authentifizieren und ihren Tresor mit einem auf dem Gerät gespeicherten Verschlüsselungsschlüssel zu entschlüsseln, wodurch die Notwendigkeit entfällt, ein Master-Passwort einzugeben. Vertrauenswürdige Geräte müssen entweder im Voraus der Anmeldeversuch registriert werden, oder durch ein paar verschiedene Methoden genehmigt werden.

SSO mit vertrauenswürdigen Geräten bietet Geschäftsendbenutzern ein passwortloses Erlebnis, das auch Zero-Knowledge und Ende-zu-Ende verschlüsselt ist. Dies verhindert, dass Benutzer aufgrund vergessener Master-Passwörter gesperrt werden und ermöglicht ihnen ein vereinfachtes Erlebnis mit den Zugangsdaten.

Beginnen Sie mit der Verwendung von vertrauenswürdigen Geräten.

Um die Verwendung von SSO mit vertrauenswürdigen Geräten zu starten:

1. Richten Sie SSO mit vertrauenswürdigen Geräten für Ihr Unternehmen ein.
2. Stellen Sie Administratoren Informationen darüber zur Verfügung, wie sie Geräteanfragen genehmigen können.
3. Stellen Sie Endbenutzern Informationen darüber zur Verfügung, wie man vertrauenswürdige Geräte hinzufügt.

Wie es funktioniert

Die folgenden Tabs beschreiben Verschlüsselungsprozesse und Schlüsselaustausche, die während verschiedener Verfahren mit vertrauenswürdigen Geräten auftreten:

⇒Einarbeitung

Wenn ein neuer Benutzer einer Organisation beitritt, wird ein **Wiederherstellungsschlüssel für das Konto** (mehr erfahren) erstellt, indem ihr Kontoverschlüssel mit dem öffentlichen Schlüssel der Organisation verschlüsselt wird. Die Wiederherstellung des Kontos ist erforderlich, um SSO mit vertrauenswürdigen Geräten zu ermöglichen.

Dann wird der Benutzer gefragt, ob er sich an das Gerät erinnern oder ihm vertrauen möchte. Wenn sie sich dafür entscheiden:

1. Ein neuer **Geräteschlüssel** wird vom Client generiert. Dieser Schlüssel verlässt den Client nie.
2. Ein neues RSA-Schlüsselpaar, **Gerät Privatschlüssel** und **Gerät Öffentlicher Schlüssel**, wird vom Client generiert.
3. Der Verschlüsselungsschlüssel des Benutzerkontos wird mit dem unverschlüsselten öffentlichen Schlüssel des Geräts verschlüsselt und der resultierende Wert wird als **öffentlich verschlüsselter Benutzerschlüssel** an den Server gesendet.
4. Der **öffentliche Schlüssel des Geräts** wird mit dem Verschlüsselungsschlüssel des Benutzerkontos verschlüsselt und der resultierende Wert wird als **Benutzerschlüssel-verschlüsselter öffentlicher Schlüssel** an den Server gesendet.
5. Der **Gerät Privatschlüssel** wird mit dem ersten **Geräteschlüssel** verschlüsselt und der resultierende Wert wird als der **Geräteschlüssel-verschlüsselter Privatschlüssel** an den Server gesendet.

Der **mit dem öffentlichen Schlüssel verschlüsselte Benutzerschlüssel** und der **mit dem Geräteschlüssel verschlüsselte private Schlüssel** werden entscheidend vom Server zum Client gesendet, wenn eine Anmeldung initiiert wird.

Der **Benutzerschlüssel-verschlüsselter öffentlicher Schlüssel** wird verwendet, wenn der Benutzer seinen Konto-Verschlüsselungsschlüssel erneuern muss.

⇒Anmelden

Wenn ein Benutzer sich mit SSO auf einem bereits vertrauenswürdigen Gerät authentifiziert:

1. Der vom Server an den Client gesendete **öffentlich verschlüsselte Benutzerschlüssel**, der eine verschlüsselte Version des Kontoverschlüsselungsschlüssels ist, der zum Entschlüsseln von Tresor-Daten verwendet wird.

2. Der **Geräteschlüssel-verschlüsselter privater Schlüssel** des Benutzers, dessen unverschlüsselte Version benötigt wird, um den **öffentlichen Schlüssel-verschlüsselten Benutzerschlüssel** zu entschlüsseln, wird vom Server an den Client gesendet.

3. Der Client entschlüsselt den **Geräteschlüssel-verschlüsselten privaten Schlüssel** mit dem **Geräteschlüssel**, der niemals den Client verlässt.

4. Der jetzt unverschlüsselte **Gerät Privatschlüssel** wird verwendet, um den **mit dem öffentlichen Schlüssel verschlüsselten Benutzerschlüssel** zu entschlüsseln, was in dem Verschlüsselungsschlüssel des Benutzerkontos resultiert.

5. Der Verschlüsselungsschlüssel des Benutzerkontos entschlüsselt die Daten im Tresor.

⇒Genehmigend

Wenn ein Benutzer sich mit SSO authentifiziert und sich dafür entscheidet, seinen Tresor mit einem nicht vertrauenswürdigen Gerät zu entschlüsseln (d.h. ein **Gerätesymmetrischer Schlüssel** existiert nicht auf diesem Gerät), muss er eine Methode zur Genehmigung des Geräts auswählen und kann es optional für die zukünftige Nutzung ohne weitere Genehmigung als vertrauenswürdig einstufen. Was als nächstes passiert, hängt von der ausgewählten Option ab:

- **Von einem anderen Gerät aus genehmigen** :
  1. Der in diesem Dokument beschriebene Prozess wird ausgelöst, was dazu führt, dass der Client den Verschlüsselungsschlüssel für das Konto erhalten und entschlüsselt hat.
  2. Der Benutzer kann jetzt seine Tresor Daten mit dem entschlüsselten Konto-Verschlüsselungsschlüssel entschlüsseln. Wenn sie sich entschieden haben, dem Gerät zu vertrauen, wird das Vertrauen mit dem Client hergestellt, wie im **Onboarding** Tab beschrieben.

- **Administrator Genehmigung anfordern**
  1. Der initiierende Client sendet eine POST-Anfrage, die die E-Mail-Adresse des Kontos, einen einzigartigen **auth-request öffentlichen Schlüssel**[a] und einen Zugangscode enthält, an eine Authentifizierungsanforderungstabelle in der Bitwarden-Datenbank.
  2. Administratoren können die Anfrage auf der Gerät-Freigabeseite genehmigen oder ablehnen.
  3. Wenn die Anfrage von einem Administrator genehmigt wird, verschlüsselt der genehmigende Client den Verschlüsselungsschlüssel des Benutzerkontos mit dem im Antrag enthaltenen **auth-request öffentlichen Schlüssel**.
  4. Der genehmigende Client stellt dann den verschlüsselten Kontoschlüssel in den Authentifizierungsanforderungsdatensatz und markiert die Anforderung als erfüllt.
  5. Der initiierende Client GETs den verschlüsselten Konto-Verschlüsselungsschlüssel und entschlüsselt ihn **lokal** mit dem **Auth-Anfrage-Privatschlüssel**.
  6. Mit dem entschlüsselten Verschlüsselungsschlüssel des Kontos wird das Vertrauen mit dem Client hergestellt, wie im **Onboarding** Tab beschrieben.

[a] - **Auth-Anforderung öffentlicher** und **privater Schlüssel** werden einzigartig für jede Anfrage ohne Zugangsdaten generiert und existieren nur so lange wie die Anfrage selbst. Nicht genehmigte Anfragen verfallen nach 1 Woche.

- **Genehmigen mit Master-Passwort**

1. Der Verschlüsselungsschlüssel des Benutzerkontos wird abgerufen und entschlüsselt, wie im Abschnitt Benutzerzugangsdaten des Sicherheits-Whitepapers dokumentiert.

2. Mit dem entschlüsselten Verschlüsselungsschlüssel des Kontos wird das Vertrauen zum Client hergestellt, wie im **Onboarding** Tab beschrieben.

⇒Schlüsselerneuerung

> **Note**
> Nur Benutzer, die ein Master-Passwort haben, können ihren Verschlüsselungsschlüssel für das Konto erneuern. Erfahren Sie mehr.

Wenn ein Benutzer seinen Konto-Verschlüsselungsschlüssel erneuert, während des normalen Erneuerungsprozesses:

1. Der **Benutzerschlüssel-verschlüsselter öffentlicher Schlüssel** wird vom Server an den Client gesendet und anschließend mit dem alten Konto-Verschlüsselungsschlüssel (auch bekannt als) entschlüsselt. **Benutzerschlüssel**), was zur **Gerät-Öffentlicher Schlüssel** führt.

2. Der neue Verschlüsselungsschlüssel des Benutzerkontos wird mit dem unverschlüsselten öffentlichen Schlüssel des Geräts verschlüsselt und der resultierende Wert wird als neuer **öffentlich verschlüsselter Benutzerschlüssel** an den Server gesendet.

3. Der **öffentliche Schlüssel des Geräts** wird mit dem neuen Verschlüsselungsschlüssel des Benutzerkontos verschlüsselt und der resultierende Wert wird als neuer **Benutzerschlüssel-verschlüsselter öffentlicher Schlüssel** an den Server gesendet.

4. Vertrauenswürdige Verschlüsselungsschlüssel für Geräte für alle anderen Geräte, die auf dem Server gespeichert sind, werden für den Benutzer gelöscht. Dies lässt nur die drei erforderlichen Schlüssel (**Öffentlicher Schlüssel-verschlüsselter Benutzerschlüssel**, **Benutzerschlüssel-verschlüsselter öffentlicher Schlüssel** und **Geräteschlüssel-verschlüsselter privater Schlüssel**, der durch diesen Prozess nicht geändert wurde) für dieses einzelne Gerät auf dem Server bestehen.

Jeder jetzt nicht vertrauenswürdige Client muss das Vertrauen durch eine der in der **Genehmigen** Tab beschriebenen Methoden wiederherstellen.

Schlüssel für vertrauenswürdige Geräte

Diese Tabelle bietet weitere Informationen zu jedem in den oben beschriebenen Verfahren verwendeten Schlüssel:

Schlüssel	Einzelheiten
Geräteschlüssel	AES-256 CBC HMAC SHA-256, 512 Bit lang (256 Bit für den Schlüssel, 256 Bit für HMAC)
Gerät Privatschlüssel & Gerät Öffentlicher Schlüssel	RSA-2048 OAEP SHA1, 2048 Bits lang
Öffentlich verschlüsselter Benutzerschlüssel	RSA-2048 OAEP SHA1

Schlüssel	Einzelheiten
Benutzerschlüssel-verschlüsselter öffentlicher Schlüssel	AES-256 CBC HMAC SHA-256
Geräteschlüssel-verschlüsselter Privatschlüssel	AES-256 CBC HMAC SHA-256

Auswirkungen auf Master-Passwörter

Während SSO mit vertrauenswürdigen Geräten die Notwendigkeit eines Master-Passworts beseitigt, beseitigt es nicht in allen Fällen das Master-Passwort selbst:

- Wenn ein Benutzer **vor** der Aktivierung von SSO mit vertrauenswürdigen Geräten an Bord gebracht wird, oder wenn sie **Konto erstellen** aus der Organisationseinladung auswählen, behält ihr Konto sein Master-Passwort.
- Wenn ein Benutzer onboarding **nach** der Aktivierung von SSO mit vertrauenswürdigen Geräten durchführt und sie **Anmelden** → **Enterprise SSO** aus der Einladung der Organisation für JIT-Provisioning auswählen, wird ihr Konto kein Master-Passwort haben.

> ⚠ **Warning**
>
> Für jene Konten, die aufgrund von SSO mit vertrauenswürdigen Geräten kein Master-Passwort haben, wird ihre Entfernung aus Ihrer Organisation oder die Widerrufung ihres Zugangs jeglichen Zugang zu ihrem Bitwarden-Konto unterbinden, es sei denn:
>
> 1. Sie weisen ihnen vorher ein Master-Passwort zu, indem Sie die Kontowiederherstellung verwenden.
> 2. Der Benutzer meldet sich mindestens einmal nach der Konto-Wiederherstellung an, um den Workflow zur Konto-Wiederherstellung vollständig abzuschließen.

Auswirkungen auf andere Funktionen

Abhängig davon, ob ein Master-Passwort-Hash im Speicher für Ihren Client verfügbar ist, was davon abhängt, wie Ihre Client-Anwendung ursprünglich aufgerufen wird, kann es folgende Verhaltensänderungen zeigen:

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. Wenn der Benutzer kein Master-Passwort verwendet, um auf den Client zuzugreifen, ersetzen **all diese Funktionen** die Bestätigung des Master-Passworts durch eine E-Mail-basierte TOTP-Verifizierung.

Funktion	Aufprall
Tresor sperren/entsperren	Unter normalen Umständen kann ein gesperrter Tresor entsperrt werden, indem man ein Master-Passwort verwendet. Wenn der Benutzer kein Master-Passwort verwendet, um auf den Client zuzugreifen, 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. Zum Entsperren und Anmelden ist **immer** eine Internetverbindung erforderlich.
Master-Passwort erneut abfragen	Wenn der Benutzer seinen Tresor nicht mit einem Master-Passwort entsperrt, wird die erneute Aufforderung des Master-Passworts deaktiviert.
Kommandozeile	Benutzer, die kein Master-Passwort haben, **werden nicht** in der Lage sein, auf den Passwort-Manager CLI zuzugreifen.