Over vertrouwde apparaten

Over vertrouwde apparaten

Met SSO met vertrouwde apparaten kunnen gebruikers zich verifiëren met SSO en hun kluis ontsleutelen met behulp van een versleutelingscode die op het apparaat is opgeslagen, waardoor het niet meer nodig is om een hoofdwachtwoord in te voeren. Vertrouwde apparaten moeten worden geregistreerd voordat ze proberen in te loggen of moeten worden goedgekeurd via een aantal verschillende methoden.

SSO met vertrouwde apparaten geeft zakelijke eindgebruikers een wachtwoordloze ervaring die ook zero-knowledge en end-to-end versleuteld is. Dit voorkomt dat gebruikers worden buitengesloten door vergeten hoofdwachtwoorden en zorgt voor een gestroomlijnde aanmeldervaring.

Vertrouwde apparaten gaan gebruiken

Om aan de slag te gaan met SSO met vertrouwde apparaten:

1. SSO instellen met vertrouwde apparaten voor uw organisatie.
2. Voorzie beheerders van informatie over het goedkeuren van apparaataanvragen.
3. Geef eindgebruikers informatie over hoe ze vertrouwde apparaten kunnen toevoegen.

Hoe het werkt

De volgende tabbladen beschrijven versleutelingsprocessen en sleuteluitwisselingen die plaatsvinden tijdens verschillende procedures voor vertrouwde apparaten:

⇒Inwerken

Wanneer een nieuwe gebruiker zich aansluit bij een organisatie, wordt een **Account Recovery Key**(meer informatie) gemaakt door de coderingssleutel van hun account te versleutelen met de openbare sleutel van de organisatie. Accountherstel is vereist om SSO met vertrouwde apparaten mogelijk te maken.

De gebruiker wordt vervolgens gevraagd of hij het apparaat wil onthouden of vertrouwen. Als ze daarvoor kiezen:

1. De client genereert een nieuwe **Device Key** . Deze sleutel verlaat de client nooit.
2. Een nieuw RSA sleutelpaar, **de Device Private Key** en **de Device Public Key**, wordt gegenereerd door de client.
3. De coderingssleutel van de gebruikersaccount wordt versleuteld met de onversleutelde Device Public Key en de resulterende waarde wordt naar de server gestuurd als de **Public Key-Encrypted User Key**.
4. De **openbare sleutel van het apparaat** wordt versleuteld met de coderingssleutel van de gebruikersaccount en de resulterende waarde wordt naar de server gestuurd als de **versleutelde openbare sleutel van de gebruikerssleutel**.
5. De **privésleutel van het apparaat** wordt versleuteld met de eerste **apparaatsleutel** en de resulterende waarde wordt naar de server verzonden als de **versleutelde privésleutel van de apparaatsleutel**.

De **openbare sleutel versleutelde gebruikerssleutel** en **de apparaatsleutel versleutelde privésleutel** worden van cruciaal belang van de server naar de client verzonden wanneer er wordt aangemeld.

De **versleutelde openbare sleutel van de gebruikerssleutel** wordt gebruikt als de gebruiker de versleutelingscode van zijn account moet draaien.

⇒Inloggen

Als een gebruiker zich verifieert met SSO op een apparaat dat al vertrouwd is:

1. De **Public Key-Encrypted User Key** van de gebruiker, een versleutelde versie van de encryptiesleutel van de account die wordt gebruikt om kluisgegevens te ontsleutelen, wordt van de server naar de client gestuurd.

2. De **Device Key-gecodeerde privésleutel** van de gebruiker, waarvan de ongecodeerde versie nodig is om de **Public Key-gecodeerde gebruikerssleutel** te decoderen, wordt van de server naar de client gestuurd.

3. De client decodeert de **versleutelde privésleutel** met behulp van de **Device Key**, die de client nooit verlaat.

4. De nu onversleutelde **Device Private Key** wordt gebruikt om de **Public Key-Encrypted User Key** te ontsleutelen, wat resulteert in de versleutelingssleutel van de gebruikersaccount.

5. De accountcoderingssleutel van de gebruiker ontsleutelt de kluisgegevens.

⇒Goedkeuring

Als een gebruiker zich verifieert met SSO en ervoor kiest om zijn kluis te ontsleutelen met een niet-vertrouwd apparaat (d.w.z. er bestaat geen **Device Symmetric Key** op dat apparaat), dan moet hij een methode kiezen om het apparaat goed te keuren en optioneel te vertrouwen voor toekomstig gebruik zonder verdere goedkeuring. Wat er vervolgens gebeurt, hangt af van de geselecteerde optie:

- **Goedkeuren vanaf een ander apparaat**:
    1. Het proces dat hier wordt gedocumenteerd, wordt geactiveerd, wat ertoe leidt dat de cliënt de coderingssleutel van de account heeft verkregen en gedecodeerd.

    2. De gebruiker kan nu zijn kluisgegevens ontsleutelen met de ontsleutelde coderingssleutel van de account. Als ze ervoor hebben gekozen om het apparaat te vertrouwen, wordt er vertrouwen opgebouwd met de client zoals beschreven in het tabblad **Onboarding** .

- **Administratieve goedkeuring aanvragen**:
    1. De initiërende cliënt POST een verzoek, met daarin het e-mailadres van het account, een unieke **openbare sleutel[α] van het auth-verzoek** en een toegangscode, naar een Authenticatieverzoek-tabel in de Bitwarden database.

    2. Beheerders kunnen het verzoek goedkeuren of afwijzen op de pagina Apparaatgoedkeuringen.

    3. Als het verzoek wordt goedgekeurd door een beheerder, versleutelt de goedkeurende client de coderingssleutel van de gebruikersaccount met behulp van de **openbare sleutel van de auth-request** die in het verzoek is ingesloten.

    4. De goedkeurende client PUT vervolgens de versleutelde coderingssleutel van de account naar de Authentication Request record en markeert het verzoek als voldaan.

    5. De initiërende cliënt GET de versleutelde coderingssleutel van de account en ontsleutelt deze **lokaal** met de **privésleutel van de auth-request**.

    6. Met behulp van de ontsleutelde coderingssleutel van de account wordt vertrouwen opgebouwd met de klant zoals beschreven in het tabblad **Onboarding** .

[α] - **Auth-request publieke** en **privésleutels** worden uniek gegenereerd voor elke wachtwoordloze aanmeldingsaanvraag en bestaan alleen zolang de aanvraag bestaat. Niet-goedgekeurde verzoeken vervallen na 1 week.

- **Goedkeuren met hoofdwachtwoord**:
    1. De encryptiesleutel van de gebruikersaccount wordt opgehaald en gedecodeerd zoals gedocumenteerd in het gedeelte Gebruikersaanmelding van de Whitepaper Beveiliging.

2. Met behulp van de ontsleutelde coderingssleutel van de account wordt vertrouwen opgebouwd met de klant zoals beschreven in het tabblad **Onboarding** .

⇒Sleutelomwenteling

> **Note**
> Alleen gebruikers met een hoofdwachtwoord kunnen de coderingssleutel van hun account draaien. Meer informatie.

Wanneer een gebruiker zijn accountcoderingssleutel roteert, tijdens het normale rotatieproces:

1. De **versleutelde openbare sleutel van de gebruikerssleutel** wordt van de server naar de client gestuurd en vervolgens ontsleuteld met de oude versleutelingssleutel van de account (ook bekend als de versleutelde openbare sleutel van de server). **Gebruikerssleutel**), wat resulteert in de **openbare sleutel van het apparaat**.

2. De nieuwe coderingssleutel van de gebruiker wordt versleuteld met de onversleutelde Device Public Key en de resulterende waarde wordt naar de server gestuurd als de nieuwe **Public Key-Encrypted User Key**.

3. De **openbare sleutel van het apparaat** wordt versleuteld met de nieuwe coderingssleutel van de account van de gebruiker en de resulterende waarde wordt naar de server gestuurd als de nieuwe **openbare sleutel van de gebruikerssleutel**.

4. Encryptiesleutels voor vertrouwde apparaten voor alle andere apparaten die naar de serveropslag worden doorgezet, worden voor de gebruiker gewist. Hierdoor blijven alleen de drie benodigde sleutels**(Openbare sleutel-gecodeerde gebruikerssleutel**, **Gebruikerssleutel-gecodeerde openbare sleutel** en **Apparaat-sleutel-gecodeerde privésleutel** die niet door dit proces is gewijzigd) voor dat ene apparaat op de server staan.

Elke client die nu niet meer wordt vertrouwd, moet het vertrouwen herstellen via een van de methoden die worden beschreven op het tabblad **Goedkeuren** .

Sleutels gebruikt voor vertrouwde apparaten

Deze tabel geeft meer informatie over elke sleutel die wordt gebruikt in de hierboven beschreven procedures:

Sleutel	Details
Toets apparaat	AES-256 CBC HMAC SHA-256, 512 bits lang (256 bits voor sleutel, 256 bits voor HMAC)
Particuliere sleutel en openbare sleutel van apparaat	RSA-2048 OAEP SHA1, 2048 bits lang
Openbare sleutel-gecodeerde gebruikerssleutel	RSA-2048 OAEP SHA1
Gebruikerssleutel-Gecodeerde openbare sleutel	AES-256 CBC HMAC SHA-256

Sleutel	Details
Versleutelde privé-sleutel van apparaat	AES-256 CBC HMAC SHA-256

Invloed op hoofdwachtwoorden

Hoewel SSO met vertrouwde apparaten de noodzaak voor een hoofdwachtwoord elimineert, elimineert het niet in alle gevallen het hoofdwachtwoord zelf:

- Als een gebruiker aan boord is **voordat** SSO met vertrouwde apparaten is geactiveerd, of als hij **account maken** selecteert in de organisatie-uitnodiging, dan behoudt zijn account zijn hoofdwachtwoord.
- Als een gebruiker wordt aangemeld **nadat** SSO met vertrouwde apparaten is geactiveerd en hij/zij **Log in** → **Enterprise SSO** selecteert vanuit de organisatie-uitnodiging voor JIT-provisioning, dan heeft zijn/haar account geen hoofdwachtwoord.

> ⚠ **Warning**
>
> Voor accounts die geen hoofdwachtwoord hebben als gevolg van SSO met vertrouwde apparaten, zal het verwijderen uit uw organisatie of het intrekken van hun toegang alle toegang tot hun Bitwarden-account afsluiten, tenzij:
>
> 1. Je wijst hen vooraf een hoofdwachtwoord toe met behulp van accountherstel.
> 2. De gebruiker logt ten minste één keer in na het accountherstel om de workflow voor accountherstel volledig te voltooien.

Invloed op andere functies

Afhankelijk van het feit of een hoofdwachtwoord hash beschikbaar is in het geheugen voor je client, wat wordt bepaald door hoe je clienttoepassing initieel wordt benaderd, kan het de volgende gedragsveranderingen vertonen:

Functie	Impact
Verificatie	Er zijn een aantal functies in Bitwarden-clienttoepassingen waarvoor normaal gesproken een hoofdwachtwoord moet worden ingevoerd om ze te kunnen gebruiken, zoals het exporteren van kluisgegevens, het wijzigen van de instellingen voor tweestapsaanmelding, het ophalen van API-sleutels en meer. Als de gebruiker geen hoofdwachtwoord gebruikt om toegang te krijgen tot de client, zullen **al deze functies** de bevestiging van het hoofdwachtwoord vervangen door TOTP-verificatie via e-mail.
Kluis vergrendelen/ontgrendelen	Onder normale omstandigheden kan een vergrendelde kluis worden ontgrendeld met een hoofdwachtwoord. Als de gebruiker geen hoofdwachtwoord gebruikt om toegang te krijgen tot de client, kunnen vergrendelde clienttoepassingen alleen worden ontgrendeld met een PIN-code of met biometrische gegevens.

Functie	Impact
	Als noch PIN noch biometrie zijn ingeschakeld voor een clienttoepassing, zal de kluis altijd uitloggen in plaats van vergrendelen. Voor ontgrendelen en inloggen is **altijd** een internetverbinding nodig.
Hoofdwachtwoord opnieuw vragen	Als de gebruiker zijn kluis niet ontgrendelt met een hoofdwachtwoord, zal de herprompt van het hoofdwachtwoord uitgeschakeld worden.
CLI	Gebruikers die geen hoofdwachtwoord hebben , hebben geen toegang tot Password Manager CLI.