bitwarden | Artikel Helpcentrum

BEVEILIGING

Encryptie

Weergeven in het Helpcentrum:
https://bitwarden.com/help/what-encryption-is-used/

Encryptie

Bitwarden gebruikt AES-CBC 256-bits encryptie voor uw kluisgegevens en PBKDF2 SHA-256 of Argon2 om uw encryptiesleutel af te leiden.

Bitwarden versleutelt en/of hasht uw gegevens **altijd** op uw lokale apparaat voordat iets naar cloudservers wordt verzonden voor opslag. **Bitwarden-servers worden alleen gebruikt voor het opslaan van versleutelde gegevens.** Zie Opslag voor meer informatie.

Kluisgegevens kunnen alleen worden ontsleuteld met de sleutel die is afgeleid van je hoofdwachtwoord. Bitwarden is een zero knowledge-encryptieoplossing, wat betekent dat u de enige partij bent met toegang tot uw sleutel en de mogelijkheid om uw kluisgegevens te ontsleutelen.

> **Tip**
>
> We raden u aan onze Interactieve Cryptografie-pagina te bezoeken om zelf te zien hoe Bitwarden uw gegevens versleutelt.
>
> Als je meer wilt weten over hoe deze encryptiesleutels worden gebruikt om je kluis te beschermen, kun je ook onze Security Whitepaper bekijken.

AES-CBC

AES-CBC (cipher block chaining), gebruikt om kluisgegevens te versleutelen, is een standaard in cryptografie en wordt gebruikt door de Amerikaanse overheid en andere overheidsinstellingen over de hele wereld voor het beschermen van topgeheime gegevens. Met de juiste implementatie en een sterke encryptiesleutel (je hoofdwachtwoord), wordt AES als onbreekbaar beschouwd.

PBKDF2

PBKDF2 SHA-256 wordt gebruikt om de coderingssleutel van je hoofdwachtwoord af te leiden, maar je kunt ook Argon2 als alternatief kiezen. Bitwarden verzilt en hashed uw hoofdwachtwoord met uw e-mailadres **lokaal**, voordat het naar onze servers wordt verzonden. Zodra een Bitwarden-server het gehashte wachtwoord ontvangt, wordt het opnieuw gezouten met een cryptografisch veilige willekeurige waarde, opnieuw gehasht en opgeslagen in onze database.

De standaard iteratietelling die wordt gebruikt met PBKDF2 is 600.001 iteraties op de client (de iteratietelling aan de clientkant is instelbaar via je accountinstellingen), en dan nog eens 100.000 iteraties als het wordt opgeslagen op onze servers (standaard in totaal 700.001 iteraties). De organisatiesleutel wordt gedeeld via RSA-2048.

> **Tip**
>
> Het aantal standaard iteraties dat wordt gebruikt door Bitwarden is verhoogd in februari 2023. Accounts die na die tijd zijn aangemaakt, zullen 600.001 gebruiken, maar als je je account voor die tijd hebt aangemaakt, moet je het aantal iteraties verhogen. Instructies hiervoor vindt u in de volgende sectie.

De gebruikte hashfuncties zijn eenrichtingshashes, wat betekent dat ze **niet kunnen worden omgekeerd** door iemand bij Bitwarden om uw hoofdwachtwoord te onthullen. Zelfs als Bitwarden gehackt zou worden, is er geen methode waarmee uw hoofdwachtwoord verkregen zou kunnen worden.

KDF iteraties wijzigen

Bitwarden gebruikt een veilige standaardinstelling, zoals hierboven vermeld, maar u kunt het aantal iteraties wijzigen via het menu **Instellingen** → **Beveiliging** → **Sleutels** van de webkluis.

Het veranderen van het aantal iteraties kan helpen om je hoofdwachtwoord te beschermen tegen brute forcering door een aanvaller, maar moet niet worden gezien als een vervanging voor het gebruik van een sterk hoofdwachtwoord. Het veranderen van de iteratieteller zal de beschermde symmetrische sleutel opnieuw versleutelen en de authenticatie hash updaten, net zoals een normale hoofdwachtwoord

verandering, maar zal de symmetrische coderingssleutel niet roteren zodat kluisgegevens niet opnieuw versleuteld worden. Kijk hier voor informatie over het opnieuw versleutelen van je gegevens.

Als u uw KDF iteraties te hoog instelt, kan dit leiden tot slechte prestaties bij het aanmelden bij (en ontgrendelen van) Bitwarden op apparaten met langzamere CPU's. We raden aan de waarde te verhogen in stappen van 100.000 en vervolgens al je apparaten te testen.

Als je de iteratieteller wijzigt, word je afgemeld bij alle clients. Hoewel het risico van het roteren van je encryptiesleutel niet bestaat bij het wijzigen van het aantal KDF iteraties, raden we toch aan om je vault vooraf te exporteren.

Argon2id

Argon2, de winnaar van de 2015 Password Hashing Competition, is beschikbaar als alternatief voor PBKDF2(meer informatie). Er zijn drie versies van het algoritme en Bitwarden heeft Argon2id geïmplementeerd zoals aanbevolen door OWASP. Argon2id is een hybride van andere versies en gebruikt een combinatie van data-afhankelijke en data-onafhankelijke geheugentoegang. Hierdoor heeft het iets van de weerstand van Argon2i tegen side-channel cache timing aanvallen en veel van de weerstand van Argon2d tegen GPU cracking aanvallen(bron).

Standaard is Bitwarden ingesteld om 64 MB geheugen toe te wijzen, er 3 keer overheen te gaan en dit over 4 threads te doen. Deze standaardinstellingen liggen boven de huidige aanbevelingen van OWASP, maar hier volgen enkele tips voor het geval je ervoor kiest om je instellingen te wijzigen:

- Als **de KDF iteraties** toenemen, neemt de looptijd lineair toe.
- De hoeveelheid **KDF parallellisme** die je kunt gebruiken hangt af van de CPU van je machine. Over het algemeen is Max. Parallellisme = aantal cores x 2.

> **Note**
>
> Argon2id gebruikers met een KDF geheugenwaarde hoger dan 48 MB krijgen een waarschuwingsdialoog elke keer als iOS autofill wordt gestart of een nieuwe Send wordt aangemaakt via het Share sheet. Om deze melding te voorkomen, moet u de instellingen van Argon2id aanpassen of ontgrendelen met biometrie inschakelen.

Aangevraagde cryptobibliotheken

Bitwarden schrijft geen cryptografische code. Bitwarden gebruikt alleen crypto van populaire en gerenommeerde cryptobibliotheken die zijn geschreven en worden onderhouden door cryptografie-experts. De volgende cryptobibliotheken worden gebruikt:

- JavaScript (webaanval, browserextensie, desktop en CLI)
  - Webcrypto
  - Node.js crypto
  - Smederij
- C# (Mobiel)
  - CommonCrypto (iOS, Apple)
  - Javax.Crypto (Android, Oracle)
  - Springkasteel (Android)