PASSWORD MANAGER > BITWARDEN SEND

Codering verzenden

Codering verzenden

Sturen is een veilig en efemeer mechanisme om gevoelige informatie naar iedereen te versturen, inclusief platte tekst en bestanden. Zoals het artikel Over verzenden opmerkt, zijn verzendingen **end-to-end versleuteld**, wat betekent dat versleuteling (hieronder beschreven) en ontsleuteling client-side plaatsvinden. Wanneer u een Verzenden maakt:

1. Er wordt een nieuwe 128-bits geheime sleutel gegenereerd voor de Send.
2. Met HKDF-SHA256 wordt een 512-bits coderingssleutel afgeleid van de geheime sleutel.
3. De afgeleide sleutel wordt gebruikt om het bericht AES-256 te versleutelen, inclusief de bestands/tekstgegevens en metagegevens (naam, bestandsnaam, notities en meer).

> **Tip**
>
> Wachtwoorden die worden gebruikt om een verzending te beveiligen **, zijn niet betrokken bij het versleutelen** en ontsleutelen van een verzending. Wachtwoorden zijn puur een verificatiemethode, maar met een wachtwoord beveiligde verzendingen worden geblokkeerd voor ontsleuteling totdat de wachtwoordverificatie is geslaagd.

4. De versleutelde Send wordt geüpload naar de Bitwarden-servers, inclusief een unieke ID die Bitwarden gebruikt om de Send te identificeren voor ontsleuteling, maar **exclusief** de versleutelingssleutel.

Anatomie verzenden

Verzendingen worden gedecodeerd door de verzendlink te openen, die is opgebouwd uit een unieke verzend-ID en de afgeleide coderingssleutel:

```
https://vault.bitwarden.com/#/send_id/encryption_key
```

Dit heeft verschillende componenten:

Component	Voorbeeld
Protocol	https://
Domein	kluis.bitwarden.com
Anker/fragment/hash	Het anker/fragment/hash bevat de verzend-id en verzend-sleutel van de URL. In de voorbeeldkoppeling wordt dit weergegeven als `#/send_id/encryption_key`.

Het anker/fragment/hash wordt niet naar de server gestuurd. Deze informatie wordt lokaal in de browser gebruikt om de identiteit vast te stellen en het verzenden te decoderen.

Ontcijfering verzenden

Wanneer u een verzendkoppeling opent:

1. De webbrowser vraagt een Send access-pagina op bij de Bitwarden-servers.
2. Bitwarden servers sturen de Send access pagina terug als een web vault client.
3. De webkluiscliënt parseert lokaal het URL-fragment dat de verzend-ID en de coderingssleutel bevat.
4. De webkluiscliënt vraagt gegevens op bij de server op basis van de geparseerde verzend-ID. De coderingssleutel wordt **nooit** opgenomen in netwerkverzoeken.
5. Bitwarden-servers sturen de versleutelde Send terug naar de webvault-client.
6. De webvaultclient decodeert de Send lokaal met behulp van de coderingssleutel.

> **Tip**
> Als uw Verzending is beveiligd met een wachtwoord, wordt de ontcijfering van de Verzending **geblokkeerd door de verificatie**. De server valideert het wachtwoord en stuurt alleen de Send terug als het wachtwoord correct is. Dit moet niet verward worden met het wachtwoord dat gebruikt wordt voor ontcijfering.

Beveiliging verzenden

Bij het verzenden van een Bitwarden Verzendlink zijn er optionele stappen die u kunt nemen voor extra beveiliging:

1. Voeg een wachtwoord toe aan de Send en deel het wachtwoord via een apart kanaal.
2. Stuur de link zonder de sleutel (alles voor de laatste forward slash) en stuur de sleutel via een apart kanaal.
3. Gebruik beide bovenstaande opties.

> **Tip**
> Wanneer u een URL verzendt, zorg er dan voor dat u zowel de Verzend-ID als de coderingssleutel toevoegt.
>
> Voorbeeld: `https://vault.bitwarden.com/#/send/send_id/encryption_key`