PASSWORD MANAGER > BITWARDEN SEND

Verschlüsselung senden

Verschlüsselung senden

Sends sind ein sicherer und vergänglicher Mechanismus zum Übertragen sensibler Informationen an jeden, einschließlich Klartext und Dateien. Wie im Artikel Über Send erwähnt, sind Sends **Ende-zu-Ende verschlüsselt**, was bedeutet, dass die Verschlüsselung (unten beschrieben) und Entschlüsselung auf der Client-Seite erfolgen. Wenn Sie einen Send erstellen:

1. Ein neuer 128-Bit-Geheimer Schlüssel wird für den Send generiert.
2. Mit HKDF-SHA256 wird ein 512-Bit-Verschlüsselungsschlüssel aus dem geheimen Schlüssel abgeleitet.
3. Der abgeleitete Schlüssel wird verwendet, um das Senden, einschließlich seiner Datei-/Textdaten und Metadaten (Name, Dateiname, Notizen und mehr) mit AES-256 zu verschlüsseln.

   > **Tip**
   >
   > Jedes Passwort, das zum Schutz eines Send verwendet wird, **ist nicht an der Verschlüsselung** und Entschlüsselung eines Send beteiligt. Passwörter sind rein eine Authentifizierungsmethode, jedoch werden passwortgeschützte Sends vom Entschlüsseln blockiert, bis die Passwort-Authentifizierung erfolgreich ist.

4. Der verschlüsselte Versand wird auf die Server von Bitwarden hochgeladen, einschließlich einer eindeutigen ID, die Bitwarden verwendet, um den Versand zur Entschlüsselung zu identifizieren, jedoch **ohne** den Verschlüsselungsschlüssel.

Anatomie senden

Sends werden entschlüsselt, indem man den Send-Link öffnet, der aus einer einzigartigen Send-ID und dem abgeleiteten Verschlüsselungsschlüssel besteht:

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

Dies hat mehrere Komponenten:

Komponente	Beispiel
Protokoll	https://
Domain	vault.bitwarden.com
Anker/Fragment/Hash	Der Anker/Fragment/Hash enthält die senden ID und den senden Schlüssel der URL. Im Beispiel-Link wird dies als `#/send_id/encryption_key` dargestellt.

Der Anker/Fragment/Hash wird nicht an den Server gesendet. Diese Informationen werden lokal innerhalb des Browsers verwendet, um die Identität zu bestimmen und das Senden zu entschlüsseln.

Entschlüsselung senden

Wenn Sie auf einen Send-Link zugreifen:

1. Der Web-Browser fordert eine Send-Zugriffsseite von den Bitwarden-Servern an.
2. Bitwarden-Server geben die Send-Zugriffsseite als Web-Tresor-Client zurück.
3. Der Web-Tresor-Client parst lokal den URL-Fragment, der die Senden-ID und den Verschlüsselungsschlüssel enthält.
4. Der Web-Tresor-Client fordert Daten vom Server an, basierend auf der geparsten Senden-ID. Der Verschlüsselungsschlüssel ist **nie** in Netzwerkanfragen enthalten.
5. Bitwarden-Server geben den verschlüsselten Send an den Web-Tresor-Client zurück.
6. Der Web-Tresor-Client entschlüsselt den Send lokal mit dem Verschlüsselungsschlüssel.

> **Tip**
>
> Wenn Ihr Send passwortgeschützt ist, wird die Entschlüsselung des Send durch die **Authentifizierung blockiert**. Der Server überprüft das Passwort und gibt das Send nur zurück, wenn das Passwort korrekt ist. Dies sollte nicht mit dem Passwort verwechselt werden, das zur Entschlüsselung verwendet wird.

Sicherheit senden

Bei der Übertragung eines Bitwarden Send-Links gibt es optionale Schritte, die Sie für zusätzliche Sicherheit unternehmen können:

1. Fügen Sie ein Passwort zum Send hinzu und teilen Sie das Passwort über einen separaten Kanal.
2. Senden Sie den Link ohne den Schlüssel (alles vor dem letzten Schrägstrich) und senden Sie den Schlüssel über einen separaten Kanal.
3. Nutzen Sie beide der oben genannten Optionen.

> **Tip**
>
> Wenn Sie eine Send-URL neu zusammenstellen, stellen Sie sicher, dass sowohl die Send-ID als auch der Verschlüsselungsschlüssel enthalten sind.
>
> Beispiel: `https://vault.bitwarden.com/#/senden/send_id/encryption_key`