



# **Guard**

## **Gebbruikershandleiding**



## **Guard: Gebruikershandleiding**

publicatie datum vrijdag, 24. juli 2015 Version 2.0.0

Copyright © 2006-2013 OPEN-XCHANGE Inc. , Dit document is intellectueel eigendom van Open-Xchange Inc.

Dit document mag geheel of gedeeltelijk gekopieerd worden zolang elke kopie deze copyright melding heeft. De informatie in dit boek is met de grootste zorg samengesteld. Toch kunnen foutieve gegevens niet worden uitgesloten. Open-Xchange Inc, de auteurs en de vertalers zijn niet aansprakelijk voor mogelijke fouten en hun gevolgen. De namen van software en hardware die in deze handleiding gebruikt worden zijn mogelijk geregistreerde handelsmerken, ze worden gebruikt zonder garantie van vrije bruikbaarheid. Open-Xchange Inc volgt in het algemeen de spelling van de producenten. De reproductie van merknamen, handelsnamen, logo's, enz. in dit boek (zelfs zonder speciale markering) kan in geen geval de zienswijze rechtvaardigen dat dergelijke namen vrij beschouwd kunnen worden (voor hetdoel van handelsmerk en merknaamregelgeving).

---

# Inhoudsopgave

<b>1 Over Deze Documentatie .....</b>	<b>5</b>
<b>2 Wat is het doel van Guard ? .....</b>	<b>7</b>
<b>3 Gebruik van de Guard .....</b>	<b>9</b>
3.1 Instellen van <i>Guard</i> .....	10
3.2 E-mailconversaties Versleutelen .....	11
3.2.1 Versleutelde e-mailberichten lezen .....	11
3.2.2 Versleutelde e-mailberichten verzenden .....	11
3.2.3 Toegang voor externe deelnemers .....	12
3.3 Versleutelde bestanden .....	13
3.3.1 Versleutelde bestanden .....	13
3.3.2 Nieuwe bestanden versleutelen .....	13
3.3.3 Versleutelde bestanden openen .....	13
3.3.4 Versleutelde bestanden downloaden .....	14
3.3.5 Bestanden ontcijferen .....	14
3.4 Afmelden uit Guard .....	15
3.5 Guard-instellingen .....	16
3.5.1 Guard Security Instellingen .....	16
3.5.2 Guard standaardinstellingen .....	17
3.5.3 Sleutels beheren .....	18
<b>Register .....</b>	<b>21</b>

---

---

# 1 Over Deze Documentatie

De volgende informatie zal u helpen bij het beter benutten van de documentatie.

- [Voor welke Doelgroep is deze documentatie bedoeld?](#)
- [Welke Inhoud is in deze Documentatie Beschreven?](#)
- [Overige Hulp](#)

## **Voor welke Doelgroep is deze documentatie bedoeld?**

Deze documentatie is voor gebruikers die gebruik willen maken van encryptie voor het beveiligen van hun e-mailverkeer en bestanden tegen ongeautoriseerde toegang.

## **Welke Inhoud is in deze Documentatie Beschreven?**

Deze documentatie bevat de volgende informatie:

- In [Wat is het doel van Guard?](#) vindt u een korte beschrijving van de Guard.
- In [Gebruik van de Guard](#) vindt u een beschrijving voor het gebruik van de Guard.

Deze documentatie beschrijft de werking van een gangbare groupware installatie en configuratie. De geïnstalleerde versie en de configuratie van uw groupware omgeving kan afwijken van wat hierin beschreven is.

## **Overige Hulp**

Een volledige handleiding voor de groupware kan u vinden in de OX App Suite Gebruikershandleiding.



---

## 2 Wat is het doel van Guard ?

Guard is een groupware beveiligingscomponent die het mogelijk maakt om e-mailberichten en bestanden te versleutelen.

- Versleutel uw e-mailcommunicatie met andere gebruikers of externe partijen.
- Versleutel individuele bestanden. Deel de versleutelde gegevens met andere gebruikers.
- Gebruik de beveiligingsmogelijkheden om het beveiligingsniveau in te stellen.
- De versleutelde gegevens worden beveiligd met een wachtwoord. Gebruik de wachtwoordherstelfunctie om u te beschermen tegen de gevolgen van het verliezen van het wachtwoord.





---

## 3 Gebruik van de Guard

Leer hoe u de *Guard* applicatie kan gebruiken.

- basis instellingen [toepassen](#)
- versleutel [E-mailcommunicatie](#)
- versleutel [bestanden](#)
- beveiligingsinstellingen [toepassen](#)

## 3.1 Instellen van *Guard*


Voordat u gebruik kan maken van *Guard*, moet u eerst een aantal basisinstellingen toepassen.

- U begint met het opgeven van het Guard security wachtwoord dit wordt gebruikt voor het versleutelen van gegevens en het benaderen van versleutelde gegevens.
- Geef een alternatief E-mailadres op voor het geval dat u uw Guard security wachtwoord vergeet. In dat geval dit is gebeurt, gebruikt u de functie voor het herstellen van het Guard security wachtwoord. Een nieuw wachtwoord zal naar u worden verzonden. Voor beveiligingsredenen is het daarom handig een alternatief E-mailadres op te geven. Anders wordt het nieuwe wachtwoord naar uw primaire E-mailadres gestuurd.

Er zijn twee opties voor het maken van de basisinstellingen:

- Definieer de basisinstellingen **terwijl** u een versleutelingsfunctie voor het eerst gebruikt.
- Definieer de basisinstellingen in de instellingenpagina van de groupware **voordat** u een versleutelingsfunctie gebruikt.

### **Het bewerken van de basisinstellingen, terwijl u de eerste keer een versleutelingsfunctie gebruikt, gaat als volgt:**

1. Schakel de versleuteling van e-mailberichten in, Versleutel een bestand of upload een nieuw bestand door op het **Versleutelen** pictogram te klikken .
2. U wordt achter elkaar gevraagd om een Guard security wachtwoord en een alternatief e-mailadres. Voer deze gegevens in.

### **Het instellen van de basisinstellingen voordat u gebruik maakt van versleuteling gaat als volgt:**

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik in de zijbalk op **Guard Security Instellingen**.  
Bij het eerste keer selecteren van de Guard Security instellingen wordt het *Guard Security Sleutels aanmaken* scherm geopend.
3. In het **Wachtwoord** veld geeft u het wachtwoord op welke u wilt gebruiken voor het versleutelen van uw gegevens.  
Bevestig het wachtwoord in het **Bevestiging** veld door het nogmaals op te geven.
4. In het **Geef nieuw alternatief e-mailadres** veld geeft u het e-mailadres op waar u het tijdelijke wachtwoord wilt ontvangen voor het herstellen van uw Guard security wachtwoord.
5. Klik op **OK**.

## 3.2 E-mailconversaties Versleutelen

U heeft de volgende mogelijkheden:

- [Versleutelde e-mailberichten lezen](#)
- [Versleutelde e-mailberichten verzenden](#)
- [Toegang voor externe deelnemers](#)

### 3.2.1 Versleutelde e-mailberichten lezen

Om versleutelde e-mailberichten te lezen is minstens het Guard security wachtwoord nodig. De verzender van een versleuteld e-mailbericht kan het bericht met een extra wachtwoord beveiligen.

#### Een versleuteld e-mailbericht lezen gaat als volgt:

1. Selecteer een e-mailbericht met het *Versleuteld* pictogram . In het detailoverzicht wordt de melding *Versleuteld e-mailbericht. Geef uw Guard security wachtwoord.* getoond.
2. Geef het Guard security wachtwoord.  
U kan opgeven hoe lang het beveiligingswachtwoord wordt onthouden. Om dit in te stellen schakelt u **Aangemeld blijven bij Guard**. Selecteert een waarde uit de lijst.  
De verzender kan het e-mailbericht met een extra wachtwoord hebben beveiligd. In dit geval wordt een extra invoerveld getoond. Geef het extra wachtwoord in dit invoerveld.
3. Klik op **OK**. De inhoud worden getoond als platte tekst.  
Als het e-mailbericht bijlagen heeft, worden functies voor het gebruik van de versleutelde en gedecodeerde versies van de bijlagen getoond.


**Opmerking:** U kan alleen reageren of doorsturen door dit e-mailbericht te verzenden als versleuteld bericht.

### 3.2.2 Versleutelde e-mailberichten verzenden

U heeft de volgende mogelijkheden:

- Verstuur een versleuteld e-mailbericht. Alleen u én de ontvanger kunnen de e-mailinhoud lezen.  
**Waarschuwing:** Als u een een concept versleuteld e-mailbericht, het concept wordt verwijderd uit de *Concepten* map als u het bericht map.
- Verzend een e-mailbericht met een handtekening. De handtekening verzekert u dat de ontvanger kan controleren of de inhoud van het e-mailbericht niet is veranderd tijdens het transport.
- Verzend een versleuteld e-mailbericht met een handtekening.

#### Een nieuw versleuteld e-mailbericht stuurt u als volgt:

1. Stel zoals gebruikelijk een e-mailbericht samen in de *E-mail* app.  
In het *Nieuw e-mailbericht opstellen* scherm, klikt u op het **Versleutelen** pictogram  in de rechterbovenhoek.  
U kan ook op **Beveiligingsopties** klikken aan de linkerkant. Activeer **Versleuteld verzenden (PGP)**.
2. Om het e-mailbericht ook te ondertekenen schakelt u **Onderteken e-mail** in.  
In het geval dat het e-mailprogramma van de ontvanger geen PGP ondersteund moet de mail toch leesbaar blijven, schakel daarom **Gebruik inline PGP (compatibiliteit)** in. Als u deze instelling gebruikt, kan u geen e-mailberichten in html formaat versturen.
3. Klik op **Beveiligd verzenden**.  
Als u naar externe ontvangers stuurt wordt een scherm getoond welke het mogelijk maakt om een [beschrijving voor het openen van het beveiligde e-mailbericht \[12\]](#) mee te sturen.

### 3.2.3 Toegang voor externe deelnemers

U kan ook versleutelde e-mailberichten versturen naar externe ontvangers die geen groupware gebruiker zijn. Bij het versturen van het eerste versleutelde e-mailbericht naar naar een externe ontvanger zal het volgende gebeuren:

- Er wordt automatisch een speciaal account aangemaakt voor de externe ontvanger.
- U geeft aan of de externe ontvanger een automatisch standaardbericht of een persoonlijke notificatie krijgt over het versleutelde e-mailbericht.
- De externe ontvanger krijgt een e-mailbericht met een notificatie en een gegenereerd wachtwoord. Afhankelijk van de configuratie van de groupware kan u een 4 cijferige pin aan de ontvanger doorgeven om dit automatische wachtwoord te beveiligen.
- De externe ontvanger krijgt een e-mailbericht met een link naar de aanmeldpagina van het speciale account.
- De externe ontvanger voert het automatisch gegenereerde wachtwoord in op de aanmeldpagina. Daarna moet de ontvanger het automatisch gegenereerde wachtwoord veranderen. Om het account te herstellen in het geval van het verliezen van een wachtwoord, moet ook een veiligheidsvraag opgegeven worden met een bijbehorend antwoord.  
Het versleutelde e-mailbericht wordt getoond.
- De externe ontvanger kan een versleuteld antwoord versturen op het e-mailbericht.

Bij het versturen van het volgende versleutelde e-mailbericht naar deze externe ontvanger gebeurt het volgende:

- De externe ontvanger krijgt een e-mailbericht met een link naar de aanmeldpagina voor het speciale account.
- Op de aanmeldpagina geeft de ontvanger het wachtwoord op dat deze heeft ingevoerd bij het ontvangen van het eerste versleutelde bericht.  
Als de ontvanger het wachtwoord niet meer weet kan een nieuw wachtwoord worden aangevraagd. Om dit te doen moet de beveiligingsvraag beantwoord worden.

## 3.3 Versleutelde bestanden

U heeft de volgende mogelijkheden:


- [Versleutelde bestanden](#)
- [Nieuwe bestanden versleutelen](#)
- [Versleutelde bestanden openen](#)
- [Versleutelde bestanden downloaden](#)
- [Bestanden ontcijferen](#)


### 3.3.1 Versleutelde bestanden

Bij het versleutelen van een bestand wordt alleen de laatste versie versleuteld. Alle andere versies worden verwijderd.

#### U kunt bestanden als volgt versleutelen:

**Waarschuwing:** Als u een bestand versleuteld worden alle versies van dit bestand verwijderd, op de laatste na. Als u een oudere versie wilt bewaren moet u deze opslaan voordat u het bestand versleuteld.

1. In de *Bestanden* app, klikt u op een bestand in het hoofdgebied. In de pop-up klikt u op het **Meer** pictogram . Klik op **Versleutelen** in het menu.

U kan ook een bestand selecteren. Klik op het **Meer** pictogram  in de werkbalk. Klik op **Versleutelen** in het menu.

2. Als het bestand meerdere versies bevat wordt het *Versleutelen van bestanden* scherm getoond. Bevestig dat u het bestand wilt versleutelen en alle oude versies gaat verwijderen door op **OK** te klikken.

Als het bestand maar één versie heeft zal deze versleuteld worden zonder verdere vragen.

### 3.3.2 Nieuwe bestanden versleutelen

U kan nieuwe versleutelde bestanden maken door een lokaal bestand te uploaden met versleuteling.


#### Een nieuw versleuteld bestand maakt u als volgt:

1. Open een map in de mappenboom.

**Opmerking:** Selecteer eerst een map waarin u voldoende rechten heeft om objecten aan te maken.

2. Klik op **Nieuw** in de werkbalk. Klik op **Upload nieuw bestand**.

3. In het *Upload nieuwe bestanden* scherm, klik op **Selecteer bestand**. Selecteer één of meerdere bestanden.

Klik het **Versleutelen** pictogram  in de rechterbovenhoek van de menubalk.

4. U kan bestandsgegevens ingeven in het *Omschrijving* veld.

5. Klik op **Versleutelen** in het menu.

**Tip:** U kan ook nieuwe versleutelde bestanden maken door deze vanuit het bureaublad van uw systeem naar de *Bestanden* app scherm te slepen en te laten vallen in het bovenste gedeelte.

### 3.3.3 Versleutelde bestanden openen

U kan versleutelde bestanden openen en lezen. De bestanden blijven versleuteld op de server staan.

**Een versleuteld bestand opent u als volgt:**

1. In de *Bestanden* app klikt u op een bestand in het detailoverzicht. In het pop-up scherm klikt u op **Ontcijferen en Openen**.
2. Vanuit het *Geef het Guard Security Wachtwoord* scherm geeft u het Guard security wachtwoord. U kan opgeven hoe lang het beveiligingswachtwoord wordt kan worden onthouden. Om dit in te stellen schakelt u **Wachtwoord onthouden** in. Selecteer een waarde uit de lijst. Klik op **OK**.

**3.3.4 Versleutelde bestanden downloaden**

U kan versleutelde bestanden downloaden om deze lokaal te lezen of te bewerken. De bestanden blijven versleuteld op de server staan.



**Een versleuteld bestand download u als volgt:**

1. In de *Bestanden* app, klikt u op een bestand in het hoofdgebied. In de pop-up klikt u op het **Meer** pictogram . Klik op **Ontcijferde versie Downloaden** in het menu >. **Opmerking:** Als u in plaats hiervan klikt op **Download** in de pop-up, blijft het gedownloadde bestand versleuteld.
2. Vanuit het *Geef het Guard Security Wachtwoord* scherm geeft u het Guard security wachtwoord. Klik op **OK**.

**3.3.5 Bestanden ontcijferen**

U kan de versleuteling van een bestand verwijderen door deze te ontcijferen.

**U kunt bestanden als volgt ontcijferen:**


1. In de *Bestanden* app, klikt u op een versleuteld bestand in het hoofdgebied. In de pop-up klikt u op het **Meer** pictogram . Klik op **Versleuteling verwijderen** in het menu. U kan ook een bestand selecteren. Klik op het **Meer** pictogram  in de werkbalk. Klik op **Versleuteling verwijderen** in het menu.
2. Vanuit het *Geef het Guard Security Wachtwoord* scherm geeft u het Guard security wachtwoord. U kan opgeven hoe lang het Guard beveiligingswachtwoord moet worden onthouden. Om dit in te stellen schakelt u **Wachtwoord onthouden** in. Selecteer een waarde uit de lijst. Klik op **OK**.

## 3.4 Afmelden uit Guard

U kan zich afmelden uit Guard zonder de groupware te sluiten. Om een versleuteld e-mailbericht, bestand of map te openen moet u opnieuw uw Guard security wachtwoord opgeven.

**Opmerking:** Deze functie is alleen beschikbaar als u **Wachtwoord onthouden** inschakelt, bij het openen van een versleuteld e-mailbericht of bestand.

### **Afmelden uit Guard gaat als volgt:**

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk.
2. Klik op **Afmelden uit Guard** in het menu.

## 3.5 Guard-instellingen

Er zijn de volgende mogelijkheden:

- Om uw Guard security wachtwoord te beheren, gebruikt u de [Guard security instellingen](#).
- Om de standaardinstellingen voor het verzenden van beveiligde e-mailberichten te veranderen, gebruikt u de [Guard default settings](#).
- U kan [uw PGP sleutels beheren](#).

### 3.5.1 Guard Security Instellingen


Er zijn de volgende mogelijkheden:

- [wijzig](#) het Guard security wachtwoord
- Als u uw Guard security wachtwoord bent vergeten kan u een tijdelijk wachtwoord laten e-mailen door uw Guard security wachtwoord te [herstellen](#).
- [wijzig](#) het alternatieve e-mailadres


#### Zo kunt u het Guard security wachtwoord wijzigen

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik in de zijbalk op **Guard Security Instellingen**.
3. In het **Geef het huidige Guard security wachtwoord** veld onder *Wachtwoord* geeft u het wachtwoord op welke u heeft gebruikt voor het versleutelen van uw gegevens.  
In het **Geef het nieuwe Guard security wachtwoord** veld geeft u het wachtwoord op welke u wilt gebruiken voor het versleutelen van uw gegevens.  
Bevestig het wachtwoord in het **Bevestig het nieuwe Guard security wachtwoord** veld door het nogmaals op te geven.
4. Klik op **Guard security wachtwoord wijzigen**.

#### Zo kunt u het Guard security wachtwoord herstellen:

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik in de zijbalk op **Guard Security Instellingen**.
3. Klik op **Herstellen Guard security wachtwoord**. Een nieuw wachtwoord wordt naar uw alternatieve e-mailadres gestuurd.  
Als u geen alternatief e-mailadres heeft opgegeven wordt het nieuwe wachtwoord naar uw primaire e-mailadres gestuurd.
4. Dit nieuwe wachtwoord is nu uw huidige Guard security wachtwoord. U moet direct dit wachtwoord [wijzigen](#).

#### Het wijzigen van uw alternatieve e-mailadres voor het herstellen van het versleutel wachtwoord gaat als volgt:


1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik in de zijbalk op **Guard Security Instellingen**.
3. Geef het wachtwoord voor het versleutelen van uw gegevens in het **Geef het huidige Guard security wachtwoord** veld onder *Alternative E-Mail*.  
In het **Geef nieuw alternatief e-mailadres** veld geeft u het e-mailadres op waar u het tijdelijke wachtwoord wilt ontvangen voor het herstellen van uw Guard security wachtwoord.  
Klik op **E-mailadres wijzigen**.



## 3.5.2 Guard standaardinstellingen

De standaardinstellingen bepalen de waarden die als basis beschikbaar zijn bij het maken van e-mailberichten. Bij het opstellen van nieuwe e-mailberichten kunnen de standaardinstellingen aangepast worden voordat het e-mailbericht wordt verstuurd.

### De standaardinstellingen wijzigt u als volgt:

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik in de zijbalk op **Guard PGP Instellingen**.
3. Verander een instelling onder *PGP Versleutelingsinstellingen*

De volgende opties zijn beschikbaar:

### Standaard bij het opstellen van versleutelde e-mailberichten

Geeft aan of een nieuw e-mailbericht standaard met PGP wordt versleuteld.

### Standaard ondertekening toevoegen aan uitgaande e-mailberichten

Geeft aan of een nieuw e-mailbericht standaard met PGP wordt versleuteld.

### PGP standaard ingesteld op inline PGP voor compatibiliteit


Definieert of de PGP versleuteling inline wordt uitgevoerd. Gebruik deze instelling alleen als het e-mailprogramma van een ontvanger geen PGP ondersteund maar het bericht wel leesbaar moet zijn. Als u deze instelling gebruikt kan u geen e-mailberichten versturen in html opmaak.

### 3.5.3 Sleutels beheren

Om versleutelde e-mailberichten te verzenden of te ontvangen zijn de functies voor het beheren van de sleutels meestal niet noodzakelijk. Deze functies kan u echter wel gebruiken bij de volgende taken:

- U wil uw Guard PGP sleutels gebruiken in andere e-mailprogramma's zoals bijvoorbeeld een lokaal e-mailprogramma.
- U heeft PGP sleutels vanuit een andere PGP applicatie. U wilt deze sleutels gebruiken in Guard.
- U heeft de publieke sleutel van een externe partner. Om de versleutelde berichten van deze partner te lezen zonder toegang tot de sleutelservers, moet u de publieke sleutel van deze partner importeren in Guard.
- U wil uw publieke sleutel aan een ontvanger geven zodat deze leestoegang heeft tot uw versleutelde berichten zonder toegang tot de sleutelservers.

#### De pagina voor het beheren van uw sleutels opent u als volgt:

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik in de zijbalk op **Guard PGP Instellingen**.

De pagina bevat de volgende elementen.

- Opties voor het instellen van de [Guard standaard instellingen](#).
- *Uw Sleutels* sectie. Bevat functies voor het beheren van uw privé en uw publieke PGP sleutels.
- *Publieke Sleutels* sectie. Toont de publieke sleutels die gedeeld zijn door u of andere gebruikers. Als de publieke sleutel van een gebruiker in de lijst staat mag u aannemen dat deze gebruiker de berichten die u versleuteld verstuurd ook kan decoderen.

De volgende mogelijkheden zijn beschikbaar:

- [download](#) uw publieke sleutel
- [verstuur uw publieke sleutel per e-mail](#)
- [nieuwe sleutels toevoegen](#) aan uw bestaande sleutels door lokale sleutels te uploaden of door nieuwe Guard sleutels te maken
- [download](#) uw privésleutel
- [upload](#) een publieke sleutel van een externe partner


#### U kunt uw publieke sleutel als volgt downloaden:

1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik op **Download PGP Publieke Sleutel** onder *Uw Sleutels*.

#### Uw publieke sleutel verzend u als volgt in een e-mailbericht:


1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik op **e-mail uw Publieke PGP Sleutel** onder *Uw Sleutels*.

**Een nieuwe sleutel toevoegen gaat als volgt:**


1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik het **Toevoegen** pictogram  naast de *Uw Sleutel Lijst* onder *Uw Sleutels*. Het *Sleutels toevoegen* scherm opent.
3. U heeft de volgende mogelijkheden:
  - Om een privé sleutel toe te voegen, klikt u op **Privésleutel uploaden**. Selecteer het bestand dat de privésleutel bevat. Het *Privésleutel uploaden* scherm wordt geopend.  
Om een nieuwe sleutel te uploaden geeft u uw Guard security wachtwoord. Geef een nieuwe wachtwoord voor de nieuwe sleutel.
  - Om een publieke sleutel toe te voegen klikt u op **Alleen Publieke sleutel uploaden**. Selecteer het bestand met een publieke sleutel.
  - Om een nieuw sleutelbaar te maken klikt u op **Nieuwe Sleutels Aanmaken**. Het *Guard Security Sleutels aanmaken* scherm wordt geopend.  
Geef een wachtwoord voor de nieuwe sleutel. Bevestig dit wachtwoord.  
De nieuwe sleutel wordt getoond onder de *Uw Sleutel Lijst*.

**Uw privésleutel downloaden gaat als volgt:**

**Opgepast:** Het downloaden van uw privésleutel naar uw lokale machine is een beveiligingsrisico. Zorg er voor dat geen andere personen toegang kunnen krijgen tot uw privésleutel.

1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik op het **Downloaden** pictogram  naast de ondertekening.

**Uploaden van de publieke sleutel van een externe partner gaat als volgt:**

1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik op het **Toevoegen** pictogram  naast de *PGP Publieke Sleutellijst* onder *Publieke sleutels*. Selecteer het bestand met een publieke sleutel.



---

# Register

## A

- Afmelden
  - Wijzig wachtwoord, 15

## D

- Documentatie, 5
- Download versleutelde bestanden, 14

## G

- Guard, 7, 9
  - afmelden, 15
  - beheer sleutels, 18
  - beveiligingsinstellingen, 16
  - instellen, 10
  - instellingen, 16
  - standaardinstellingen, 17
- Guard PGP instellingen
  - PGP standaard ingesteld op inline PGP voor compatibiliteit, 17
  - Standaard bij het opstellen van versleutelde e-mailberichten, 17
  - Standaard ondertekening toevoegen aan uitgaande e-mailberichten, 17
- Guard-instellingen
  - Het wachtwoord herstellen, 16
  - Wijzig wachtwoord, 16

## H

- Het wachtwoord wijzigen, 16

## N

- Nieuwe versleutelde bestanden aanmaken, 13

## O

- Ontcijfer bestanden, 14
- Open versleutelde bestanden, 13

## V

- Versleutel E-mailconversaties, 11
- Versleutelde bestanden, 13
  - downloaden, 14
  - Ontcijferen, 14
  - openen, 13
- Versleutelde e-mailberichten
  - blokkeren, 11
  - lezen, 11
  - toegang voor externe deelnemers, 12
  - verstuur, 11
- Versleutelen
  - Bestanden, 13
  - E-mailconversatie, 11
  - nieuwe versleutelde bestanden aanmaken, 13

