



Guard

Gebbruikershandleiding



Guard: Gebruikershandleiding

publicatie datum woensdag, 09. november 2016 Version 2.6.0

Copyright © 2016-2013 OX Software GmbH , Dit document is intellectueel eigendom van OX Software GmbH

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. OX Software GmbH, 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. OX Software GmbH 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

1 Over Deze Documentatie	5
2 Wat is het doel van Guard ?	7
3 Gebruik van de Guard	9
3.1 Instellen van <i>Guard</i>	10
3.2 E-mailconversaties Coderen	11
3.2.1 Gecodeerde e-mailberichten lezen	11
3.2.2 Gecodeerde e-mailberichten verzenden	11
3.2.3 Hoe kan een externe ontvanger een gecodeerd bericht lezen?	12
3.3 Gecodeerde bestanden	13
3.3.1 Gecodeerde bestanden	13
3.3.2 Nieuwe bestanden coderen	13
3.3.3 Gecodeerde bestanden openen	13
3.3.4 Gecodeerde bestanden downloaden	14
3.3.5 Bestanden decoderen	14
3.4 Guard afmelden	15
3.5 Guard Instellingen	16
3.5.1 Guard beveiligingsinstellingen	16
3.5.2 Gecodeerde bestanden	17
3.5.3 Sleutels beheren	18
Register	21

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 Groupware 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](#)
- codeer [E-mailcommunicatie](#)
- codeer [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 beveiligingswachtwoord dit wordt gebruikt voor het coderen van gegevens en het benaderen van gecodeerde gegevens.
- Geef een alternatief E-mailadres op voor het geval dat u uw Guard beveiligingswachtwoord vergeet. In dat geval dit is gebeurt, gebruikt u de functie voor het herstellen van het Guard beveiligingswachtwoord. 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 coderingsfunctie voor het eerst gebruikt.
- Definieer de basisinstellingen in de instellingenpagina van de groupware **voordat** u een coderingsfunctie gebruikt.

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

1. Schakel de codering van e-mailberichten in, Codeer een bestand of upload een nieuw bestand door op het **Coderen** pictogram te klikken 🗝️ naast de mapnaam in de mappenboom.
2. U wordt achter elkaar gevraagd om een Guard beveiligingswachtwoord en een alternatief e-mailadres. Voer deze gegevens in.

Het instellen van de basisinstellingen voordat u gebruik maakt van codering gaat als volgt:

1. Klik op het **Systeemmenu** pictogram ☰ aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Klik op **Guard Beveiliging** in de zijbalk.
Als u voor de eerste keer de Guard beveiligingsinstellingen opent, opent het *Guard Aanmaken Beveiligingsleutels* scherm.
3. In het **Wachtwoord** veld geeft u het wachtwoord op welke u wilt gebruiken voor het coderen 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 beveiligingswachtwoord.
5. Klik op **OK**.

3.2 E-mailconversaties Coderen


U heeft de volgende mogelijkheden:

- [Gecodeerde e-mailberichten lezen](#)
- [Gecodeerde e-mailberichten verzenden](#)
- [Hoe kan een externe ontvanger een gecodeerd bericht lezen?](#)

3.2.1 Gecodeerde e-mailberichten lezen

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

Een gecodeerd e-mailbericht lezen gaat als volgt:

1. Selecteer een e-mailbericht met het *Gecodeerd* pictogram . In het detailoverzicht wordt de melding *Gecodeerd e-mailbericht. Geef uw Guard beveiligingswachtwoord.* getoond.

Opmerking: Als u, toen u de vorige keer Guard heeft gebruikt, heeft ingesteld dat Guard het beveiligingswachtwoord moest onthouden, zal het e-mailbericht direct getoond worden, afhankelijk van de instelling.

2. Geef het Guard beveiligingswachtwoord.

U kan aangeven hoe lang het beveiligingswachtwoord onthouden moet worden door Guard. Om dit te doen schakelt u Blijf aangemeld bij **Guard**. Selecteer een waarde uit de lijst.

3. Klik op **OK**. De inhoud worden getoond als platte tekst.

Als het e-mailbericht bijlagen heeft, worden functies voor het gebruik van de gecodeerde en gedecodeerde versies van de bijlagen getoond.

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

3.2.2 Gecodeerde e-mailberichten verzenden

U heeft de volgende mogelijkheden:

- Verstuur een codeert e-mailbericht. Alleen u én de ontvangers kunnen de e-mailinhoud lezen.
Waarschuwing: Als u een een concept gecodeerd 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 gecodeerd e-mailbericht met een handtekening.

Een nieuw gecodeerd e-mailbericht stuurt u als volgt:

1. Stel zoals gebruikelijk een e-mailbericht samen in de *E-mail* app.
In het *Samenstellen* scherm, klikt u op het **Coderen** pictogram  in de rechterbovenhoek.
U kan ook klikken op **Beveiligingsopties** onder het onderwerp. Activeer **Coderen**.
Pictogrammen naast de ontvanger geven aan of het bericht gecodeerd kan worden voor deze ontvanger. Als u over het pictogram zweeft wordt een omschrijving getoond.
2. Om meer mogelijkheden zichtbaar te maken klikt u op **Beveiliging**. U kan de volgende mogelijkheden gebruiken.
Om het e-mailbericht ook te ondertekenen, schakel **Ondertekenen** in.
In het geval dat het e-mailprogramma van de ontvanger geen PGP ondersteund moet de mail toch leesbaar blijven, schakel daarom **PGP Inline** in. Als u deze instelling gebruikt, kan u geen e-mailberichten in html formaat versturen.
Om de e-mailontvanger in staat te stellen gecodeerde antwoorden te sturen, moet deze uw publieke sleutel hebben. U kan uw publieke sleutel als een bijlage sturen. Om dit te doen schakelt u **Mijn sleutel toevoegen** in.
3. Klik op **Gecodeerd verzenden**.
Als u naar externe ontvangers stuurt wordt een scherm getoond welke het mogelijk maakt om een [beschrijving voor het openen van het gecodeerde e-mailbericht \[12\]](#) mee te sturen.
Als u voor de eerste keer een gecodeerd e-mailbericht naar een externe ontvanger stuurt, zal deze een e-mailbijlage ontvangen met uw publieke sleutel.

3.2.3 Hoe kan een externe ontvanger een gecodeerd bericht lezen?

U kan ook gecodeerde e-mailberichten versturen naar externe ontvangers die geen groupware gebruikers zijn. Als u een externe ontvanger toevoegt controleert Guard of er een publieke sleutel beschikbaar is voor deze ontvanger. Afhankelijk van het resultaat kiest Guard verschillende procedures voor het verzenden van gecodeerde e-mailberichten.

- Als er een publieke sleutel aanwezig is voor de ontvanger:
 - Het bericht wordt gecodeerd verzonden met deze sleutel. De ontvanger kan het bericht lezen met zijn of haar privésleutel.
 - Om de ontvanger de gelegenheid te geven om een gecodeerd antwoord te sturen wordt uw publieke sleutel meegestuurd als bijlage. Deze bijlage heet `public.asc`. De ontvanger kan deze importen in zijn of haar e-mailapplicatie.
- Als er geen publieke sleutel is gevonden voor de ontvanger:
 - Als de externe gebruiker al een gastaccount heeft ontvangt deze een e-mailbericht met een link naar de aanmeldpagina voor zijn of haar gastaccount. Als zij of hij is aangemeld kan het gecodeerde bericht gelezen worden op de gastpagina. Hij/zij kan een gecodeerd antwoord terugsturen vanaf deze pagina.
 - Als er geen gastaccount is wordt deze aangemaakt. De externe ontvanger krijgt een e-mailbericht met een link naar de gastpagina en een gegenereerd wachtwoord. De gebruiker kan zich aanmelden met het automatisch gegenereerde wachtwoord. Daarna kan hij/zij een eigen wachtwoord ingeven.
Afhankelijk van de configuratie wordt het automatisch aangemaakte wachtwoord en de link naar de gastpagina verzonden in afzonderlijke berichten.
 - Afhankelijk van de instellingen van de groupware, worden gast accounts na een specifiek aantal dagen verwijderd. Om de e-mailberichten achteraf beschikbaar te maken bevat het e-mailbericht naast de link naar de gastpagina ook een bijlage met het gecodeerde bericht. Deze bijlage heet `encrypted.asc`. Deze bijlage kan worden geüpload en vervolgens gelezen worden op de gastpagina.

3.3 Gecodeerde bestanden

U heeft de volgende mogelijkheden:



- [Gecodeerde bestanden](#)
- [Nieuwe bestanden coderen](#)
- [Gecodeerde bestanden openen](#)
- [Gecodeerde bestanden downloaden](#)
- [Bestanden decoderen](#)

3.3.1 Gecodeerde bestanden

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

U kunt bestanden als volgt coderen:

Waarschuwing: Als u een bestand codeert 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 codeert.

1. Selecteer een of meerdere bestanden in de *Bestanden* app. Klik het **Acties** pictogram  in de werkbalk. Klik op **Coderen** in het menu.
U kan ook op het **Acties** pictogram  in de *Viewer*. Klik op **Versleutelen** in het menu.
2. Als het bestand meerdere versies bevat wordt het *Coderen van bestanden* scherm getoond. Bevestig dat u het bestand wilt coderen en alle oude versies gaat verwijderen door op **OK** te klikken.
Als het bestand maar één versie heeft zal deze gecodeerd worden zonder verdere vragen.

3.3.2 Nieuwe bestanden coderen

U kan nieuwe gecodeerde bestanden maken door een lokaal bestand te uploaden met codering.


Een nieuw gecodeerd bestand maakt u als volgt:

1. In de *Bestanden* app selecteert u een map uit 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 **Toevoegen en coderen van lokale bestanden**.
 3. Selecteer één of meerdere bestanden in het *Bestand uploaden* scherm.
Klik op **Openen**. Het hoofdgebied toont de status van de voortgang.
Om het proces te stoppen klikt u op **Bestandsdetails** in de rechteronderhoek van het hoofdgebied.
Klik op **Annuleren** naast de bestandsnaam in het *Upload voortgang* scherm.
- Tip:** U kan ook nieuwe gecodeerde 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 Gecodeerde bestanden openen

U kan gecodeerde bestanden openen en lezen. De bestanden blijven gecodeerd op de server staan.

Een gecodeerd bestand opent u als volgt:

1. In de *Bestanden* app, selecteert u een gecodeerd bestand in het hoofdgebied. Klik het **Viewer** pictogram  in de werkbalk.
2. Het *Geef Guard beveiligingswachtwoord* scherm opent. Geef het Guard beveiligingswachtwoord. U kan opgeven hoe lang het beveiligingswachtwoord mag worden onthouden door Guard. Om dit in te stellen schakelt u **Wachtwoord onthouden** in. Selecteer een waarde uit de lijst. Klik op **OK**.

3.3.4 Gecodeerde bestanden downloaden

U kan gecodeerde bestanden downloaden om deze lokaal te lezen of te bewerken. De bestanden blijven gecodeerd de server staan.


Een gecodeerd bestand download u als volgt:

1. In de *Bestanden* app, selecteert u een gecodeerd bestand in het hoofdgebied. Klik het **Viewer** pictogram  in de werkbalk.
Opmerking: Als u in plaats hiervan klikt op **Download** in de pop-up, blijft het gedownloade bestand gecodeerd.
2. Het *Geef Guard beveiligingswachtwoord* scherm opent. Geef het Guard beveiligingswachtwoord. U kan opgeven hoe lang het beveiligingswachtwoord mag worden onthouden door Guard. Om dit in te stellen schakelt u **Wachtwoord onthouden** in. Selecteer een waarde uit de lijst. Klik op **OK**.
3. Klik het **Acties** pictogram  in de Viewer. Klik op **Gedecodeerde versie Downloaden**.

3.3.5 Bestanden decoderen

U kan de codering van een bestand verwijderen door deze te decoderen.

U kunt bestanden als volgt decoderen:


1. In de *Bestanden* app, klikt u op een gecodeerd bestand in het hoofdgebied. Klik op het **Acties** pictogram  in de werkbalk. Klik in het menu op **Codering Verwijderen**.
2. Het *Geef Guard beveiligingswachtwoord* scherm opent. Geef het Guard beveiligingswachtwoord. 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 Guard afmelden

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

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

Afmelden van Guard gaat als volgt:

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

3.5 Guard Instellingen

Er zijn de volgende mogelijkheden:

- Om uw Guard beveiligingswachtwoord te beheren, gebruikt u de [Guard beveiligingsinstellingen](#).
- Om de standaardinstellingen voor het verzenden van gecodeerde e-mailberichten te veranderen, gebruikt u de [PGP coderingsinstellingen](#).
- U kan [uw PGP sleutels beheren](#).

3.5.1 Guard beveiligingsinstellingen


Er zijn de volgende mogelijkheden:

- [verander](#) het Guard beveiligingswachtwoord
- Als u Guard wilt gebruiken maar het beveiligingswachtwoord bent vergeten, kan u een tijdelijk Guard beveiligingswachtwoord krijgen door het [herstellen](#) van het Guard beveiligingswachtwoord.
- [wijzig](#) het alternatieve e-mailadres


Verander het Guard beveiligingswachtwoord 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 Beveiliging**.
3. In het **Geef huidig Guard beveiligingswachtwoord** veld onder *Wachtwoord*, geeft u het wachtwoord waarmee u tot nu toe uw gegevens heeft gecodeerd.
In het **Geef nieuw Guard beveiligingswachtwoord** veld, geeft u het wachtwoord wat u wilt gebruiken om vanaf nu uw gegevens te coderen.
Bevestig het wachtwoord in het **Bevestig nieuw Guard beveiligingswachtwoord** veld door het nogmaals in te voeren.
4. Klik op **Wijzig Guard beveiligingswachtwoord**.

U kan het Guard beveiligingswachtwoord als volgt 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 Beveiliging**.
3. Klik op **Herstel Guard beveiligingswachtwoord**. 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 beveiligingswachtwoord. U moet direct dit wachtwoord [wijzigen](#).


Het wijzigen van uw alternatieve e-mailadres voor het herstellen van het coderingswachtwoord 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 Beveiliging**.
3. Geef het wachtwoord voor het coderen van uw gegevens in het **Geef huidig Guard beveiligingswachtwoord** veld onder *Alternatief e-mailadres*.
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 beveiligingswachtwoord.
Klik op **E-mailadres wijzigen**.

3.5.2 Gecodeerde bestanden

De PGP coderingsinstellingen 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 PGP coderingsinstellingen wijzigt u als volgt:

1. Klik op het **Systeemmenu** pictogram  aan de rechterkant van de menubalk. Klik op **Instellingen** uit het menu.
2. Selecteer de optie **Guard Beveiliging** uit de zijbalk. Klik op **Geavanceerde instellingen**.
3. Verander een instelling onder *PGP Coderingsinstellingen*

De volgende opties zijn beschikbaar:

Standaard bij het opstellen van gecodeerde e-mailberichten

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

Standaard ondertekening toevoegen aan uitgaande e-mailberichten

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

Schakel geavanceerde PGP mogelijkheden in

Geef aan of PGP opties zoals sleutelbeheer, getoond moeten worden.

PGP inline standaard ingesteld voor nieuwe berichten

Om deze instelling to tonen schakelt u het aankruisvakje **Geavanceerde PGP mogelijkheden inschakelen** in.


Definieert of de PGP codering 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 gecodeerde 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 gecodeerde 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 leestoeegang heeft tot uw gecodeerde 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. Selecteer de optie **Guard Beveiliging** uit de zijbalk. Klik op **Geavanceerde Instellingen**. Selecteer **Geavanceerde PGP mogelijkheden inschakelen**.

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. Uw bestaande sleutels worden getoond onder *Uw Sleutellijst*. De Sleutellijst bevat twee sleutels:
 - Een hoofdsleutel. Deze sleutel wordt onder andere gebruikt voor het ondertekenen van uw e-mailberichten.
 - Een subsleutel. Deze sleutel wordt gebruikt voor het coderen en decoderen van e-mailberichten en bestanden.

Het onderscheid tussen een hoofd- en een subsleutel is één van de eigenschappen van de PGP codeertechniek. Elke hoofdsleutel en elke subsleutel bevatten een publieke en privésleutel. Afhankelijk van de eisen gebruikt Guard automatisch de specifieke sleutel.

- *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 gecodeerd verstuurd ook kan decoderen.
- Verlopen sleutels worden rood afgebeeld.

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
- [verander een sleutel naar de huidige sleutel](#)
- [toon details](#) van een sleutel
- [verwijder](#) een sleutel
- [download](#) uw privésleutel
- [voeg een extra E-Mailaccount toe](#) aan een sleutel
- [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 beveiligingswachtwoord. 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 sleutelpaar te maken klikt u op **Nieuwe Sleutels Aanmaken**. Het *Guard Beveiligingssleutels aanmaken* scherm wordt geopend.
Geef een wachtwoord voor de nieuwe sleutel. Bevestig dit wachtwoord.
De nieuwe sleutel bestaat uit een hoofdsleutel en een subsleutel.
De nieuwe sleutel wordt boven aan de lijst toegevoegd. De nieuwe sleutel wordt de huidige sleutel.


Een willekeurige sleutel de huidige sleutel maken gaat als volgt:

U kan deze functie gebruiken als uw sleutellijst meerdere hoofdsleutels met subsleutels bevat. Vanaf dit moment zal de huidige sleutel gebruikt worden voor codering.


1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Vanuit *Uw Sleutellijst*, klikt u op een aankruisvakje in de kolom **Huidige**. Als u een hoofdsleutel markeert als huidige sleutel worden de overeenkomstige subsleutels ook gemarkeerd en vice versa.

De details van de sleutels kan u als volgt zien:

U kan meer detail van sleutels zien. Deze details zijn vooral van belang voor gebruikers met kennis van PGP.


1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik het **Details** pictogram  naast de sleutel onder *Uw Sleutel Lijst*. Het *Sleutel Details* scherm opent.
Om de handtekening van de sleutel te zien klikt u op **Handtekeningen**.

Het verwijderen van een sleutel gaat als volgt:

1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
 2. Klik het **Verwijderen** pictogram  naast *Uw Sleutellijst* onder *Uw Sleutels*. Het *Verwijder Privésleutel* scherm opent.
 3. U heeft de volgende mogelijkheden:
 - Om een privésleutel in te trekken klikt u op **Intrekken**.
Geeft het wachtwoord van de privésleutel. Indien nodig geeft u de reden op waarom u de sleutel intrekt.
Klik op **Intrekken**.
 - Om een privésleutel te verwijderen klikt u op **Verwijderen**.
Geeft het wachtwoord van de privésleutel.
Klik op de **Verwijderen** knop.
- Als u een hoofdsleutel verwijderd worden de overeenkomstige subsleutels ook verwijderd.


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 het **Download** pictogram  naast een sleutel in de privésleutellijst onder *Uw Sleutels*.

Voeg een extra E-Mailaccount als volgt toe aan een sleutel:

Als u meerdere gebruikersID's aan een sleutel koppelt kan u de sleutel voor meerdere e-mailaccounts gebruiken.

1. Vanuit de instellingen, [open](#) de pagina om sleutels te beheren.
2. Klik het **Bewerken** pictogram  naast de *Uw Sleutellijst* onder *Uw Sleutels*. Het *Gebruikers ID toevoegen* scherm opent.
3. Geef een naam voor de gebruikers ID. Geef het e-mailadres welke u wilt gebruiken voor deze sleutel. Geef uw wachtwoord voor deze sleutel.
Klik op **OK**.

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

Wachtwoord wijzigen, 15

C

Codeer E-mailconversaties, 11

Coderen

Bestanden, 13

E-mailconversatie, 11

nieuwe gecodeerde bestanden aanmaken, 13

D

Decodeer bestanden, 14

Documentatie, 5

Download gecodeerde bestanden, 14

G

Gecodeerde bestanden, 13

Decoderen, 14

downloaden, 14

Openen, 13

Gecodeerde e-mailberichten

blokkeren, 11

lezen, 11

toegang voor externe deelnemers, 12

verstuur, 11

Guard, 7, 9

afmelden, 15

beheer sleutels, 18

beveiligingsinstellingen, 16

instellen, 10

Instellingen, 16

PGP coderingsinstellingen, 17

Guard Guard PGP Instellingen

PGP inline standaard ingesteld voor nieuwe berichten, 17

Schakel geavanceerde PGP mogelijkheden in, 17

Standaard bij het opstellen van gecodeerde e-mailberichten, 17

Standaard ondertekening toevoegen aan uitgaande e-mailberichten, 17

Guard Instellingen

Het wachtwoord herstellen, 16

Wachtwoord wijzigen, 16

H

Het wachtwoord wijzigen, 16

N

Nieuwe gecodeerde bestanden aanmaken, 13

O

Open gecodeerde bestanden, 13

