

Ein Schlüsselpaar erstellen

Sie haben wahrscheinlich schon ein PGP-Schlüsselpaar für sich erstellt, entweder mit dem PGP Desktop Setup-Assistenten oder mit einer früheren Version von PGP Desktop. Ist dies nicht der Fall, müssen Sie es jetzt nachholen. Fast alles, was Sie mit PGP Desktop tun, erfordert ein Schlüsselpaar.

Achtung: Es ist nicht empfehlenswert, für sich selbst immer neue Schlüssel zu erstellen. Ein PGP-Schlüsselpaar ist wie ein digitaler Führerschein oder Pass. Wenn Sie zu viele davon erstellen, verwirren Sie am Ende nicht nur sich selbst, sondern auch die Leute, die Ihnen verschlüsselte Nachrichten senden wollen. Am besten besitzen Sie nur einen einzigen Schlüssel, der alle von Ihnen verwendeten E-Mail-Adressen enthält. Das PGP Global Directory veröffentlicht nur ein Schlüsselpaar pro E-Mail-Adresse.

So erstellen Sie ein PGP-Schlüsselpaar

1. Achten Sie darauf, dass das Bedienfeld **PGP Keys** ausgewählt ist.
2. Klicken Sie auf **Datei > Neuer PGP-Schlüssel** oder drücken Sie **Strg+N**. Der erste Bildschirm des PGP-Schlüsselerstellungs-Assistenten wird angezeigt.
3. Lesen Sie die Informationen auf diesem Bildschirm.
4. Falls Sie Ihr neues PGP-Schlüsselpaar auf einem Token oder einer Smartcard erstellen wollen, stellen Sie sicher, dass der Token bzw. die Smartcard an das System angeschlossen ist, und markieren Sie die Option **Schlüssel erstellen auf Token: [Name der Smartcard oder des Token im System]**. Weitere Informationen über Smartcards und Tokens finden Sie unter [Schlüssel auf Smartcards und Tokens sichern](#).
5. Klicken Sie auf **Weiter**. Der Bildschirm „Zuweisung von Name und E-Mail“ wird angezeigt.
6. Geben Sie im Feld **Vollständiger Name** Ihren richtigen Namen und im Feld **Primäre E-Mail** Ihre korrekte E-Mail-Adresse ein. Es ist nicht unbedingt notwendig, Ihren echten Namen oder Ihre E-Mail-Adresse einzugeben. Durch die Verwendung Ihres echten Namens können andere Anwender Sie jedoch einfacher als den Besitzer Ihres öffentlichen Schlüssels identifizieren. Ihre echte E-Mail Adresse ist ebenfalls erforderlich, wenn Sie Ihren öffentlichen Schlüssel auf das PGP Global Directory hochladen (das ihn auf einfache Weise für andere PGP Desktop-Anwender verfügbar macht).
7. Falls Sie dem Schlüssel, den Sie erstellen, weitere E-Mail-Adressen hinzufügen wollen, klicken Sie auf **Mehr**. Geben Sie die Adressen in die entsprechenden Felder ein.
8. Falls Sie erweiterte Einstellungen für den Schlüssel angeben wollen, den Sie erstellen, klicken Sie auf **Erweitert**. Das Dialogfenster [Erweiterte Schlüsseleinstellungen](#) wird angezeigt. In diesem Dialogfeld können Sie den Typ, die Größe, die Gültigkeitsdauer und andere Einstellungen für den Schlüssel festlegen.
9. Wählen Sie Einstellungen für die folgenden Punkte aus:
 - **Schlüsseltyp**. Wählen Sie zwischen Diffie-Hellman/DSS und RSA.
 - **Separaten Signatur-Unterschlüssel generieren**. Markieren Sie dieses Feld, wenn Sie einen separaten Unterschlüssel zum Signieren benötigen. Zusammen mit dem neuen Schlüsselpaar wird ein separater Signatur-Unterschlüssel erstellt. Nachdem der neue Schlüssel erstellt wurde, können Sie jederzeit weitere Signatur- oder Verschlüsselungsschlüssel erstellen. Weitere

Informationen zu separaten Signatur- und Verschlüsselungsunterschlüsseln finden Sie unter [Unterschlüssel verwenden](#).

- **Schlüsselgröße.** Geben Sie zwischen 1024 Bit und 4096 Bit ein. Je größer der Schlüssel, desto sicherer ist er, desto länger dauert aber auch seine Erstellung. Einige Smartcards und Token begrenzen die Schlüsselgröße auf 1024 Bit.
 - **Ablaufdatum.** Wählen Sie „**Nie**“ aus oder geben Sie ein Datum an, an dem das Schlüsselpaar, das Sie erstellen, abläuft.
 - **Zulässige Algorithmen.** Entfernen Sie die Markierung aller Algorithmen, die vom erstellten Schlüsselpaar nicht unterstützt werden sollen.
 - **Bevorzugter Algorithmus.** Wählen Sie den Algorithmus aus, der in Fällen verwendet werden soll, für die kein Algorithmus festgelegt wurde. Nur ein zulässiger Algorithmus kann als bevorzugt festgelegt werden.
 - **Zulässige Hashes.** Entfernen Sie die Markierung aller Hashes, die vom erstellten Schlüsselpaar nicht unterstützt werden sollen.
 - **Bevorzugter Hash.** Wählen Sie den Hash aus, der in Fällen verwendet werden soll, für die kein Hash festgelegt wurde. Nur ein zulässiger Hash kann als bevorzugt festgelegt werden.
10. Klicken Sie auf **OK**, um das Dialogfeld „Erweiterte Schlüsseleinstellungen“ zu schließen.
 11. **Klicken Sie auf Weiter.**
 12. Wenn Ihr Computer zu einer mit PGP Universal zentral verwalteten Umgebung gehört, wird u. U. das Dialogfenster „Unternehmenseinstellungen“ angezeigt. Hier werden die Schlüssel aufgeführt, die der PGP-Administrator zu Ihrer Version von PGP Desktop hinzufügt (z. B. den Additional Decryption Key (ADK) des Unternehmens oder den Unternehmensschlüssel).

Der Bildschirm „Zuweisung des Passworts“ erscheint.

13. Geben Sie das Passwort ein, das Sie verwenden wollen, um den exklusiven Zugriff auf den privaten Schlüssel des erstellten Schlüsselpaars beizubehalten.
14. Zur Bestätigung Ihrer Eingabe drücken Sie die **Tabulatortaste**, um den Cursor in das Bestätigungsfeld zu setzen. Geben Sie dasselbe Passwort nochmals ein. Weitere Informationen zur Passwort-Qualitätsanzeige finden Sie unter [Passwort-Qualitätsanzeige](#).

Hinweis: Als zusätzliche Sicherheitsmaßnahme werden die für das Passwort eingegebenen Zeichen gewöhnlich nicht auf dem Bildschirm angezeigt. Wenn Sie jedoch sicher sind, dass Sie nicht beobachtet werden, und die Zeichen beim Eingeben des Passworts sehen möchten, aktivieren Sie die Option **Tastatureingabe anzeigen**.

Warnung: Niemand, auch nicht die PGP Corporation, kann einen Schlüssel wiederherstellen, dessen Passwort vergessen wurde, es sei denn, Ihr PGP-Administrator hat eine PGP-Schlüssel-Wiederherstellungsrichtlinie für Ihr Unternehmen implementiert.

15. Klicken Sie auf **Weiter**, um den Schlüsselerstellungsvorgang zu starten. PGP Desktop erstellt Ihr neues Schlüsselpaar.

Dieser Vorgang kann einige Minuten dauern.

16. Wenn der Schlüsselerstellungsvorgang anzeigt, dass er abgeschlossen ist, klicken Sie auf **Weiter**. Sie werden aufgefordert, den öffentlichen Teil des soeben erstellten Schlüssels zum PGP Global Directory hinzuzufügen.
17. Lesen Sie den Text auf dem Bildschirm, und klicken Sie auf **Weiter**, um den neuen Schlüssel dem PGP Global Directory hinzuzufügen (empfohlen). Klicken Sie auf **Überspringen**, wenn Sie nicht wollen, dass der öffentliche Schlüssel im PGP Global Directory veröffentlicht wird.
18. Klicken Sie auf **Fertig stellen**. Ihr neues PGP-Schlüsselpaar wurde erstellt. Es sollte im Arbeitsbereich von PGP Keys zu sehen sein. Falls es dort nicht aufgelistet ist, stellen Sie sicher, dass im Bedienfeld von PGP-Schlüssel **Alle Schlüssel** oder **Meine privaten Schlüssel** ausgewählt ist.

Achtung: Sie sollten an diesem Punkt eine Sicherheitskopie Ihrer privaten Schlüssel an einem sicheren Speicherort anfertigen. Ihre privaten Schlüssel sind sehr wichtig. Sollten sie abhanden kommen, könnte dies katastrophale Auswirkungen haben, wenn Sie Daten damit verschlüsselt haben. Weitere Informationen finden Sie unter [Privaten Schlüssel schützen](#).

Ihren privaten Schlüssel sichern

So sichern Sie Ihren privaten Schlüssel

1. Klicken Sie in PGP Desktop auf das PGP Key-Bedienfeld und wählen Sie **Eigene private Schlüssel** aus.
2. Wählen Sie das Symbol für Ihr Schlüsselpaar aus.
3. Klicken Sie auf **Datei > Exportieren**.
4. Geben Sie einen Dateinamen ein.
5. Aktivieren Sie das Kontrollkästchen **Inkl. private(n) Schlüssel**. Die ist wichtig, da sonst nur Ihr öffentlicher Schlüssel exportiert wird.
6. Klicken Sie auf **Speichern**.
7. Kopieren Sie die Datei (mit der Erweiterung .asc) an einen sicheren Speicherort. Hierbei kann es sich um eine CD handeln, die sorgfältig archiviert wird, um einen anderen PC oder um einen USB-Stick, der an einem sicheren Ort aufbewahrt wird. Denken Sie daran, dass diese Datei nicht an andere Personen weitergegeben werden darf, da sie sowohl Ihren privaten als auch Ihren öffentlichen Schlüssel enthält.