GnuPG

Schnellübersicht

Befehl	Kommentar
`gpg -e -r <Empfänger-Schlüssel-ID> <Datei>`	Datei verschlüsseln
`gpg -d <verschlüsselte-Datei.gpg> > entschlüsselte-Datei`	Datei entschlüsseln
`gpg --import private-key.asc`	Schlüssel importieren
`gpg --delete-key`	Gefolgt vom Namen oder Fingerabdruck

Komplettübersicht

Befehl	Kommentar
gpg -k	Liste der Schlüssel

Verschlüsseln

Um eine Datei mit GnuPG auf einem Debian Linux zu verschlüsseln, können Sie die folgenden Schritte ausführen:

GnuPG installieren

GnuPG installieren Falls GnuPG noch nicht auf Ihrem Debian Linux-System installiert ist, können Sie es mit folgendem Befehl installieren:

```
sudo apt-get update sudo apt-get install gnupg
```

Schlüsselpaar generieren

GnuPG-Schlüsselpaar generieren Falls Sie noch keinen GnuPG-Schlüssel haben, müssen Sie zuerst ein Schlüsselpaar generieren. Hierzu können Sie den folgenden Befehl ausführen:

```
gpg --gen-key
```

Dieser Befehl startet den Assistenten zur Schlüsselerstellung, der Sie durch die Schritte zur Erstellung eines Schlüsselpaars führt. Sie werden unter anderem nach Ihrem Namen, Ihrer E-Mail-Adresse und einem Passwort gefragt. Nachdem der Assistent abgeschlossen ist, wird Ihr Schlüsselpaar generiert und in Ihrem GnuPG-Schlüsselring gespeichert.

Datei verschlüsseln

Um eine Datei zu verschlüsseln, verwenden Sie den folgenden Befehl:

```
gpg -e -r <Empfänger-Schlüssel-ID> <Datei>
```

Ersetzen Sie `<Empfänger-Schlüssel-ID>` durch die Schlüssel-ID des Empfängers, an den Sie die verschlüsselte Datei senden möchten. Sie können die Schlüssel-ID des Empfängers entweder in dessen öffentlichem Schlüssel oder in einem Keyserver finden.

Beispiel:

```
gpg -e -r john@example.com secret.txt
```

Dieser Befehl verschlüsselt die Datei `secret.txt` mit dem öffentlichen Schlüssel, der mit der E-Mail-Adresse `john@example.com` verknüpft ist.

Schritt 4: Verschlüsselte Datei speichern Nachdem die Datei erfolgreich verschlüsselt wurde, wird eine neue Datei mit der Erweiterung `.gpg` erstellt, die die verschlüsselten Daten enthält. Sie können diese Datei nun an den Empfänger senden oder anderweitig speichern.

Das war's! Sie haben erfolgreich eine Datei mit GnuPG auf Debian Linux verschlüsselt. Der Empfänger kann die Datei mit seinem privaten Schlüssel entschlüsseln, um auf den Inhalt zuzugreifen

Entschlüsseln am Mac

Verschlüsseln mit GnuPG

Um Ihren privaten Schlüssel von einem Debian Linux-System auf einen Mac zu übertragen und eine mit GnuPG verschlüsselte Datei zu entschlüsseln, können Sie die folgenden Schritte ausführen:

Privaten Schlüssel exportieren

Auf Ihrem Debian Linux-System können Sie Ihren privaten Schlüssel mit dem folgenden Befehl exportieren:

```
gpg --export-secret-keys -o private-key.asc
```

Dieser Befehl exportiert Ihren privaten Schlüssel in eine Datei mit dem Namen `private-key.asc`. Sie sollten diese Datei sicher speichern, da sie Ihren privaten Schlüssel enthält und Zugriff darauf Dritten ermöglichen würde.

Privaten Schlüssel auf den Mac übertragen

Sie können den privaten Schlüssel `private-key.asc` auf den Mac übertragen, z.B. per E-Mail, USB-Stick oder über das Netzwerk.

GnuPG auf dem Mac installieren

Falls GnuPG noch nicht auf Ihrem Mac installiert ist, können Sie es mit folgendem Befehl installieren:

```
brew install gnupg
```

Hinweis: Sie müssen Homebrew auf Ihrem Mac installiert haben, um den obigen Befehl auszuführen. Informationen zur Installation von Homebrew finden Sie unter https://brew.sh/.

Privaten Schlüssel auf dem Mac importieren

Nachdem Sie den privaten Schlüssel `private-key.asc` auf den Mac übertragen haben, können Sie ihn mit dem folgenden Befehl importieren:

```
gpg --import private-key.asc
```

GnuPG importiert den privaten Schlüssel in Ihren Schlüsselring auf dem Mac.

Datei entschlüsseln

Nachdem Sie Ihren privaten Schlüssel erfolgreich auf dem Mac importiert haben, können Sie die mit GnuPG verschlüsselte Datei entschlüsseln. Verwenden Sie dazu den folgenden Befehl:

```
gpg -d <verschlüsselte-Datei.gpg> > entschlüsselte-Datei
```

Ersetzen Sie `<verschlüsselte-Datei.gpg>` durch den Dateinamen der verschlüsselten Datei und `<entschlüsselte-Datei>` durch den gewünschten Dateinamen für die entschlüsselte Datei.

Beispiel:

```
gpg -d secret.txt.gpg > secret-decrypted.txt
```

Dieser Befehl entschlüsselt die Datei `secret.txt.gpg` und speichert den entschlüsselten Inhalt in der Datei `secret-decrypted.txt`.

Das war's! Sie haben erfolgreich Ihren privaten Schlüssel von Debian Linux auf einen Mac übertragen und eine mit GnuPG verschlüsselte Datei entschlüsselt. Beachten Sie bitte, dass der private Schlüssel sensitiv ist und mit Vorsicht behandelt werden sollte, um unbefugten Zugriff zu vermeiden

Öffentlichen Schlüssel exportieren

Um einen öffentlichen Schlüssel zu exportieren, müssen Sie den öffentlichen Schlüssel in einer geeigneten Datei speichern. Hier ist ein Beispiel, wie Sie dies mit dem GnuPG (GNU Privacy Guard) Tool tun können, das oft für die Verwaltung von Schlüsselpaaren verwendet wird:

Öffnen Sie ein Terminal auf Ihrem Linux Debian-System.
Überprüfen Sie zunächst, ob GnuPG installiert ist. Wenn es nicht installiert ist, können Sie es mit dem folgenden Befehl installieren:

```
sudo apt-get update
sudo apt-get install gnupg
```

Exportieren Sie den öffentlichen Schlüssel mit dem gpg Befehl und speichern Sie ihn in einer Datei. Hier ist ein Beispielbefehl:

```
gpg --output <Dateiname>.asc --armor --export <Key-ID>
```

Ersetzen Sie `<Dateiname>` durch den gewünschten Dateinamen, unter dem der öffentliche Schlüssel gespeichert werden soll, und `<Key-ID>` durch die ID des öffentlichen Schlüssels, den Sie exportieren möchten. Sie können die ID Ihres öffentlichen Schlüssels mit dem Befehl `gpg --list-keys` anzeigen lassen.

Beachten Sie, dass der --armor-Schalter verwendet wird, um den exportierten Schlüssel im ASCII-Rüstungformat zu speichern, das häufig für die Weitergabe von Schlüsseln über Text basierte Kanäle wie E-Mail verwendet wird.

Nachdem der Befehl ausgeführt wurde, wird der öffentliche Schlüssel in der angegebenen Datei mit der Erweiterung .asc gespeichert. Sie können die Datei mit einem Texteditor öffnen, um den exportierten öffentlichen Schlüssel anzuzeigen oder ihn auf andere Weise weiterzugeben, z. B. per E-Mail oder auf einer Webseite.
Bitte beachten Sie, dass der öffentliche Schlüssel allgemein zugänglich ist und von jedermann verwendet werden kann, um Ihnen verschlüsselte Nachrichten zu senden oder Ihre Signaturen zu überprüfen. Schützen Sie daher den exportierten öffentlichen Schlüssel sorgfältig und übertragen Sie ihn sicher an die beabsichtigten Empfänger

Öffentlichen Schlüssel importieren

Um einen öffentlichen Schlüssel zu importieren und damit Dateien zu verschlüsseln, können Sie das GnuPG (GNU Privacy Guard) Tool verwenden. Hier ist ein Beispiel, wie Sie dies auf einem Linux Debian-System tun können:

Öffnen Sie ein Terminal auf Ihrem Linux Debian-System.
Überprüfen Sie zunächst, ob GnuPG installiert ist. Wenn es nicht installiert ist, können Sie es mit dem folgenden Befehl installieren:

```
sudo apt-get update
sudo apt-get install gnupg
```

Laden Sie den öffentlichen Schlüssel herunter oder erhalten Sie ihn von der Person, die Ihnen die Dateien verschlüsselt hat. Der öffentliche Schlüssel wird normalerweise in einer Datei mit der Erweiterung .asc oder .gpg bereitgestellt.
Importieren Sie den öffentlichen Schlüssel mit dem gpg Befehl. Hier ist ein Beispielbefehl:

```
gpg --import <Dateiname>.asc
```

Ersetzen Sie `<Dateiname>` durch den tatsächlichen Namen der Datei, die den öffentlichen Schlüssel enthält.

GnuPG wird den öffentlichen Schlüssel importieren und in Ihrem GnuPG-Schlüsselbund speichern. Sie können nun Dateien mit dem importierten öffentlichen Schlüssel verschlüsseln. Verwenden Sie dazu den gpg Befehl und geben Sie den Dateinamen als Argument an. Hier ist ein Beispielbefehl:

```
gpg --encrypt --recipient <Empfänger> <Dateiname>
```

Ersetzen Sie <Empfänger> durch den Namen oder die E-Mail-Adresse des Empfängers, für den Sie die Dateien verschlüsseln möchten, und <Dateiname> durch den Namen der Datei, die Sie verschlüsseln möchten.

GnuPG erstellt eine verschlüsselte Version der Datei mit der Erweiterung .gpg. Diese verschlüsselte Datei kann an den Empfänger gesendet werden. Der Empfänger kann die Datei dann mit seinem privaten Schlüssel entschlüsseln.
Bitte beachten Sie, dass der private Schlüssel, der zum Entschlüsseln der Dateien benötigt wird, geheim und sicher aufbewahrt werden muss und nicht an unbefugte Personen weitergegeben werden darf

Keyserver

Unter keyserver2.gnupg.org kann man seinen Key Hochladen und auch andere finden.

Schlüssel vertrauen

1. Schlüssel überprüfen: Überprüfen Sie Ihren eigenen Schlüssel, um sicherzustellen, dass er korrekt erstellt wurde. Sie können dies tun, indem Sie den Fingerabdruck Ihres Schlüssels überprüfen und ihn mit anderen vertrauenswürdigen Quellen, z.B. Ihrer eigenen Notiz oder einem vertrauenswürdigen Freund, abgleichen.
2. Vertrauenseinstellungen ändern: Ändern Sie die Vertrauenseinstellungen für Ihren eigenen Schlüssel. Verwenden Sie dazu den Befehl `gpg --edit-key` gefolgt von Ihrem Schlüsselnamen oder Fingerabdruck. Dies öffnet den GnuPG-Editor für Ihren Schlüssel.
3. Vertrauensstellung festlegen: Im GnuPG-Editor können Sie die Vertrauensstellung für Ihren eigenen Schlüssel festlegen. Verwenden Sie den Befehl `trust`, gefolgt von der gewünschten Vertrauensstufe, die Sie für Ihren eigenen Schlüssel festlegen möchten. Zum Beispiel können Sie die Vertrauensstufe "Ultimate" (höchstes Vertrauen) festlegen, indem Sie `5` eingeben und mit Enter bestätigen.
4. Änderungen speichern: Speichern Sie die vorgenommenen Änderungen im GnuPG-Editor mit dem Befehl `save` und bestätigen Sie die Speicherung mit Enter.
5. Editor verlassen: Verlassen Sie den GnuPG-Editor mit dem Befehl `quit`, um zum Hauptterminal zurückzukehren.

Schlüssel löschen

- Geben Sie den Befehl `gpg --list-keys` ein, um eine Liste der vorhandenen Schlüssel in Ihrem GnuPG-Schlüsselbund anzuzeigen. Finden Sie den Schlüssel, den Sie entfernen möchten, anhand seines Namens oder seines Fingerabdrucks.
- Geben Sie den Befehl `gpg --delete-key` gefolgt von dem Namen oder Fingerabdruck des Schlüssels ein, den Sie entfernen möchten. Zum Beispiel: `gpg --delete-key JohnDoe` oder `gpg`

`--delete-key 0x12345678`.

Revision #8
Created 12 April 2023 18:32:04 by Admin
Updated 14 April 2023 10:35:55 by Hermann