Konfigurieren der Authentifizierung mit dem privaten Schlüssel mithilfe der ISE

Inhalt

Einleitung

Voraussetzungen

- Anforderungen
- Verwendete Komponenten

Konfigurieren

- Erstellen des privaten und öffentlichen Schlüssels in Windows
- Erstellen der privaten und öffentlichen Schlüssel über in MacOS
- Konfigurieren des Zertifikats für die Anmeldung bei der ISE

Überprüfung

- Anmelden in Windows
- Anmelden in MacOS
- Anmelden Putty

Fehlerbehebung

- Fehler beim Importieren des öffentlichen Schlüssels

Einleitung

In diesem Dokument wird beschrieben, wie Sie einen privaten SSH-Schlüssel (Secure Shell) für die Authentifizierung bei der CLI der Identity Secure Engine (ISE) erstellen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Repository in der ISE.
- Authentifizierung des Zertifikats.

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

- ISE 3.3 Patch 3
- Windows 10
- MacOS X

- SSH-Client-Putty

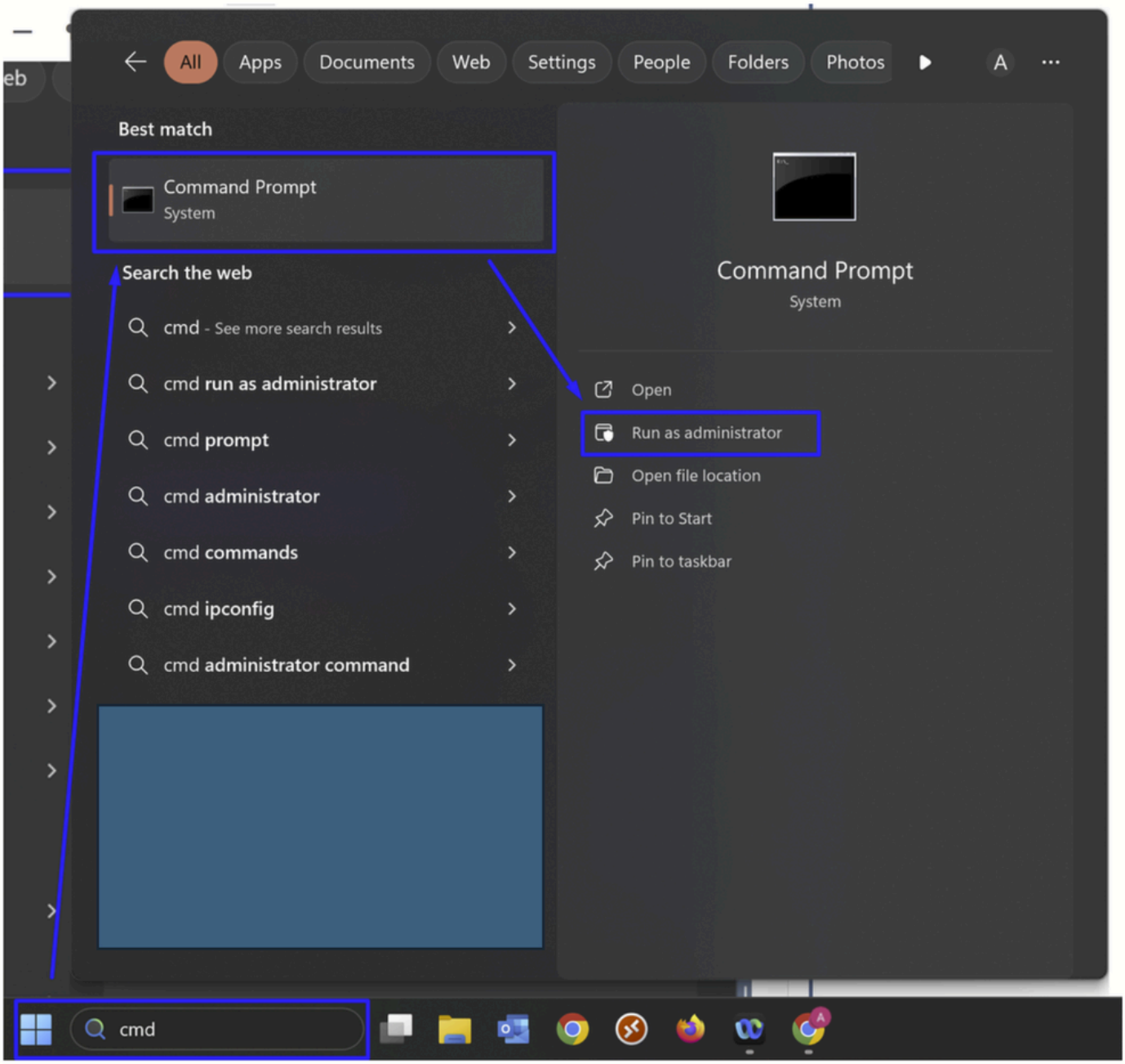
Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Konfigurieren

Erstellen des privaten und öffentlichen Schlüssels in Windows

Klicken Sie in der Taskleiste auf das Symbol Search (Suchen):

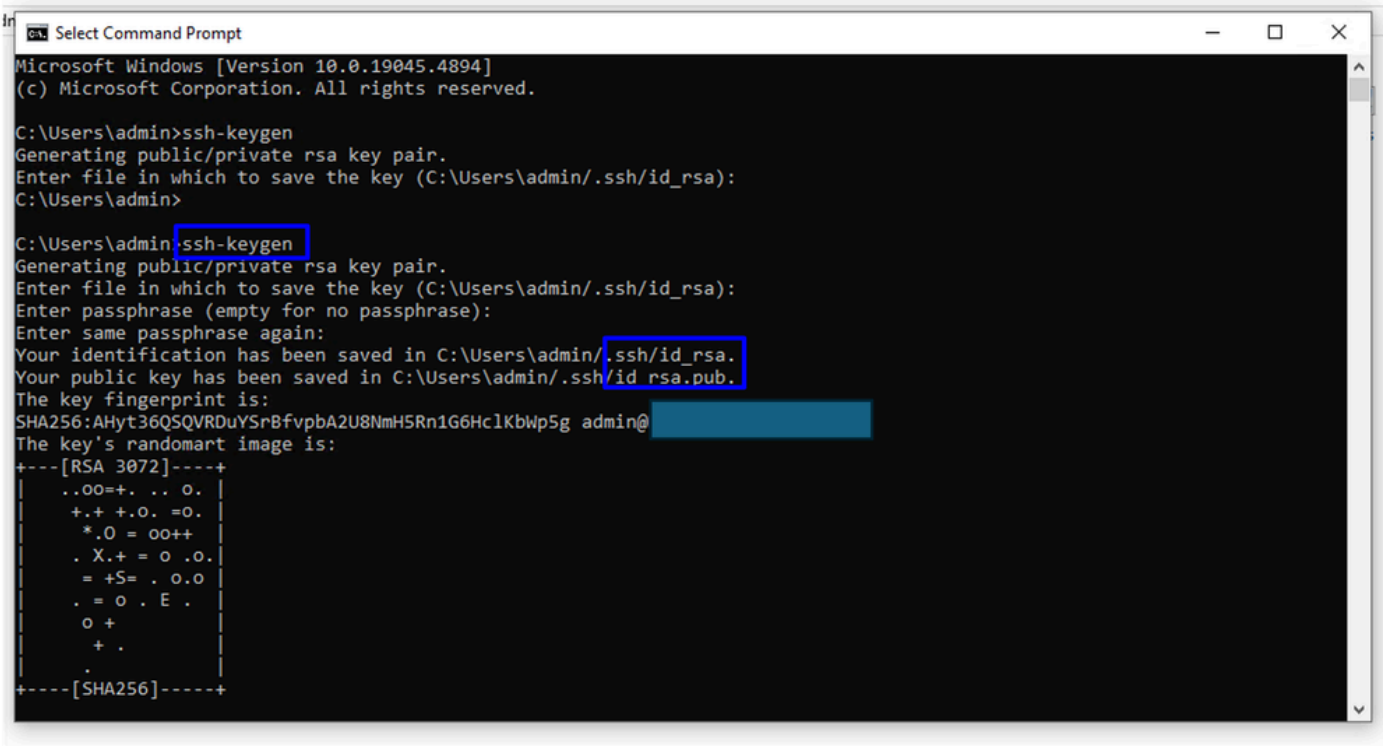
- Geben Sie cmd in die Suchleiste ein
- Klicken Sie in den Suchergebnissen mit der rechten Maustaste auf Eingabeaufforderung, und wählen Sie Als Administrator ausführen aus. Dadurch wird sichergestellt, dass Sie über die erforderlichen Berechtigungen zum Ausführen von Befehlen verfügen.



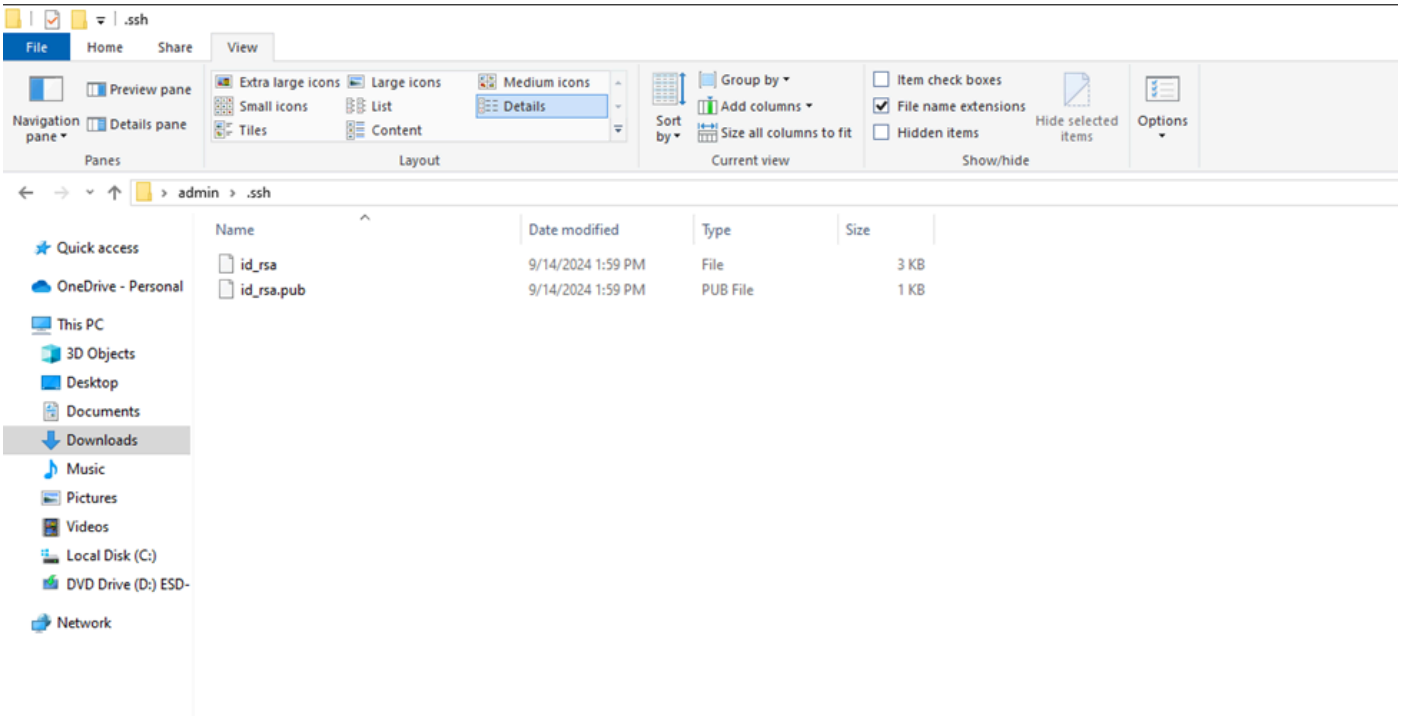
- Führen Sie den nächsten Befehl aus:

```
ssh-keygen
```

- Sie werden aufgefordert, den Verschlüsselungsschlüssel zweimal einzugeben. Speichern Sie das Kennwort, da es für die Authentifizierung gegenüber der ISE als neues Kennwort verwendet wird. Danach werden zwei Dateien erstellt, die privaten (id_rsa) und die öffentlichen (id_rsa.pub) Schlüssel. Speichern Sie die Dateien in einem Verzeichnis. Zum Beispiel wurde die Standardeinstellung verwendet



- Überprüfen Sie, wo die Dateien gespeichert sind



Übertragen Sie den öffentlichen Schlüssel **(id_rsa.pub)** in den Datei-Repository-Ordner, der auf der ISE konfiguriert ist.

Erstellen der privaten und öffentlichen Schlüssel über in MacOS

Klicken Sie auf das **Finder** Symbol im Dock.

- Navigieren Sie zum **Applications folder**
- Suchen Sie im Ordner Utilities **Applications folder**(Dienstprogramme), und öffnen Sie ihn.
- Suchen Sie in der Liste Dienstprogramme nach **Terminal**
- Doppelklicken Sie auf **Terminal** , um es zu öffnen.
- Geben Sie im **Terminal** Fenster "ssh-keygen -t rsa" ein, und drücken Sie die Eingabetaste, um die Eingabe auszuführen.
- Schreiben Sie den Verschlüsselungsschlüssel zweimal und **save it**
- Gehe zum Dateispeicherort

Übertragen Sie den öffentlichen Schlüssel **(id_rsa.pub)** in den Datei-Repository-Ordner, der auf der ISE konfiguriert ist.

```
Your identification has been saved in /Users/myname/.ssh/id_rsa.
Your public key has been saved in /Users/myname/.ssh/id_rsa.pub.
The key fingerprint is:
ae:89:72:0b:85:da:5a:f4:7c:1f:c2:43:fd:c6:44:38 myname@mymac.local
The key's randomart image is:
+--[ RSA 2048]----+
|                 |
|          .      |
|         E .     |
|    .    . o     |
|  o . . S .      |
| + + o . +       |
|. + o = o +      |
| o...o * o       |
|.  oo.o .        |
+-----------------+
```

Konfigurieren des Zertifikats für die Anmeldung bei der ISE

Bestätigen Sie, ob sich die öffentliche Datei unter dem Repository befindet, indem Sie den folgenden Befehl verwenden:

```
show repository
```

```
ise-primary-33/admin#
ise-primary-33/admin#show repository Sever_all
Backup-Cisco-CFG10-240222-0915.tar.gpg
cisco-secure-client-win-5.0.05040-core-vpn-webdeploy-k9.msi
cisco-secure-client-win-5.0.05040-webdeploy-k9.pkg
Ethernet1.xml
FullReport_29-Mar-2024.csv
grise04conf-CFG10-240213-2200.tar.gpg
id_rsa.pub
```

- Importieren Sie die Datei mit dem öffentlichen Schlüssel **(id_rsa.pub)** mithilfe des Befehls im privilegierten Modus:

```
crypto key import

        repository
```

```
ise-primary-33/admin#crypto key import public.pub repository Sever all
```

- Wechseln Sie in den globalen Konfigurationsmodus, und verwenden Sie den folgenden Befehl:

```
service sshd PubkeyAuthentication
```

```
ise-primary-33/admin(config)#service sshd PubkeyAuthentication
  Enabling key pair authentication automatically disables password-based
authentication.
%
% To enable key pair authentication in this Cisco ISE node,
% add at least one public key to the node. You must add
% a public key even if you want to configure private key usage in a later
step.
% If you don't already have a public key file in your system,
% add one to a repository now. Then, import the key file with the following
command:
% crypto key import <public key filename> repository <repository name>
```

Verwenden Sie den Befehl, um sicherzustellen, dass Sie beim Importieren des öffentlichen Schlüssels keine Fehler erhalten. Es wird empfohlen, diesen Vorgang über den Konsolenport fortzusetzen, um einen Verlust des Zugriffs auf die ISE zu vermeiden.

Überprüfung

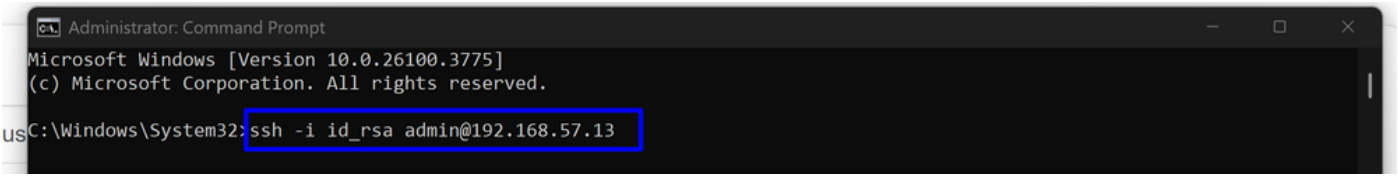
Anmelden in Windows

Versuchen Sie, mithilfe des folgenden Befehls auf die ISE zuzugreifen**cmd**:

```
ssh -i

        @


EXAMPLE:
ssh -i id_rsa admin@192.168.57.13
```



Verwenden Sie den Verschlüsselungsschlüssel, der im Schritt Erstellen der privaten und öffentlichen Schlüssel in Windows konfiguriert wurde, um sich zu authentifizieren.

Anmelden in MacOS

Geben Sie den folgenden Befehl in das Terminal ein:

```
ssh -i

        @
```

```
EXAMPLE:
ssh -i id_rsa admin@192.168.57.13
```

Oder

```
ssh -i ~/.ssh/
```

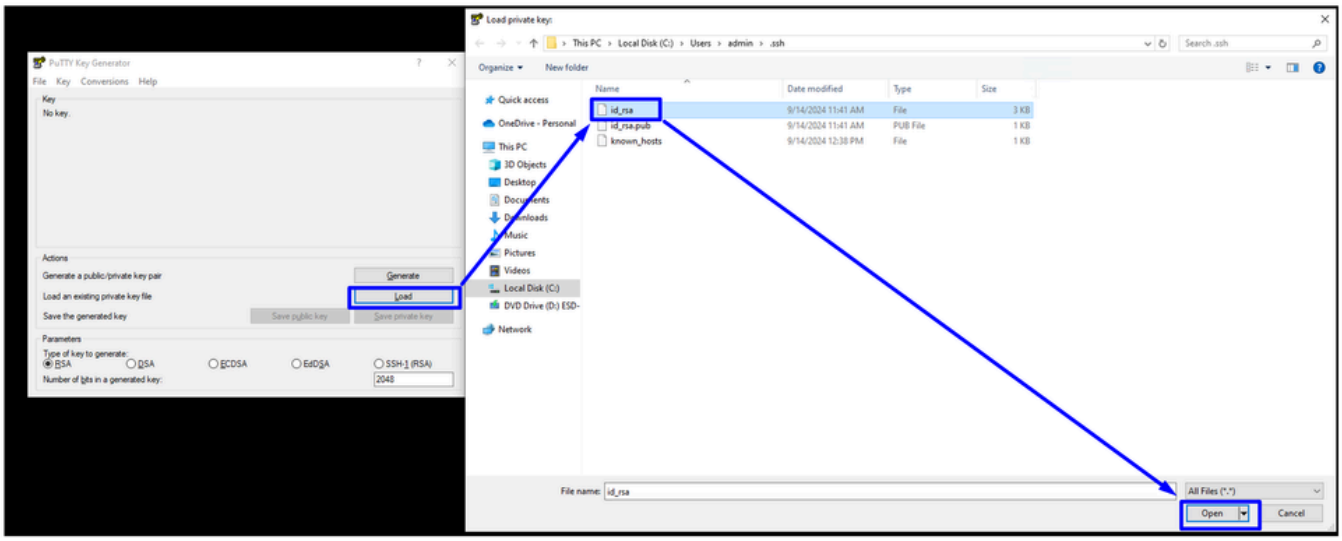
```
        @
```

```
EXAMPLE:
ssh -i ~/.ssh/id_rsa admin@192.168.57.13
```

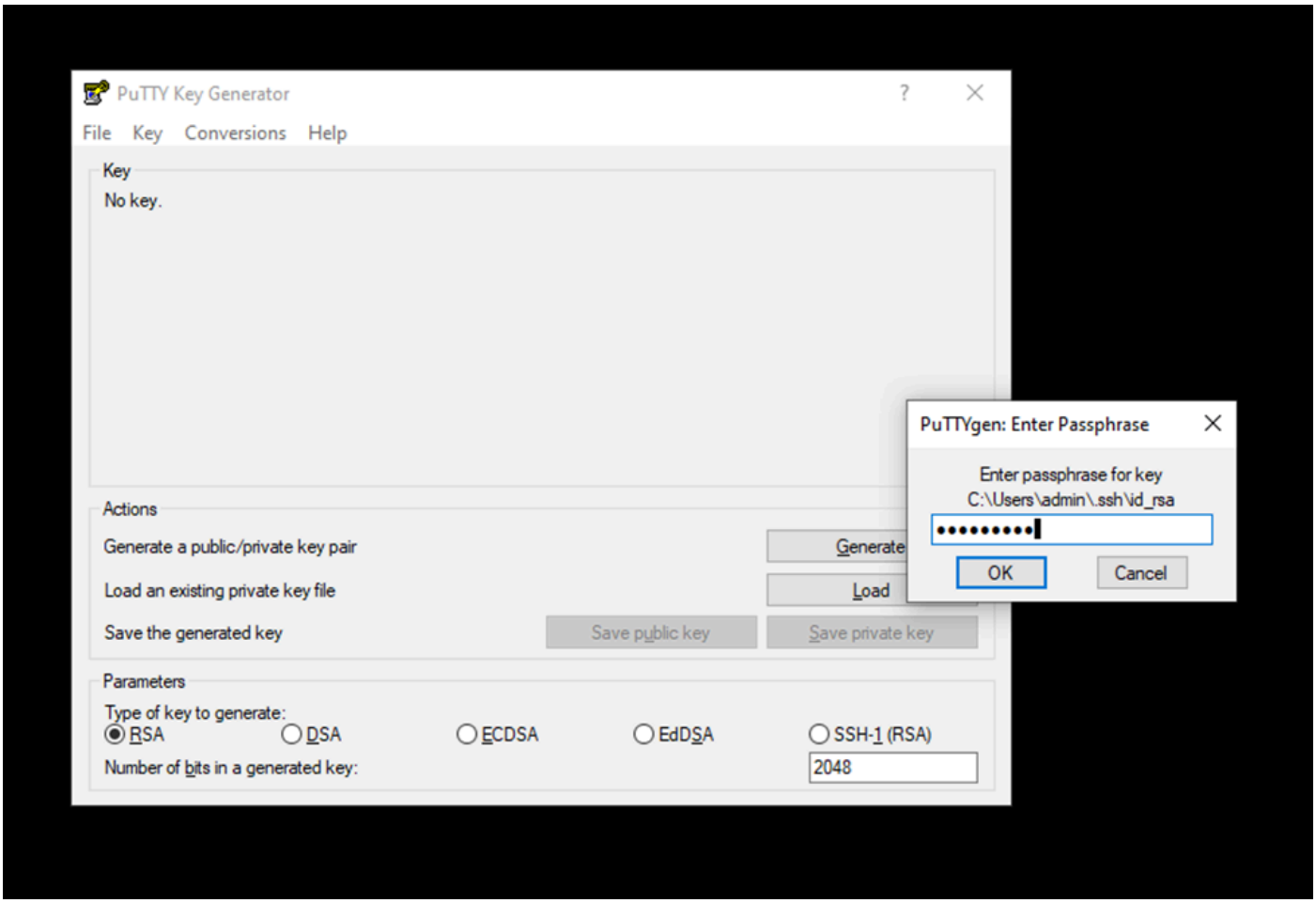
Verwenden Sie den im Schritt konfigurierten Verschlüsselungsschlüssel [Erstellen Sie die privaten und öffentlichen Schlüssel über in MacOS](), um sich zu authentifizieren.

Anmelden Putty

Öffnen PuTTy key generator (Suche nach PuttyGen in der Start-Suchleiste), klicken Sie auf Laden, wählen Sie alle Dateien, und öffnen Sie den privaten Schlüssel von cmd (Windows) oder Terminal (MacOS) generiert:

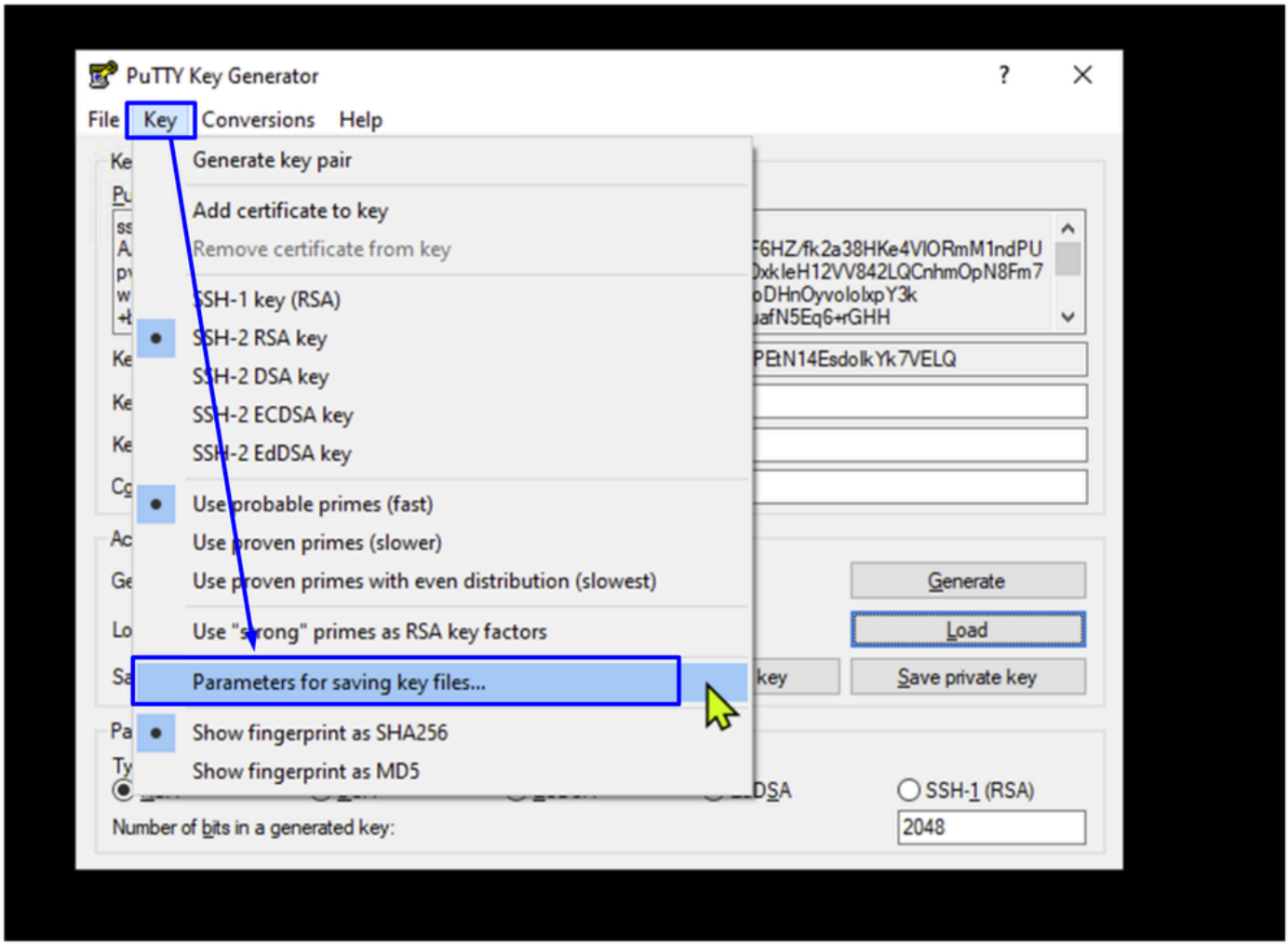


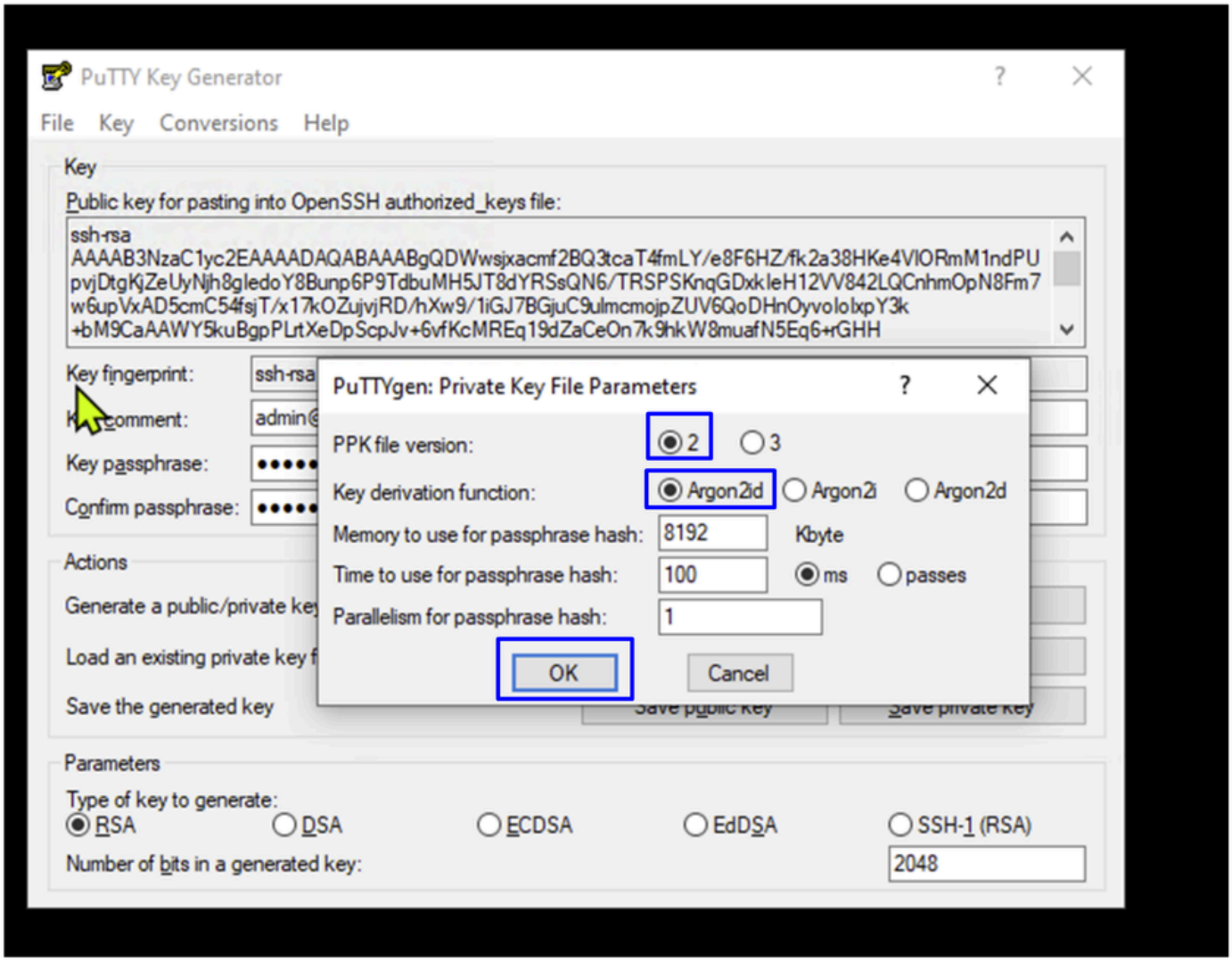
- Schreiben Sie den zuvor im Befehl oder Terminal verwendeten Verschlüsselungsschlüssel.



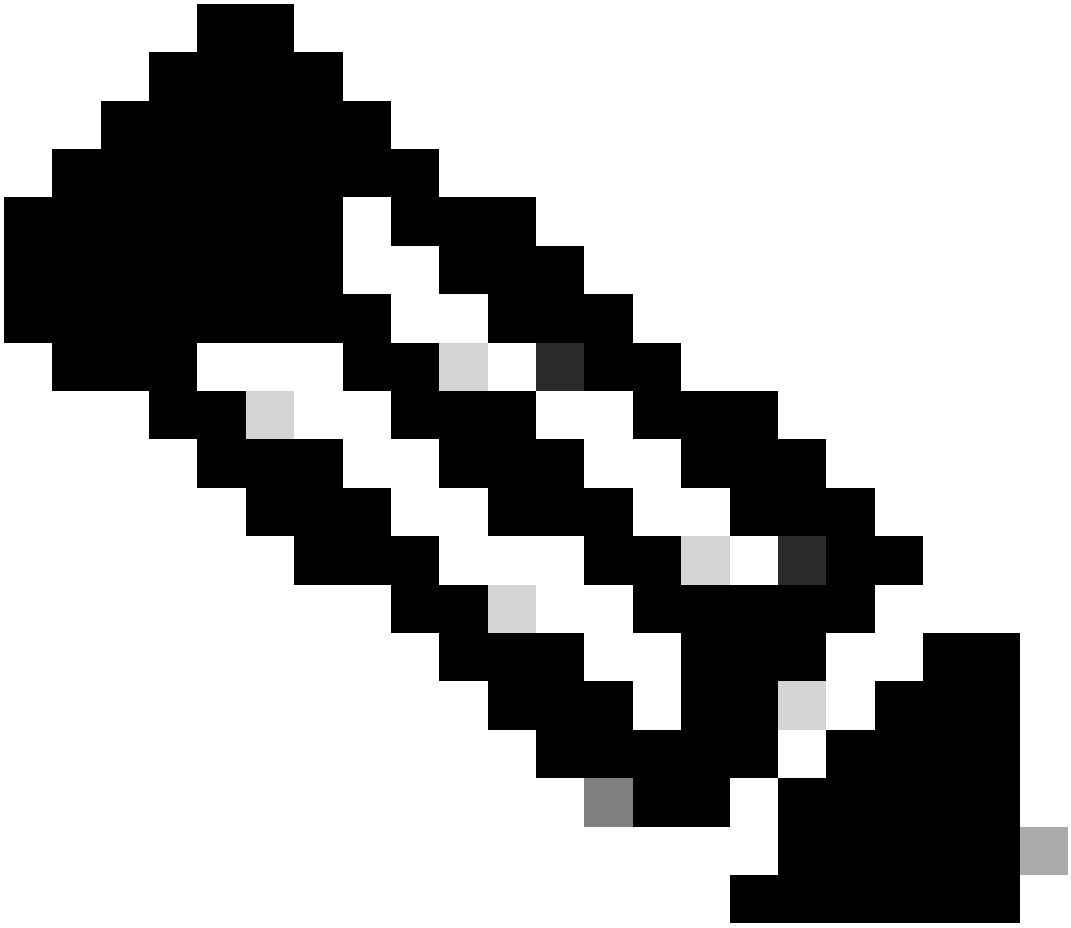
Konvertieren Sie diese Datei in eine Putty-Version kompatibel, indem Sie die folgenden Schritte ausführen:

- Klicken Sie auf Schlüssel > Parameter zum Speichern von Schlüsseldateien


PuTTY Key Generator
File
Key
Conversions
Help
Generate key pair
Add certificate to key
Remove certificate from key
SSH-1 key (RSA)
SSH-2 RSA key
SSH-2 DSA key
SSH-2 ECDSA key
SSH-2 EdDSA key
Use probable primes (fast)
Use proven primes (slower)
Use proven primes with even distribution (slowest)
Use "strong" primes as RSA key factors
Parameters for saving key files...
Show fingerprint as SHA256
Show fingerprint as MD5
Generate
Load
Save private key
SSH-1 (RSA)
Number of bits in a generated key:
2048

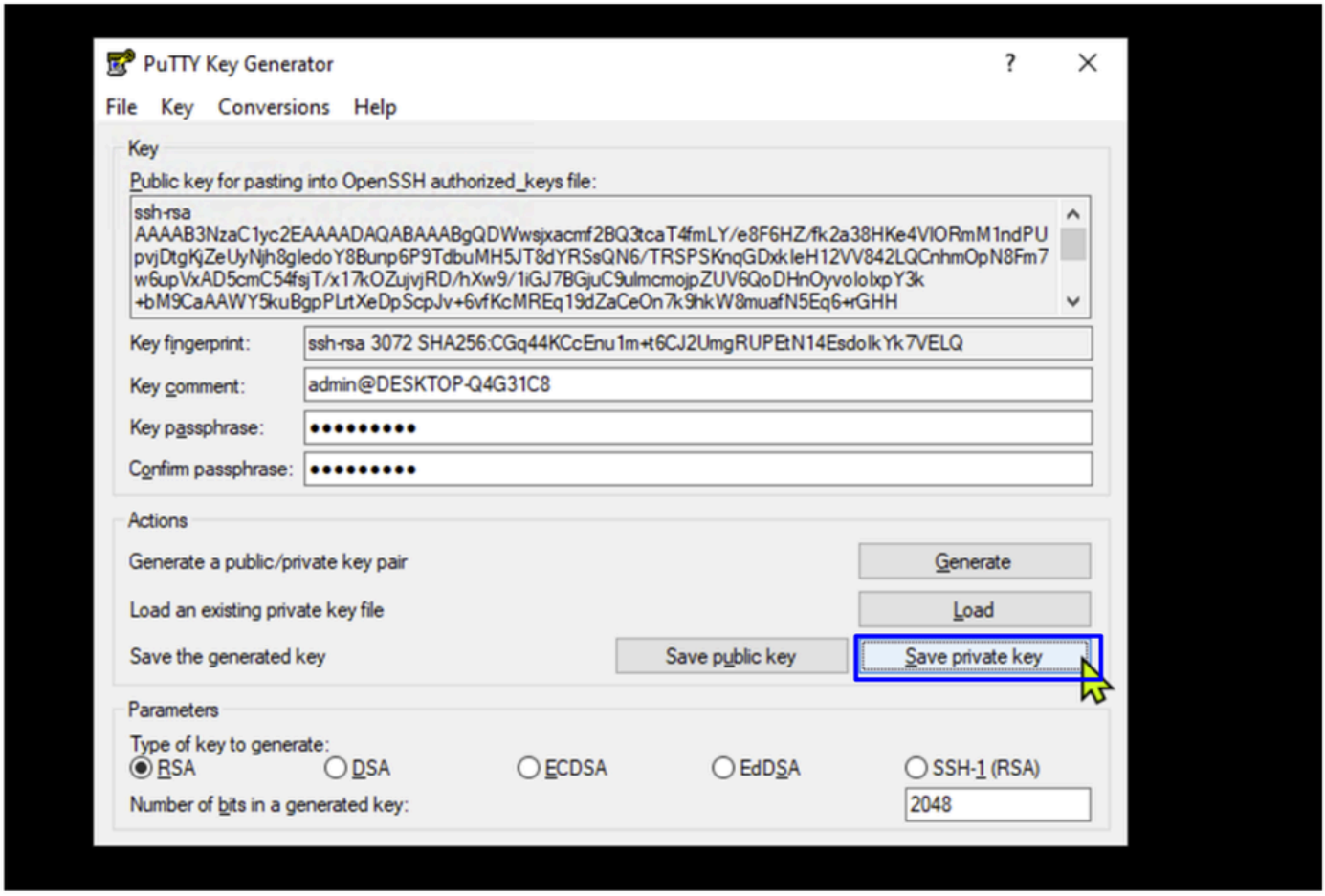


- PPK file version : 2 auswählen
- **Key derivation function**: Argon2id auswählen



Anmerkung: Verwenden Sie für die übrigen Parameter die Standardwerte.

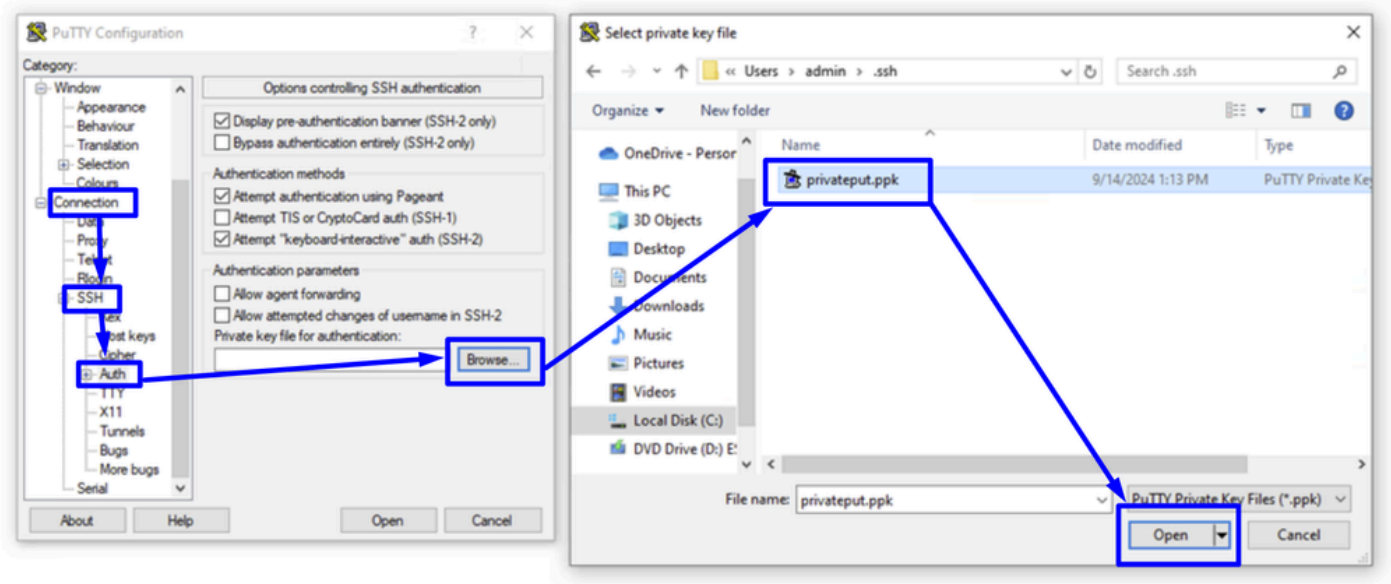
- Klicken Sie auf Ok



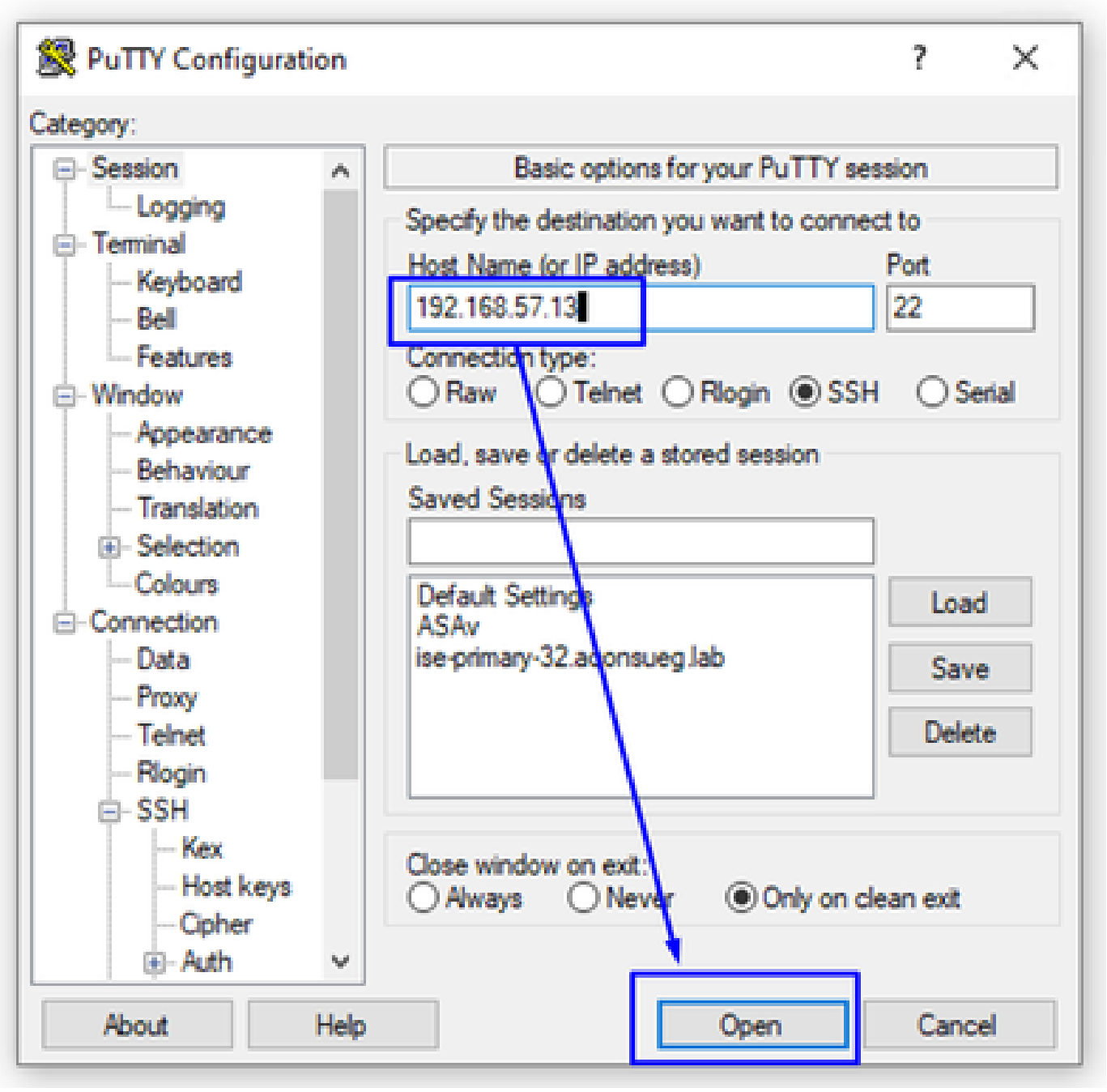
- Klicken Sie Save private Key

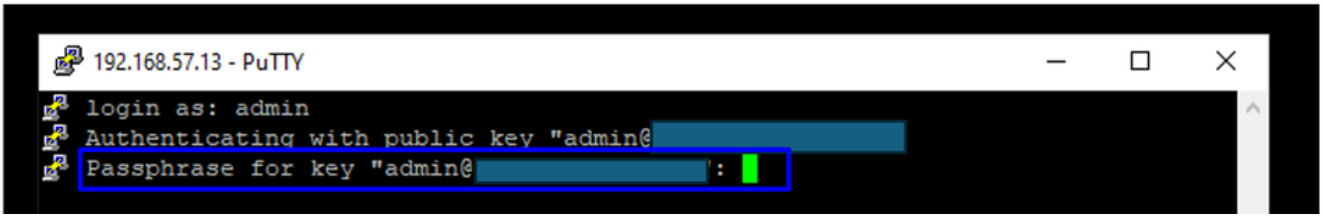
Nachdem Sie den Schlüssel auf Ihrem Computer gespeichert haben, können Sie ihn verwenden, indem Sie auf die folgenden Beispiele verweisen:

- Putt öffnen
- Klicken Sie auf **Connection > SSH > Auth > Browse**
- Wählen Sie Ihren privaten Schlüssel aus, und klicken Sie auf Open



- Kehren Sie zu Sitzung zurück, und legen Sie die IP-Adresse oder den Hostnamen (FQDN) der ISE fest.
- Öffnen





Verwenden Sie den im Schritt konfigurierten Verschlüsselungsschlüssel Erstellen Sie die privaten und öffentlichen Schlüssel über in MacOS oder Erstellen Sie die privaten und öffentlichen Schlüssel in Windows, um sich zu authentifizieren.

Fehlerbehebung

Auschecken von Fehlermeldungen vom Endpunktstandort, Hinzufügen des Flags -v zur SSH-Verbindung

```
Example for Windows:
ssh -v -i id_rsa admin@192.168.57.13
```

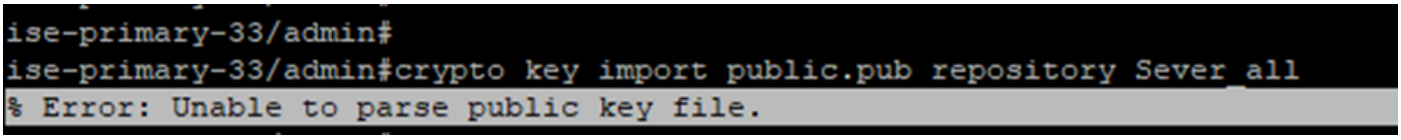
```
Example for MacOS:
ssh -v -i id_rsa admin@192.168.57.13
```

Oder

```
ssh -v -i ~/.ssh/id_rsa admin@192.168.57.13
```

Fehler beim Importieren des öffentlichen Schlüssels

% Fehler: Die Datei mit dem öffentlichen Schlüssel kann nicht analysiert werden.



Wenn Sie beim Importieren mehrerer öffentlicher Schlüssel Schwierigkeiten haben, wenden Sie sich an den Cisco Support.

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.