Docusnap X - Linux Inventarisierung mit Authentifizierung per RSA-Schlüssel

RSA-Schlüssel in Docusnap verwenden

TITEL	Docusnap X - Linux Inventarisierung mit Authentifizierung per RSA-Schlüssel
AUTOR	Docusnap Consulting
DATUM	18.12.2018
VERSION	1.1 | gültig ab 26.09.2018

INHALTSVERZEICHNIS

1. Einleitung

Für die remote Inventarisierung von Linux Systemen mit Docusnap benötigen Sie den root-User. Nur mit dem root-User ist sichergestellt, dass Sie alle Informationen des Systems inventarisieren können. Sollte bei Ihnen der root-User nicht zur Verfügung stehen oder der Zugriff mittels root-User über SSH gesperrt sein, haben Sie zwei weitere Möglichkeiten, wie Sie die Inventarisierung Ihrer Linux Systeme durchführen können.

1. Verwenden Sie die skriptbasierte Inventarisierung für Linux Systeme - Zum HowTo
2. Nutzen Sie einen RSA-Schlüssel zur Authentifizierung an remote Systemen

Dieses HowTo beschreibt das Anlegen eines RSA-Schlüssels. Diesen RSA-Schlüssel können Sie anschließend zur Authentifizierung an den Linux Systemen verwenden, um diese zu inventarisieren.

WICHTIG: Ab der Version 10.0.884.3 wird das OpenSSH-Format für die Generierung des privaten SSH Schlüssels in Docusnap verwendet. Wenn Sie bereits in einer der Vorversionen von Docusnap einen RSA Schlüssel zur Authentifizierung verwendet haben, können Sie diesen zunächst weiter nutzen. Sie sollten diesen jedoch zeitnah ersetzen - Kapitel 4.

Folgend finden Sie die, in diesem HowTo beschriebenen, Schritte zur Einrichtung des RSA-Schlüssels:

Kapitel 2 beschreibt, wie Sie grundsätzlich die Nutzung eines RSA-Schlüssels in Docusnap aktivieren und diesen RSA-Schlüssel in Docusnap erstellen können.

Kapitel 3 beschreibt Ihnen die Möglichkeit, einen RSA-Schlüssel mit dem PuTTY Key Generator zu erstellen.

Kapitel 4 beschreibt, wie Sie einen vorhandenen RSA-Schlüssel in das OpenSSH-Format konvertieren können, damit Sie diesen RSA-Schlüssel weiterhin in Docusnap verwenden können.

Kapitel 5 zeigt Ihnen, wie Sie den konvertierten RSA-Schlüssel in Docusnap importieren und anschließend nutzen können.

Kapitel 6 beschreibt Ihnen die Vorgehensweise, wie Sie den zuvor erstellten oder konvertierten RSA-Schlüssel auf den Linux Systemen hinterlegen.

2. Erstellung und Nutzung eines RSA-Schlüssels in Docusnap

Docusnap bietet Ihnen die Möglichkeit, einen RSA-Schlüssel für die Linux Inventarisierung zu erstellen. Den RSA Schlüssel können Sie in den Inventarisierungs-Optionen erstellen.

Bitte beachten Sie, dass Sie nur einen RSA-Schlüssel in Docusnap anlegen können!

Rufen Sie dazu den Options-Dialog auf.

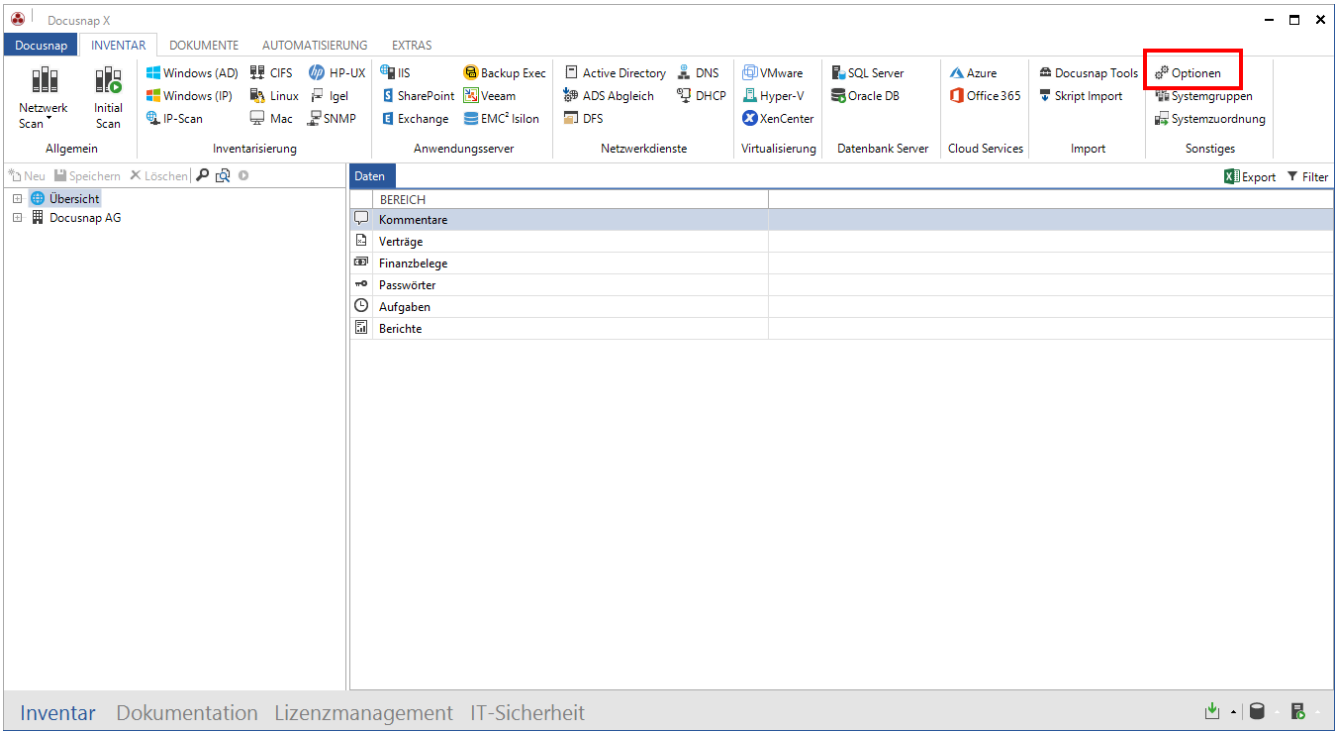

Abbildung 1 - Inventarisierungs-Optionen aufrufen

Im nächsten Schritt aktivieren Sie die Option **RSA-Schlüssel für die Inventarisierung verwenden** und erstellen den RSA-Schlüssel über die Schaltfläche **Neu**.

Das Schlüsselpaar wird mit der RSA Methode verschlüsselt. Der verwendete Schlüssel wird anschließend nochmals verschlüsselt und in der Datenbank abgelegt. Eine Passphrase wird nicht erstellt.

Möchten Sie die Sicherheit erhöhen und zusätzlich eine Passphrase hinterlegen, können Sie den RSA-Schlüssel mit einem Drittprodukt (z. B. PuTTY Key Gen) erstellen. In diesem Fall beachten Sie bitte Kapitel 3.

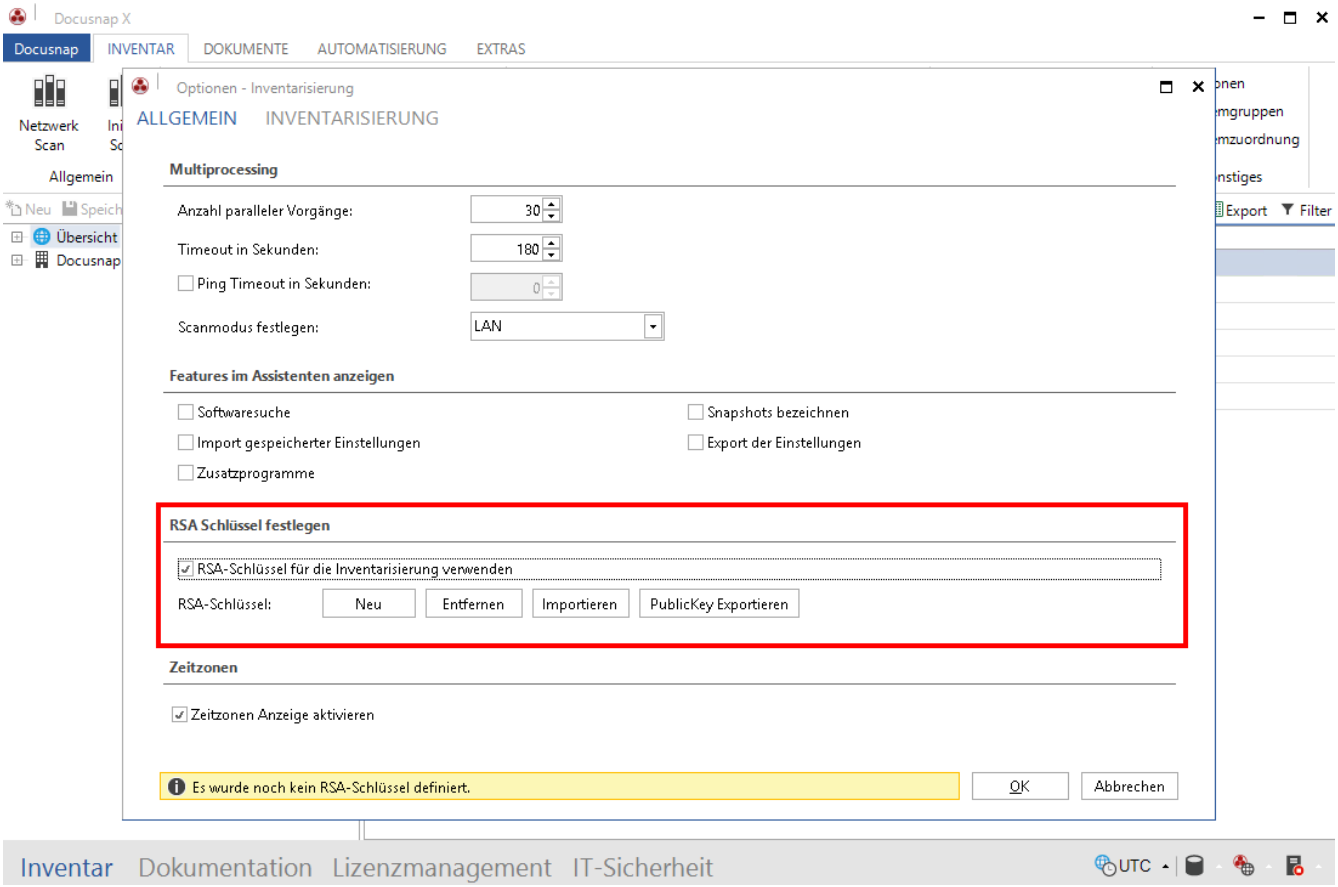

Abbildung 2 - RSA-Schlüssel aktivieren und erstellen

Über die Schaltfläche **PublicKey Exportieren** können Sie den öffentlichen Schlüssel exportieren und auf den Linux Systemen hinterlegen - siehe Kapitel 6.

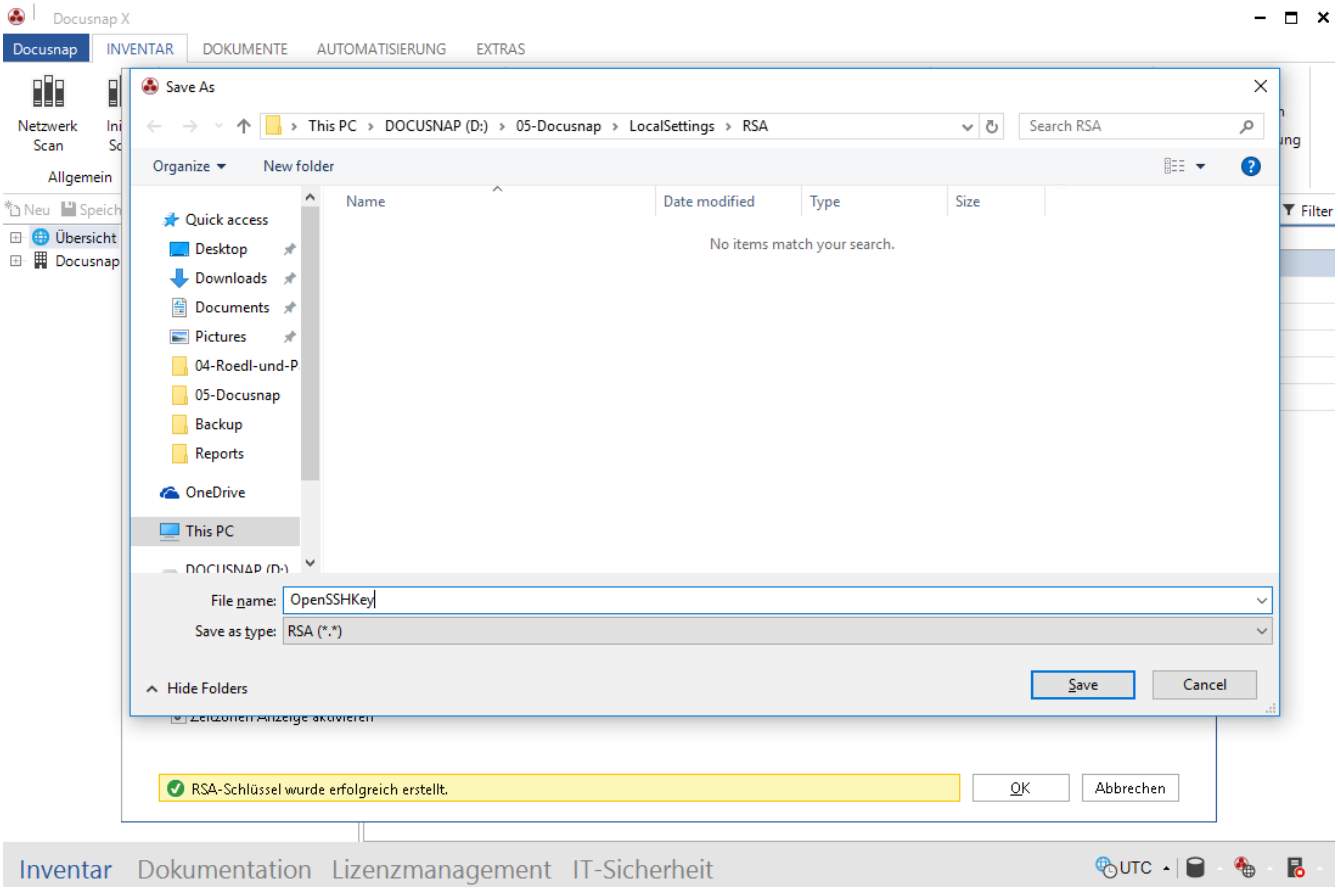

Abbildung 3 - Export des RSA-Schlüssels

3. Erstellung eines RSA-Schlüssels mit PuTTY Key Generator

Damit Sie den RSA-Schlüssel erstellen können, öffnen Sie das Programm PuTTY Key Generator (puttygen.exe).

Wählen Sie die entsprechenden Parameter für die Erstellung des Schlüssels - z. B. RSA, Bit Stärke 4096. Im Anschluss wählen Sie die Schaltfläche **Generate** und bewegen die Maus willkürlich im Programmfenster, solange bis der Fortschrittsbalken das Ende erreicht hat.

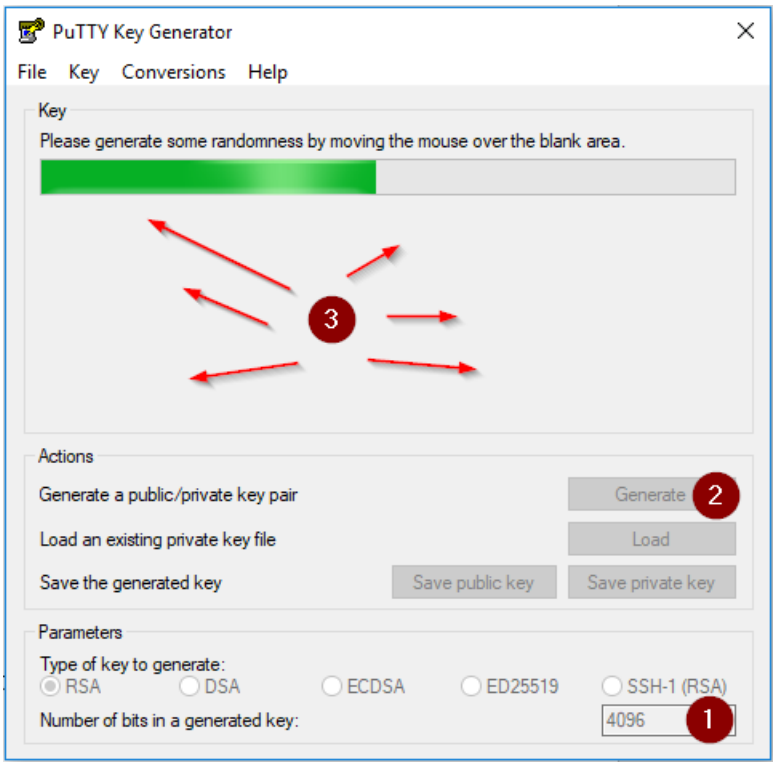

Abbildung 4 - Erstellung des RSA-Schlüssels in PuTTY

Nachdem der Schlüssel erstellt wurde, können Sie für eine erhöhte Sicherheit eine **Passphrase** definieren. Im Anschluss wählen Sie das Register **Conversions** und exportieren den **OpenSSH key**.

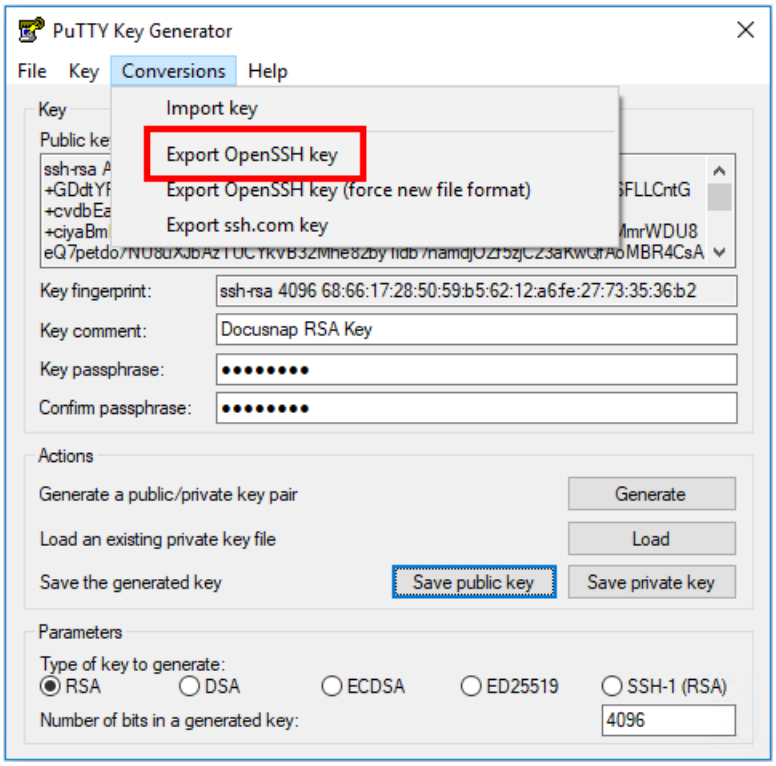

Abbildung 5 - Export des Keys in das OpenSSH Format

4. Migration eines RSA-Schlüssels in das OpenSSH Format

Ab der Version 10.0.884.3 wird ein neues Format (OpenSSH) des privaten SSH Schlüssels verwendet. Wird bereits ein Schlüssel verwendet, der nicht im OpenSSH Format vorliegt, sollten Sie diesen konvertieren.

Beachten Sie die folgenden Punkte, bevor Sie den privaten Schlüssel konvertieren:

- Erstellen Sie ein Datenbankbackup vor der Konvertierung.
- Der bereits verwendete private Schlüssel muss als Datei vorhanden sein, da ein Export des in Docusnap verwendeten privaten Schlüssels nicht möglich ist.
- Alle bestehenden Linux-Inventarisierungs-Jobs, die mit dem früheren RSA-Schlüssel Format erstellt wurden, müssen nachdem der neue OpenSSH Schlüssel importiert wurde, editiert und abgespeichert werden. Nachdem dies durchgeführt wurde, wird der neue RSA-Schlüssel für die Inventarisierung verwendet.

Für die Konvertierung des Schlüssels benötigen Sie das Programm **PuTTY Key Generator** (puttygen.exe).

Öffnen Sie PuTTY Key Generator und laden den privaten Schlüssel. Wenn Sie eine Passphrase verwenden, werden Sie aufgefordert diese einzutragen.

Öffnen Sie das Register **Conversions** und exportieren Sie den privaten Schlüssel als **OpenSSH key**.

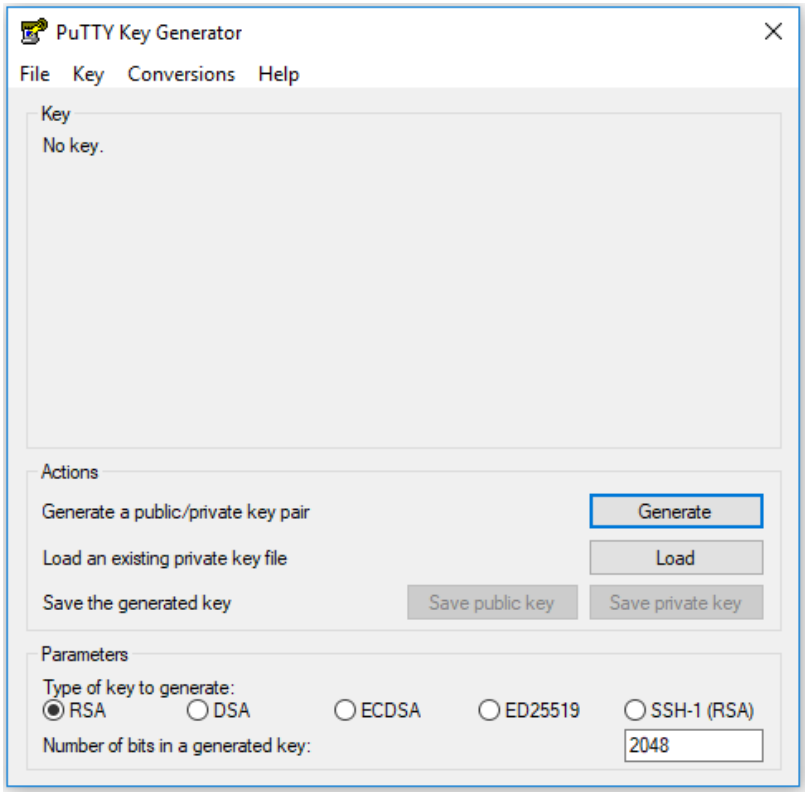

Abbildung 6 - Privaten Schlüssel in PuTTY Key Generator laden

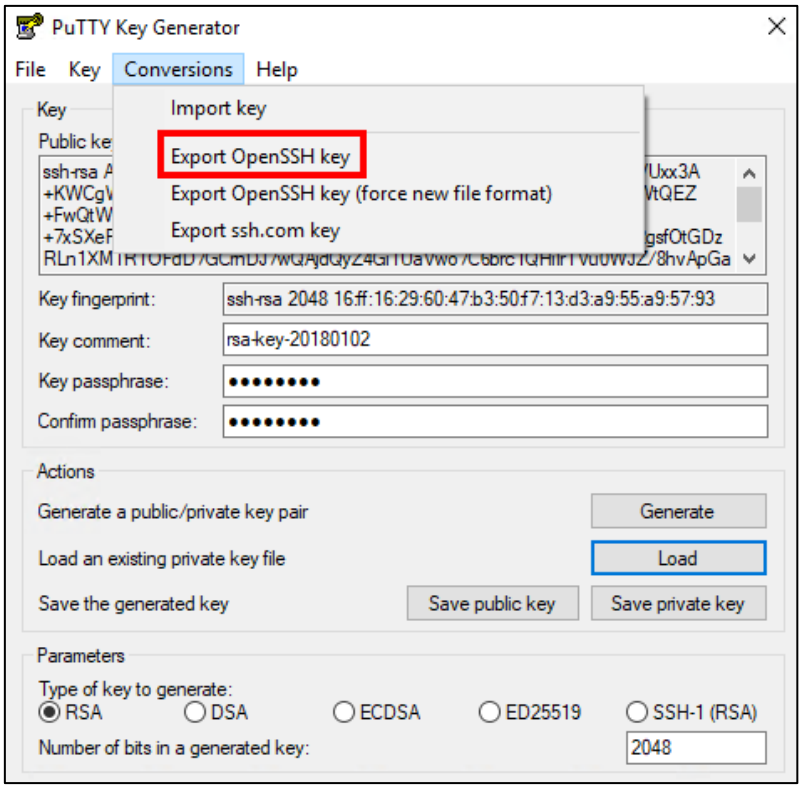

Abbildung 7 - Privaten Schlüssel exportieren

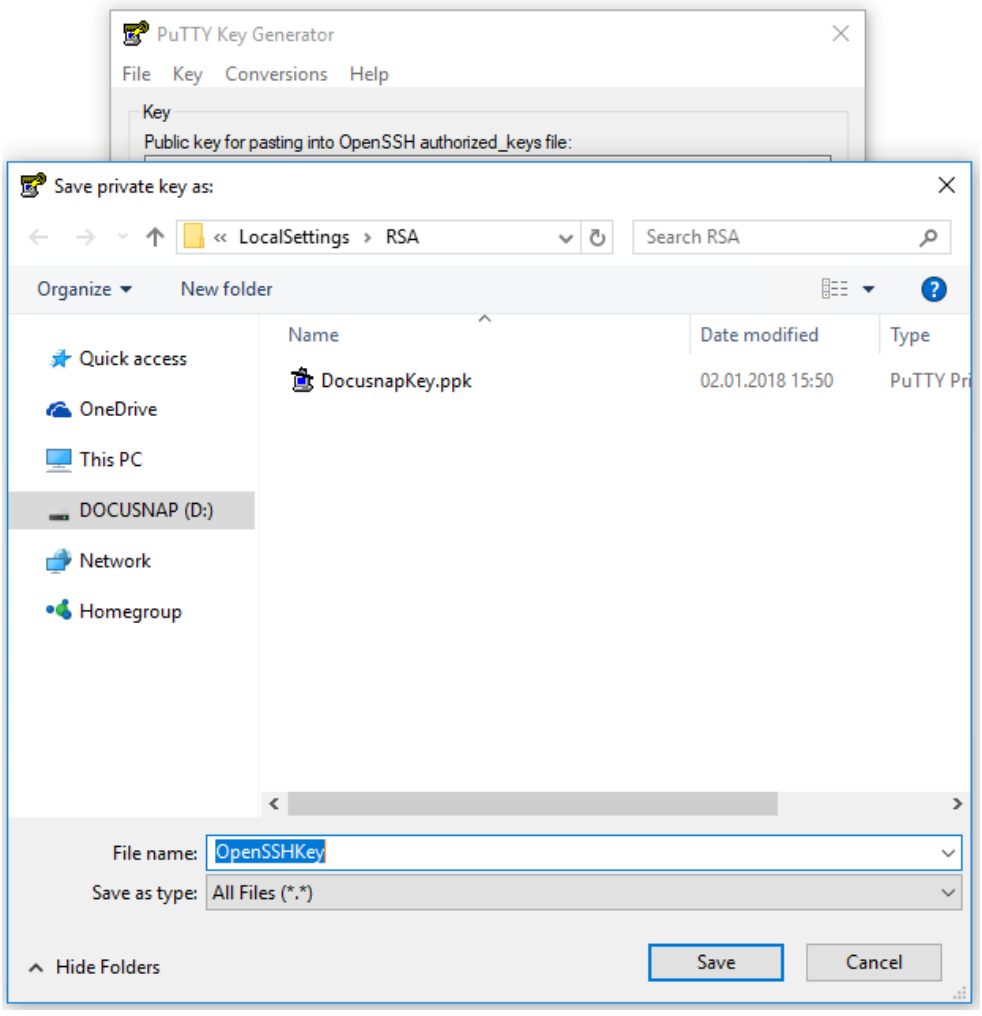

Abbildung 8 - Privaten Schlüssel exportieren II

5. Importieren eines RSA-Schlüssels in Docusnap

Um den konvertierten oder neu erstellten RSA-Schlüssel nach Docusnap zu importieren, rufen Sie die Inventarisierungs-Optionen auf - Importieren - und wählen nun den privaten Open SSH Key aus.

Wichtig:

Wenn Sie bereits einen RSA-Schlüssel verwenden, Entfernen Sie diesen zunächst über die Schaltfläche Entfernen.

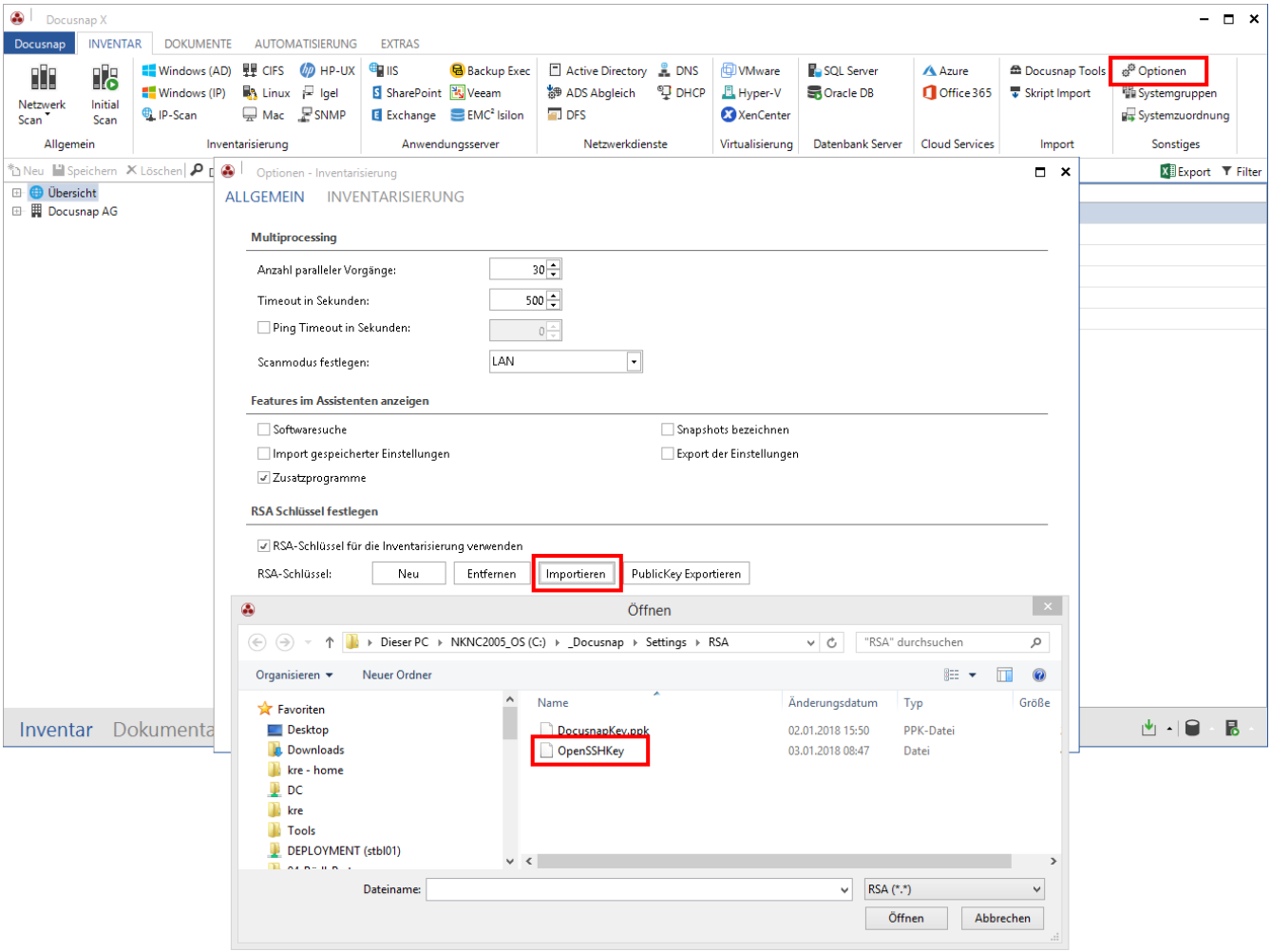

Abbildung 9 - Import des konvertierten Schlüssels

Wenn eine Passphrase für den Schlüssel verwendet wird, werden Sie nach dieser gefragt. Im Anschluss ist der konvertierte Schlüssel in Docusnap hinterlegt.

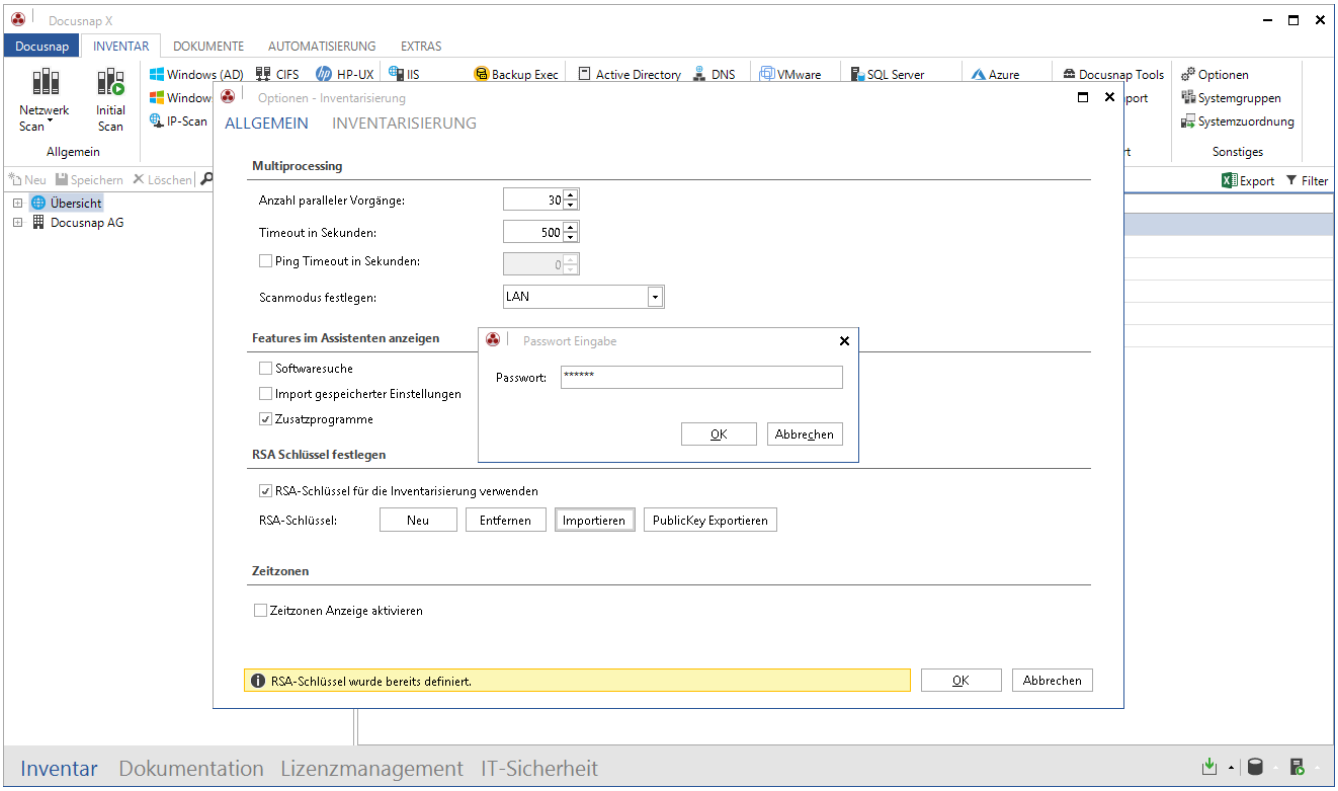

Abbildung 10 - Eingabe der Passphrase

Sollten Sie bereits einen RSA-Schlüssel mit dem früheren Format verwendet und Linux-Inventarisierungs-Jobs eingeplant haben, müssen Sie diese vorhandenen Jobs editieren und nochmals abspeichern. Wechseln Sie dafür auf den Reiter **Automatisierung** in der Hauptoberfläche von Docusnap und öffnen Sie die **Aufträge**. Suchen Sie Ihren Linux Inventarisierungsjob heraus und **bearbeiten** diesen. Sie müssen keine Änderung am Job selbst durchführen, sondern diesen einfach nur nochmals „durchklicken“, damit der Job nochmals abgespeichert wird.

6. RSA-Schlüssel auf dem Linux System hinterlegen

Die beschriebenen Schritte könnten sich ggf. unter den Linux Distributionen unterscheiden. Bitte informieren Sie sich vorab, in welchem Verzeichnis und welcher Datei der öffentliche Schlüssel für die besagte Distribution einzutragen ist. Das folgende Anwendungsbeispiel wird auf einem Ubuntu System (14.04 64-bit) durchgeführt.

In diesem HowTo wird die Software WinSCP verwendet, damit der öffentliche Schlüssel auf dem Linux System hinterlegt wird.

Öffnen Sie WinSCP und bauen die Verbindung zu dem Linux System auf.
Falls der Server beim Client noch nicht bekannt ist, wird eine Sicherheitsmeldung angezeigt. Klicken Sie auf „Yes" um den Hostschlüssel in die Liste der vertrauenswürdigen Rechner aufzunehmen.

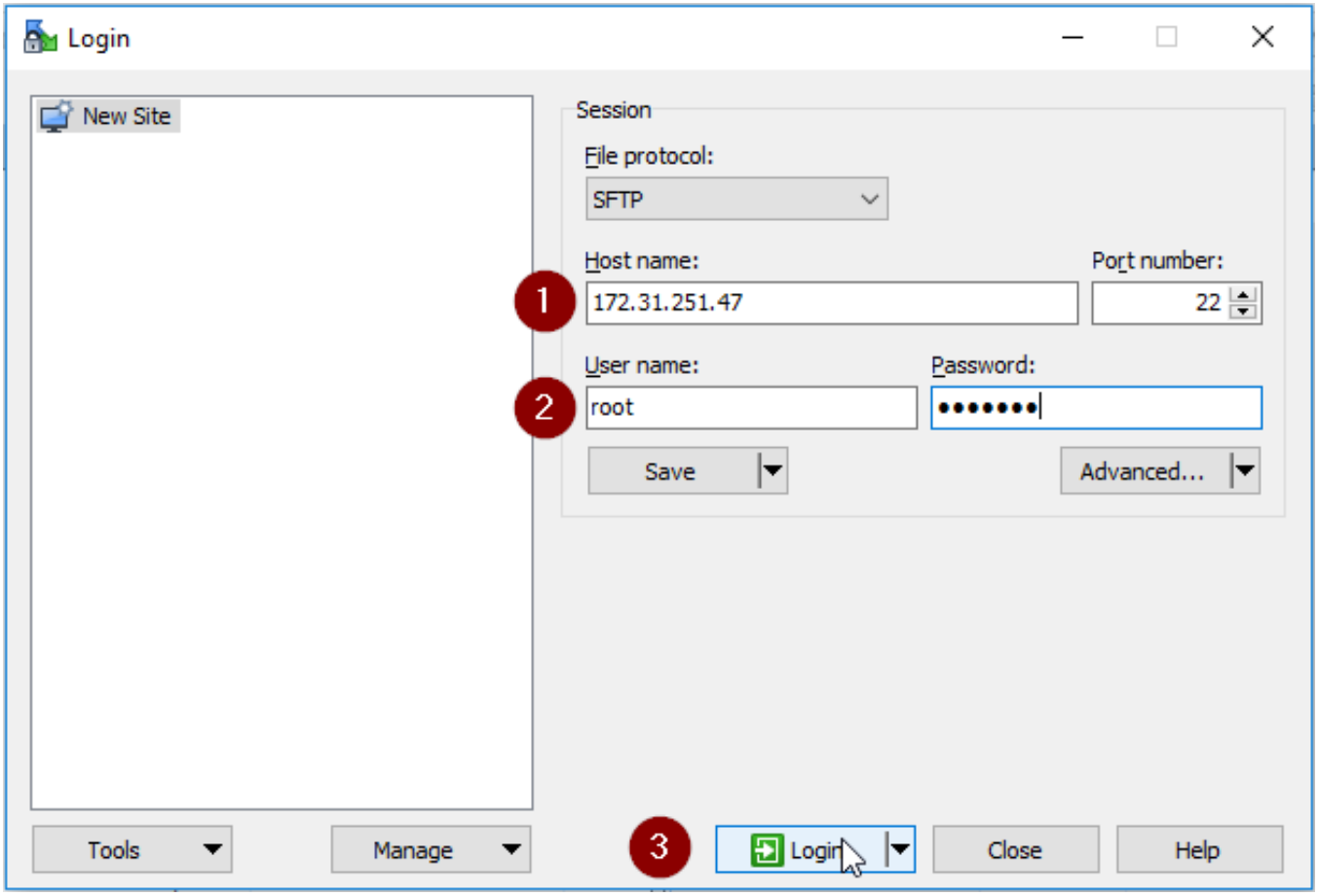

Abbildung 11 - WinSCP Verbindung aufbauen

Schritt 1

Nach dem Login wechselt WinSCP in das Homeverzeichnis des angemeldeten Benutzers. Sollte dies nicht der Benutzer sein mit dem Sie sich zukünftig über SSH verbinden, wechseln Sie in das entsprechende Homeverzeichnis.

Schritt 2

Werden versteckte Dateien und Ordner nicht angezeigt, dann klicken Sie bitte auf das Etikett, welches die Anzahl an versteckten Dateien anzeigt.

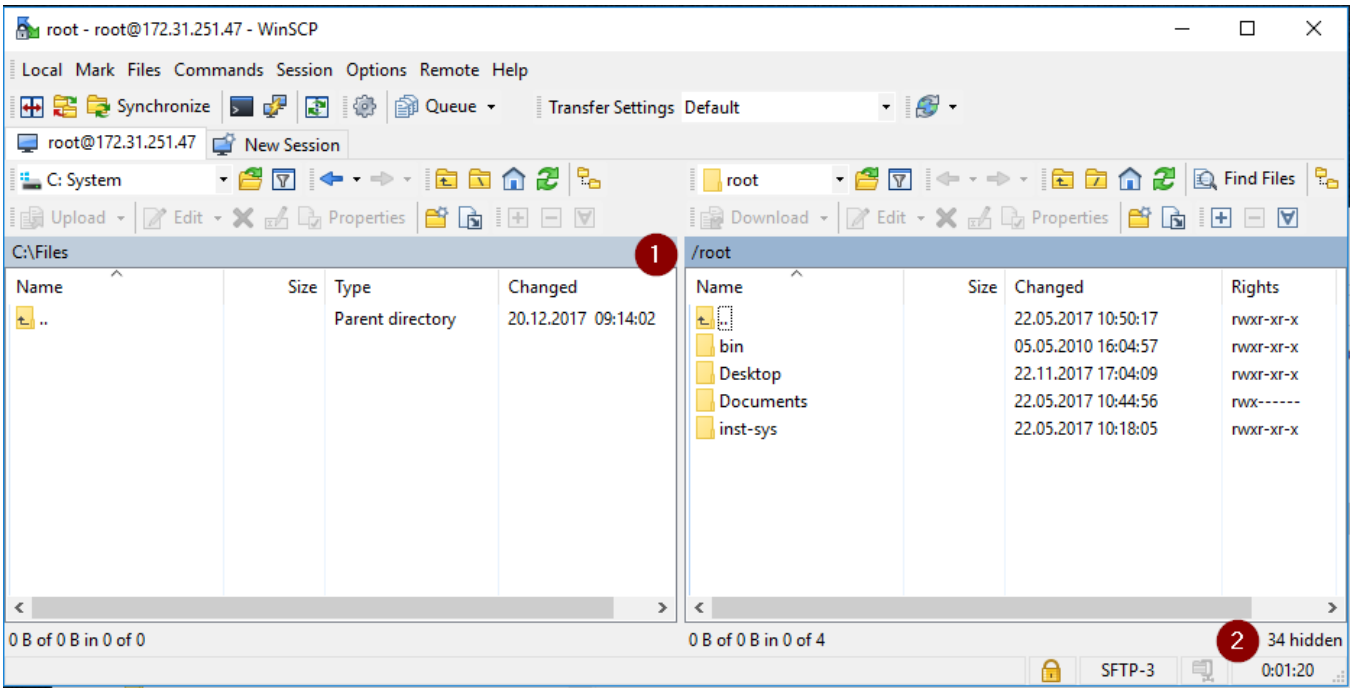

Abbildung 12 - Verbindung zum Zielsystem wurde aufgebaut

Wechseln Sie in das Verzeichnis .ssh und editieren dort die Datei authorized_keys.

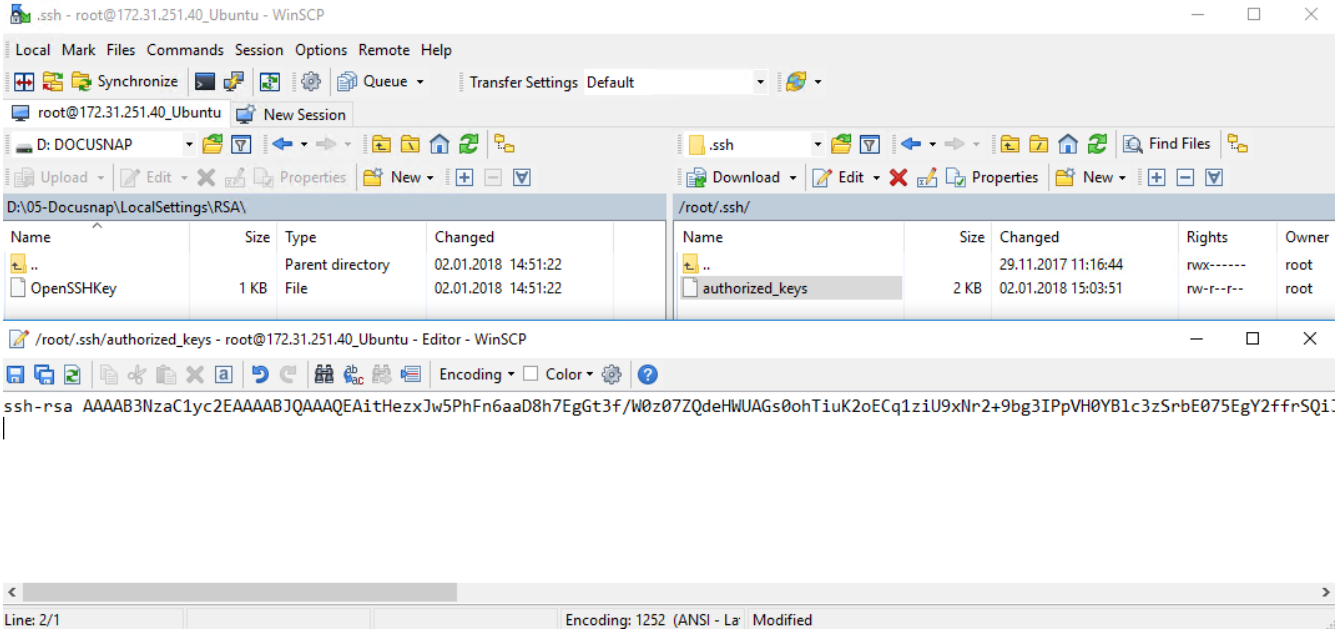

Abbildung 13 - Editieren der Datei authorized_keys

Um den zuvor erstellten RSA-Schlüssel zu hinterlegen, wird ein Export des PublicKeys aus Docusnap benötigt. Öffnen Sie dazu die **Inventarisierungs-Optionen** und wählen die Schaltfläche **PublicKey Exportieren** - Speichern Sie die Datei ab. Öffnen Sie die Datei mit einem Texteditor und kopieren den PublicKey in die Zwischenablage.

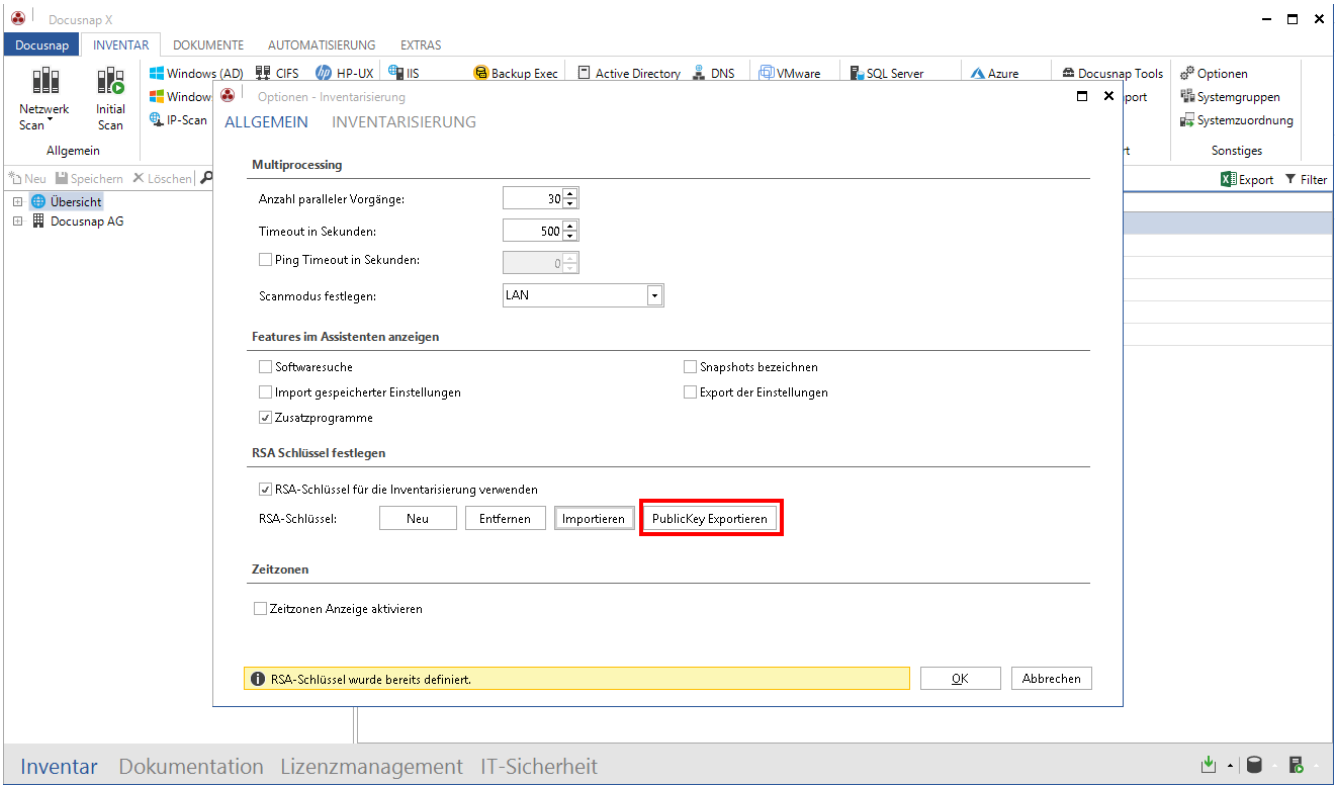

Abbildung 14 - Docusnap PublicKey exportieren

Wechseln Sie zurück nach WinSCP und fügen Sie den PublicKey in einer neuen Zeile ein. Speichern Sie die Datei ab.

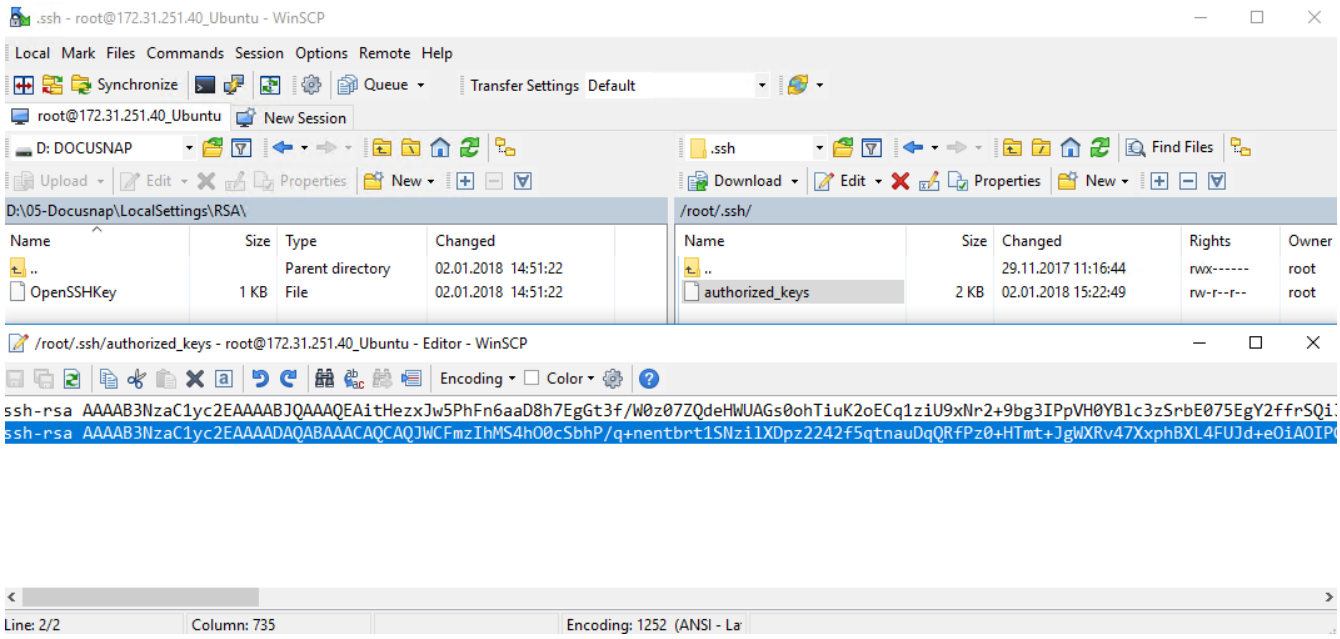

Abbildung 15 - RSA-Schlüssel hinterlegen

Nun ist der PublicKey auf dem Zielsystem hinterlegt. Die Inventarisierung kann nun durchgeführt werden. Sie müssen nur den Benutzernamen in dem Assistenten angeben.

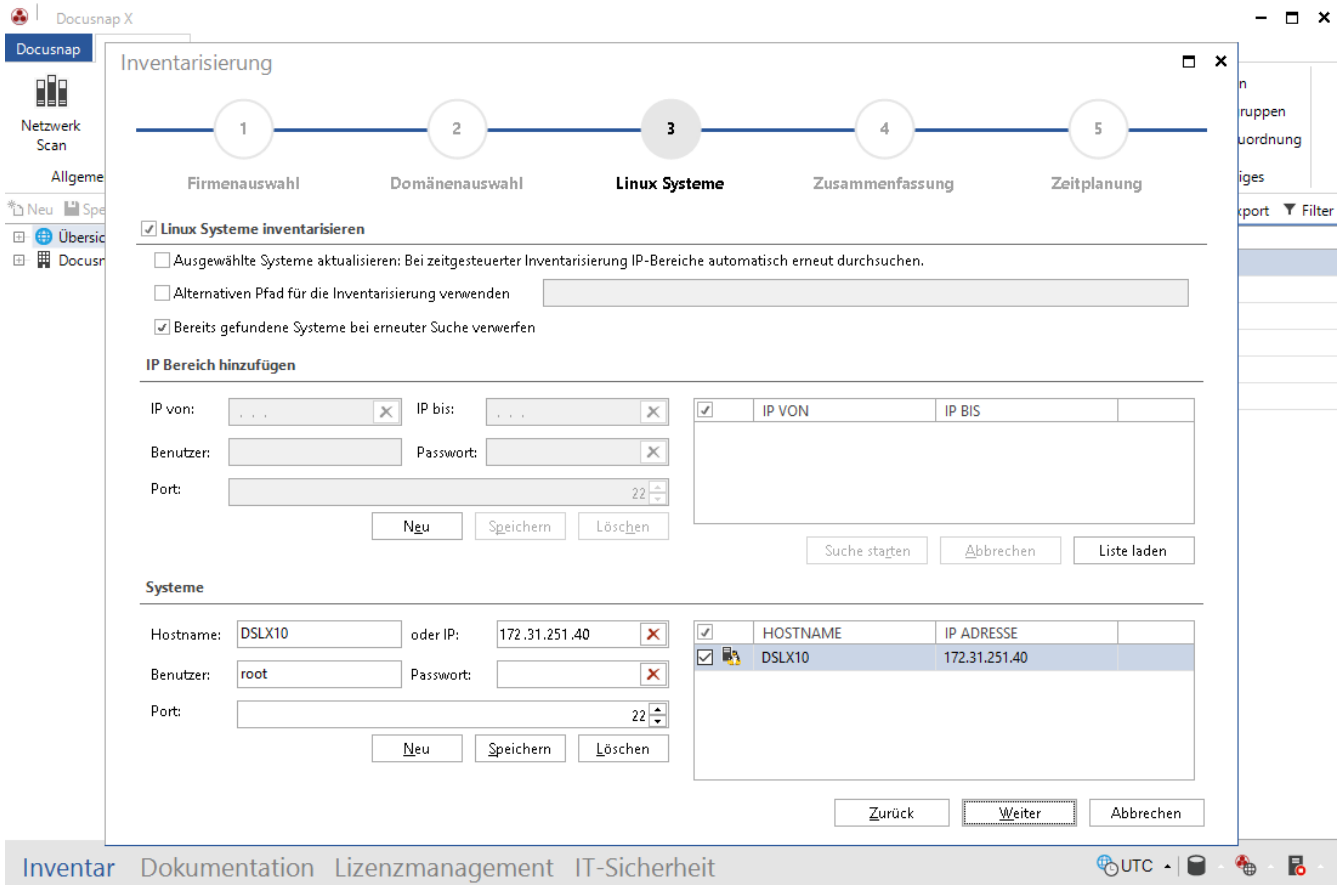

Abbildung 16 - Linux Inventarisierungs-Assistent

ABBILDUNGSVERZEICHNIS

VERSIONSHISTORIE

Datum	Beschreibung
11.01.2018	Version 1.0 erstellt
24.10.2018	Screenshots angepasst