

Certificate Import Tool



Administrationsanleitung für Systembetreiber

31.05.2022

Originalanleitung

Produktlinie Neo, Version 7

Die beschriebenen Funktionen können mit folgenden ASC-Produkten verwendet werden:

EVOIP^{neo}

EVOLUTION^{neo} / XXL / eco

Im Partnerbereich unserer Webseite <https://www.asctechnologies.com> finden Sie immer die aktuellsten technischen Dokumente und Produktaktualisierungen.

Copyright © 2022 ASC Technologies AG. Alle Rechte vorbehalten.

Windows ist ein eingetragenes Markenzeichen der Microsoft Corporation. VMware® ist ein eingetragenes Markenzeichen von VMware, Inc. Alle anderen hier erwähnten Marken und Produktnamen sind das Eigentum ihrer jeweiligen Inhaber.

Inhaltsverzeichnis

1	Allgemeine Hinweise	4
2	Einleitung	5
3	HTTPS-Zertifikate.....	6
3.1	HTTPS Certificate.....	6
3.1.1	Registerkarte About	6
3.1.2	Registerkarte Current Certificate	6
3.1.3	Registerkarte Import Certificate	7
3.2	HTTPS Trust.....	8
3.2.1	Registerkarte About	8
3.2.2	Registerkarte Current Trusted	9
3.2.3	Registerkarte Import Trusted Certificate.....	10
4	PBX-Zertifikate	11
4.1	PBX Certificate	11
4.1.1	Registerkarte About	11
4.1.2	Registerkarte Current Certificate	11
4.1.3	Registerkarte Import Certificate	12
4.2	PBX Trust	13
4.2.1	Registerkarte About	14
4.2.2	Registerkarte Current Trusted	14
4.2.3	Registerkarte Import Trusted Certificate.....	14
5	Generate Certificate.....	17
5.1	Generic Certificate Import.....	17
5.2	Generic Trust Import.....	17
6	Generate Request	19
6.1	Generate Certificate.....	19
6.2	Generate CSR	20
7	Reset all with self signed	21
8	Certimporter über die Kommandozeile aufrufen	22
	Abbildungsverzeichnis	24
	Tabellenverzeichnis.....	25
	Glossar	26

Allgemeine Hinweise

ASC steht im Kontext dieses Dokuments für die ASC Technologies AG, deren Tochtergesellschaften, Niederlassungen und Vertriebsbüros. Deren aktuelle Übersicht kann auf der Webseite unter <https://www.asctechnologies.com> eingesehen werden.

ASC übernimmt keinerlei Gewähr für die Aktualität, Korrektheit, Vollständigkeit oder Qualität der in den Anleitungen bereitgestellten Informationen.

ASC kontrolliert regelmäßig den Inhalt der veröffentlichten Anleitungen auf Übereinstimmung mit der beschriebenen Hard- und Software. Dennoch können Abweichungen nicht ausgeschlossen werden. Notwendige Korrekturen sind in den nachfolgenden Auflagen enthalten.

Einige Aspekte der ASC-Technologie werden in allgemeiner Form beschrieben, um das Eigentum und die vertraulichen Informationen und/oder Geschäftsgeheimnisse von ASC zu schützen.

Die Softwareprogramme und Anleitungen von ASC sind urheberrechtlich geschützt. Alle Rechte an den Anleitungen sind vorbehalten, auch die der Reproduktion und/oder Vervielfältigung in jeglicher Form, sei es fotomechanisch, drucktechnisch oder auf digitalen Datenträgern. Dies gilt auch für Übersetzungen. Nachdruck der Anleitungen, vollständig oder auszugsweise, ist nur mit schriftlicher Genehmigung von ASC gestattet.

Maßgebend ist, soweit nicht anders angegeben, der technische Stand zum Zeitpunkt der Auslieferung von Software, Geräten und Anleitungen durch ASC. Technische Änderungen ohne gesonderte Ankündigung bleiben vorbehalten. Bisherige Anleitungen verlieren ihre Gültigkeit.

Es gelten die Allgemeinen Verkaufs- und Lieferbedingungen von ASC in ihrer jeweils gültigen Fassung.

Das Certificate Import Tool wird standardmäßig mit der Neo-Software ausgeliefert.

Es dient dazu Zertifikate selbst zu erstellen, Zertifikate von Zertifizierungsstellen anzufordern und Zertifikate zu importieren.

1. Öffnen Sie auf dem Aufzeichnungsserver das Verzeichnis
C:\Program Files (x86)\ASC\ASC Product Suite\scripts.
2. Starten Sie die Datei *certimporter.exe* als Administrator.
⇒ Das Fenster Certificate Import Tool erscheint.

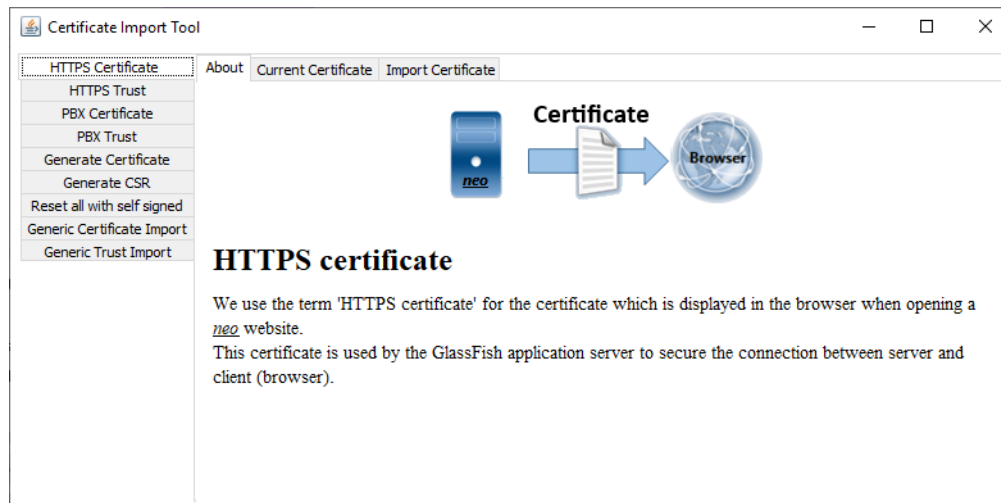


Abb. 1: Certificate Import Tool starten

3

HTTPS-Zertifikate

3.1

HTTPS Certificate

In dieser Sektion steht das eigene Zertifikat, das der Web-Server z. B. dem Browser beim Aufruf der Web-Oberfläche präsentiert.

Es stehen 3 Registerkarten zur Verfügung:

- *About*
Informationen über das Zertifikat, Anzeige und Verwendung, siehe [Kapitel "Registerkarte About", S. 6](#).
- *Current Certificate*
Informationen, wie z. B. Version, Aussteller, Gültigkeit, IP-Adressen, DNS, Algorithmus, siehe [Kapitel "Registerkarte Current Certificate", S. 6](#)
- *Import Certificate*
Output Keystore Pfadangabe, Formatauswahl, Pfadangaben zum Zertifikat, siehe [Kapitel "Registerkarte Import Certificate", S. 7](#).

3.1.1

Registerkarte About

In dieser Registerkarte steht eine kurze Erklärung, wozu das Zertifikat dient.

Wir verwenden den Begriff *HTTPS Certificate* für das Zertifikat, das beim Öffnen einer Neo-Website im Browser angezeigt wird. Dieses Zertifikat wird vom GlassFish-Anwendungsserver verwendet, um die Verbindung zwischen Server und Client (Browser) zu sichern.

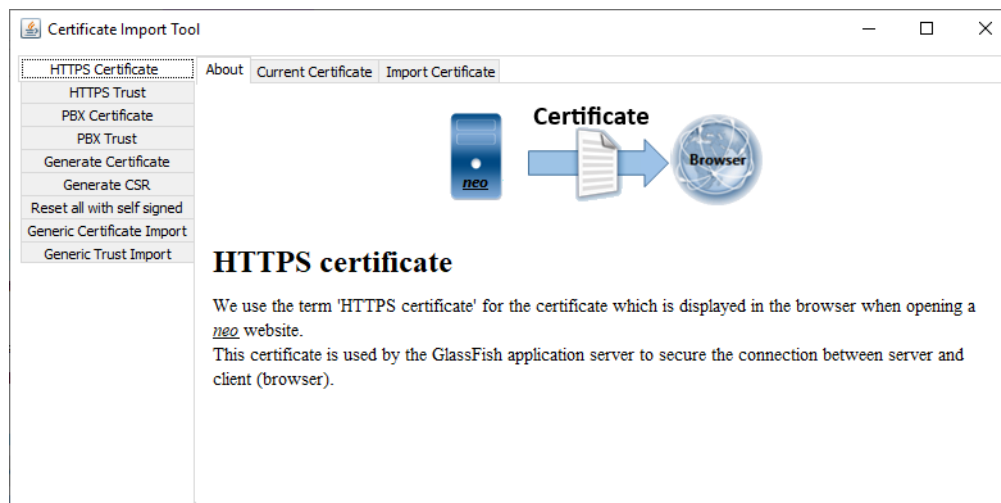


Abb. 2: HTTPS Certificate - Registerkarte About

3.1.2

Registerkarte Current Certificate

In dieser Registerkarte werden alle Informationen des [HTTPS](#)-Zertifikates angezeigt. Dies ist das Zertifikat, dass der Aufzeichnungsserver verwendet, um sich an einem Client, z. B. einem Browser, zu authentifizieren.

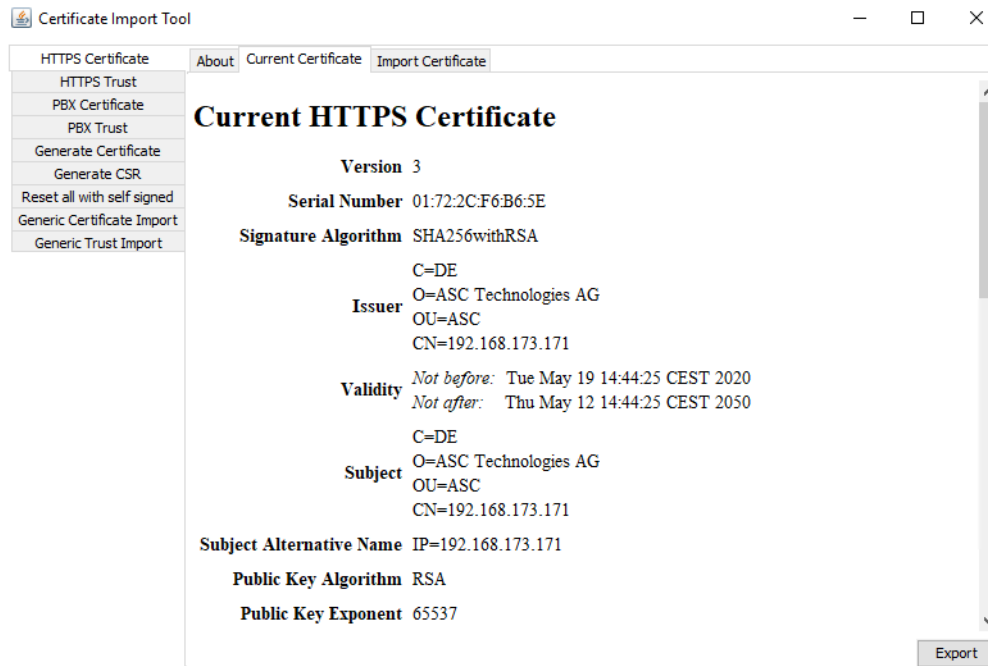


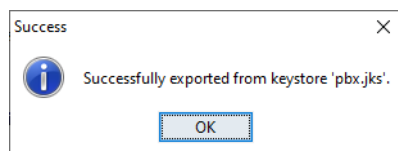
Abb. 3: Informationen über das aktuelle Zertifikat

Folgende Informationen stehen zur Verfügung:

- *Version*
- *Seriennummer*
- *Signatur Algorithmus*
- *Aussteller*
- *Gültigkeit*
- *Serverdetails*
- *Alternativer Servername oder DNS*
- *Public Key Algorithm*
- *Public Key Exponent*
- *Public Key*

Über die Schaltfläche *Export* können Sie das Zertifikat auch exportieren.

1. Klicken Sie auf die Schaltfläche *Export*, um das aktuelle selbstsignierte Zertifikat zu exportieren.
2. Wählen Sie einen geeigneten Speicherort für das Zertifikat.
3. Klicken Sie auf die Schaltfläche *Save*.
 - ⇒ Eine Erfolgsmeldung erscheint.



3.1.3 Registerkarte Import Certificate

In dieser Registerkarte können Sie ein [HTTPS](#)-Zertifikat importieren.

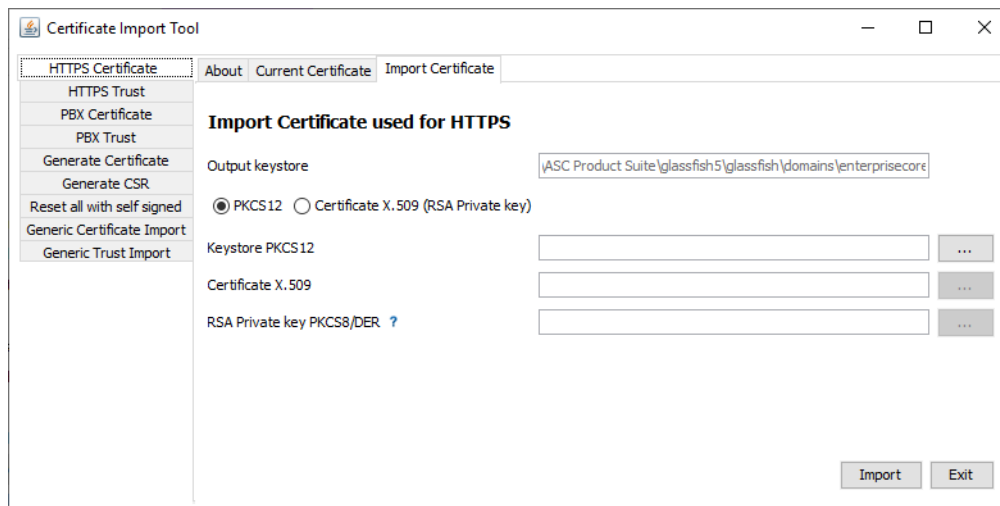


Abb. 4: HTTPS Certificate - Registerkarte Import Certificate

Folgende Formate werden unterstützt:

- **PKCS12**
ist ein Keystore Format, das den Public Key und den Private Key in einer Datei beinhaltet.
 - **X.509**
ist das Dateiformat eines Zertifikates, das den öffentlichen Schlüssel beinhaltet. Wenn Sie das X.509 **RSA** Zertifikat über einen **CSR** angefordert haben, dürfen Sie das Feld **RSA Private Key** nicht füllen, da der private Schlüssel schon auf dem System vorhanden ist.
Wenn Sie das X.509 **RSA** Zertifikat nicht über einen **CSR** angefordert haben, müssen Sie den privaten Schlüssel separat über das Feld **RSA Private Key** importieren.
1. In dem Feld *Output keystore* steht der Pfad zum Verzeichnis, in dem externe Applikationen die Zertifikate finden.
 2. Wählen Sie den Typ des Zertifikates aus, indem Sie das Optionsfeld aktivieren.
 3. Wählen Sie über die Schaltfläche ... neben dem entsprechenden Format die Datei aus dem Explorerpfad aus.
 4. Klicken Sie auf die Schaltfläche *Import*.
- ⇒ Es erscheint eine Erfolgsmeldung.

3.2 HTTPS Trust

In dieser Sektion stehen die vertrauenswürdigen Stammzertifikate (Root Certificates) oder auch **CA** genannt (Certification Authorities).

Es stehen 3 Registerkarten zur Verfügung:

- **About**
Informationen über das Zertifikat, Anzeige und Verwendung, siehe [Kapitel "Registerkarte About", S. 8](#).
- **Current Trusted**
Informationen, wie z. B. Version, Aussteller, Gültigkeit, IP-Adressen, DNS, Algorithmus, siehe [Kapitel "Registerkarte Current Trusted", S. 9](#)
- **Import Trusted Certificate**
Output Keystore Pfadangabe, Formatauswahl, Pfadangaben zum Zertifikat, siehe [Kapitel "Registerkarte Import Trusted Certificate", S. 10](#).

3.2.1 Registerkarte About

In dieser Registerkarte steht eine kurze Erklärung, wozu das Zertifikat dient.

Wir verwenden den Begriff *HTTPS Trust* für Zertifikate, denen der GlassFish-Anwendungsserver vertraut. Dies ist nur in seltenen Fällen relevant, in denen der Anwendungsserver eine Verbindung zu einem anderen Web-Dienst herstellen muss oder für die Verwendung von [LDAP](#).

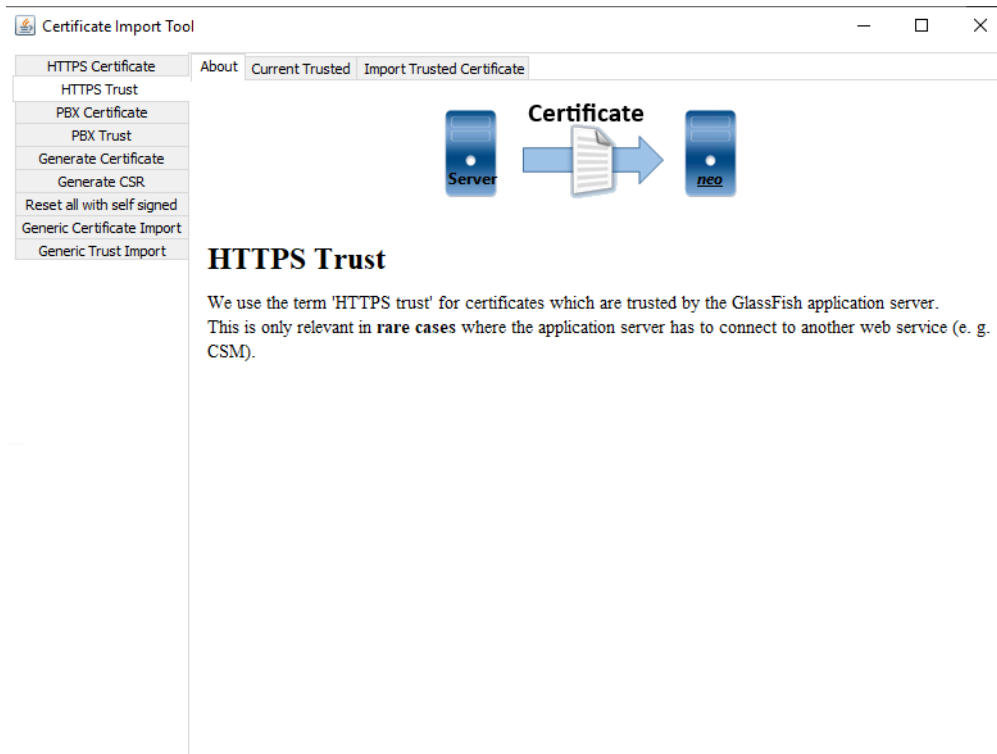


Abb. 5: HTTPS Trust - Registerkarte About

3.2.2 Registerkarte Current Trusted

In dieser Registerkarte werden alle Informationen der HTTPS-Trust-Zertifikate angezeigt.

Dies ist eine Liste aller verfügbaren [CA](#)-Zertifikate, die sich im [Truststore](#) befinden und denen der Aufzeichnungsserver vertraut.

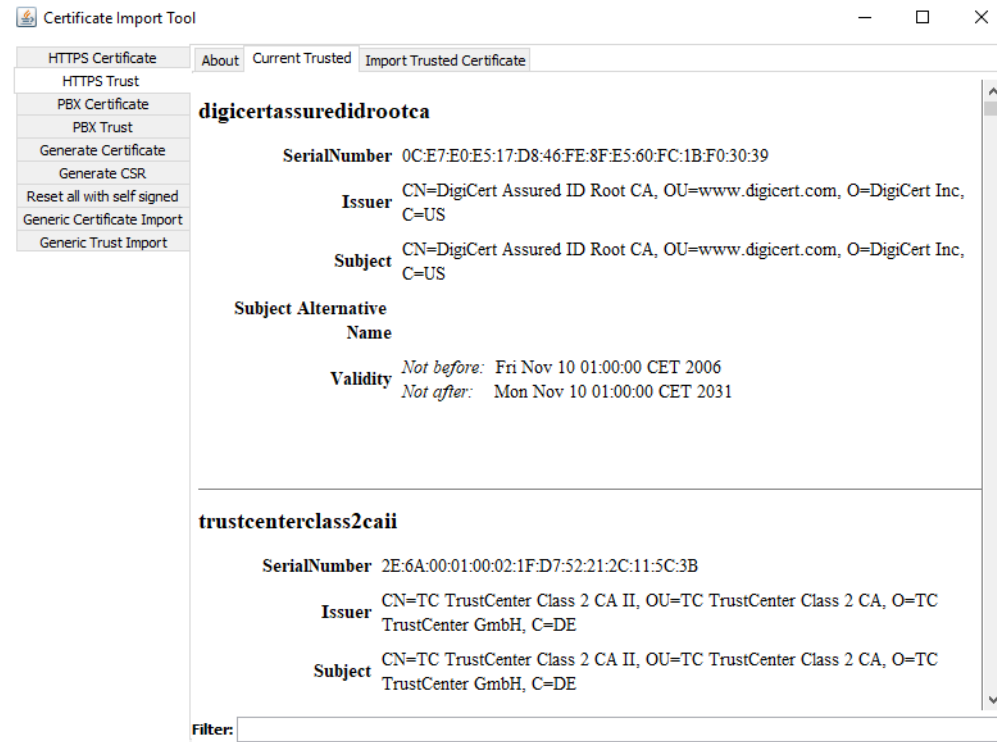


Abb. 6: HTTPS Trust Certificate - Registerkarte Current Trusted

Über das Kontextmenü können Sie die einzelnen Zertifikate auch herauslöschen.

3.2.3 Registerkarte Import Trusted Certificate

In dieser Registerkarte können Sie ein [HTTPS](#)-Trust-Zertifikat importieren.

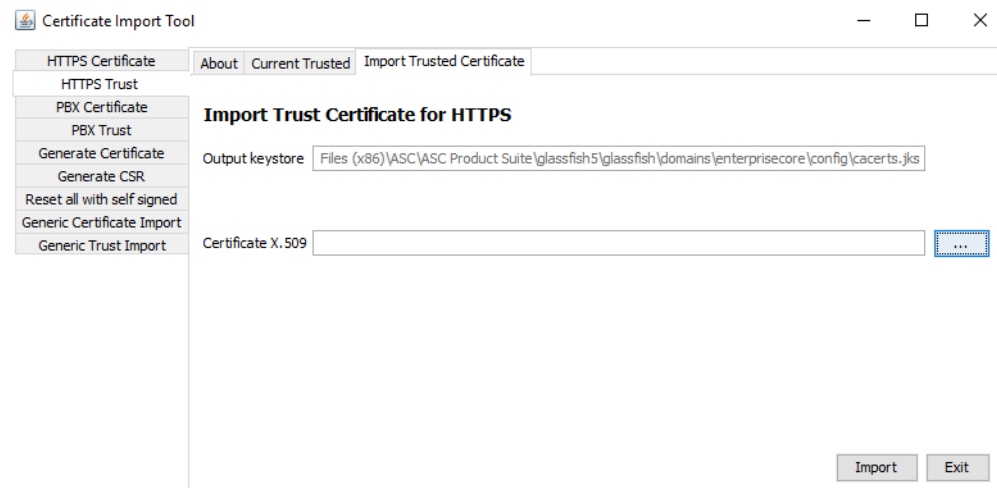


Abb. 7: HTTPS Trust - Registerkarte Import Trusted Certificate

1. In dem Feld *Output keystore* steht der Pfad zum Verzeichnis, in dem externe Applikationen die Zertifikate finden.
 2. Wählen Sie neben dem Feld *Certificate X.509* über die Schaltfläche ... die Datei aus dem Explorerpfad aus, die Sie importieren möchten.
 3. Klicken Sie auf die Schaltfläche *Import*.
- ⇒ Es erscheint eine Erfolgsmeldung.

4 PBX-Zertifikate

4.1 PBX Certificate

Das PBX-Zertifikat dient zur Authentifizierung des Aufzeichnungsservers an der PBX. Damit die Verbindung erfolgreich aufgebaut werden kann, muss die PBX dem Zertifikat vertrauen.

Es stehen 3 Registerkarten zur Verfügung:

- *About*
Informationen über das Zertifikat, Anzeige und Verwendung, siehe [Kapitel "Registerkarte About", S. 11](#).
- *Current Certificate*
Informationen, wie z. B. Version, Aussteller, Gültigkeit, IP-Adressen, DNS, Algorithmus, siehe [Kapitel "Registerkarte Current Certificate", S. 11](#)
- *Import Certificate*
Output Keystore Pfadangabe, Formatauswahl, Pfadangaben zum Zertifikat, siehe [Kapitel "Registerkarte Import Certificate", S. 12](#).

4.1.1 Registerkarte About

In dieser Registerkarte steht eine kurze Erklärung, wozu das Zertifikat dient.

Das Zertifikat dient der Authentifizierung des Aufzeichnungsservers, wenn die PBX sich auf den Aufzeichnungsserver verbindet. Das Zertifikat muss von der PBX bestätigt werden. Die PBX muss diesem Zertifikat vertrauen, damit eine gesicherte Verbindung aufgebaut werden kann.

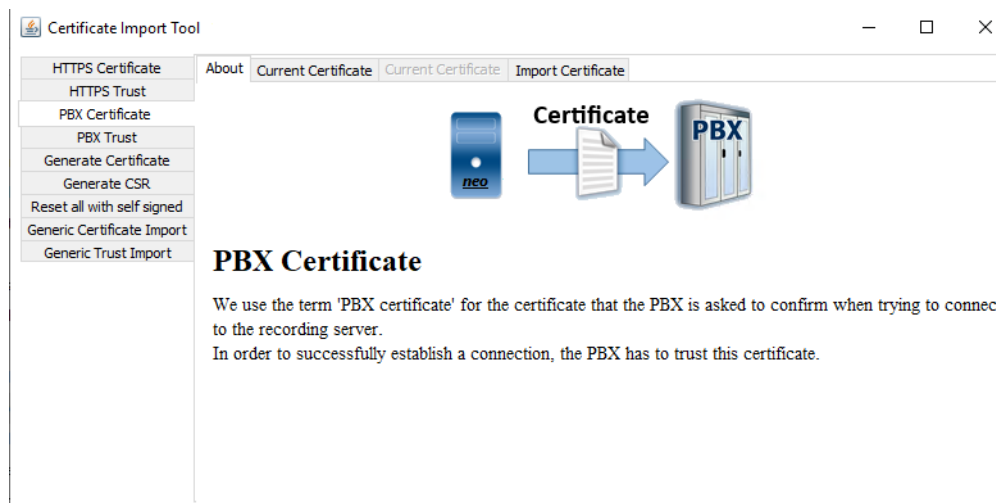


Abb. 8: PBX Certificate - Registerkarte About

4.1.2 Registerkarte Current Certificate

In dieser Registerkarte werden die Informationen des aktuellen Zertifikats des Aufzeichnungsservers angezeigt. Hier können Sie das aktuelle Zertifikat auch exportieren.

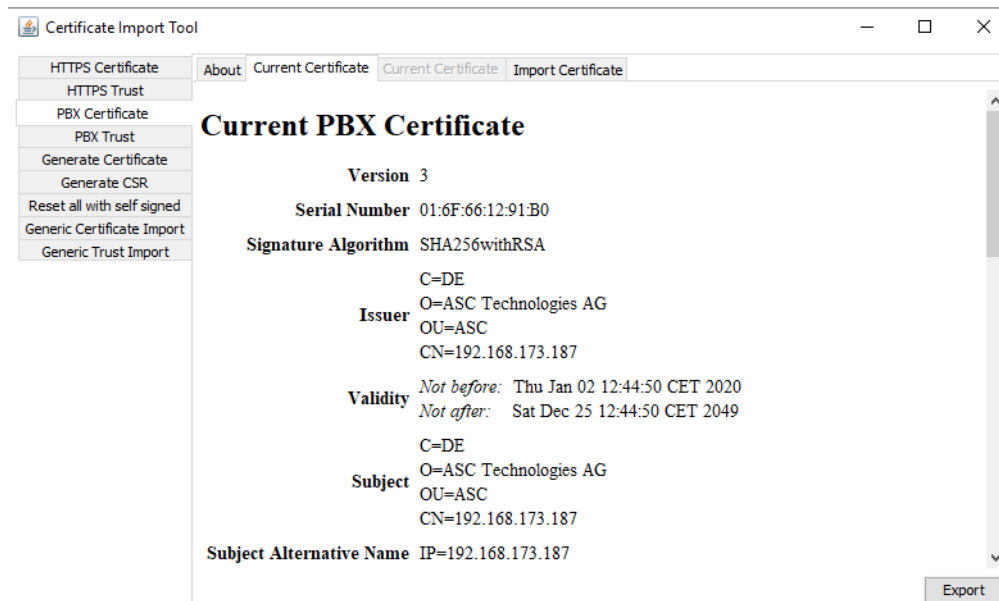


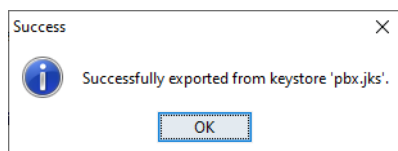
Abb. 9: PBX Certificate - Registerkarte Current Certificate

Folgende Informationen stehen zur Verfügung:

- *Version*
- *Seriennummer*
- *Signatur Algorithmus*
- *Aussteller*
- *Gültigkeit*
- *Serverdetails*
- *Alternativer Servername oder DNS*
- *Public Key Algorithm*
- *Public Key Exponent*
- *Public Key*

Über die Schaltfläche *Export* können Sie das Zertifikat auch exportieren.

1. Klicken Sie auf die Schaltfläche *Export*, um das aktuelle selbstsignierte Zertifikat zu exportieren.
2. Wählen Sie einen geeigneten Speicherort für das Zertifikat.
3. Klicken Sie auf die Schaltfläche *Save*.
 - ⇒ Eine Erfolgsmeldung erscheint.



4.1.3 Registerkarte Import Certificate

In dieser Registerkarte können Sie das Zertifikat von der PBX importieren.

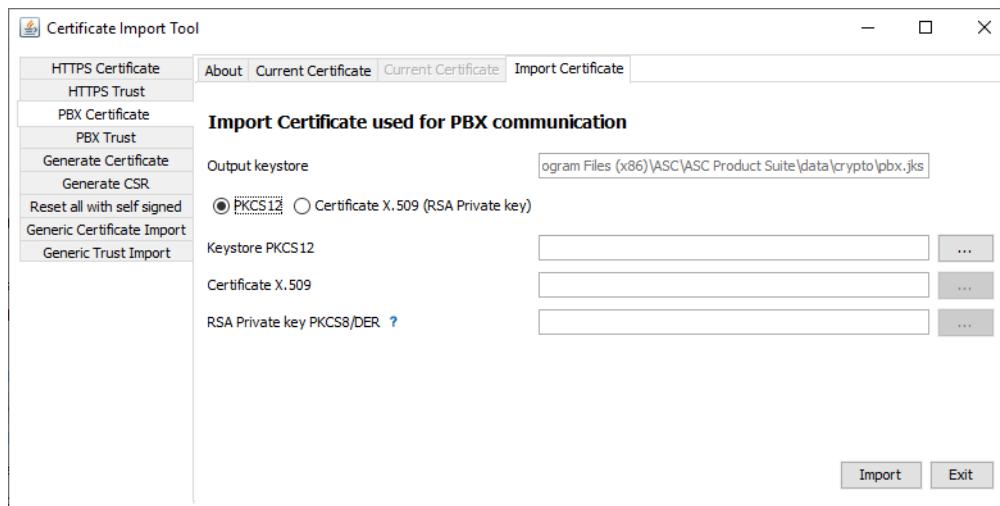



Abb. 10: PBX Certificate - Registerkarte Import Certificate

Folgende Formate werden unterstützt:

- **PKCS12**
ist ein Keystore Format, das den Public Key und den Private Key in einer Datei beinhaltet.
 - **X.509**
ist das Dateiformat eines Zertifikates, das den öffentlichen Schlüssel beinhaltet. Wenn Sie das X.509 **RSA** Zertifikat über einen **CSR** angefordert haben, dürfen Sie das Feld **RSA Private Key** nicht füllen, da der private Schlüssel schon auf dem System vorhanden ist.
Wenn Sie das X.509 **RSA** Zertifikat nicht über einen **CSR** angefordert haben, müssen Sie den privaten Schlüssel separat über das Feld **RSA Private Key** importieren.
1. In dem Feld *Output keystore* steht der Pfad zum Verzeichnis, in dem externe Applikationen die Zertifikate finden.
 2. Wählen Sie das Format des Zertifikates aus, indem Sie das entsprechende Optionsfeld aktivieren.
 3. Wählen Sie über die Schaltfläche  neben dem entsprechenden Format die Datei aus dem Explorerpfad aus.
 4. Klicken Sie auf die Schaltfläche *Import*.
- ⇒ Es erscheint eine Erfolgsmeldung.

4.2

PBX Trust

Das PBX-Zertifikat dient zur Authentifizierung der PBX am Aufzeichnungsserver. Damit die Verbindung erfolgreich aufgebaut werden kann, muss der Aufzeichnungsserver dem Zertifikat der PBX vertrauen.

Es stehen 3 Registerkarten zur Verfügung:

- **About**
Informationen über das Zertifikat, Anzeige und Verwendung, siehe [Kapitel "Registerkarte About"](#), S. 14.
- **Current Trusted**
Informationen, wie z. B. Version, Aussteller, Gültigkeit, IP-Adressen, DNS, Algorithmus, siehe [Kapitel "Registerkarte Current Trusted"](#), S. 14
- **Import Trusted Certificate**
Output Keystore Pfadangabe, Formatauswahl, Pfadangaben zum Zertifikat, siehe [Kapitel "Registerkarte Import Trusted Certificate"](#), S. 14.

4.2.1 Registerkarte About

In dieser Registerkarte steht eine kurze Erklärung, wozu das Zertifikat dient.

Das PBX-Trust-Zertifikat dient der Authentifizierung der PBX an dem Aufzeichnungsserver. Beim Aufbau einer Verbindung von der PBX zum Aufzeichnungsserver muss der Aufzeichnungsserver das Zertifikat bestätigen. Der Aufzeichnungsserver muss dem Zertifikat vertrauen, damit die Verbindung erfolgreich aufgebaut werden kann.



Abb. 11: PBX Trust - Registerkarte About

4.2.2 Registerkarte Current Trusted

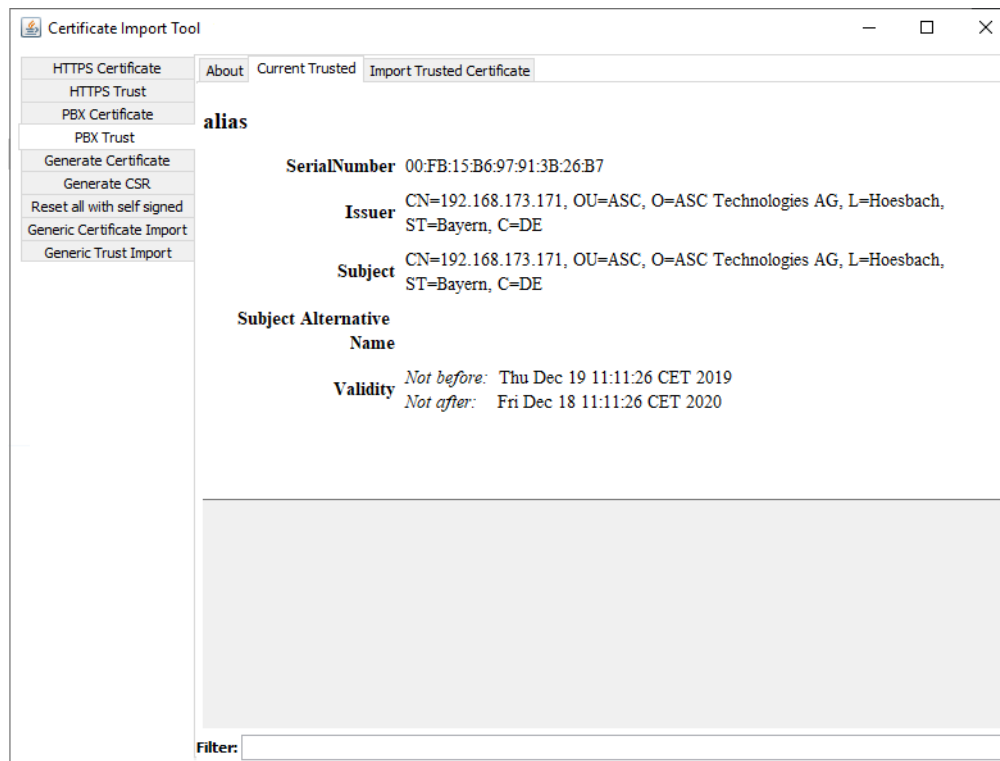


Abb. 12: PBX Trust - Registerkarte Current Trusted

4.2.3 Registerkarte Import Trusted Certificate

In dieser Registerkarte können Sie ein vertrauenswürdiges PBX-Zertifikat importieren.

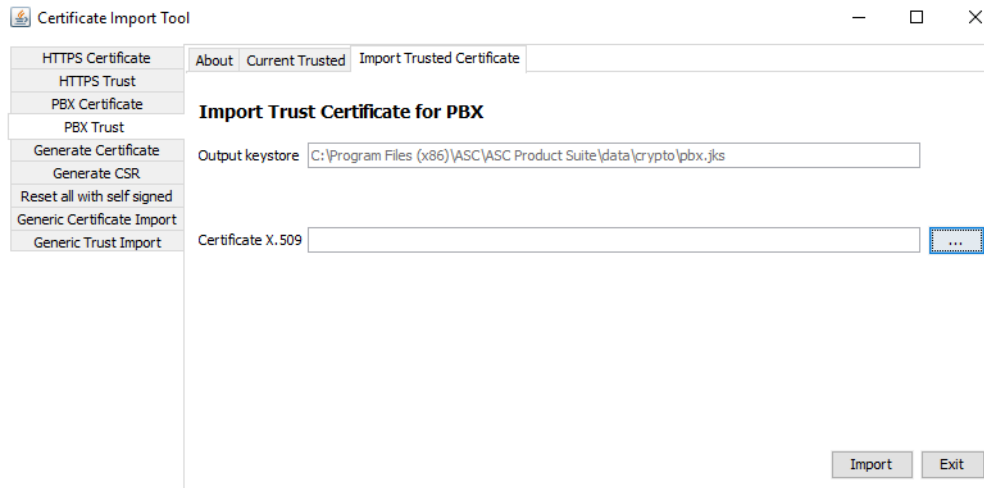


Abb. 13: PBX Trust - Registerkarte Import Trusted Certificate

1. Im Feld *Output keystore* steht der Pfad zum Verzeichnis, in dem externe Applikationen das Zertifikat finden.
2. Wählen Sie über die Schaltfläche ... neben dem entsprechenden Format die Datei aus dem Explorerpfad aus.
3. Klicken Sie auf die Schaltfläche *Import*.
⇒ Der Eingabedialog für den Alias erscheint.

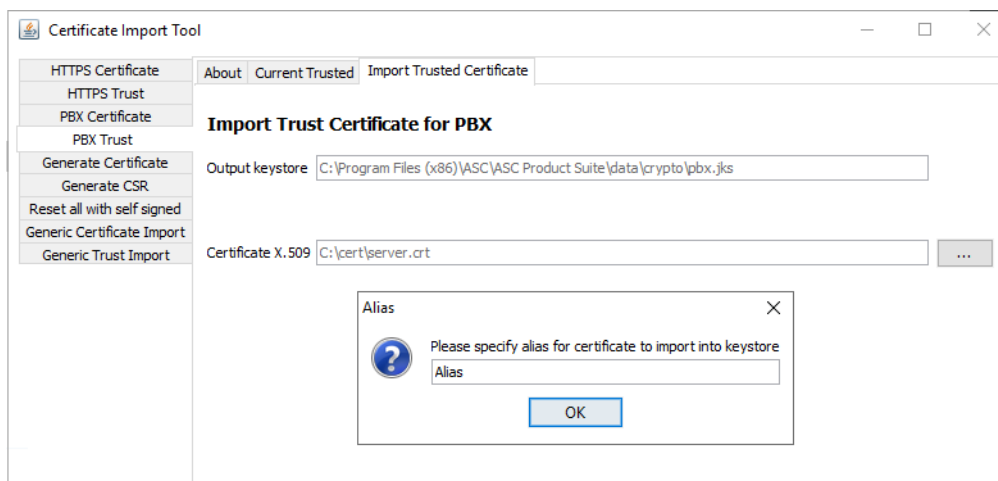


Abb. 14: Eingabedialog für den Alias

4. Geben Sie den Alias ein und klicken Sie auf die Schaltfläche *OK*.
⇒ Es erscheint eine Erfolgsmeldung, wenn der Import korrekt erfolgt ist.

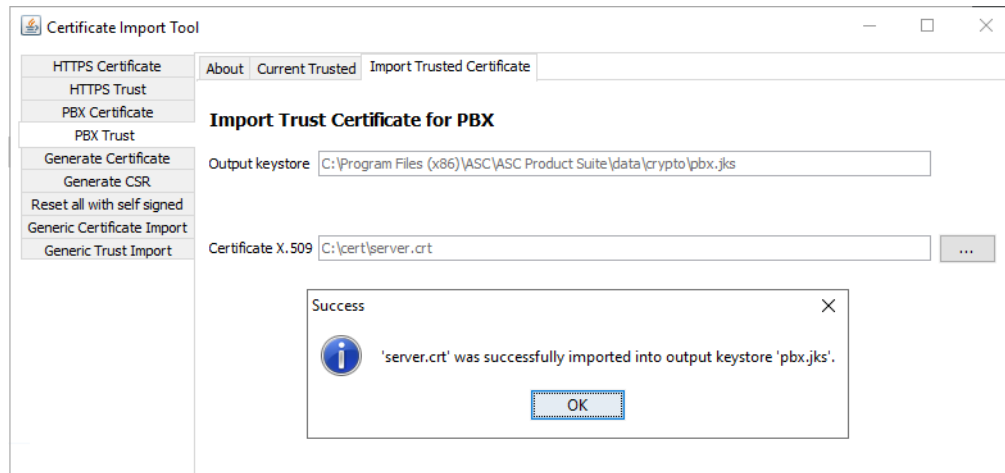


Abb. 15: Meldung über den erfolgreichen Import

5

Generate Certificate

5.1

Generic Certificate Import

In dieser Registerkarte können Sie ein Zertifikat in einen ausgewählten Keystore importieren. Der Keystore muss nicht zwingend der des Neo-Systems sein.

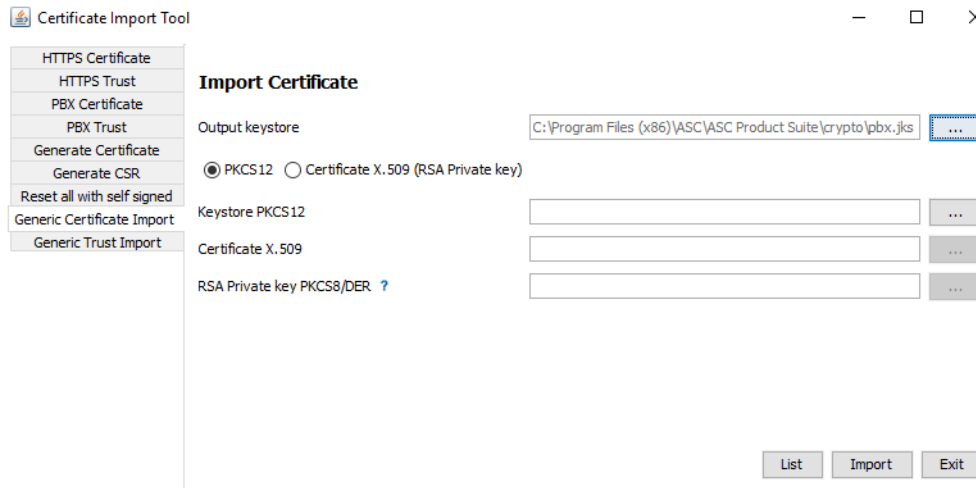


Abb. 16: Generate Certificate - Generic Certificate Import

1. Wählen Sie über die Schaltfläche ... neben dem Feld *Output keystore* das Verzeichnis, in dem externe Applikationen die Zertifikate finden.
 2. Wählen Sie das Format des Zertifikates aus, indem Sie das entsprechende Optionsfeld aktivieren.
 3. Wählen Sie über die Schaltfläche ... neben dem entsprechenden Format die Datei aus dem Explorerpfad aus.
 4. Klicken Sie auf die Schaltfläche *Import*.
- ⇒ Es erscheint eine Erfolgsmeldung.

5.2

Generic Trust Import

In dieser Registerkarte können Sie ein CA-Zertifikat in einen ausgewählten Keystore importieren. Der Keystore muss nicht zwingend der des Neo-Systems sein.

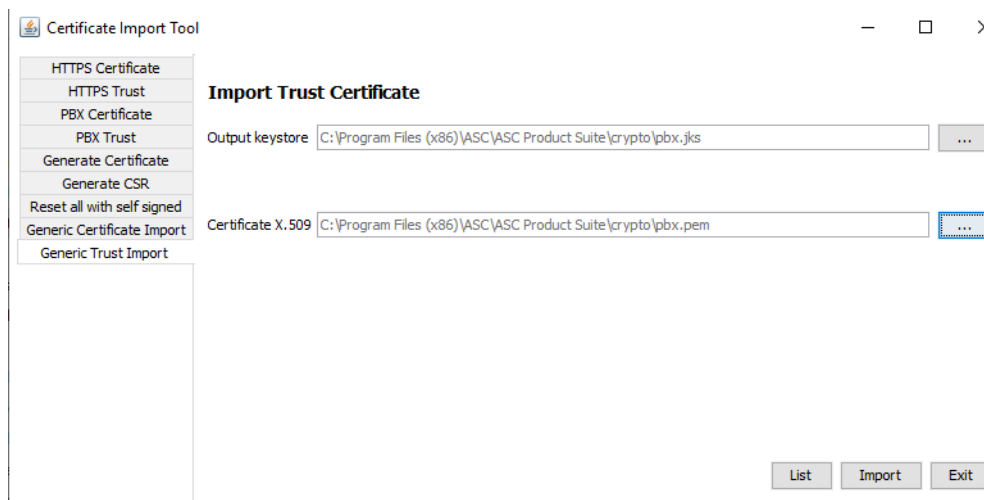


Abb. 17: Generate Certificate - Generic Trust Import

1. Wählen Sie über die Schaltfläche ... neben dem Feld *Output keystore* das Verzeichnis, in dem externe Applikationen das CA-Zertifikat finden.

2. Wählen Sie über die Schaltfläche ... neben dem Feld *Certificate X.509* die Datei aus dem Explorerpfad aus.
 3. Klicken Sie auf die Schaltfläche *Import*.
- ⇒ Es erscheint eine Erfolgsmeldung.

6 Generate Request

6.1 Generate Certificate

In dieser Registerkarte können Sie ein selbst signiertes Zertifikat generieren. Das Zertifikat ist nicht automatisch vertrauenswürdig. Sie können die Datei aber optional in den vertrauenswürdigen Keystore importieren, damit sie im internen Netzwerk als vertrauenswürdig erachtet wird.

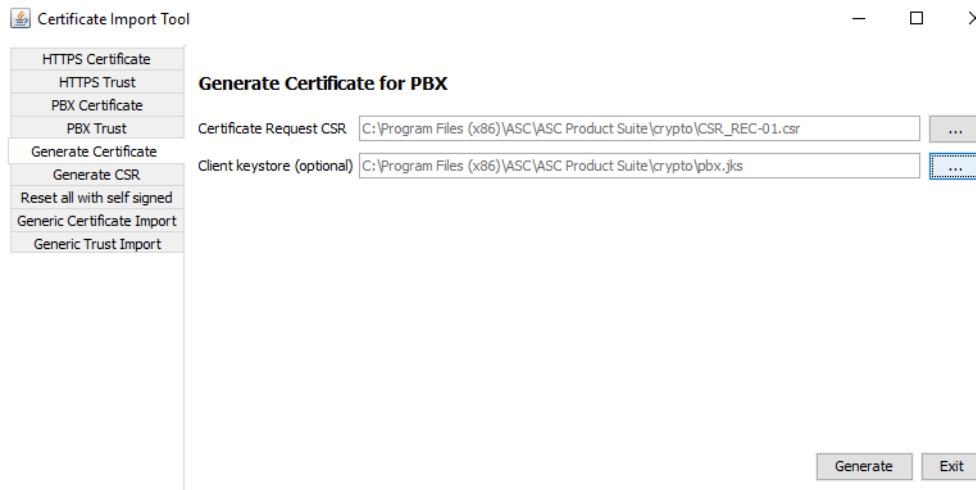


Abb. 18: Generate Certificate

1. Wählen Sie in der Navigationsleiste den Menüpunkt *Generate Certificate*.
2. Stellen Sie im Feld *Certificate Request CSR* über die Schaltfläche ... die zuvor erstellte [CRS](#)-Datei ein.
3. Stellen Sie im Feld *Client keystore* den Pfad zum Client-Keystore ein.
Sie finden die Datei auf dem Aufzeichnungsserver im Verzeichnis
C:\Program Files (x86)\ASC\ASC Product Suite\data\crypto.
4. Klicken Sie auf die Schaltfläche *Generate*, um die Eingaben zu bestätigen und die Zertifikate zu generieren.
5. Geben Sie das Passwort für den Keystore ein.
6. Klicken Sie auf die Schaltfläche *OK*.
⇒ Die erstellten Zertifikate und der erweiterte Client-Keystore werden in einer ZIP-Datei gespeichert.
7. Geben Sie einen Dateinamen für die ZIP-Datei ein.
8. Klicken Sie auf die Schaltfläche *Save*.
⇒ Die ZIP-Datei wird gespeichert.
⇒ Sie können die erstellte ZIP-Datei nun an einer beliebigen Stelle entpacken.

Die ZIP-Datei enthält folgende 3 Dateien:

Datei	Inhalt
<i>ca.crt</i>	Öffentliches ASC CA -Zertifikat. Das CA-Zertifikat ist ebenfalls selbstsigniert. Sie können die Datei aber in den vertrauenswürdigen Keystore importieren, damit sie im internen Netzwerk als vertrauenswürdig erachtet wird.
<i>cert.crt</i>	Serverzertifikat, das auf Grundlage der Zertifikatanfrage erstellt wurde.
<i>pbx.jks</i>	PBX Client-Keystore, erweitert um das CA -Zertifikat Das .jks-Format ist ein proprietäres Java-Format und enthält alle Angaben der importierten Zertifikate.

6.2 Generate CSR

In dieser Registerkarte können Sie eine Anfrage für ein Zertifikat von einer CA-Zertifizierungsstelle stellen.

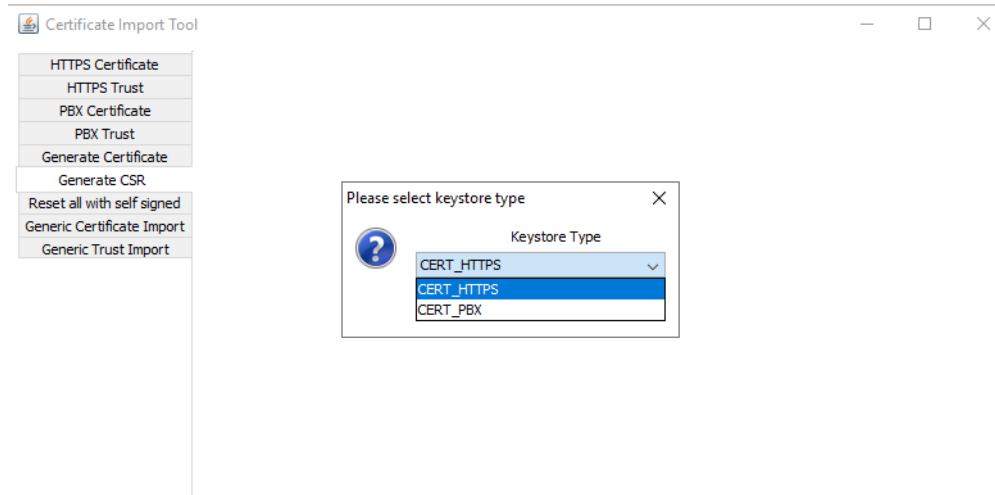


Abb. 19: Generate CSR - Anfrage an einer CA-Zertifizierungsstelle stellen

1. Wählen Sie den Typ des Zertifikates aus der Dropdown-Liste aus.

Folgende Optionen stehen zur Verfügung:

- *CERT_HTTPS*
 - *CERT_PBX*
2. Geben Sie in dem folgenden Fenster die Informationen für das Zertifikat ein:
- *Common Name*
 - *Business name*
 - *Department Name*
 - *Town/City*
 - *Province*
 - *Country*
 - *Email address*
 - *Subject alt names (DNS)*
 - *Subject alt names (IP)*
3. Klicken Sie auf die Schaltfläche *Ok*, um die Eingaben zu übernehmen.
4. Wählen Sie über das Dialogfenster den Speicherort und vergeben Sie einen Namen für die Datei.
- ⇒ Eine Erfolgsmeldung erscheint.

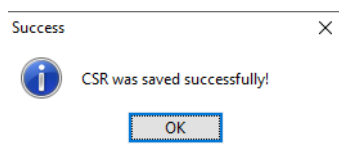


Abb. 20: Generate CSR - Datei speichern

Die erstellte **CSR**-Datei können Sie jetzt an eine Zertifizierungsstelle schicken.

Das Zertifikat, dass von der autorisierten Zertifizierungsstelle zurückkommt, können Sie dann über den entsprechenden Menüpunkt importieren:

- *CERT_HTTPS* siehe [Kapitel "Registerkarte Import Certificate", S. 7](#)
- *CERT_PBX* siehe [Kapitel "Registerkarte Import Certificate", S. 12](#)

Reset all with self signed

In diesem Menüpunkt können Sie alle importierten Zertifikate auf selbst signierte Zertifikate zurücksetzen.



Bestehende Verbindungen, die über zuvor konfigurierte Zertifikate bei anderen Systemen als vertrauenswürdig gelten, funktionieren nach dieser automatischen Erstellung nicht mehr. Das bedeutet, dass beim Öffnen der angeforderten Seite im Browser wieder die ursprüngliche, bekannte Warnung auftaucht. Für **PBX**-Verbindungen und andere **HTTPS**-Verbindungen gilt das ebenso.

1. Falls Sie alle verwendeten Zertifikate und privaten Keys überschreiben möchten, bestätigen Sie die kommenden Sicherheitsabfragen.

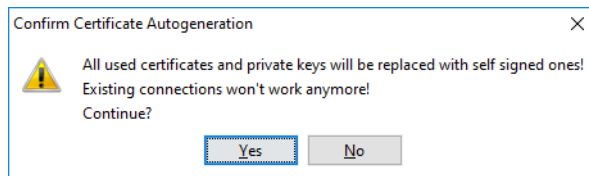


Abb. 21: Sicherheitsabfrage zum Zurücksetzen aller Zertifikate

Certimporter über die Kommandozeile aufrufen

Einige Funktionen des Certificate Import Tools können Sie nicht über die GUI ausführen. Dafür können Sie die *certimporter.exe* über die Kommandozeile aufrufen.

1. Öffnen Sie die PowerShell in folgendem Pfad:
C:\Program Files (x86)\ASC\ASC Product Suite\scripts>
2. Führen Sie den folgenden Befehl aus:
java -jar .\certimporter.exe -h
⇒ Die Hilfe, die Funktionen und die verfügbaren Parameter werden angezeigt.

```

-----
DESCRIPTION
-----
--interactive           : Ask alias and password in interactive mode
--autogenerate          : Reset all certificates with self signed
--winTrust              : Import autogenerated certificates as trusted root into windows certificate store
                        : Also rewrites the links on the desktop to refer to IP used in the certificate
--force                 : Force file overwriting (Must be first parameter)

--https                 : Mode for HTTPS certificates
--https-trust           : Mode for HTTPS Trust certificates
--pbx                   : Mode for PBX certificates
--pbx-trust             : Mode for PBX Trust certificates
--transmission          : Mode for Transmission certificate

--list                  : List certificates
--import                : Import certificate
--importalias <string>  : Import given certificate as alias into keystore

--generate              : Generate certificate
--auto                  : Auto generate mode
--cert-csr              : Generate certificate from CSR
--cert-key              : Generate certificate and key
--validity <int>        : Validity in years of auto generated certificate
--ip-address            : IP Address to autogenerate certificate for
--altNames              : A list of alternate names for the machine (SAN) separated by spaces
--export-x509 <path>    : Export path for generated X509 Certificate
--export-pkey <path>    : Export path for generated PKCS8 private key
--csr <path>            : Path to CSR file

--x509 <path>           : Path to X509 certificate
--pkcs12 <path>         : Path to PKCS12 keystore
--pkcs12pw <string>     : PKCS12 keystore password
--pkcs12alias <string>  : Alias for certificate inside PKCS12 keystore
--privatekey <path>    : Path to PKCS8 private key
--privatekeypw <string> : PKCS8 Private key password

Convert your private key to PKCS8 with 'openssl pkcs8 -topk8 -outform DER -in <paht> -out <path>'

Invocations with the --interactive flag will query the user for parameters like aliases, passwords,
ipAddresses and the validity in years.
-----

```

Abb. 22: Beschreibung der Certimporter-Funktionen

```

-----
USAGE
-----

Autogenerate mode
  Shorthand for "--generate --auto". See below for more details.

Generate mode
  Generate a selfsigned certificate for the neo server and import it for all certificate types.
  "--generate --auto [--winTrust] --ip-address <ipAddress> [--validity <years>] [--altNames <name>
  [2ndName] ...]"
  "--generate --auto [--winTrust] [--altNames <name> [2ndName] ...] --interactive"

  Generate a signed certificate from the specified certification request, using the current pbx key and
  certificate as certification authority.
  "--generate --cert_csr --csr <filePath> {--https|--pbx-trust|--pbx|--pbx-trust|--transmission}"

  Generate a selfsigned certificate and private key.
  "[--force] --generate --cert_key --export-x509 <outCertPath> --export-pkey <outKeyPath> --ip-address
  <ipAddress> [--validity <years>] [--altNames <name> [name ...]]"

List mode
  List current certificate details for the specified type.
  "--list {--https|--pbx-trust|--transmission|--pbx|--pbx-trust}"

Import mode
  Import a certificate to add to the trust store of the specified type under the given alias.
  "--import {--https-trust|--pbx-trust} --x509 <filePath> --importalias <alias>"
  "--import {--https-trust|--pbx-trust} --x509 <filePath> --interactive"

  Import a certificate and associated private key for the given type from separate files.
  "--import {--https|--pbx|--transmission} --x509 <filePath> --privatekey <filePath> [--privatekeypw
  <password>]"
  "--import {--https|--pbx|--transmission} --x509 <filePath> --privatekey <filePath> --interactive"

  Import a certificate and associated private key for the given type from one pkcs12 keystore.
  "--import {--https|--pbx|--transmission} --pkcs12 <filePath> --pkcs12alias <alias> --pkcs12pw <password>"
  "--import {--https|--pbx|--transmission} --pkcs12 <filePath> --interactive"

PS C:\Program Files (x86)\ASC\ASC Product Suite\scripts>

```

Abb. 23: Bedienung des Certimporter Tools über die Kommandozeile

Abbildungsverzeichnis

Abb. 1	Certificate Import Tool starten	5
Abb. 2	HTTPS Certificate - Registerkarte About.....	6
Abb. 3	Informationen über das aktuelle Zertifikat.....	7
Abb. 4	HTTPS Certificate - Registerkarte Import Certificate.....	8
Abb. 5	HTTPS Trust - Registerkarte About.....	9
Abb. 6	HTTPS Trust Certificate - Registerkarte Current Trusted	10
Abb. 7	HTTPS Trust - Registerkarte Import Trusted Certificate.....	10
Abb. 8	PBX Certificate - Registerkarte About	11
Abb. 9	PBX Certificate - Registerkarte Current Certificate.....	12
Abb. 10	PBX Certificate - Registerkarte Import Certificate	13
Abb. 11	PBX Trust - Registerkarte About	14
Abb. 12	PBX Trust - Registerkarte Current Trusted.....	14
Abb. 13	PBX Trust - Registerkarte Import Trusted Certificate	15
Abb. 14	Eingabedialog für den Alias	15
Abb. 15	Meldung über den erfolgreichen Import.....	16
Abb. 16	Generate Certificate - Generic Certificate Import	17
Abb. 17	Generate Certificate - Generic Trust Import	17
Abb. 18	Generate Certificate.....	19
Abb. 19	Generate CSR - Anfrage an einer CA-Zertifizierungsstelle stellen.....	20
Abb. 20	Generate CSR - Datei speichern.....	20
Abb. 21	Sicherheitsabfrage zum Zurücksetzen aller Zertifikate.....	21
Abb. 22	Beschreibung der Certimporter-Funktionen.....	22
Abb. 23	Bedienung des Certimporter Tools über die Kommandozeile	23

Tabellenverzeichnis

Glossar

CA

Certification Authority ist eine Zertifizierungsstelle. CA stellt X.509-Zertifikate für verschiedene Einsatzzwecke aus.

CRS

Certificate Signing Request, Anfrage zur Erstellung eines Zertifikates von einer autorisierten Zertifizierungsstelle.

CSR

Certificate Signing Request

HTTPS

Hypertext Transfer Protocol Secure (HTTPS, englisch für „sicheres Hypertext-Übertragungsprotokoll“) ist ein Kommunikationsprotokoll im World Wide Web, mit dem Daten abhörsicher übertragen werden können. Es stellt eine Transportverschlüsselung dar. (Quelle: Wikipedia 23.10.2019)

LDAP

Lightweight Directory Access Protocol

PBX

Private Branch Exchange, Telefonanlage

RSA

RSA ist ein asymmetrisches kryptographisches Verfahren, das sowohl zum Verschlüsseln als auch zum digitalen Signieren verwendet werden kann.[1] Es verwendet ein Schlüsselpaar, bestehend aus einem privaten Schlüssel, der zum Entschlüsseln oder Signieren von Daten verwendet wird, und einem öffentlichen Schlüssel, mit dem man verschlüsselt oder Signaturen prüft. Der private Schlüssel wird geheim gehalten und kann nur mit extrem hohem Aufwand aus dem öffentlichen Schlüssel berechnet werden. (Quelle: Wikipedia, 23.04.2018)

Truststore

Sammlung von Zertifikaten, die als vertrauenswürdige CA angesehen werden.