ECOS Appliances

Import externer Zertifikate

Admin-Tutorial

Version: 1.0

Datum: 11/2022

IT-Security Solutions

Made in Germany

ECOS TECHNOLOGY GMBH | Sant' Ambrogio-Ring 13 a-b | D-55276 Oppenheim | Tel: +49 6133 939-0 | Fax: +49 6133 939-333

Inhalt

Einführung

ECOS Appliances bieten eine Funktion zur Verwaltung von externen Zertifikaten, die von einer externen Certificate Authority bzw. PKI erstellt wurden.

Externe Zertifikate können in allen gängigen Dateiformaten entweder per Massenupload im Zertifikatcontainer oder als einzelne Datei direkt in ein Zertifikatobjekt importiert werden. Ebenso können die dazugehörigen privaten Schlüssel nebst Kennwörtern importiert werden.

Diese Anleitung richtet sich an Administratorinnen und Administratoren von ECOS Appliances und beschreibt Schritt für Schritt den Importvorgang.

Bitte lesen Sie die Abschnitte *Wichtige Hinweise* und *Vorbereitungen* vor Beginn sorgfältig durch und bewahren Sie diese Anleitung zur weiteren Verwendung auf.

Vorbereitungen

Die folgenden Hinweise und Maßnahmen sollten vor dem Import externer Zertifikate beachtet werden.

Unterstützte Dateiformate

Folgende Dateiformate werden für den Zertifikatimport unterstützt:

Dateiformat	Unterstützt		Import Zertifikat + priv. Schlüssel
DER-Formate (binärcodiert)	.cer	✓	✗
	.der	✓	✗
PEM-Formate (base64-codiert)	.crt	✓	✗
	.pem	✓	✗
PKCS#7	.p7b	✓	✗
PKCS#12	.p12	✓	✓

Bei PKCS#12-Dateien wird der private Schlüssel automatisch mit dem Zertifikat importiert.

Zertifikathierarchie prüfen

Beim Import von Zertifikathierarchien ist zwingend zu beachten, dass die Stufen sukzessive von oben nach unten (root-to-end) importiert werden müssen.

Bei lücken- oder fehlerhafter Importreihenfolge während eines Massenimports können signierende CA-Zertifikate den von ihnen zu signierenden Zertifikaten weder während des Importvorgangs noch nachträglich zugeordnet werden. In einem solchen Fall müssen die importierten Zertifikate gelöscht und der Importvorgang neu begonnen werden.

Stellen Sie vor Beginn eines Massenimports sicher, dass die zu importierenden Zertifikatdateien eine hierarchisch-konsistente Namensgebung aufweisen. Importieren Sie anderenfalls jede Stufe gesondert root-to-end.

Ein CA-Zertifikat darf auf der Appliance nur einmal vorhanden sein. CA-Zertifikate, die bereits importiert wurden, egal in welchen Container, können nicht erneut hochgeladen werden. Sollte es zu Importfehlern kommen, muss das CA-Zertifikatobjekt gelöscht und der Import neu begonnen werden.

Kennwortliste in CSV-Format (optional)

Enthalten die zu importierenden Zertifikate kennwortgeschützte private Schlüssel, werden diese Kennwörter während des Importvorgangs abgefragt. Der Massenimport kann mithilfe einer zweispaltigen Liste im CSV-Format automatisiert werden.

Die CSV-Datei muss folgende Voraussetzungen erfüllen:

- die erste Spalte enthält die Namen der Zertifikatdateien ohne Dateinamenserweiterung
- die zweite Spalte enthält die dazugehörigen Kennwörter

Beispiel:

```
#Dateiname;#Passwort
pw cert 001;as3df/v76Xhg81dI
pw cert 003;yx7cfdBvF*ro8utT
pw cert 004;S2df?0g5fgVeTn9v
pw cert 005;?sdF85g/Wzou4Gx6
pw cert 006;q73r9KrOf!Dy2ptr
```

Die Spaltenüberschriften können beliebig und der Zeilenumbruch sowohl LF- als auch CR LF-codiert sein.

Wird während des Imports kein passendes Kennwort zu einem Zertifikat in der CSV-Datei gefunden oder ist ein Kennwort falsch angegeben, erscheint automatisch ein Dialog zur manuellen Kennworteingabe. Bei korrekter Kennworteingabe wird das Zertifikat angelegt, anderenfalls wird es übersprungen.

Massenimport über Zertifikatcontainer

Zertifikatimport

Öffnen Sie den **Container: Zertifikate** und führen Sie folgende Schritte aus:

Allgemein

- (OPTIONAL) KENNWÖRTER FÜR ZERTIFIKATIMPORT: Öffnen Sie den Dateiauswahldialog mit Klick auf UPLOAD.

  Wählen Sie die zu importierende CSV-Datei aus und bestätigen Sie die Auswahl mit ÖFFNEN.

  Siehe auch *Kennwortliste in CSV-Format (optional)*.

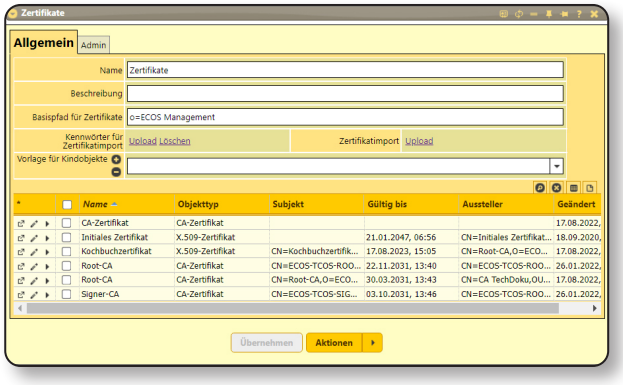

Abb. 1.01: *Importfunktion in Zertifikatcontainer*

- ZERTIFIKATIMPORT: Öffnen Sie den Dateiauswahldialog mit Klick auf UPLOAD.

  Wählen Sie die zu importierenden Dateien aus und bestätigen Sie die Auswahl mit ÖFFNEN.

- Der Importvorgang startet...

Während des Importvorgangs wird automatisch ein neuer Untercontainer mit dem Namen **Upload** angelegt.

Für jede importierte Zertifikatdatei wird automatisch ein passendes CA- oder X.509-Zertifikatobjekt erzeugt. Dabei werden alle Felder des Zertifikatsobjekts mit den Werten des jeweiligen Zertifikats befüllt. Das Zertifikatobjekt erhält den Common Name (CN) aus der Subjektzeile des Zertifikats.

Wird eine PKCS#7- oder PKCS#12-Datei hochgeladen, die mehrere Zertifikate enthält, werden beim Import alle Zertifikate automatisch angelegt.

Nach Abschluss des Importvorgangs ändert sich die Anzeige im Feld STATUSANZEIGE zu **Zertifikat hochgeladen**.

Einzelimport über Zertifikatobjekt

1 Zertifikatobjekt anlegen

Legen Sie an geeigneter Stelle im Konfigurationsbaum ein CA- oder X.509-Zertifikatobjekt an.

Nehmen Sie folgende Einstellungen vor:

CA-Zertifikat → Allgemein

- Name: Geben Sie dem Zertifikatobjekt einen geeigneten Namen.
- Erstellung des Zertifikats: Wählen Sie ---.
- Signatur-Hashalgorithmus: Wählen Sie den Hashalgorithmus aus, der den Einstellungen des externen CA-Zertifikats entspricht.
- CA-Kennwort anfordern: Wählen Sie aus, ob und wann das Kennwort für den privaten Schlüssel der signierenden CA angefordert werden soll. Dies muss den Einstellungen des externen CA-Zertifikats entsprechen.

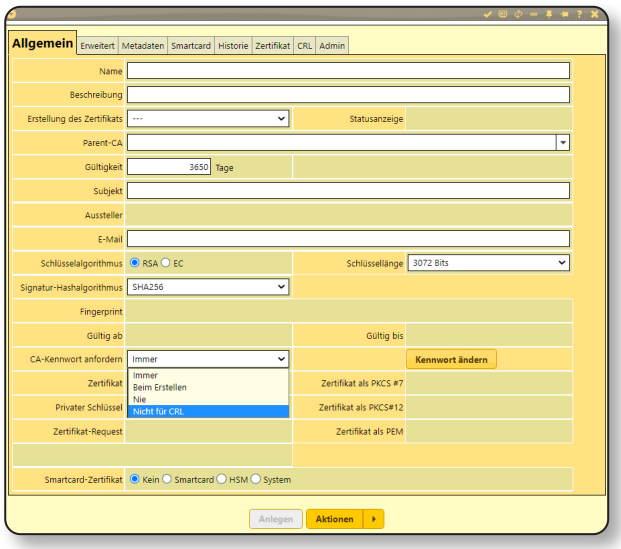

Abb. 2.01: *Anlegen eines CA-Zertifikatobjekts*

  - Immer: Das CA-Kennwort wird für jede Operation angefordert, die den privaten Schlüssel der CA erfordert. Das Kennwort wird nicht auf der Appliance gespeichert. Geht das CA-Kennwort verloren, kann es nicht mehr zurückgesetzt werden.
  - Beim Erstellen: Das CA-Kennwort wird beim Erstellen neuer Zertifikate angefordert. Für die Verlängerung bestehender Zertifikate ist kein CA-Kennwort erforderlich. Diese Einstellung wird empfohlen, wenn Zertifikate automatisch verlängert werden sollen.
  - Nie: Das CA-Kennwort wird nie angefordert. Diese Einstellung wird empfohlen, wenn eine CA Vorgänge automatisiert durchführen soll.
  - Nicht für CRL: Das CA-Kennwort wird nicht beim Erzeugen einer CRL angefordert. Diese Einstellung wird empfohlen, wenn CRLs automatisch verlängert werden sollen.
- Smartcard-Zertifikat: Wählen Sie aus, ob das Zertifikat als reines Softwarezertifikat erstellt, auf einen Hardwarespeicher (Smartcard, HSM) oder an ein externes System übertragen werden soll.

X.509-Zertifikat → Allgemein

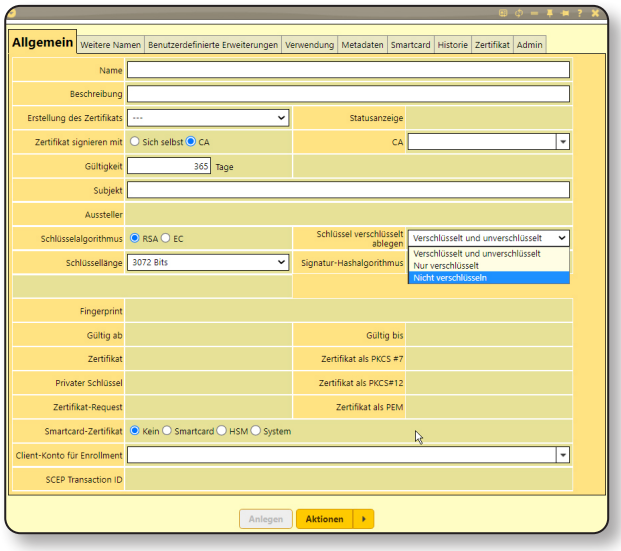

Abb. 2.02: *Anlegen eines X.509-Zertifikatobjekts*

- Name: Geben Sie dem Zertifikatobjekt einen geeigneten Namen.
- Erstellung des Zertifikats: Wählen Sie ---.
- Schlüssel verschlüsselt ablegen: Wählen Sie aus, ob der private Schlüssel beim Zertifikatimport kennwortverschlüsselt oder unverschlüsselt abgelegt werden soll.
  - Verschlüsselt und unverschlüsselt: Der private Schlüssel wird sowohl verschlüsselt als auch unverschlüsselt abgelegt. Für den Download steht nur die verschlüsselte Version bereit und der heruntergeladene Schlüssel ist nur mit dem individuellen Kennwort zu nutzen. Operationen wie VPN-Aufbau verwenden die unverschlüsselte Version des privaten Schlüssels.
  - Nur verschlüsselt: Der private Schlüssel wird verschlüsselt abgelegt. Das Kennwort wird bei jeder Operation mit dem privaten Schlüssel abgefragt.
  - Nicht verschlüsseln: Der private Schlüssel wird ohne Kennwort abgelegt. Alle Operationen, die den privaten Schlüssel benötigen, werden automatisch durchgeführt.
- Smartcard-Zertifikat: Wählen Sie aus, ob das Zertifikat als reines Softwarezertifikat erstellt, auf einen Hardwarespeicher (Smartcard, HSM) oder an ein externes System übertragen werden soll.

2 Upload der Zertifikatdatei

Allgemein

- Zertifikat: Öffnen Sie den Dateiauswahldialog mit Klick auf Upload.

  Wählen Sie die zu importierende Datei aus und bestätigen Sie die Auswahl mit Öffnen.

- Der Importvorgang startet...

Während des Importvorgangs werden die Felder des Zertifikatobjekts automatisch mit allen relevanten Werten befüllt.

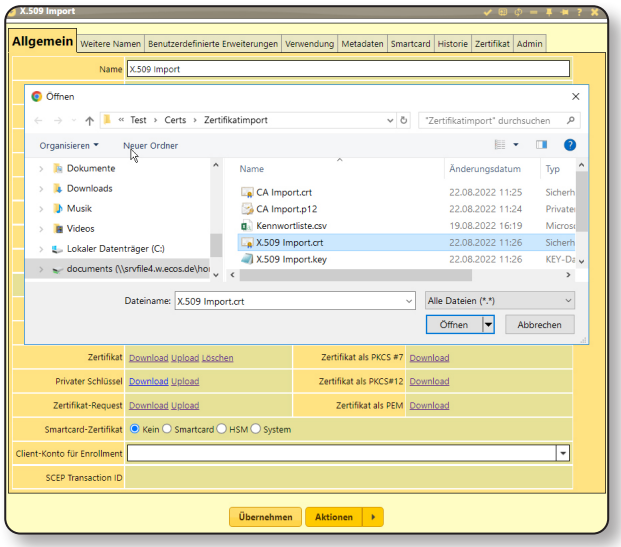

Abb. 2.03: *Upload eines Clientzertifikats*

Wird eine PKCS#7- oder PKCS#12-Datei hochgeladen, die CA- und Clientzertifikate enthält, wird automatisch das zum Objekttyp passende Zertifikat hochgeladen.

Nach Abschluss des Imports ändert sich die Anzeige im Feld STATUSANZEIGE zu **Zertifikat hochgeladen**.

3 Upload des privaten Schlüssels

Sind Zertifikat und privater Schlüssel in zwei Dateien abgespeichert, kann jetzt der dazugehörige private Schlüssel hochgeladen werden.

Allgemein

- PRIVATER SCHLÜSSEL (UNVERSCHLÜSSELT): Öffnen Sie den Dateiauswahldialog mit Klick auf UPLOAD.

  Wählen Sie die zu importierende Datei aus und bestätigen Sie die Auswahl mit ÖFFNEN.

- Geben Sie bei Aufforderung das Kennwort für den privaten Schlüssel an.

- Der private Schlüssel wird hochgeladen...

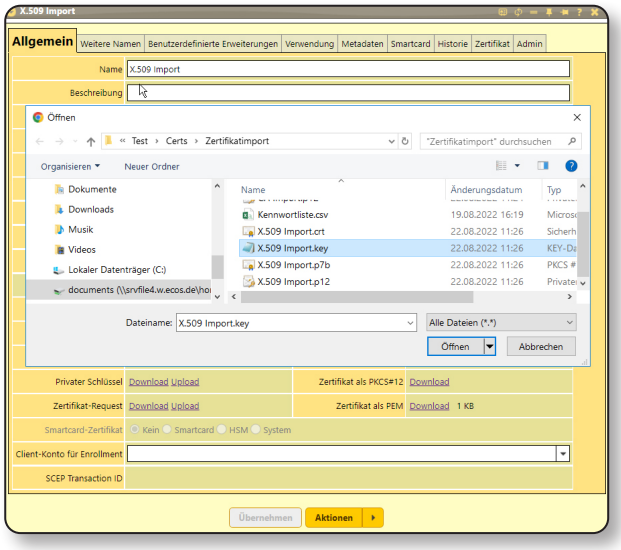

Abb. 2.04: *Upload eines privaten Schlüssels*

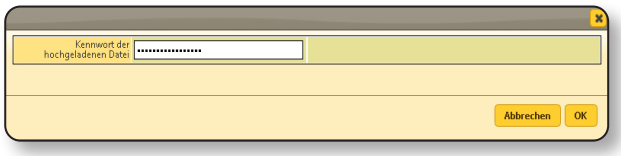

Abb. 2.05: *Abfrage des Kennworts für privaten Schlüssel*