ECOS **TrustManagementAppliance**

Zertifikat-Enrollment auf TCOS-Smartcards für SecurePIM

Admin-Tutorial

Version: 1.1

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

Diese Anleitung beschreibt Schritt für Schritt das Zertifikat-Enrollment auf TCOS-Smartcards. Sie richtet sich an Administratorinnen und Administratoren der ECOS **TrustManagementAppliance®** (TMA) und enthält Informationen zu Konfiguration und Enrollment von Zertifikaten für TCOS-Smartcards, die zum Einsatz mit SecurePIM via AirID-Leser gedacht sind.

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

Wichtige Hinweise

Folgende Hinweise sollten beachtet werden:

Keine Initialisierung

TCOS-Smartcards können nicht initialisiert werden. Das kryptografische Schlüsselmaterial kann weder von der Smartcard gelöscht noch verändert werden. Nur die von T-Systems mitgelieferten Zertifikate/Stammzertifikate können gelöscht werden.

Zero-PIN-Status

TCOS-Smartcards werden im Zero-PIN-Status ausgeliefert. Beim ersten Enrollment müssen daher einmalig PIN und PUK vergeben werden. Danach können zwar PIN und PUK mit den TCOS-Tools geändert, die Smartcard selbst jedoch nicht mehr in den Auslieferungszustand zurückgesetzt werden. Für Tests sollten die Zertifikate daher im Auslieferungszustand gesichert werden.

Zertifikat-Slots

Zertifikate werden auf TCOS-Smartcards in virtuellen Zertifikat-Slots gespeichert. Beim Zertifikat-Enrollment werden X.509-Zertifikate anhand folgender Merkmale dem korrekten Slot automatisch zugewiesen:

Slot	Zertifikat	Zuordnungsmerkmal
RCA	Root-CA-Zertifikat	Selbstsignierte CA
SCA	Signer-CA-Zertifikat	Nicht selbstsignierte CA
AUT	Authentisieren	Schlüsselverwendung Digital signieren, kritisch
ENC	Verschlüsseln	Schlüsselverwendung Schlüsselaushandlung, kritisch
ADS	Signieren	Schlüsselverwendung Nichtabstreitbarkeit, kritisch

Enrollment-Tool

Die von TCOS gelieferte PKCS#11 unterstützt weder Slots noch Elliptic-Curve-Schlüssel. Für das Zertifikat-Enrollment wird daher ein zusätzliches Tool als Middleware benötigt (siehe Abschnitt Erforderliche Tools auf Seite 6).

TCOS-Smartcards und RDP

Bitte beachten Sie, dass eine Weiterleitung von TCOS-Smartcards in eine RDP-Sitzung nicht zuverlässig möglich ist.

Verlängern von Zertifikaten

Zertifikate können wie gewohnt verlängert werden.

Zurückziehen von Zertifikaten

Zertifikate können wie gewohnt zurückgezogen, das Schlüsselmaterial kann jedoch nicht von der TCOS-Smartcard gelöscht werden. Die Smartcard kann entweder verworfen oder neu betankt werden.

Vorbereitungen

Folgende Vorbereitungen müssen vor Konfiguration des Zertifikat-Enrollment getroffen werden:

Erforderliche Tools

Folgende Tools sind für Konfiguration und Enrollment erforderlich:

- Library **P11TCOS3NetKey.dll** als Middleware (32-Bit-Version)
- Kommandozeilen-Utility **seratcosrenew.exe** für SecurePIM von devconi als Middleware
- ggf. **TeleSec CardManager** für Tests

Middleware in TMA hochladen

Vor der Konfiguration des **Dienstes: Smartcard-Enrollment** müssen das Kommandozeilen-Utility für SecurePIM sowie die Library als Middleware hochgeladen werden:

Container: Software-Update → Container → Datei für Mobile Office → seratcosrenew.exe
Container: Software-Update → Container → Datei für Mobile Office → P11TCOS3NetKey.dll

Container-Objekt für Enrollment auf TMA

Für die auszurollenden Zertifikate muss ein **Container: Zusammen auszurollende Zertifikate** an geeigneter Stelle auf der TMA angelegt werden.

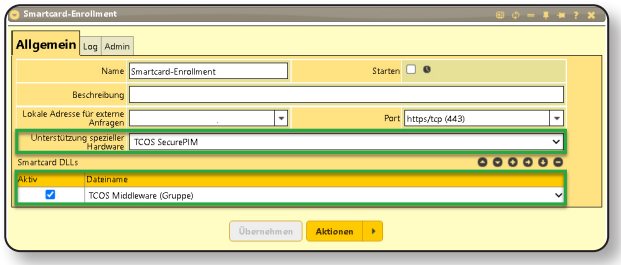
Anleitung

Sind die Vorbereitungen abgeschlossen, loggen Sie sich als Admin auf der ECOS Appliance ein.

1 Dienst: Smartcard-Enrollment einrichten

Sofern noch nicht erfolgt, legen Sie im **Container: ECOS Systeme → ECOS Appliance → Container: Dienste** den **Dienst: Smartcard-Enrollment** an und nehmen Sie folgende Einstellungen vor:

Allgemein



- Unterstützung spezieller Hardware: Wählen Sie TCOS SecurePIM aus.
- Smartcard DLLs: Wählen Sie die zuvor hochgeladene TCOS Middleware als Einzeldateien oder den Container als Gruppe aus.
- Aktiv: Aktivieren Sie die Checkbox, um die Middleware zu verwenden.
- Übernehmen/Anlegen: Speichern Sie die Einstellungen.

Wurde der Dienst: Smartcard-Enrollment sowohl für ATOS- als auch für TCOS-Karten konfiguriert, muss vor dem Start des Enrollment-Vorgangs die jeweils nicht benötigte Middleware im Feld **Smartcard DLLs** deaktiviert werden.

Wir empfehlen, ATOS- und TCOS-Middleware in jeweils separaten Containern hochzuladen. Diese Container sind im Dropdown-Menü als **Gruppe** zusammengefasst und vereinfachen das Umschalten.

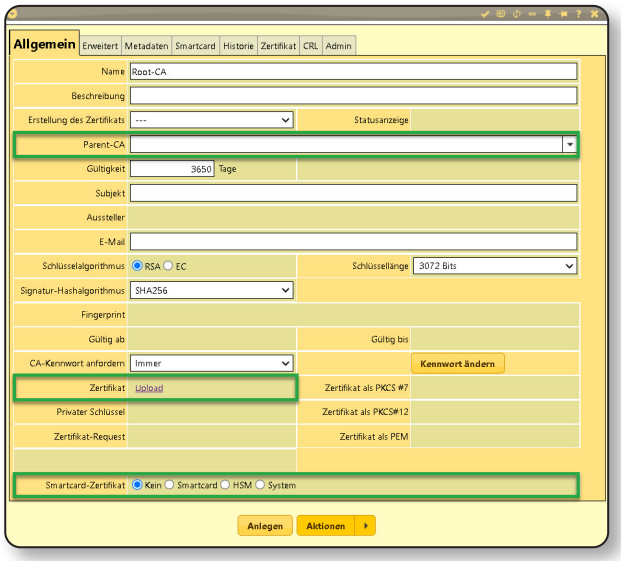
2 Import der CA-Zertifikate

Zum Signieren und Ausstellen der Smartcard-Zertifikate wird eine zweistufige CA-Kette benötigt:

Slot	Zertifikat	Parent-CA	Aufgabe
RCA	Root-CA	selbstsigniert	signiert Signer-CA
SCA	Signer-CA	Root-CA	stellt AUT-, ENC- und ADS-Zertifikat aus

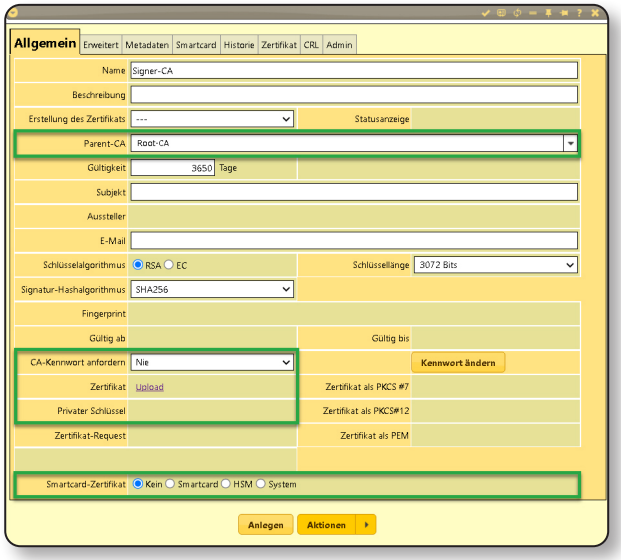
Legen Sie für den Zertifikatimport in einem passenden **Zertifikat-Container** zwei **CA-Zertifikat-Objekte** mit folgenden Einstellungen an:

Root-CA - Allgemein



- Parent-CA: Lassen Sie dieses Feld leer.
- Signatur-Hashalgorithmus: Wählen Sie den Hash-algorithmus aus, der den Einstellungen des externen CA-Zertifikats entspricht.
- Zertifikat-Upload: Importieren Sie das Root-CA-Zertifikat (ohne privaten Schlüssel).
- Smartcard-Zertifikat: Wählen Sie die Option **Kein**.

Signer-CA - Allgemein



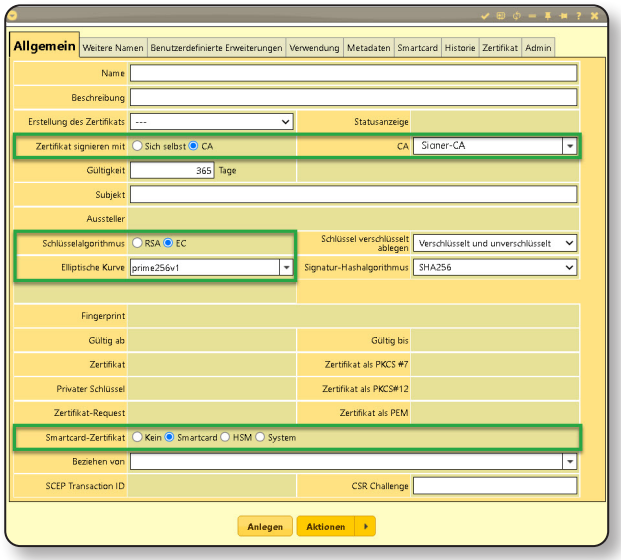
- Parent-CA: Wählen Sie die **Root-CA** aus.
- Signatur-Hashalgorithmus: Wählen Sie den Hash-algorithmus aus, der den Einstellungen des externen CA-Zertifikats entspricht.
- CA-Kennwort anfordern: Wählen Sie die Option **Nie**.
- Zertifikat-Upload: Importieren Sie das Signer-CA-Zertifikat.
- Privater Schlüssel: Laden Sie ggf. den zugehörigen privaten Schlüssel hoch (sofern Sie diesen nicht bereits mit dem CA-Zertifikat als PKCS#12 hochgeladen haben).
- Smartcard-Zertifikat: Wählen Sie die Option **Kein**.

Weitere Hinweise zum Import externer Zertifikate finden Sie im Tutorial **Import externer Zertifikate**.

3 Konfiguration der Zertifikatvorlagen

Legen Sie im **Container: Zusammen auszurollende Zertifikate** drei X-509-Zertifikat-Objekte als Vorlagen für Authentisierungs-, Verschlüsselungs- und Signierungszertifikat an und nehmen Sie folgende Einstellungen vor:

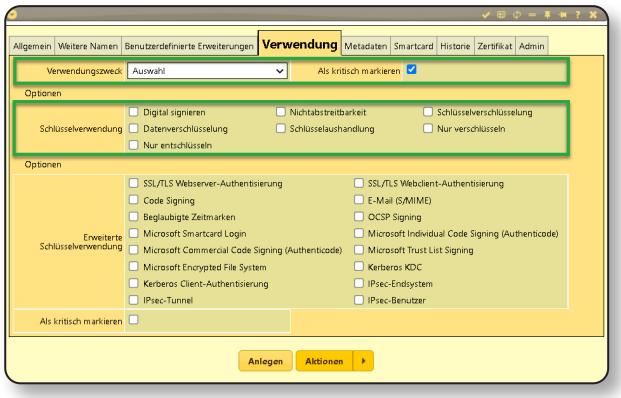
Allgemein



- ZERTIFIKAT SIGNIEREN MIT: Wählen Sie die Option **CA**.
- CA: Wählen Sie die **Signer-CA** aus.
- SCHLÜSSELALGORITHMUS: Wählen Sie die Option **EC**.
- ELLIPTISCHE KURVE: Wählen Sie **prime256v1**.
- SMARTCARD-ZERTIFIKAT: Wählen Sie die Option **Smartcard**.

Schlüsselverwendung

Jede Zertifikatvorlage muss mit einem spezifischen Schlüsselverwendungszweck konfiguriert werden, damit die Zertifikate beim Enrollment dem korrekten Slot auf der Smartcard zugeordnet werden können.



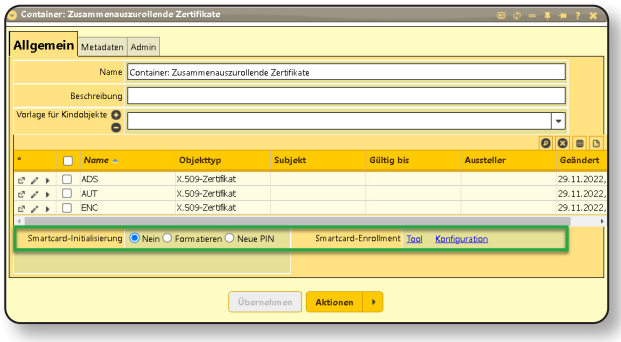
- VERWENDUNGSZWECK: Wählen Sie im Dropdown-Menü die Option **Auswahl**.
- ALS KRITISCH MARKIEREN: Aktivieren Sie die Checkbox.
- SCHLÜSSELVERWENDUNG: Aktivieren Sie die Checkboxen gem. folgender Tabelle:

Slot	Zertifikat	Schlüsselverwendungszweck
AUT	Authentisieren	Digital signieren
ENC	Verschlüsseln	Schlüsselaushandlung
ADS	Signieren	Nichtabstreitbarkeit

4 Zertifikat-Enrollment

Führen Sie im **Container: Zusammen auszurollende Zertifikate** folgende Schritte aus:

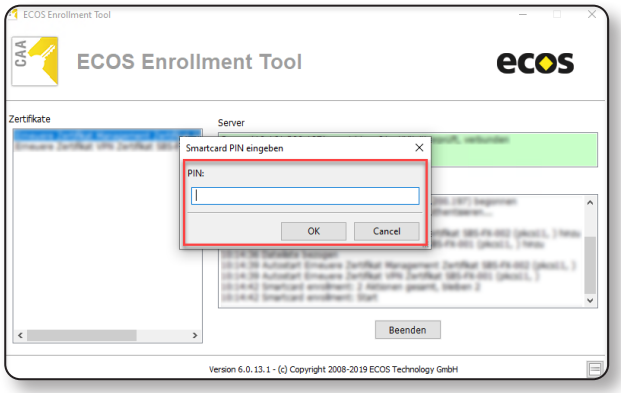
Allgemein



- SMARTCARD-INITIALISIERUNG: Wählen Sie die Option Nein.
- SMARTCARD-ENROLLMENT: Klicken Sie auf Tool und laden Sie das Enrollment-Tool herunter.

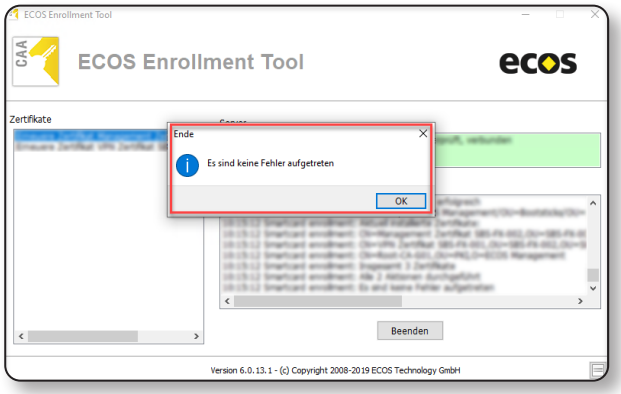
  Speichern Sie das Enrollment-Tool an geeigneter Stelle in Ihrem Dateisystem.

PIN/PUK-Vergabe



- Legen Sie die TCOS-Smartcard in den angeschlossenen Smartcard-Reader und führen Sie das zuvor heruntergeladene Enrollment-Tool per Doppelklick aus.
- Der Zero-PIN-Status wird erkannt und löst einen Dialog mit vier Feldern zur Vergabe/Bestätigung von PIN und PUK aus.
- Die PUK kann danach nicht mehr geändert werden.

Token-Objekt wird angelegt



- Während des Zertifikat-Enrollment wird für die jeweilige TCOS-Smartcard ein Token-Objekt angelegt, das deren Seriennummer und eine Verbindung zu den ausgerollten Zertifikaten enthält.