ECOS Appliances

Smartcard-Enrollment

Admin-Tutorial

Version: 1.2

Datum: 07/2024

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 3

Vorbereitungen 4

Smartcard ausrollen 9

Einführung

Die ECOS SystemManagementAppliance (SMA) bietet die Möglichkeit Zertifikate mithilfe des Smartcard-Enrollment-Tools auf eine Smartcard zu schreiben.

Um den ECOS SecureBootStick® FX/SX (SBS) zu nutzen, wird eine Smartcard benötigt, auf der die Zertifikate zur Anmeldung und zur Nutzung einer VPN-Verbindung gespeichert sind.

Diese Anleitung richtet sich an Administratorinnen und Administratoren von ECOS Appliances und führt Sie durch die verschiedenen Einstellungen des Smartcard-Enrollment-Tools.

Bitte lesen Sie den Abschnitt *Vorbereitungen* vor Beginn sorgfältig durch und bewahren Sie diese Anleitung zur weiteren Verwendung auf.

Vorbereitungen

Um Smartcards für ECOS SecureBootStick® (SBS) auszurollen, benötigen Sie einen funktionsfähigen Smartcard-Reader. Schließen Sie diesen an und setzen Sie die zu beschreibene Smartcard ein.

Auf der SMA müssen die Middleware-Dateien hochgeladen werden und die Objekte **Dienst: Smartcard-Enrollment**, **ECOS Secure Boot System** und **X.509-Zertifikat** angelegt und konfiguriert sein.

Middleware-Dateien hochladen

Um Zertifikate und Smartcards auszurollen, wird eine Middleware benötigt. Smartcards, die mit einem SBS genutzt werden, müssen mit der ATOS Middleware ausgerollt werden. Die nötigen Dateien erhalten Sie vom ECOS Support. Dabei handelt es sich um die SPE-Variante der ATOS Middleware.

Beachten Sie, dass auf dem Rechner, an dem Sie das Smartcard-Enrollment durchführen, keine ATOS Middleware-Software installiert ist.

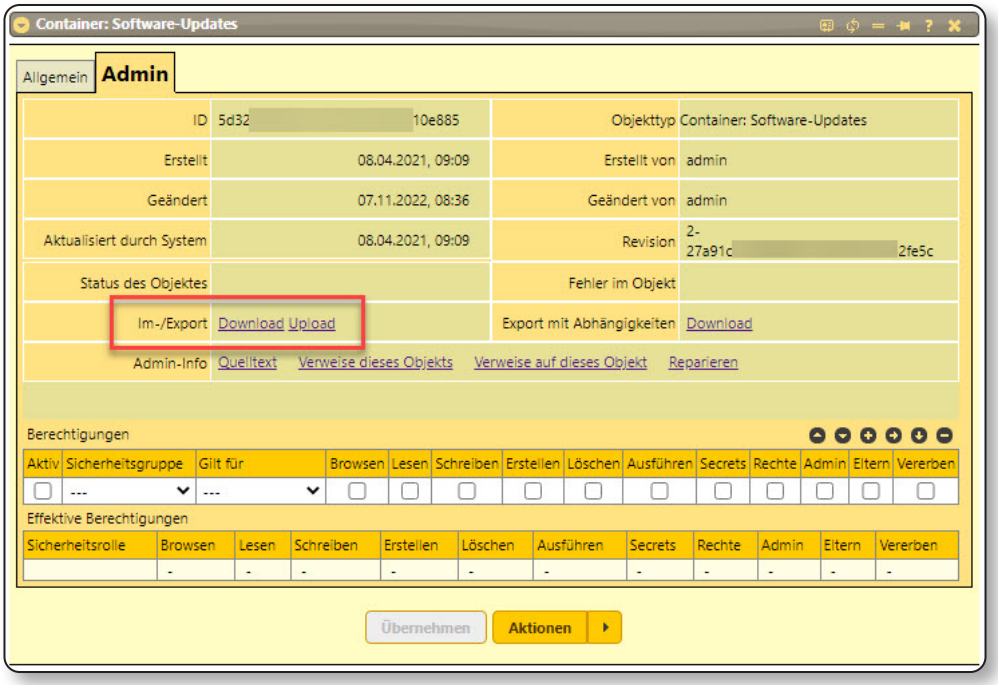

Abb. 1.01: *Container: Software-Updates - Reiter Admin*

Öffnen Sie den **Container: Software-Updates** und navigieren Sie zum Reiter Admin.

Admin

- Im-/Export: **Upload**

  Es öffnet sich der Dateiauswahldialog. Wählen Sie die ATOS Middleware-Datei aus und bestätigen Sie mit Öffnen.

  Es wird unter dem **Container: Software-Updates** automatisch ein Container **ATOS Middleware** angelegt, in dem sich die verschiedenen Dateien als **Datei für Mobile Office**-Objekte befinden.

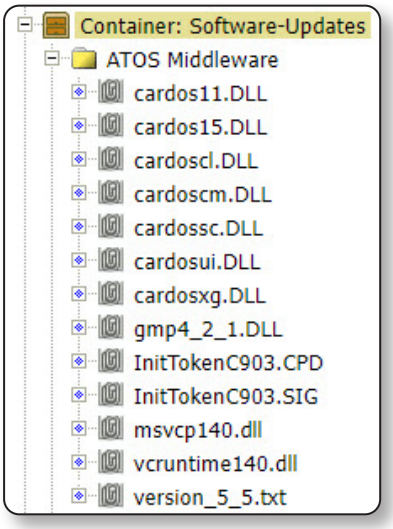

Abb. 1.02: *ATOS Middleware-Dateien*

Dienst: Smartcard-Enrollment

Der **Dienst: Smartcard-Enrollment** muss unterhalb des **ECOS Appliance**-Objekts im Baum angelegt und mit folgenden Einstellungen konfiguriert sein:

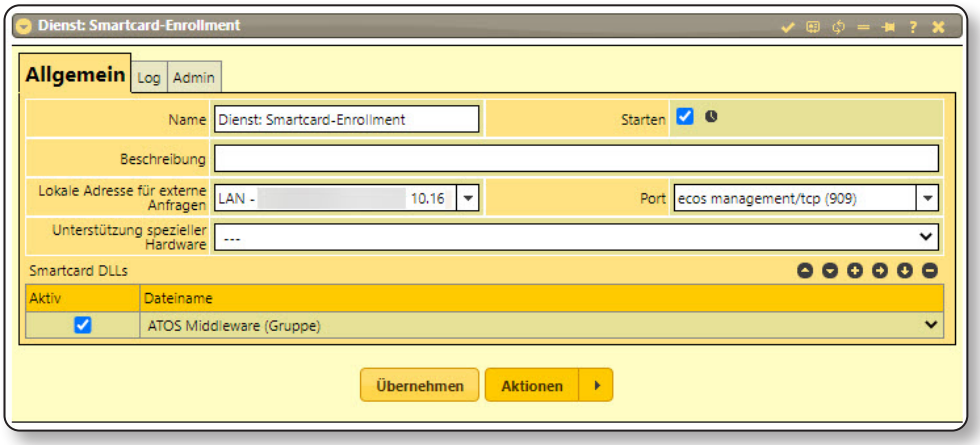

Abb. 1.03: *Dienst: Smartcard-Enrollment*

Allgemein

- Name: Vergeben Sie einen aussagekräftigen Namen.
- Starten: Aktivieren Sie diese Checkbox.
- Lokale Adresse für externe Anfragen: Wählen Sie eine Schnittstelle, um externe Anfragen zu verarbeiten. Standardmäßig können Sie die IP-Adresse der SMA auswählen.
- Port: Wählen Sie den Port für die oben angegebene Adresse. Standardmäßig können Sie den Management-Port der SMA (Port **909**) auswählen.

- Smartcard DLLs: Wählen Sie unter Dateiname entweder den oben angelegten Container **ATOS Middleware (Gruppe)** oder die einzelnen Middleware-Dateien aus und aktivieren Sie die Checkbox Aktiv. Achten Sie darauf, dass alle ATOS Middleware-Dateien aufgelistet sind, wenn Sie nicht den ganzen Container ausgewählt haben.

Speichern Sie die Änderungen mit Übernehmen.

SBS-Objekt: ECOS Secure Boot System

Ein SBS-Objekt vom Typ **ECOS Secure Boot System** muss für die Nutzung einer Smartcard mit folgenden Einstellungen konfiguriert sein:

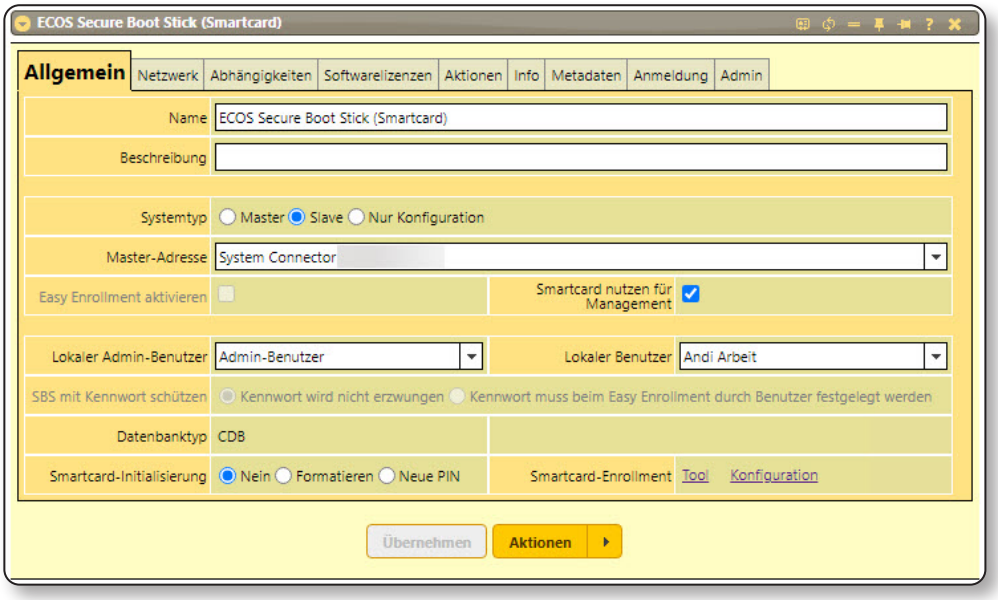

Abb. 1.04: *ECOS Secure Boot System - Reiter Allgemein*

Allgemein

- Name: Vergeben Sie einen aussagekräftigen Namen.
- Systemtyp: **Slave**
- Master-Adresse: Wählen Sie hier den **ECOS System Connector** aus.
- Smartcard nutzen für Management: Aktivieren Sie diese Checkbox.
- Lokaler Admin-Benutzer: Wählen Sie das Benutzerobjekt, das administrativen Zugriff auf den SBS erhalten soll.
- Lokaler Benutzer: Wählen Sie das Benutzerobjekt, das mit dem SBS arbeiten soll.

- SMARTCARD-INITIALISIERUNG: Die verschiedenen Optionen werden unter *Smartcard ausrollen* erklärt.

X.509-Zertifikat

Ein **X.509-Zertifikat** muss unterhalb des SBS-Objekts angelegt und mit folgenden für das Smartcard-Enrollment spezifischen Einstellungen konfiguriert werden:

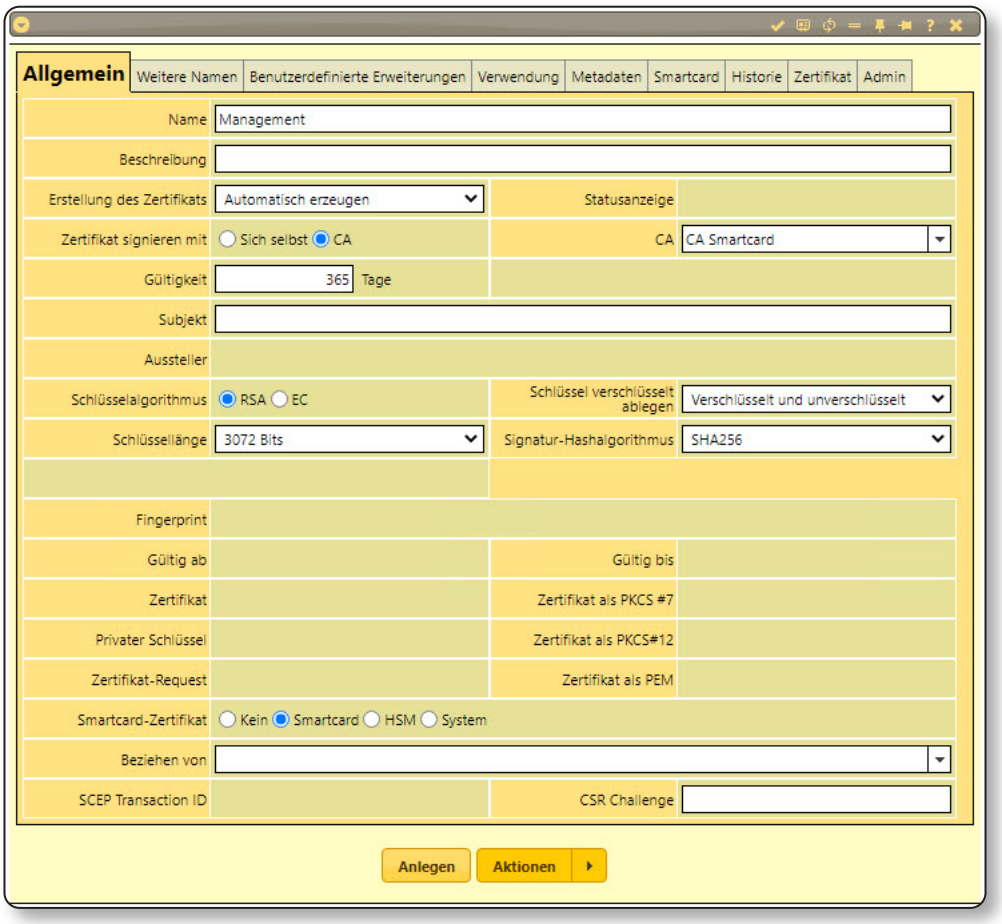

Abb. 1.05: *Zertifikat - Reiter Allgemein*

Allgemein

- ERSTELLUNG DES ZERTIFIKATS: **Automatisch erzeugen**
- SMARTCARD-ZERTIFIKAT: **Smartcard**

Verwendung

- VERWENDUNGSZWECK: **SBS, Authentisieren**

Abb. 1.06: *Zertifikat - Reiter Verwendung*

Die STATUSANZEIGE auf dem Reiter Allgemein muss nach Erstellung des Zertifikat auf **Bereit zum Erzeugen des Zertifikats (Schlüssel nur auf Token)** stehen.

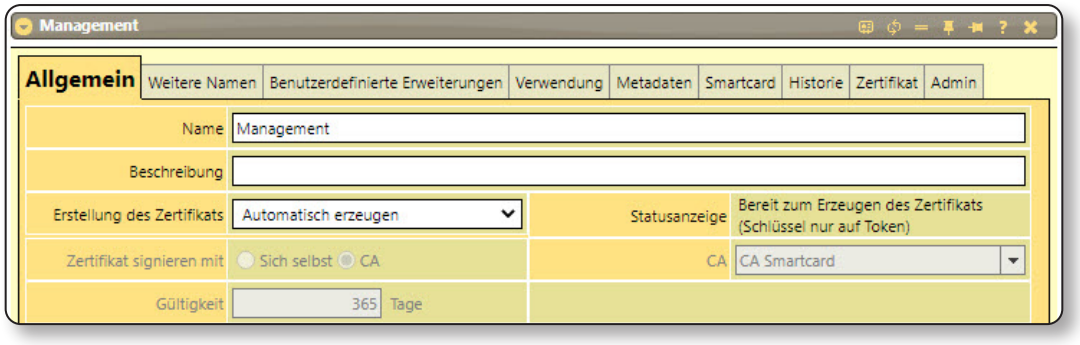

Abb. 1.07: *Zertifikat - Statusanzeige*

Weitere Informationen zu den Einstellungen im X.509-Zertifikat finden Sie in der Online-Hilfe der SMA.

Smartcard ausrollen

Öffnen Sie das SBS-Objekt, dessen Smartcard ausgerollt werden soll.

Allgemein

- Wählen Sie eine der Optionen im Feld SMARTCARD-INITIALISIERUNG aus. Änderungen speichern Sie mit ÜBERNEHMEN.
- Laden Sie das **Tool** im Feld SMARTCARD-ENROLLMENT herunter und öffnen Sie es.

Abb. 2.01: *Smartcard-Initialisierung: Nein*

Das Smartcard-Enrollment-Tool sollte auf dem Gerät ausgeführt werden, an dem auch der Smartcard-Reader angeschlossen ist, um Konflikte beim Ausrollen zu vermeiden.

Smartcard-Initialisierung: Nein

Die Einstellung **Nein** wird genutzt, um eine frische Smartcard erstmals zu initialisieren (Zero-PIN-Status) oder um bestehende Zertifikate auf der Smartcard zu verlängern.

Je nach Größe des zu erzeugenden Schlüssels kann die Initialisierung der Smartcard mehrere Minuten dauern.

Bei der Erstinitialisierung wird sowohl die **PIN** als auch die **PUK** für die Smartcard festgelegt. Die PIN lässt sich nachträglich ändern, die PUK nicht. Daher bewahren Sie die PUK sicher auf.

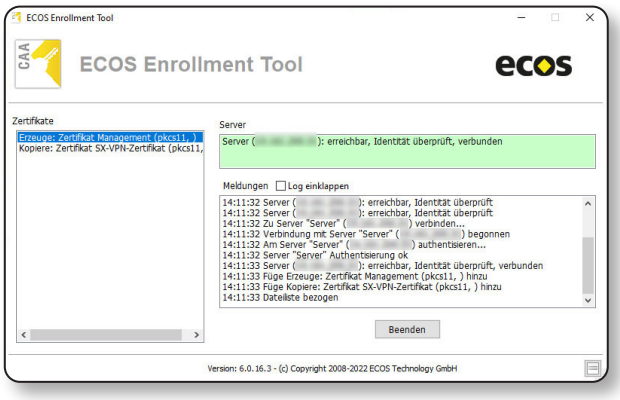

Abb. 2.02: *Erstinitialisierung der Smartcard*

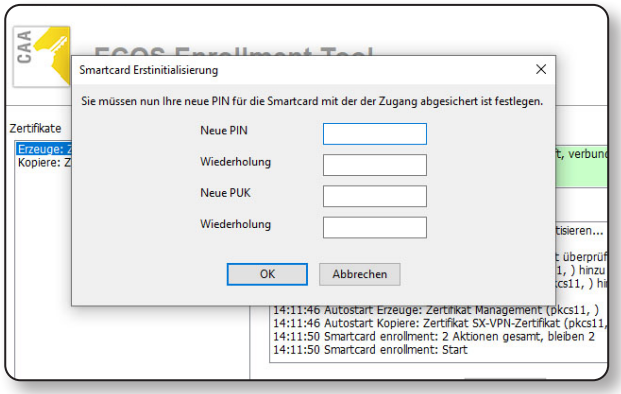

Abb. 2.03: *PIN- und PUK-Abfrage*

Smartcard-Initialisierung: Formatieren

Die Einstellung **Formatieren** wird genutzt, wenn die Daten der Smartcard überschrieben werden sollen, z.B. wenn ein Mitarbeiter das Unternehmen verlässt und die Smartcard für einen neuen Mitarbeiter ausgerollt werden soll. Je nach Größe des zu erzeugenden Schlüssels kann die Initialisierung der Smartcard mehrere Minuten dauern.

Beim Formatieren wird eine neue **PIN** festgelegt und die **PUK** abgefragt, die bei der Erstinitialisierung festgelegt wurde.

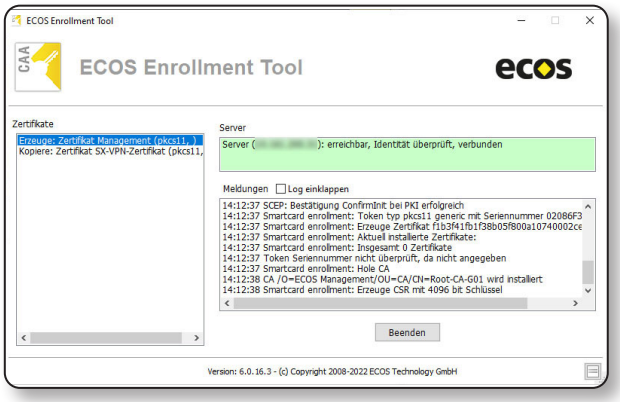

Abb. 2.04: *Schlüsselerzeugung*

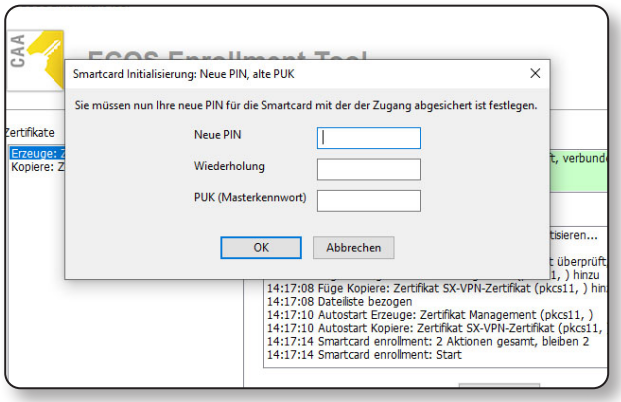

Abb. 2.05: *Smartcard formatieren*

Smartcard-Initialisierung: Neue PIN

Die Einstellung **Neue PIN** wird genutzt, um die PIN der Smartcard zu ändern. Alle anderen Daten bleiben unverändert.

Zum Ändern der **PIN** über das Smartcard-Enrollment-Tool wird die alte PIN benötigt. Ist die alte PIN nicht mehr vorhanden, muss die Smartcard-PIN über das Pinpad des SBS zurückgesetzt werden. Dafür wird die PUK benötigt.

Weitere Informationen zum Zurücksetzen der PIN finden Sie im SBS-Anwenderhandbuch.

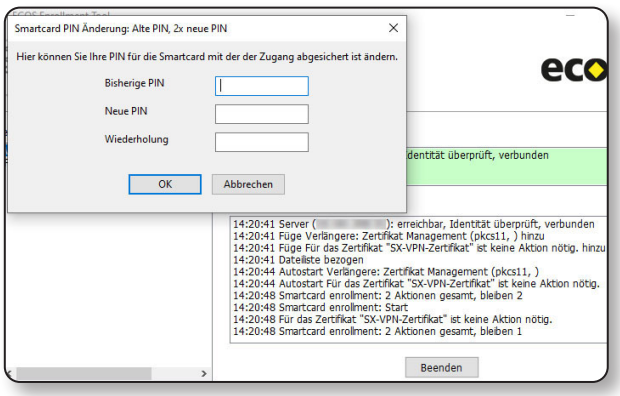

Abb. 2.06: *Neue PIN festlegen*

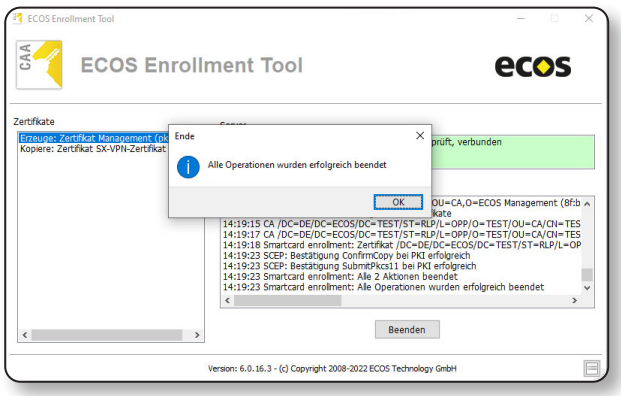

Abb. 2.07: *Smartcard-Enrollment abgeschlossen*

Einmaliges Herunterladen des Smartcard-Enrollment-Tools

Haben Sie das Smartcard-Enrollment-Tool einmalig heruntergeladen, können Sie es z.B. im Programmordner Ihres Computers speichern. Legen Sie dazu einen neuen Ordner an und benennen Sie das Tool um.

Anschließend können Sie statt des Tools, die KONFIGURATION herunterladen und mit dem Smartcard-Enrollment-Tool verknüpfen. Öffnen Sie das Kontextmenü der heruntergeladenen Konfigurationsdatei und wählen die Option ÖFFNEN MIT. Wählen Sie das Smartcard-Enrollment-Tool und aktivieren Sie die Checkbox IMMER DIESE APP ZUM ÖFFNEN VON .ECOSXENROLL-DATEIEN VERWENDEN.

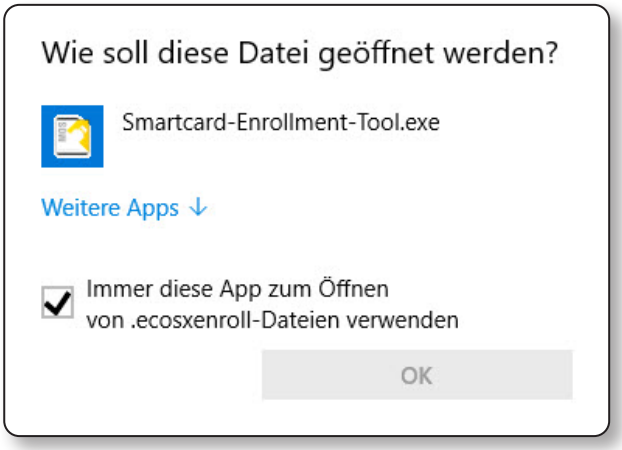

Abb. 2.08: *"Öffnen mit"-Dialog der Konfigurationsdatei*

Smartcard prüfen

Wird die Smartcard für einen SBS genutzt, prüfen Sie nach dem Ausrollen die Smartcard. Schließen Sie dazu den SBS an einen Rechner mit aktiver Internetverbindung an und booten Sie ihn, bis der SBS-Desktop erscheint.

Öffnen Sie das SBS-Objekt auf der SMA und navigieren Sie zum Reiter Info.

Info

AUSWAHL INFO: Wählen Sie die Option SMARTCARD INFO.

Es erscheinen die Informationen zu der Smartcard des SBS.

Abb. 2.09: *Smartcard-Informationen des SBS*

Prüfen Sie, ob unter INIT SW der Zusatz **PF2** angegeben wird. Fehlt der Zusatz, wurde die Smartcard nicht mit der SPE-Variante der ATOS Middleware ausgerollt. Wiederholen Sie das Smartcard-Enrollment, da es andernfalls zu Fehlern bei der Nutzung und Änderung der Smartcard-PIN kommt.

Achten Sie darauf, dass auf dem Rechner, auf dem Sie das Smartcard-Enrollment durchführen, keine Version der ATOS Middleware installiert ist. Deinstallieren Sie diese oder nutzen Sie einen anderen Rechner.

Die Information zu INIT SW wird ab der SBS-Version V7.0.28/V7.1.28 angezeigt.

Um die Firmware-Version zu prüfen, booten Sie den SBS an einem Rechner und öffnen Sie mit STRG+ALT+S den Systemstatus. Bei der Option HW VERSION muss mindestens der Zusatz **01.0e** angegeben sein.

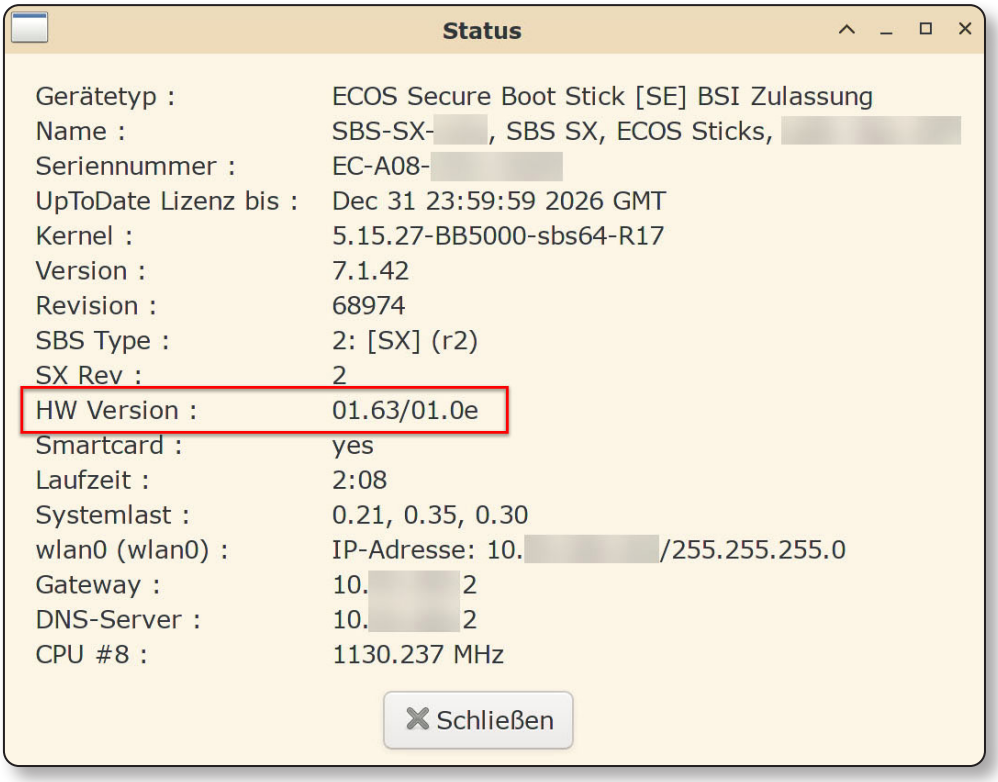

Abb. 2.10: *Systemstatus - Informationen zur installierten Firmware*