



ECOS TrustManagementAppliance®

Evolis Primacy 2 Smartcard-Drucker

Konfiguration des Smartcard-Batch-Enrollments

Admin-Tutorial

Version: 1.0

Datum: 08/2024

IT-Security Solutions

Made in Germany

Inhalt

Einführung.....	3
Wichtige Hinweise.....	4
Initiales Smartcard-Batch-Enrollment konfigurieren.....	5
Optional: Verweise auf Konfigurationsobjekte erstellen	8
Smartcard-Batch-Enrollment durchführen.....	9
PIN/PUK auslesen	11
Smartcard-Zertifikate verlängern.....	13



Einführung

Diese Anleitung richtet sich an Administratorinnen und Administratoren von ECOS Appliances und beschreibt Schritt für Schritt die Konfiguration des Smartcard-Batch-Enrollments auf der ECOS **TrustManagementAppliance**® für die Nutzung des Smartcard-Druckers Evolis Primacy 2 unter Windows.

Bitte lesen Sie den Abschnitt → **Wichtige Hinweise** sorgfältig durch und bewahren Sie diese Anleitung zur weiteren Verwendung auf.

Beachten Sie auch die Hinweise im Benutzerhandbuch für den Evolis Primacy 2-Smartcard-Drucker.



Wichtige Hinweise

Bitte beachten Sie folgende Hinweise:

➔ Lizenz

Die Nutzung des Smartcard-Druckers Evolis Primacy 2 in Kombination mit der Trust Management Appliance (TMA) erfordert eine Lizenz mit dem Feature **batch_sc**.

➔ Anschluss des Smartcard-Druckers und Treiber

Der Smartcard-Drucker wird per USB angeschlossen und benötigt unter Windows den generischen USB-Treiber **winusb.sys**. Der Treiber kann mit der Open-Source-Anwendung [Zadig](#) eingerichtet werden.

➔ Middleware und Smartcard-Enrollment-Dienst

Sofern dies noch nicht anderweitig erfolgt ist, muss im Container für Software-Updates die **ATOS-Middleware** hochgeladen werden. Außerdem muss der **Dienst: Smartcard-Enrollment** angelegt und konfiguriert sein.

Alle nötigen Informationen hierzu finden Sie in unserem Admin-Tutorial [Smartcard-Enrollment](#) im Abschnitt „Vorbereitungen“ auf Seite 4.

➔ ECOS Smartcard Printer Tool

Die Ansteuerung des Smartcard-Druckers erfolgt über das **ECOS Smartcard Printer Tool**.

Das Smartcard Printer Tool kann während des Konfigurationsprozesses als MSI-Paketdatei von der TMA bezogen und auf einem Windows-Rechner installiert werden.

Die zur Durchführung des Auftrags nötigen Daten erhält das Smartcard Printer Tool von einer Konfigurationsdatei, die vor Beginn des Enrollment- und Druckvorgangs von der TMA heruntergeladen wird.



Initiales Smartcard-Batch-Enrollment konfigurieren

Loggen Sie sich als Admin in die Expertenansicht der Trust Management Appliance (TMA) ein.

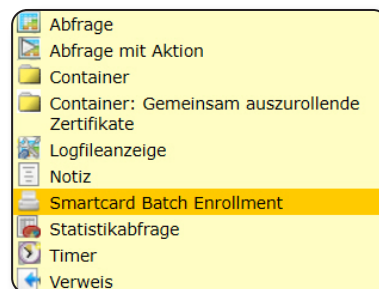


Container für Smartcard-Batch-Enrollment anlegen

Legen Sie im Zertifikatcontainer über das Kontextmenü einen Container vom Typ **Smartcard Batch Enrollment** an.

Bei gleichzeitigem Betrieb mehrerer Smartcard-Drucker benötigen Sie pro Drucker einen Smartcard-Batch-Enrollment-Container.

Nehmen Sie folgende Einstellungen vor:



Allgemein

- ➔ **Aktiv:** Aktivieren Sie die Checkbox, um den Dienst einzuschalten.

Nach Beendigung des Smartcard-Batch-Enrollments wird die Checkbox automatisch deaktiviert.

- ➔ **Drucken:** Hier legen Sie fest, ob der Smartcard-Drucker ein Label auf die Smartcards drucken soll.

Zur Auswahl stehen die Optionen **Immer**, **Nur wenn Seriennummer unbekannt** und **Nie**.

Das zu druckende Label ist der Name des Untercontainers für gemeinsam auszurollende Zertifikate. Siehe Abschnitt → *Container für gemeinsam auszurollende Zertifikate anlegen*.

- ➔ **Fehlerbehandlung:** Mit der Option **Anhalten** kann der Enrollment-Vorgang angehalten werden, bis der Fehler manuell behoben wurde.

Mit der Option **Abbrechen** wird der Enrollment-Vorgang abgebrochen.

Mit der Option **Weitermachen** kann der Enrollment-Vorgang übersprungen und der nächste Vorgang gestartet werden.

Im Fehlerfall wird eine Smartcard im Reject-Behälter des Druckers ausgegeben.

2 ECOS Smartcard Printer Tool herunterladen

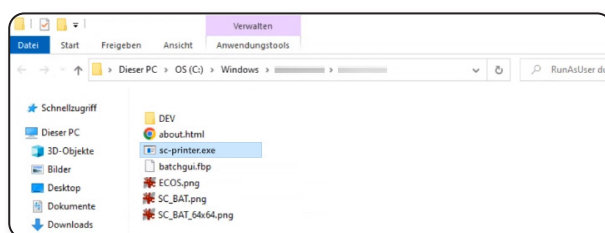
Damit der Evolis-Smartcard-Drucker unter Windows von der TMA angesteuert werden kann, muss das ECOS Smartcard Printer Tool heruntergeladen und installiert werden.

Öffnen Sie dazu den soeben angelegten Smartcard-Batch-Enrollment-Container.

Aktionen

- ➔ **Download:** Laden Sie unter [MSI-Installer](#) die Paketdatei herunter.

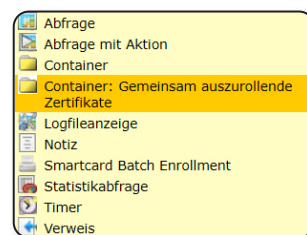
Installieren Sie das Smartcard Printer Tool unter Windows.



3 Container für gemeinsam auszurollende Zertifikate anlegen

Legen Sie im Smartcard-Batch-Enrollment-Container für jede Smartcard einen Container vom Typ **Gemeinsam auszurollende Zertifikate** an.

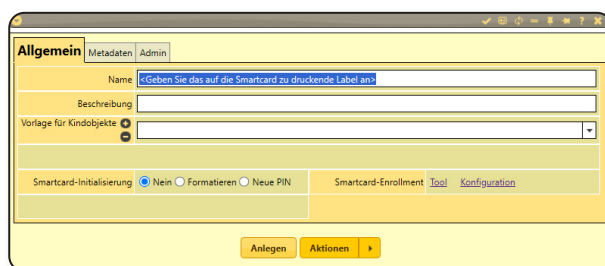
Jeder Container dieses Typs wird vom Smartcard Printer Tool als ein Job bearbeitet. Benötigt eine Smartcard lediglich ein Einzelzertifikat, kann dieses direkt im Smartcard-Batch-Enrollment-Container angelegt werden.



Nehmen Sie folgende Einstellungen vor:

Allgemein

- ➔ **Name:** Der Containername ist gleichzeitig das auf die Smartcard zu druckende Label.
- ➔ **Smartcard-Initialisierung:** Wählen Sie die Option **Nein**, um Smartcards erstmals zu initialisieren. Der Zero-Pin-Zustand wird automatisch erkannt und die Smartcard bei der Erstinitialisierung formatiert. PIN und PUK werden automatisch vergeben.



Hinweis

Wurden Smartcards nicht mit dem ECOS Smartcard Printer Tool erstinitialisiert, müssen im **Container: Smartcards/Token** passende Smartcard-Objekte mit PIN, PUK und Seriennummer vorkonfiguriert werden.



Zertifikate anlegen

Legen Sie im **Container: Gemeinsam auszurollende Zertifikate** die erforderlichen Smartcard-Zertifikate an.

Nehmen Sie mindestens folgende Einstellungen vor:

Allgemein

- ➔ **Erstellung des Zertifikats:** Wählen Sie **Automatisch erzeugen** aus.
- ➔ **Zertifikat signieren mit:** Wählen Sie **CA** aus.
- ➔ **CA-Zertifikat:** Wählen Sie die CA, die das jeweilige Zertifikat signieren soll.
- ➔ **Zertifikat auf Smartcard/HSM speichern:** Wählen Sie die Option **Smartcard**.

Übernehmen Sie die Einstellungen. Bei korrekter Konfiguration ändert sich die Statusanzeige des Zertifikats zu **Bereit zum Erzeugen des Zertifikats (Schlüssel nur auf Token)**.

i Hinweis

Nutzen Sie ggf. den Assistenten und die Objektrichtlinien im Management-Container der TMA, um Container, Zertifikate oder andere Konfigurationsobjekte mit Standardwerten vorzubelegen und automatisiert zu erzeugen.



Optional: Verweise auf Konfigurationsobjekte erstellen

Verweise sind Referenzen auf andere Konfigurationsobjekte und dienen als Stellvertreter für das eigentliche Objekt. So können Konfigurationsobjekte in Containern parallel gruppiert werden, während mehrere Smartcard-Drucker gleichzeitig operieren.

➔ Legen Sie Ihre Konfigurationsobjekte (SBS, Zertifikate etc.) wie gewohnt an.

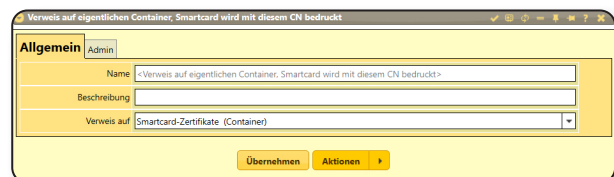
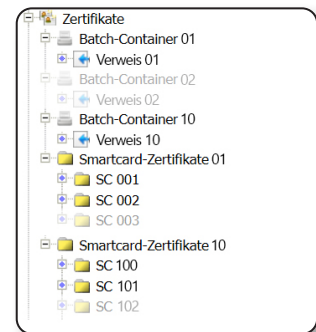
➔ Legen Sie pro Smartcard-Batch-Enrollment-Container (=Smartcard-Drucker) mindestens einen Verweis an.

Nehmen Sie folgende Einstellungen vor:

Allgemein

➔ **Name:** Der hier angegebene Name wird auf die Smartcard gedruckt.

➔ **Verweis auf:** Wählen Sie hier das Konfigurationsobjekt bzw. den übergeordneten Container aus, auf den verwiesen werden soll.





Smartcard-Batch-Enrollment durchführen

Führen Sie das Smartcard-Batch-Enrollment wie folgt durch:



Smartcards einlegen

Öffnen Sie das Kartenmagazin des Smartcard-Druckers und legen Sie die erforderliche Menge an Smartcards ein, wie im Benutzerhandbuch des Evolis Primacy 2-Kartendruckers beschrieben.



Konfigurationsdatei herunterladen

Öffnen Sie den Smartcard-Batch-Enrollment-Container.

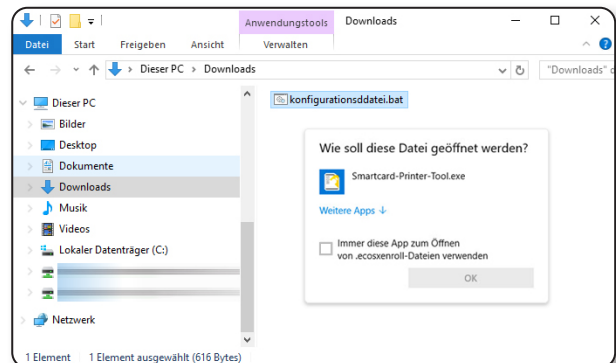
Aktionen

- ➔ **Download:** Laden Sie unter [Konfiguration](#) die Konfigurationsdatei herunter und speichern Sie sie im Downloadordner des Windows-Rechners.

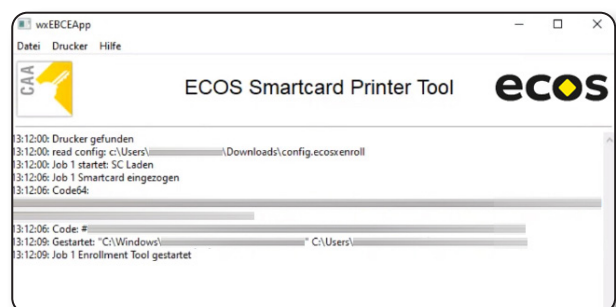


Enrollment starten

- ➔ Öffnen Sie die Konfigurationsdatei unter Windows mit dem ECOS Smartcard Printer Tool.



- ➔ Der Smartcard-Drucker wird angesteuert und der erste Job gestartet.



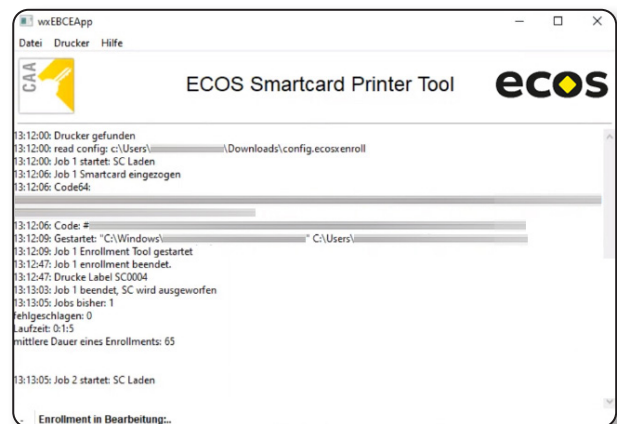
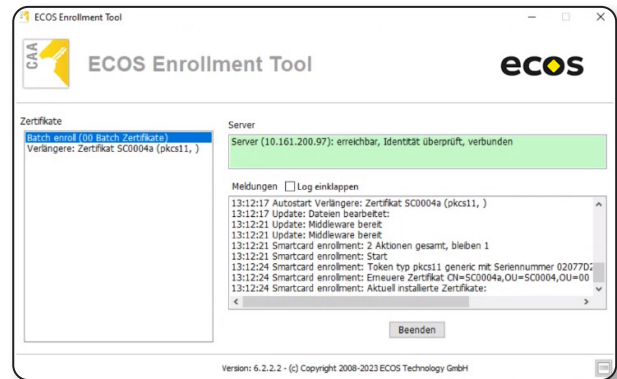
➔ Das ECOS Enrollment Tool wird gestartet.

Bei der Erstinitialisierung werden während des Enrollments PIN und PUK zufällig vergeben und mit der Seriennummer der Smartcard in automatisch erzeugten Smartcard-Objekten im **Container: Smartcards/Token** hinterlegt.

Anderenfalls hält der Prozess an und fordert zur manuellen Eingabe von PIN und PUK auf.

Nach dem Enrollment wird die jeweilige Smartcard bedruckt und vom Smartcard-Drucker ausgeworfen.

Danach wird automatisch der nächste Job gestartet.





PIN/PUK auslesen

Nach Abschluss des Smartcard-Batch-Enrollments können PINs und PUKs über eine einfache Abfrage oder die JSON-Exportdatei des Smartcard/Token-Containers ausgelesen werden.



PIN/PUK abfragen

Legen Sie an geeigneter Stelle über das Kontextmenü eine einfache **Abfrage** an.

Nehmen Sie folgende Einstellungen vor:

Abfrage

- ➔ **Objekttyp:** Wählen Sie **Zertifikat**.
- ➔ **Datenquelle:** Wählen Sie **Konfiguration**.
- ➔ **Auswahlkriterien:** Wählen Sie das Attribut **Pfad des Objekts**, den Vergleichsoperator **=~** und geben Sie die ID des Containers an, in dem die Smartcard-Zertifikate in ihren Untercontainern liegen.

Aktivieren Sie für jedes anzuwendende Auswahlkriterium die Checkbox in der Spalte **Aktiv**.

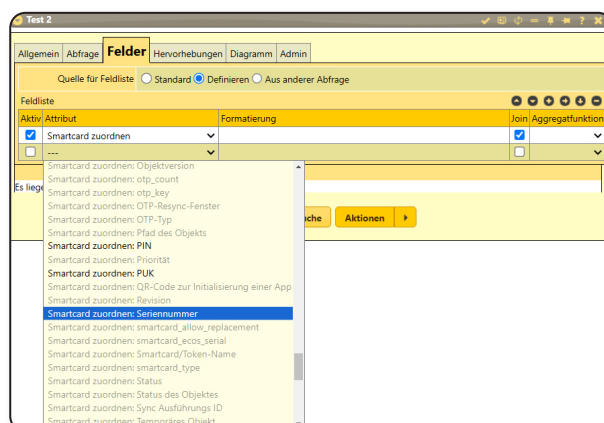
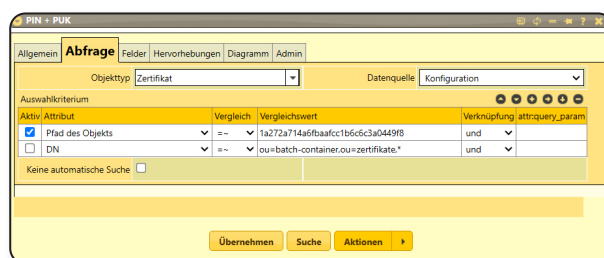
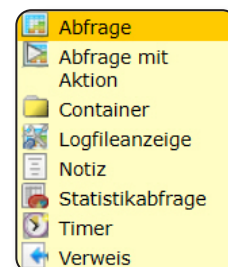
Felder

- ➔ **Quelle für Feldliste:** Wählen Sie **Definieren**.
- ➔ **Feldliste:** Wählen Sie **Smartcard zuordnen**, aktivieren Sie die Checkbox in der Spalte **Join** und speichern Sie die Einstellung.

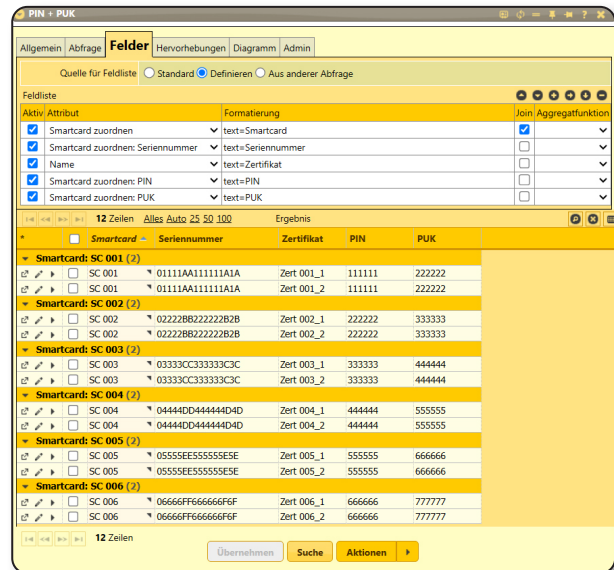
Nun werden in der Auswahlliste auch die Attribute von Smartcard-Objekten mit dem Präfix "Smartcard zuordnen:" eingebunden.

Wählen Sie die Attribute:

- ◆ Smartcard zuordnen: Seriennummer
- ◆ Smartcard zuordnen: PIN
- ◆ Smartcard zuordnen: PUK

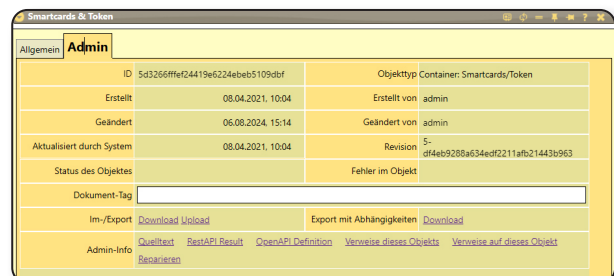


Die Ergebnisliste wird angezeigt. Mit Rechtsklick auf ein Feld im Tabellenkopf können Sie die Ergebnisse gruppieren, z.B. nach Smart-card-Objekt.

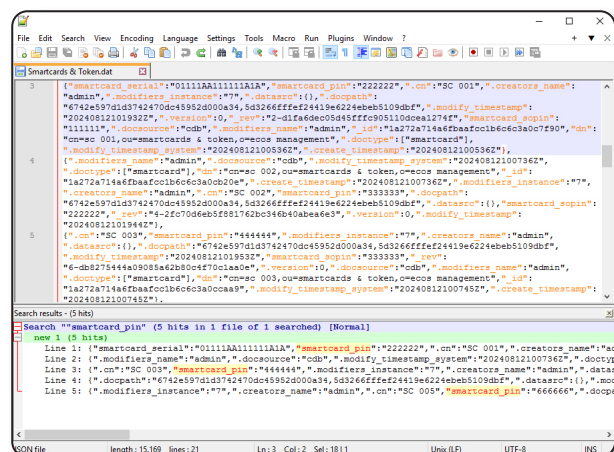


Gehen Sie zum **Container: Smartcards/Token:**

➡ **Im-/Export:** Laden Sie Im Feld [Download](#) die Exportdatei des Containers im JSON-Format herunter.



Sie finden die gewünschten Daten mit den Attributen `smartcard_serial`, `smartcard_pin` und `smartcard_sopin`.





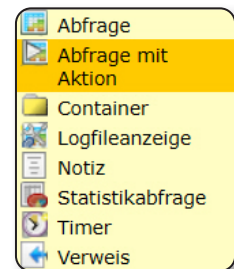
Smartcard-Zertifikate verlängern

Smartcard-Zertifikate werden über eine **Abfrage mit Aktion** verlängert und dann auf die Smartcards ausgerollt. Gehen Sie dazu wie folgt vor:

1 Einrichten der Abfrage und Verlängern der Zertifikate

Legen Sie an geeigneter Stelle über das Kontextmenü eine **Abfrage mit Aktion** an und geben Sie ihr einen aussagekräftigen Namen.

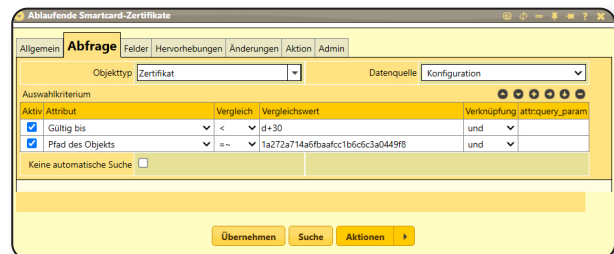
Nehmen Sie folgende Einstellungen vor:



Abfrage

➡ **Objekttyp:** Wählen Sie **Zertifikat**.

➡ **Auswahlkriterien:** Wählen Sie das Attribut **Gültig bis**, den Vergleichsoperator **kleiner als** (<) und geben Sie als Vergleichswert **d+30** an. Definieren Sie weitere Auswahlkriterien, um die Abfrageergebnisse weiter einzugrenzen, z.B. auf bestimmte Container.



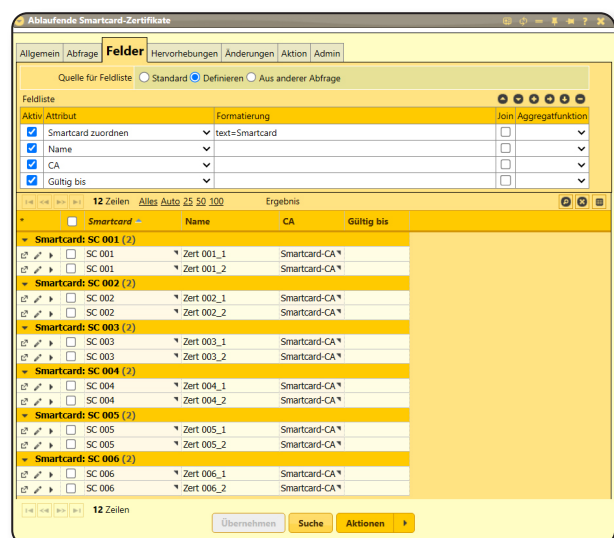
Aktivieren Sie für jedes anzuwendende Auswahlkriterium die Checkbox in der Spalte **Aktiv**.

Felder

➡ **Quelle für Feldliste:** Hier können Sie die Quelle für die Anzeige der Ergebnisliste anpassen. Sie können Felder definieren oder die Feldliste einer bereits bestehenden Abfrage übernehmen.

➡ **Feldliste:** Wählen Sie in der Spalte **Attribut** die Felder aus, die Sie zur Darstellung verwenden wollen.

Aktivieren Sie für jedes gewünschte Feld die Checkbox in der Spalte **Aktiv** und speichern Sie Ihre Einstellungen.



Mit Rechtsklick auf ein Feld im Tabellenkopf können Sie die Ergebnisse gruppieren, z.B. nach Smartcard-Objekt.

Änderungen

- ➔ **Quelle für Änderungen:** Wählen Sie die Option **Änderungen definieren**.

Aktion

- ➔ **Aktion:** Wählen Sie **Objekt ändern**.
- ➔ **Zielmenge:** Wählen Sie **Objekte aus Abfrage**.
- ➔ **Attribute die geändert werden sollen:** Wählen Sie als Attribut **Erstellung des Zertifikats** und als Wert **Verlängern**.



Aktivieren Sie die Checkbox in der Spalte **Aktiv**, um das Kriterium anzuwenden.

- ➔ **Jetzt ausführen:** Klicken Sie auf den Button, um die Aktion auszuführen. Alle Zertifikate, die die Kriterien der Abfrage erfüllen, werden nun verlängert.

2 Smartcards einlegen

Legen Sie die betreffenden Smartcards in das Kartenmagazin des Smartcard-Druckers ein.

3 Smartcard-Zertifikate ausrollen

Rollen Sie die verlängerten Zertifikate auf die Smartcards aus, wie im Abschnitt → *Smartcard-Batch-Enrollment durchführen* in den Schritten 2 und 3 beschrieben.