FP Digital
Business Solutions

FP AutoSigner

D-Trust Card 5.x Kartenunterstützung

Version 1.0 / 11.03.2024

Inhaltsverzeichnis

1 Inhalt

Dieses Dokument beschreibt die Neuerung der D-Trust Card 5.x Signatur- und Siegelkarten und deren Verwendung mit dem FP AutoSigner / FP AutoSigner DCE. Es wird auf Besonderheiten bei der Kombination von D-Trust Card 5.x und Kartenlesern eingegangen.

2 Neuerung bei den D-Trust Card 5.x Signatur- und Siegelkarten

Die D-Trust Card 5.x Signatur- und Siegelkarten verwenden ein neues System zur Authentifizierung (PACE – „Password Authenticated Connection Establishment“).

Es muss eine gesicherte (verschlüsselte) Verbindung zur Smartcard aufgebaut werden. Dazu wird im Fall der D-Trust Card 5.x die CAN (Card Access Number) der Karte benötig.

Die CAN steht direkt auf der Signaturkarte (siehe Abbildung 1).

Abbildung 1 – D-Trust Card 5.1 Signaturkarte mit CAN

Es muss also beim Starten der Signatursitzung erst die CAN eingegebene werden und dann die PIN des Signatur-Zertifikates. Die CAN kann von der Anwendung zwischengespeichert werden, sodass sie beim nächsten Starten der Signatursitzung nicht erneut eingegeben werden muss.

3 Besonderheit in Verbindung mit Kartenlesegeräten

Es gibt momentan 2 Kartenleser, die das PACE Protokoll unterstützen. Das sind der „REINER SCT cyberJack RFID komfort“ und „REINER SCT cyberJack RFID standard“. Die Firmware dieser beiden Kartenleser muss aktualisiert werden.

Dabei sollten mindesten folgende Firmware Versionen installiert sein:

- REINER SCT cyberJack RFID komfort: **Firmware Version 2.0.45**
- REINER SCT cyberJack RFID standard: **Firmware Version 1.2.70**

Bei Kombination dieser beiden Kartenleser und einer D-Trust Card 5.x Signatur- und Siegelkarte muss die PIN-Eingabe **zwingend** über das PIN Pad des Kartenlesers erfolgen. Es ist nicht erlaubt, die PIN aus der Software heraus an die Smartcard zu übermitteln.

Da die beiden Kartenleser das PACE Protokoll unterstützen, ist es auch möglich, die CAN über das PIN Pad des Kartenlesers einzugeben. Dann ist aber die Eingabe der CAN bei jedem Starten der Signatursitzung nötig.

Bei Verwendung eines anderen Kartenlesers (z.B.: SCM Microsystems Inc. SPRx32 USB Smart Card Reader) ist das Verhalten anderes. Da diese Kartenleser das PACE Protokoll nicht unterstützen, muss die Software (FP AutoSigner) diesen Part übernehmen. Dazu wir durch die Software die gesicherte (verschlüsselte) Kommunikation zur Smartcard aufgebaut. Dazu ist die Eingabe der CAN über die PC Tastatur nötig. Sobald die gesicherte Kommunikation zur Smartcard aufgebaut ist, darf kein unverschlüsselter Befehl oder Datensatz an die Smartcard übermittelt werden, da sonst die Smartcard die gesicherte Kommunikation von sich aus unterbricht.

Da Kartenleser das PACE Protokoll nicht unterstützt, kann er auch die PIN Eingabe, die über das PIN Pad des Kartenlesers erfolgt, nicht verschlüsselt an die Smartcard übermitteln. Darum ist es **zwingend** notwendig, die PIN durch die Software (FP AutoSigner) verschlüsselt an die Smartcard zu übermitteln. Die PIN Eingabe bei dieser Kombination vom Smartcard und Kartenleser muss **zwingend** von der Software übermittelt werden.

Kartenleser	Smacrtcard	PIN Eingabe
REINER SCT cyberJack RFID komfort REINER SCT cyberJack RFID standard	D-Trust Card 5.x	PIN Pad
	Keine D-Trust Card 5.x	PIN Pad oder Tastatur (Software)
Keiner der beiden oben genannten Kartenleser (z.B.: SCM Microsystems Inc. SPRx32 USB Smart Card Reader)	D-Trust Card 5.x	Tastatur (Software)
	keine D-Trust Card 5.x	PIN Pad (wenn vorhanden) oder Tastatur (Software)

Tabelle 1 – PIN Eingabe bei Kombination von Smartcard und Kartenleser

Die D-Trust Card 5.x haben eine kontaktbehaftete und eine kontaktlose (RFID) Schnittstelle. Es kann notwendig sein die kontaktlose Schnittstelle des Kartenlesers zu deaktivieren, da der FP AutoSigner DCE die kontaktbehaftete Schnittstelle verwendet. Die Vorgehensweise ist in Abbildung 2 beschrieben.

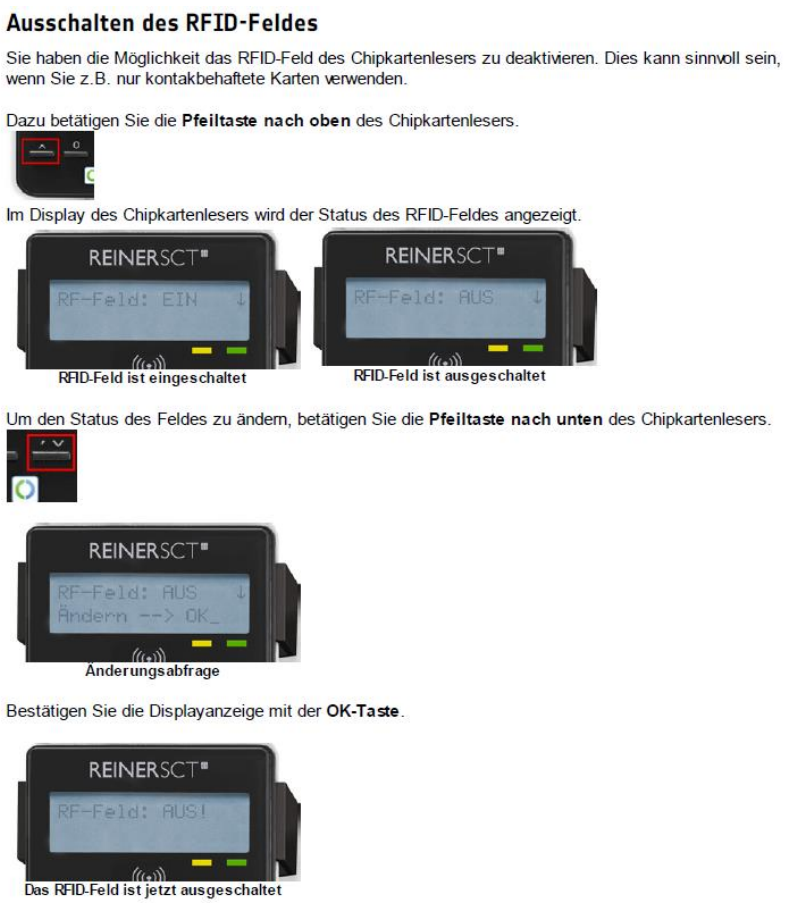

Abbildung 2 - Ausschalten des RFID Feldes des Kartenlesers

4 Verwendung der D-Trust Card 5.x Signatur- und Siegelkarten mit dem PF AutoSigner

Es wird beschrieben, wie sich der FP AutoSigner bei den der Kombination von D-Trust Card 5.x und Kartenlesern mit und ohne PACE Unterstützung verhält. Weiterhin wir die Konfiguration des FP AutoSigner DCE beschrieben, da bei einer Server Anwendung (Dienst) die CAN Eingabe nicht am Server erfolgen kann.

Die D-Trust Card 5.x Karten werden nur vom FP AutoSigner unterstützt, wenn das Mentana Smartcard-Modul verwendet wird (siehe Absatz 4.1.3)

4.1 FP AutoSigner GUI

Bei Verwendung der FP AutoSigner GUI als Signaturanwendung (z.B.: Scan-Arbeitsplatz) kann die Eingabe der Karten CAN beim Starten der Signatursitzung erfolgen. Dann ist es auch möglich die Signatur-PIN bei der Kombination von Karte und Kartenleser, die die Eingabe der Signatur-PIN über die Tastatur des PC erfordert, beim Starten der Signatursitzung über die Anwendung zu erfragen.
Bei Verwendung der FP AutoSigner DCE Variante (Dienst) lesen Sie bitte den Absatz 4.2.

4.1.1 Starten der Signatursitzung mit Kartenleser mit PACE Unterstützung

Bei Verwendung eines Kartenlesers mit PACE Unterstützung (siehe Tabelle 1) erfolgt die Eingabe der Signatur-PIN über das PIN Pad des Kartenlesers. Die Eingabe der Signatur-PIN über die Tastatur des PC ist dann nicht möglich.

Starten Sie die Signatursitzung auf die gewohnte Art und Weise (siehe Abbildung 3). Sie werden dann zur Auswahl des Signatur-Zertifikats aufgefordert (siehe Abbildung 4). Bei Verwendung der Autostart Funktion kann der Zertifikats-Auswahldialog entfallen (ja nach Konfiguration der Autostart Funktion). Haben Sie ein Zertifikats ausgewählt und die Signaturkarte benötig die CAN für den Aufbau einer gesicherten Kommunikation, dann werden Sie zur Eingabe der Karten CAN aufgefordert (siehe Abbildung 5). Sie können nun entscheiden, ob die CAN im CAN Cache der Anwendung gespeichert wird. Wenn Sie die CAN speichern, dann werden Sie beim Starten der nächsten Signatursitzung nicht mehr nach der CAN gefragt (siehe Abbildung 8). Die CAN wird zusammen mit der Seriennummer der Smartcard im CAN-Cache abgelegt und in der Konfiguration hinterlegt, sodass die CAN auch nach einen Programmstart wieder im CAN Cache zu finden ist (lesen Sie mehr dazu im Absatz 4.1.3).
Wenn Sie den Dialog abbrechen, dann erfolgt die CAN Eingabe über das PIN Pad des Kartenlesers. Dann kann die CAN aber nicht von der Anwendung zwischengespeichert werden.

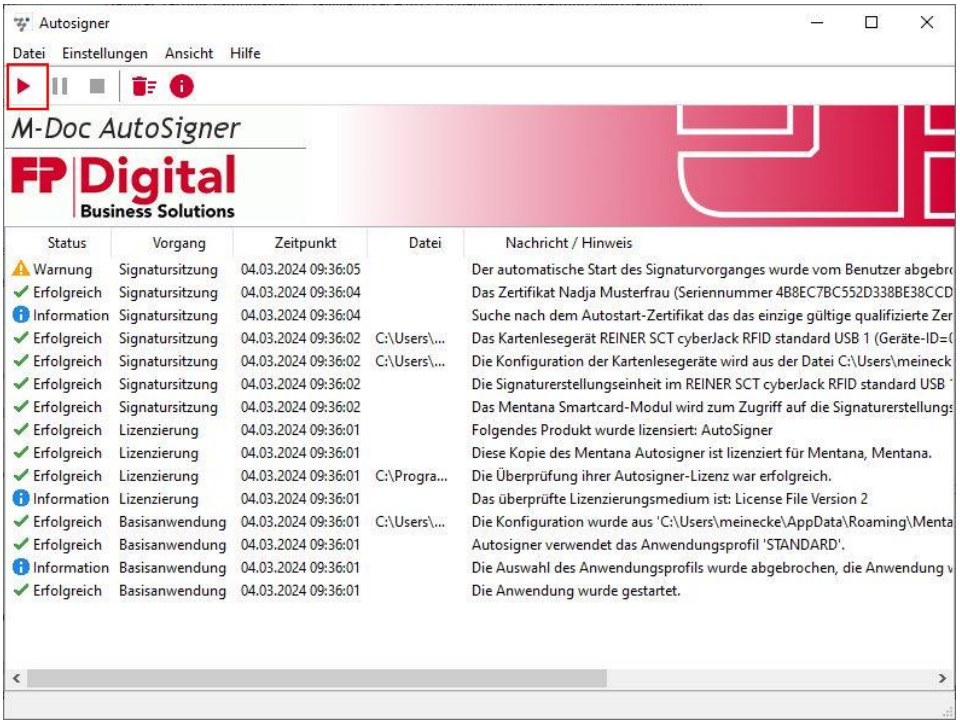

Abbildung 3 - Signatursitzung starten - Reader mit PACE

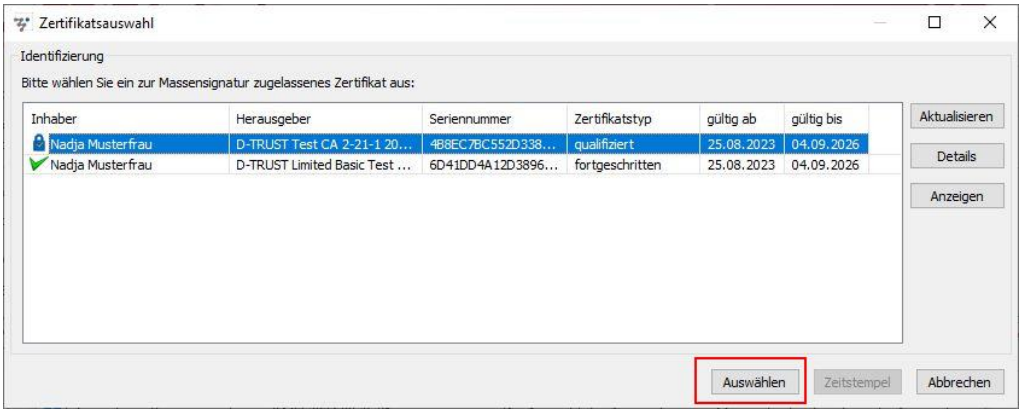

Abbildung 4 - Zertifikatsauswahl - Reader mit PACE

Abbildung 5 - CAN Eingabe - Reader mit PACE

In der Ereignisanzeige der FP AutoSigner GUI kann nachvollzogen werden, was bei der Kombination von D-Trust Card 5.x und Kartenleer mit PACE Unterstützung passiert ist (siehe Abbildung 6, Abbildung 7 und Abbildung 8). In Abbildung 6 und Abbildung 7 ist zu sehen, dass die CAN nicht im CAN Cache gefunden wurde und darum die CAN über die Tastatur eingegeben und im CAN Cache gespeichert wurde. Weiterhin ist zu sehen, das die Signatur-PIN über das PIN Pad des Kartenlesers (sichere Tastatur des Kartenlesers) eingegeben wurde.
In Abbildung 8 ist zu sehen, was passiert, wenn die CAN im CAN Cache gespeichert wird. Die Eingabe der CAN ist dann nicht mehr erforderlich.

Abbildung 6 - Log-Ausgaben - Reader mit PACE

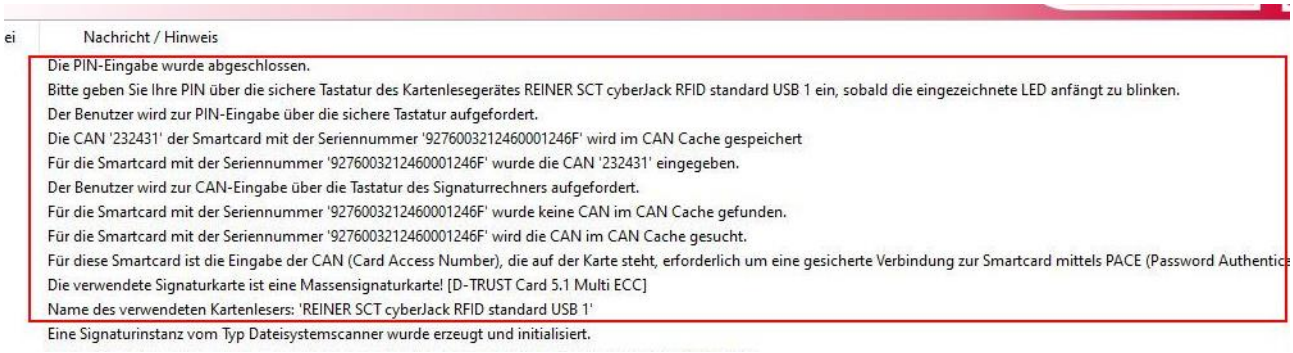

Abbildung 7 - Log-Ausgaben Zoom - Reader mit PACE

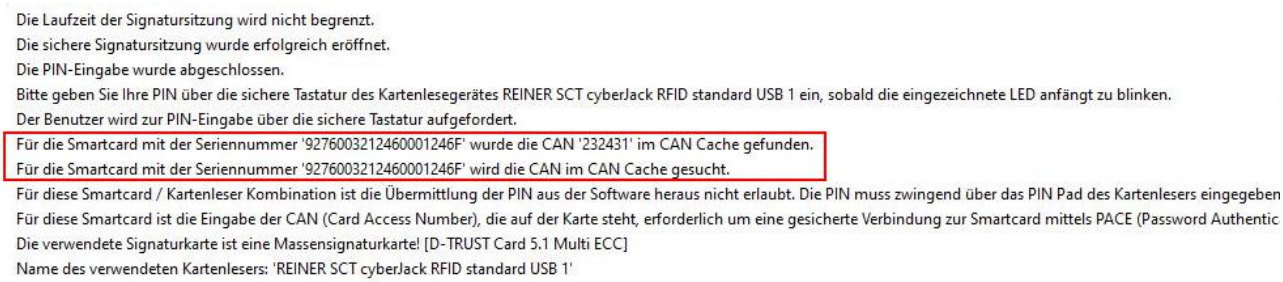

Abbildung 8 - Log-Ausgaben Zoom mit CAN im Cache - Reader mit PACE

4.1.2 Starten der Signatursitzung mit Kartenleser ohne PACE Unterstützung

Bei Verwendung eines Kartenlesers ohne PACE Unterstützung (siehe Tabelle 1) erfolgt die Eingabe der Signatur-PIN über die Tastatur des PC. Die Eingabe der Signatur-PIN über das PIN Pad des Kartenlesers dann nicht möglich.

Starten Sie die Signatursitzung auf die gewohnte Art und Weise (siehe Abbildung 9). Sie werden dann zur Auswahl des Signatur-Zertifikats aufgefordert (siehe Abbildung 10). Bei Verwendung der Autostart Funktion kann der Zertifikats-Auswahldialog entfallen (ja nach Konfiguration der Autostart Funktion). Haben Sie ein Zertifikats ausgewählt und die Signaturkarte benötig die CAN für den Aufbau einer gesicherten Kommunikation, dann werden Sie zur Eingabe der Karten CAN aufgefordert (siehe Abbildung 11). Sie können nun entscheiden, ob die CAN im CAN Cache der Anwendung gespeichert wird. Wenn Sie die CAN speichern, dann werden Sie beim Starten der nächsten Signatursitzung nicht mehr nach der CAN gefragt (siehe Abbildung 15). Die CAN wird zusammen mit der Seriennummer der Smartcard im CAN-Cache abgelegt und in der Konfiguration hinterlegt, sodass die CAN auch nach einen Programmstart wieder im CAN Cache zu finden ist (lesen Sie mehr dazu im Absatz 4.1.3). Nach Eingabe der CAN müssen Sie nun den Signatur-PIN über die Tastatur des PC eingeben (siehe Abbildung 12).
Wenn Sie einen der beiden Dialog (Abbildung 11 und Abbildung 12) abbrechen, dann wird die Signatursitzung nicht gestartet.

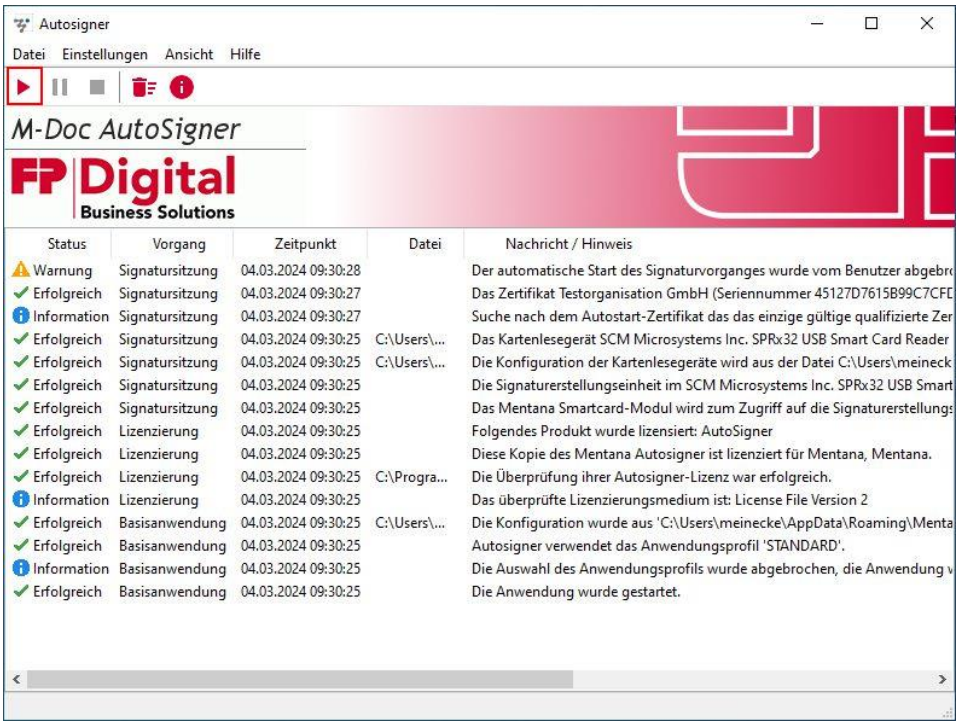

Abbildung 9 - Signatursitzung starten - Reader ohne PACE

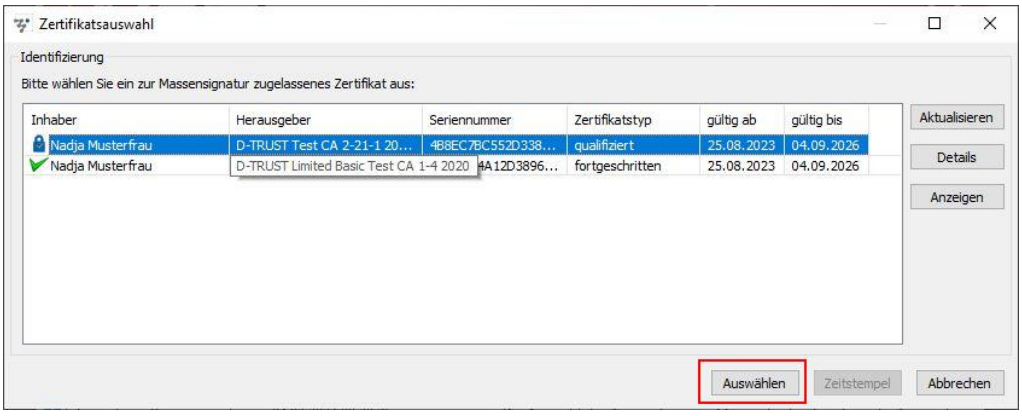

Abbildung 10 - Zertifikatsauswahl - Reader ohne PACE

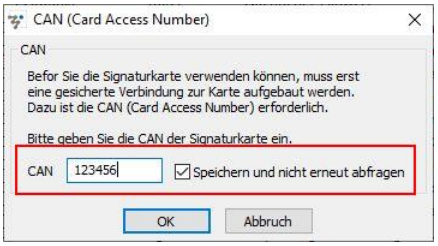

Abbildung 11 - CAN Eingabe - Reader ohne PACE

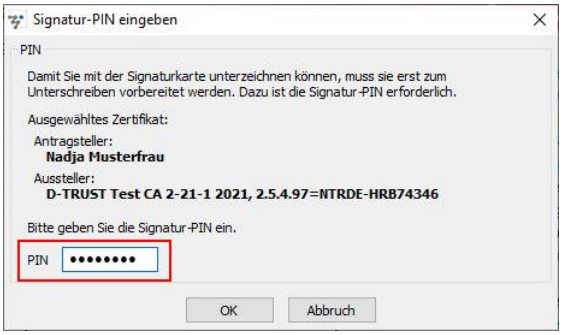

Abbildung 12 – Signatur-PIN Eingabe - Reader ohne PACE

In der Ereignisanzeige der FP AutoSigner GUI kann nachvollzogen werden, was bei der Kombination von D-Trust Card 5.x und Kartenleer ohne PACE Unterstützung passiert ist (siehe Abbildung 13, Abbildung 14 und Abbildung 15). In Abbildung 13 und Abbildung 14 ist zu sehen, dass die CAN nicht im CAN Cache gefunden wurde und darum die CAN über die Tastatur eingegeben und im CAN Cache gespeichert wurde. Weiterhin ist zu sehen, das die Signatur-PIN über die Tastatur des Signaturrechners eingegeben wurde.
In Abbildung 15 ist zu sehen, was passiert, wenn die CAN im CAN Cache gespeichert wird. Die Eingabe der CAN ist dann nicht mehr erforderlich.

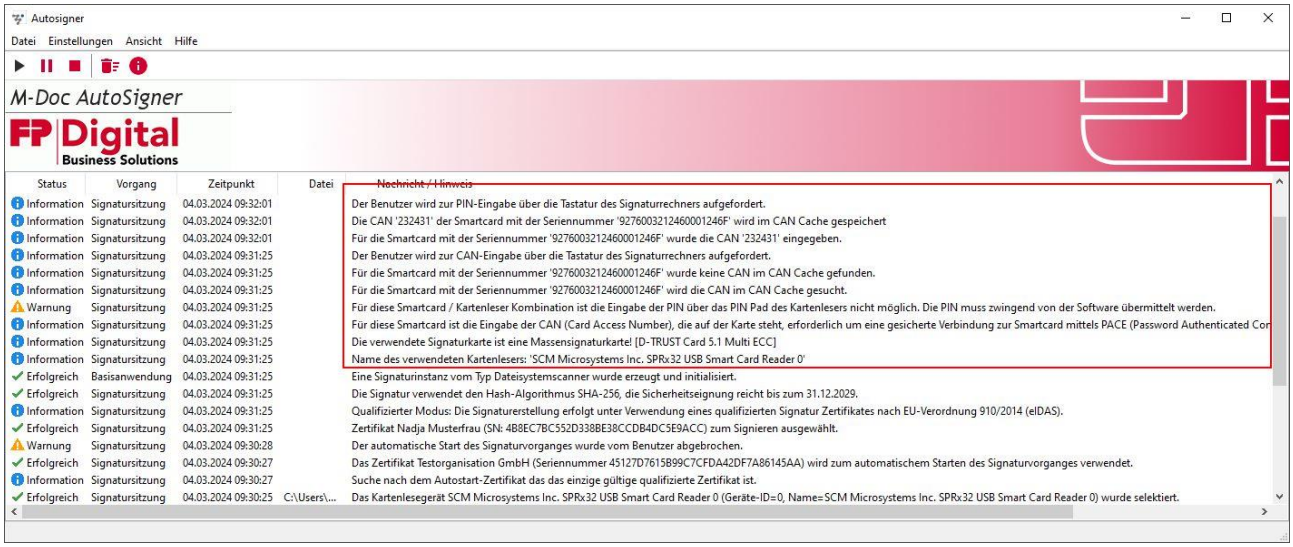

Abbildung 13 - Log-Ausgaben - Reader ohne PACE

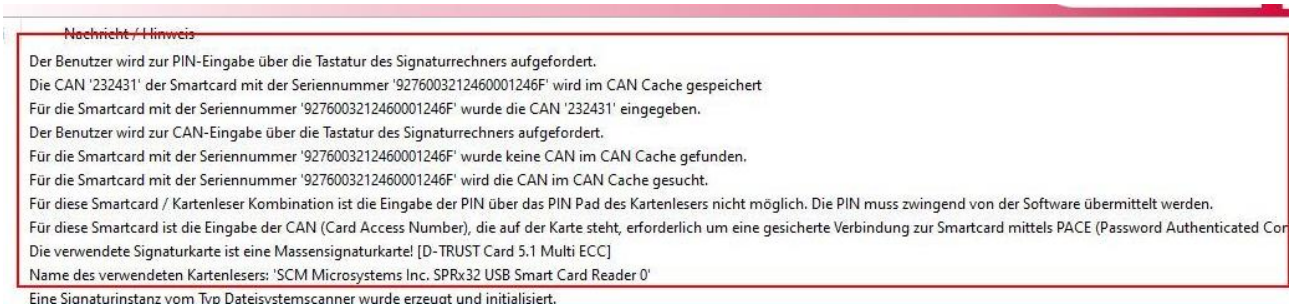

Abbildung 14 - Log-Ausgaben Zoom - Reader ohne PACE

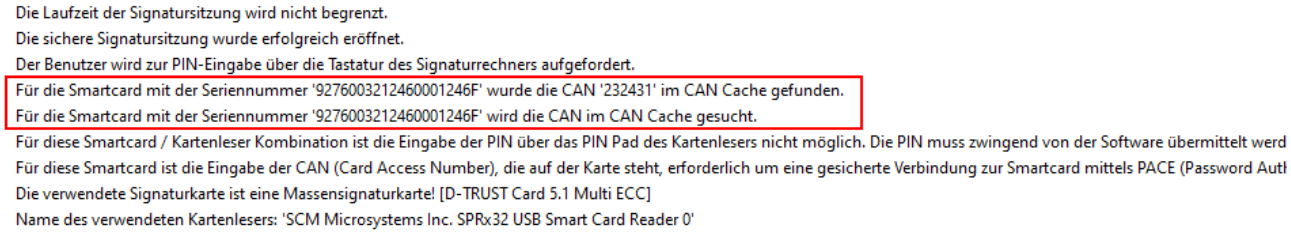

Abbildung 15 - Log-Ausgaben Zoom mit CAN im Cache - Reader ohne PACE

4.1.3 Konfiguration des Karten CAN Caches

Sie können die Karten CAN im CAN Cache des FP AutoSigner hinterlegen. Es gibt da 2 Möglichkeiten das zu tun. Die 1. Möglichkeit ist bei der Eingabe der CAN beim Starten der Signatursitzung das Speicher der CAN zu aktivieren (siehe Abbildung 5 und Abbildung 11). Die 2 Möglichkeit ist das Speicher der Karten CAN im CAN Cache mithilfe der Konfiguration des Mentana Smartcard-Moduls.
Dazu rufen Sie den Menüpunkt „Einstellungen.Smartcard-Ünterstützung“ in der FP AutoSigner GUI auf (siehe Abbildung 16).

Abbildung 16 - Einstellungen - Smartcard-Unterstützung

Wählen Sie als kryptographische Service Module das „Mentana Smartcard-Modul“ aus (siehe Abbildung 17). Nur dann werden die D-Trust Card 5.x Signaturkarten vom FP AutoSigner unterstützt.

Klicken Sie auf den Knopf „CAN Cache anzeigen“ (siehe Abbildung 17). Ihnen wird nun der CAN Cache angezeigt (siehe Abbildung 18). Befindet sich eine signaturkarte im Kartenleser, dann wird Ihnen der Kartenname und auch ob die CAN Eingabe erforderlich ist, angezeigt. Sollte die CAN der Karte noch nicht im CAN Cache hinterlegt sein (Die Seriennummer der Karte wurde nicht im CN Cache gefunden), dann können Sie durch einen klicken auf den Knopf „Karten CAN hinterlegen“ den CAN im CAN Cache ablegen. Sie werden zur Eingabe des CAN aufgefordert (siehe Abbildung 19). In Abbildung 20 ist dann die eben erfasste CAN im CAN Cache zu sehen. Sie können nun die CAN wieder aus dem CAN Cache entfernen oder den gesamten CAN Cache leeren.

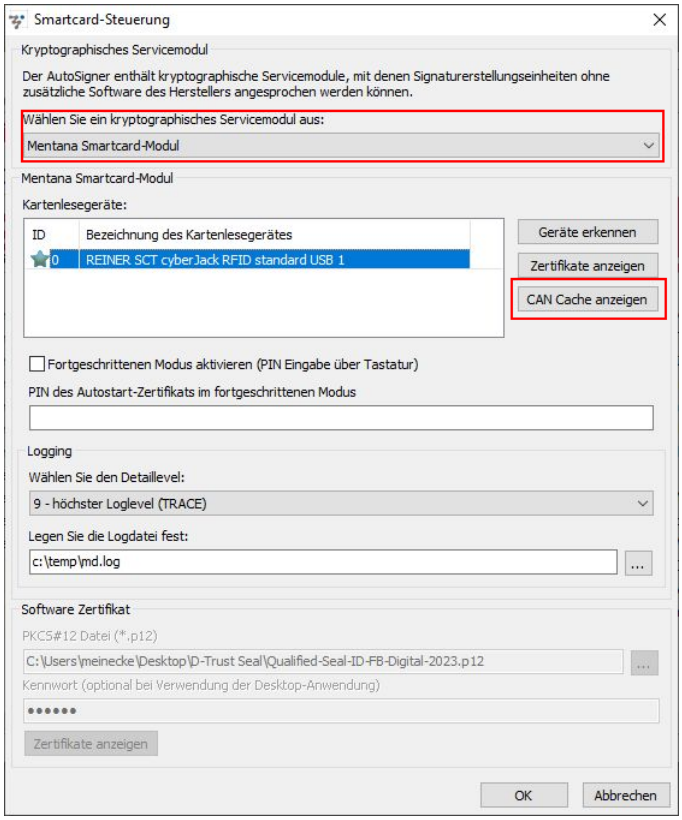

Abbildung 17 - Smartcard CAN Cache anzeigen

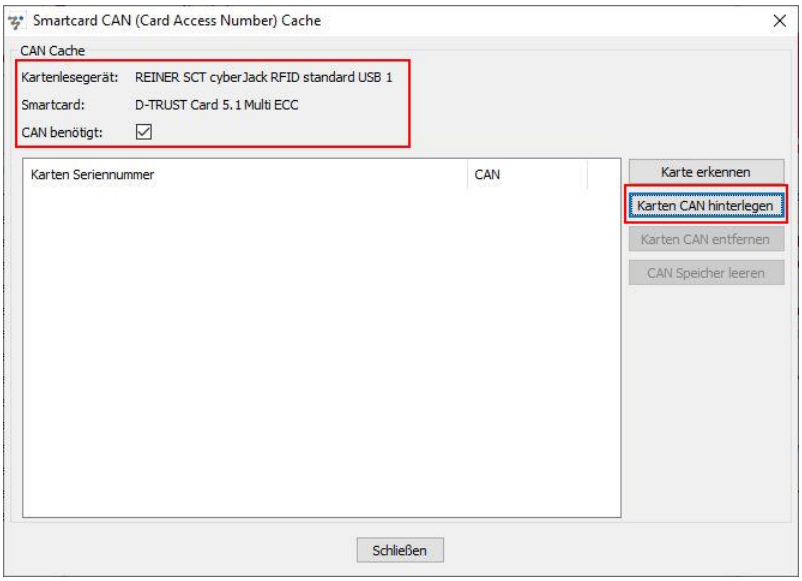

Abbildung 18 - Karten CAN im Cache hinterlegen

Abbildung 19 - Karten CAN Eingabe

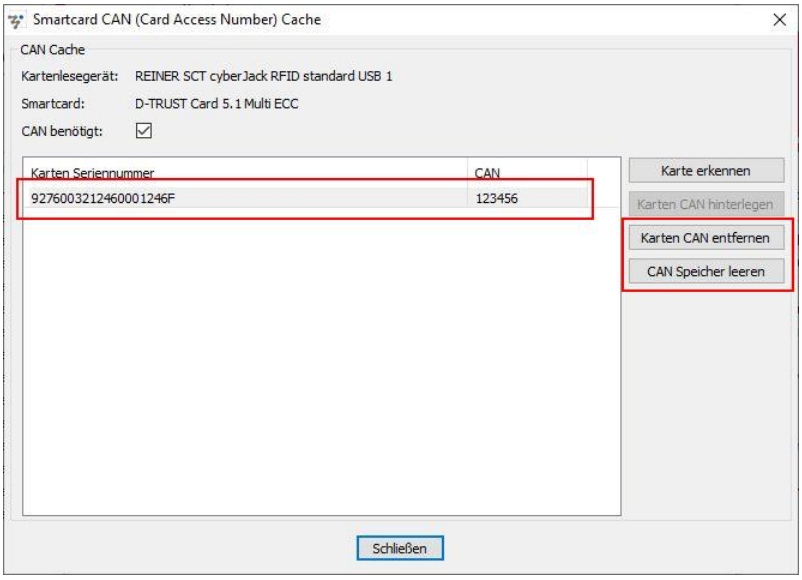

Abbildung 20 - Karten CAN im CAN Cache

Sie können eine andere Signaturkarte in den Kartenleser stecken, während Sie sich im CAN Cache Fenster befinden. Damit die neue Karte erkannt wird, müssen Sie auf den Knopf „Karte erkennen“ klicken (siehe Abbildung 21). Wenn Sie eine Signaturkarte ohne PACE Protokoll in den Kartenleser gesteckt haben, dann können Sie diese auch nicht in den CAN Cache übernehmen.

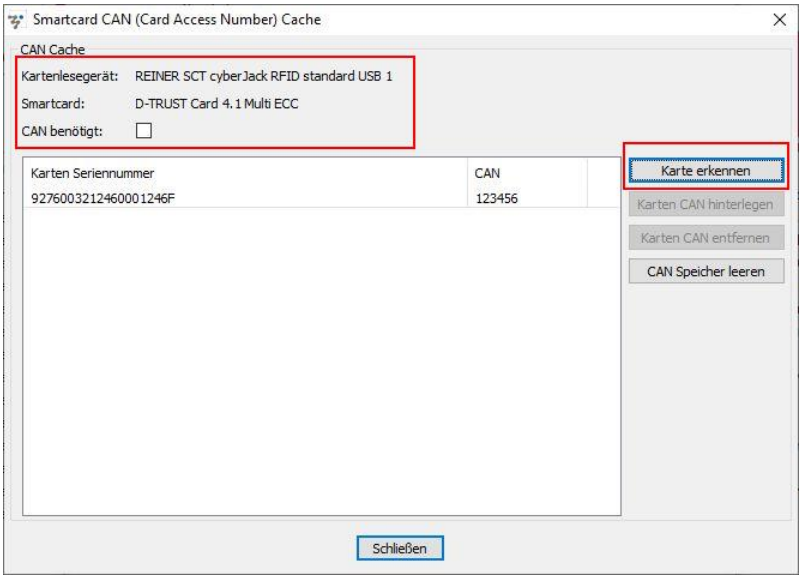

Abbildung 21 - neue Smartcard erkennen (CAN nicht benötigt)

Haben Sie eine D-Trust Card 5.x Signaturkarte in den Kartenleser gesteckt, deren Seriennummer noch nicht im CAN Cache auftaucht, dann können Sie hier gleich den CAN der Karte hinterlegen (siehe Abbildung 22 bis Abbildung 24).

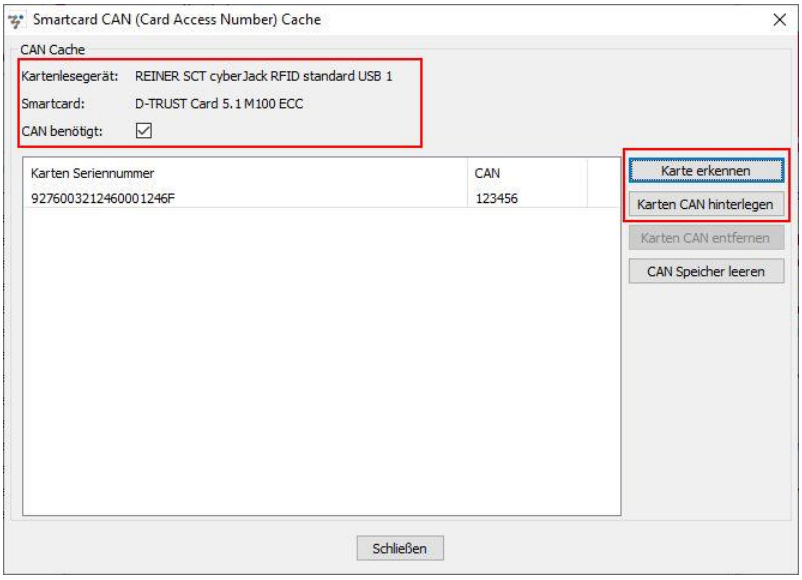

Abbildung 22 - neue Smartcard erkennen (CAN benötigt)

Abbildung 23 - neue Karten CAN hinterlegen

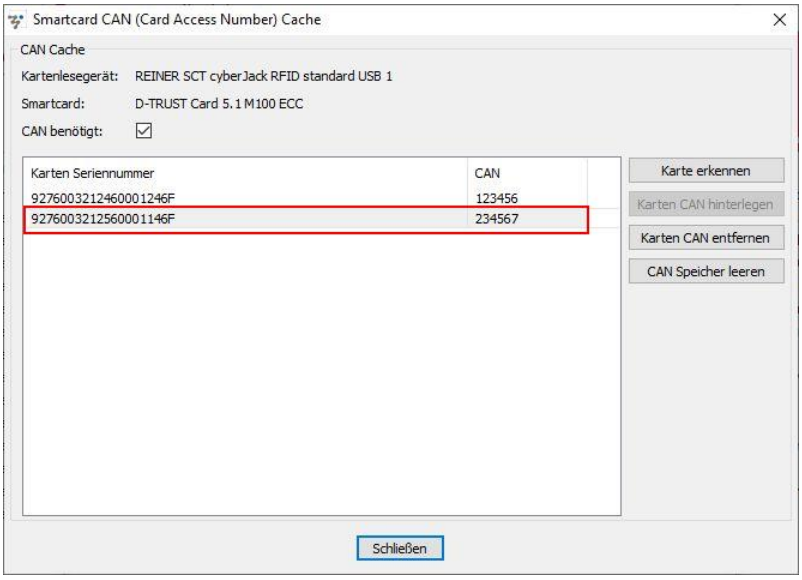

Abbildung 24 - neue Karten CAN im CAN Cache

Ist die Seriennummer der D-Trust Card 5.x Signaturkarte bereits im CAN Cache, dann wird die entsprechende Zeile im CAN Cache automatisch ausgewählt (siehe Abbildung 25). Diese Funktion können Sie verwenden, um festzustellen, ob eine Signaturkarte im CAN Cache hinterlegt ist.

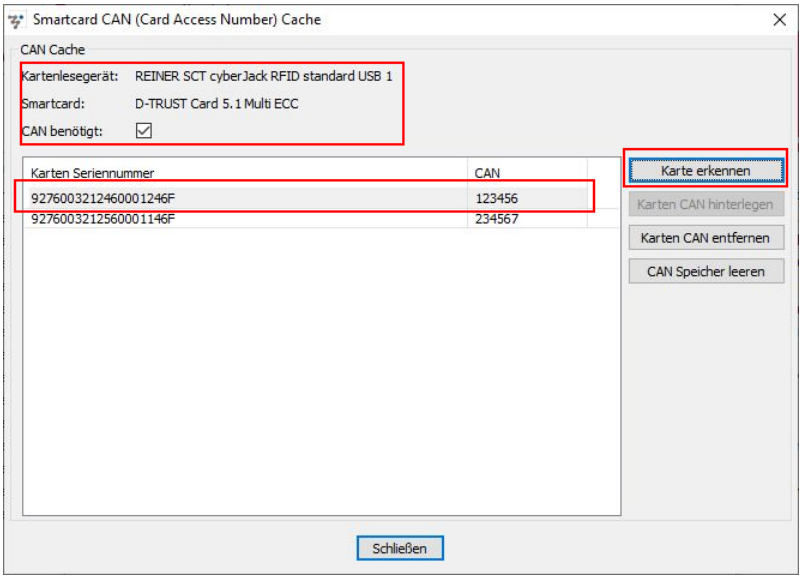

Abbildung 25 - Karten CAN im CAN Cache suchen

Sie können einen einzelnen Karten CAN nur löschen, wenn sich die betroffene Karte im Kartenleser befindet (siehe Abbildung 26). Ist das der fall, dann klicken Sie bitte auf „Karten CAN entfernen“ und bestätigen Sie die Frage aus Abbildung 27.
Wollen Sie alle gespeicherten Karten CANs löschen, dann verwenden Sie bitte den Knopf „CAN Speicher leeren“ und bestätigen die Frage aus Abbildung 29

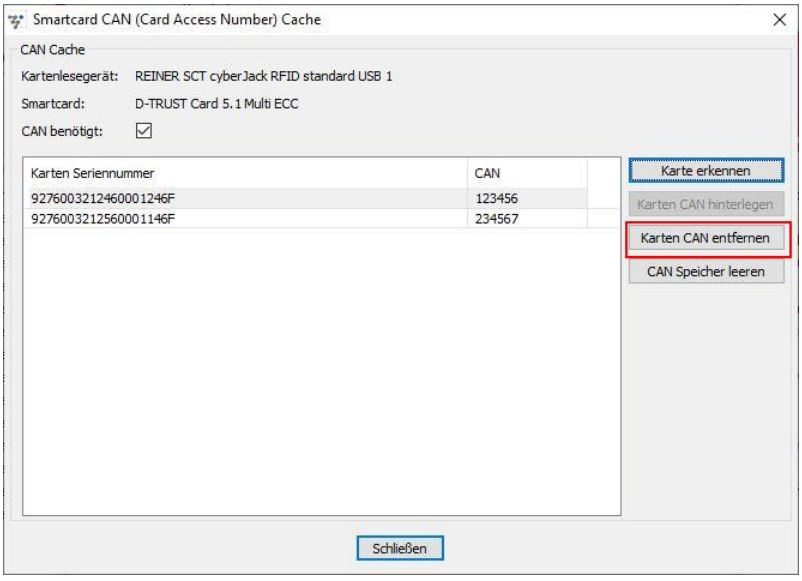

Abbildung 26 - Karten CAN aus CAN Cache entfernen

Abbildung 27 - CAN entfernen - Bestätigung

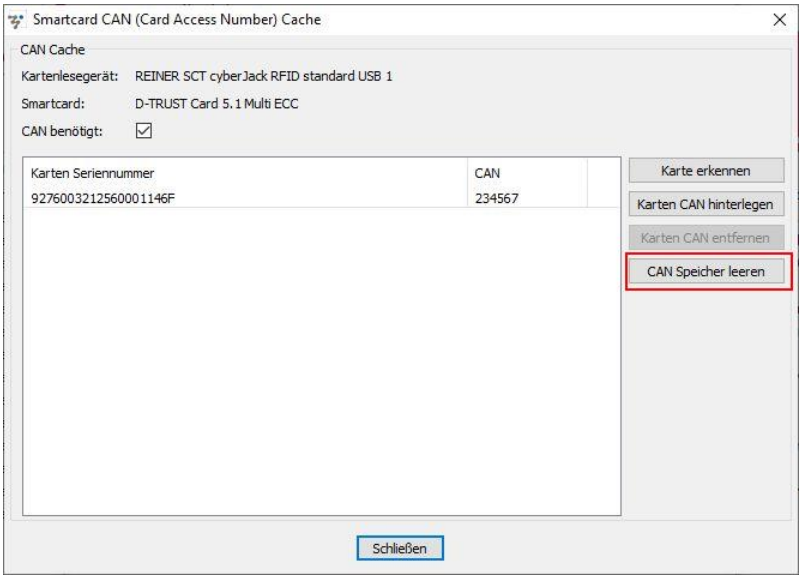

Abbildung 28 - CAN Cache leeren

Abbildung 29 - CAN Cache leeren - Bestätigung

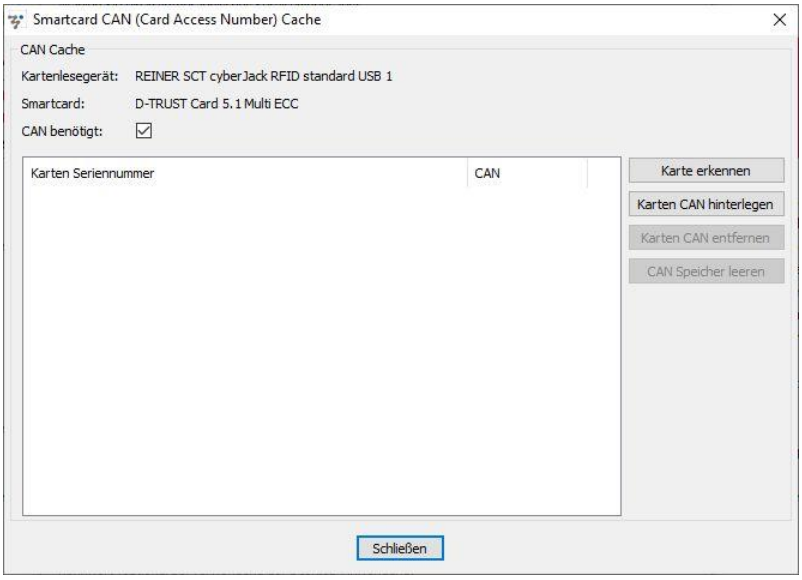

Abbildung 30 - geleerter CAN Cache

Der CAN Cache wird in der Konfiguration des FP AutoSigners in der Unter-Sektion „pacepincache“ des Sektion „smartcardsupport“ abgespeichert (siehe Abbildung 31).

config.xml

```
<!-- Smartcard support -->
<smartcardsupport>
    <!-- Smartcard reader configuration -->
    <reader>
        <!-- Smartcard reader ID -->
        <id>0</id>
        <!-- Smartcard reader name -->
        <name>SCM Microsystems Inc. SPRx32 USB Smart Card Reader 0</name>
        <!-- Smartcard reader slot -->
        <slot>0</slot>
        <!-- Smartcard reader certificate -->
        <cert>0</cert>
        <!-- Smartcard reader advanced pin -->
        <advancedpin type="appkey"/>
        <!-- Smartcard reader advanced pin restart count -->
        <restart>0</restart>
        <!-- Smartcard module logfile -->
        <logfile>c:\temp\md.log</logfile>
        <!-- Smartcard module loglevel: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 (0 -&gt; no logging, 9 -&gt; detailed logging -->
        <logdetail>9</logdetail>
    </reader>
    <!-- PIN cache for smartcards with PACE support -->
    <pacepincache>
        <!-- Save PACE PIN to configuration: false, true -->
        <savepin>true</savepin>
        <!-- PACE PIN cache item -->
        <pacepincacheitem>
            <!-- Smartcard serial number -->
            <cardserialnum>9276003212460001246F</cardserialnum>
            <!-- Smartcard PACE PIN -->
            <pacepin type="appkey">00E600E200F300B600170082</pacepin>
        </pacepincacheitem>
        <!-- PACE PIN cache item -->
        <pacepincacheitem>
            <!-- Smartcard serial number -->
            <cardserialnum>9276003212560001153F</cardserialnum>
            <!-- Smartcard PACE PIN -->
            <pacepin type="appkey">00EC00E000F000B50012008B</pacepin>
        </pacepincacheitem>
        <!-- PACE PIN cache item -->
        <pacepincacheitem>
            <!-- Smartcard serial number -->
            <cardserialnum>9276003212560001146F</cardserialnum>
            <!-- Smartcard PACE PIN -->
            <pacepin type="appkey">00E500E100F400B20013008B</pacepin>
        </pacepincacheitem>
        <!-- PACE PIN cache item -->
        <pacepincacheitem>
            <!-- Smartcard serial number -->
            <cardserialnum>9276003213160000173F</cardserialnum>
            <!-- Smartcard PACE PIN -->
            <pacepin type="appkey">00E500E100F900B200110084</pacepin>
        </pacepincacheitem>
    </pacepincache>
</smartcardsupport>
```

Abbildung 31 - CAN Cache Sektion in der Konfigurationsdatei (config.xml)

4.2 FP AutoSigner DCE

Da der FP AutoSigner DCE ein Dienst ist, kann die CAN Eingabe nicht Beim Starten der Signatursitzung erfolgen. Darum ist es erforderlich die CAN der Signaturkarte im Vorfeld im CAN Cache zu hinterlegen.

Dazu lesen Sie bitte den Absatz 4.1.3.

Haben Sie mehrere FP AutoSigner DCE Instanzen auf einem Server, dann können Sie die CANs aller Smartcard in der Konfiguration jeder Instanz speichern. Konfigurieren Sie einfach den CAN Cache einer Instanz mit der FP AutoSigner GUI und kopieren dann die Sektion „pacepincache“ aus der Konfiguration dieser Instanz an die entsprechende Stelle der Konfigurationen der anderen Instanzen (siehe Abbildung 31).

Sie können natürlich jede einzelne Instanz mithilfe der FP AutoSigner GUI konfigurieren und jeweils nur die CAN der betroffenen Karte hinterlegen.

5 Abbildungsverzeichnis

6 Tabellenverzeichnis