

# FP OfficeSigner

## D-Trust Card 5.x Kartenunterstützung

Version 1.0 / 11.03.2024



## Inhaltsverzeichnis

<b>1 Inhalt</b> .....	<b>3</b>
<b>2 Neuerung bei den D-Trust Card 5.x Signatur- und Siegelkarten</b> .....	<b>3</b>
<b>3 Besonderheit in Verbindung mit Kartenlesegeräten</b> .....	<b>3</b>
<b>4 Verwendung der D-Trust Card 5.x Signatur- und Siegelkarten mit dem FP OfficeSigner</b> .....	<b>5</b>
4.1 FP OfficeSigner .....	5
4.1.1 Starten der Signatursitzung mit Kartenleser mit PACE Unterstützung .....	5
4.1.2 Starten der Signatursitzung mit Kartenleser ohne PACE Unterstützung .....	6
4.1.3 Konfiguration des Karten CAN Caches .....	7
<b>5 Abbildungsverzeichnis</b> .....	<b>10</b>
<b>6 Tabellenverzeichnis</b> .....	<b>10</b>

## 1 Inhalt

Dieses Dokument beschreibt die Neuerung der D-Trust Card 5.x Signatur- und Siegelkarten und deren Verwendung mit dem FP OfficeSigner. 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 benötigt.

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 eingegeben 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 OfficeSigner) diesen Part übernehmen. Dazu wird 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 OfficeSigner) verschlüsselt an die Smartcard zu übermitteln. Die PIN Eingabe bei dieser Kombination vom Smartcard und Kartenleser muss **zwingend** von der Software übermitteln 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 OfficeSigner die kontaktbehaftete Schnittstelle verwendet. Die Vorgehensweise ist in Abbildung 2 beschrieben.**

#### Ausschalten des RFID-Feldes

Sie haben die Möglichkeit das RFID-Feld des Chipkartenlesers zu deaktivieren. Dies kann sinnvoll sein, wenn Sie z.B. nur kontaktbehaftete Karten verwenden.

Dazu betätigen Sie die **Pfeiltaste nach oben** des Chipkartenlesers.



Im Display des Chipkartenlesers wird der Status des RFID-Feldes angezeigt.



Um den Status des Feldes zu ändern, betätigen Sie die **Pfeiltaste nach unten** des Chipkartenlesers.



Bestätigen Sie die Displayanzeige mit der **OK-Taste**.



*Abbildung 2 - Ausschalten des RFID Feldes des Kartenlesers*

## 4 Verwendung der D-Trust Card 5.x Signatur- und Siegelkarten mit dem FP OfficeSigner

Es wird beschrieben, wie sich der FP OfficeSigner bei den der Kombination von D-Trust Card 5.x und Kartenlesern mit und ohne PACE Unterstützung verhält.

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

### 4.1 FP OfficeSigner

Bei Verwendung des FP OfficeSigners als Signaturanwendung 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.

#### 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). Haben Sie ein Zertifikats ausgewählt und die Signaturkarte benötigt die CAN für den Aufbau einer gesicherten Kommunikation, dann werden Sie zur Eingabe der Karten CAN aufgefordert (siehe Abbildung 4). 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. 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.

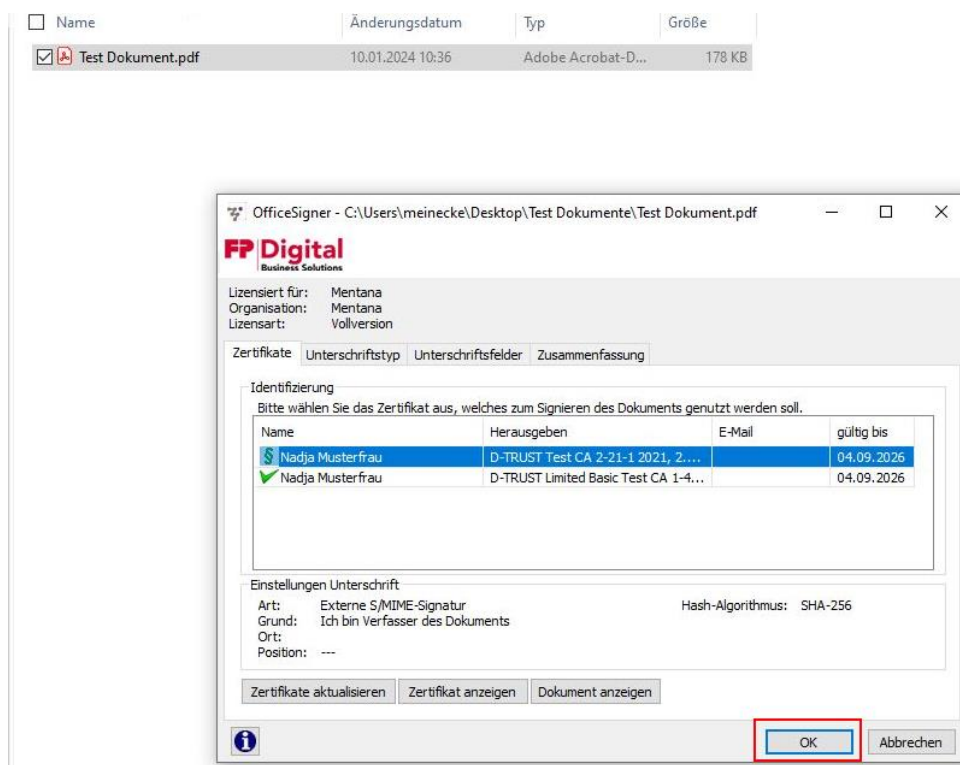


Abbildung 3 - Signatursitzung starten - Reader mit PACE



Abbildung 4 - CAN Eingabe - 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 5). Haben Sie ein Zertifikats ausgewählt und die Signaturkarte benötigt die CAN für den Aufbau einer gesicherten Kommunikation, dann werden Sie zur Eingabe der Karten CAN aufgefordert (siehe Abbildung 6). 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. Die CAN wird zusammen mit der Seriennummer der Smartcard im CAN-Cache abgelegt und in der Konfiguration hinterlegt, sodass die CAN auch nach einem 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 7).

Wenn Sie einen der beiden Dialog (Abbildung 6 und Abbildung 7) abbrechen, dann wird die Signatursitzung nicht gestartet.

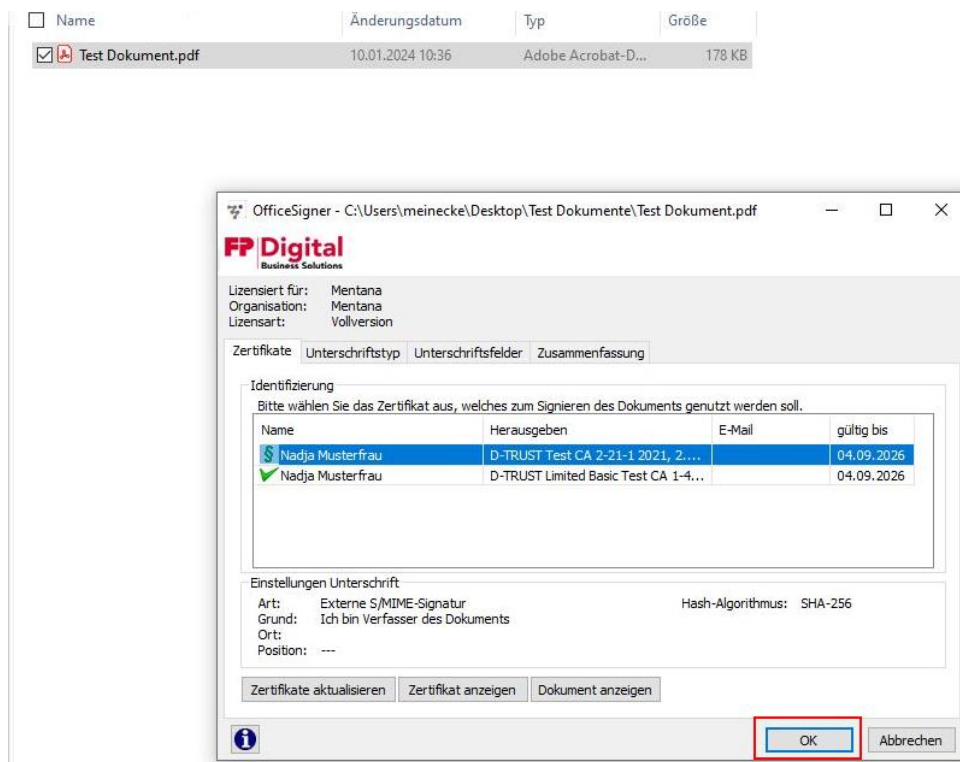


Abbildung 5 - Signatursitzung starten - Reader ohne PACE

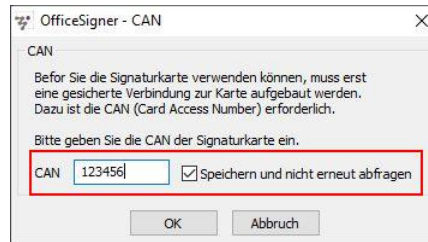


Abbildung 6 - CAN Eingabe - Reader ohne PACE



Abbildung 7 – Signatur-PIN Eingabe - Reader ohne PACE

### 4.1.3 Konfiguration des Karten CAN Caches

Sie können die Karten CAN im CAN Cache des FP OfficeSigner 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 4 und Abbildung 6). Die 2. Möglichkeit ist das Speicher der Karten CAN im CAN Cache mithilfe der Konfiguration des Mentana Smartcard-Moduls. Dazu rufen Sie die „Einstellungen“ des FP OfficeSigners auf und wechseln Sie auf das Registerblatt „Smartcard Steuerung“.

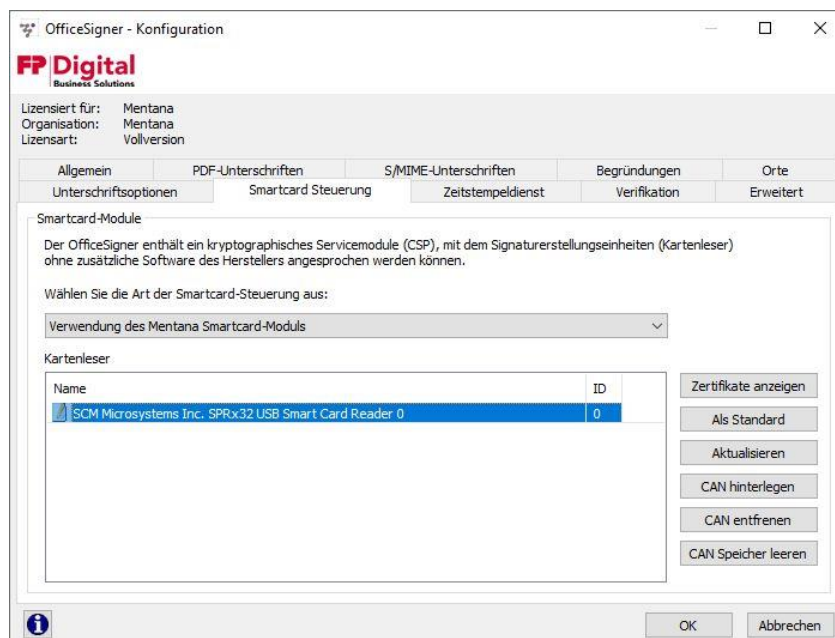


Abbildung 8 - Einstellungen – Smartcard Steuerung

**Wählen Sie als Smartcard-Module „Verwendung des Mentana Smartcard-Moduls“ aus (siehe Fehler! V erweisquelle konnte nicht gefunden werden.). Nur dann werden die D-Trust Card 5.x Signaturkarten vom FP OfficeSigner unterstützt.**

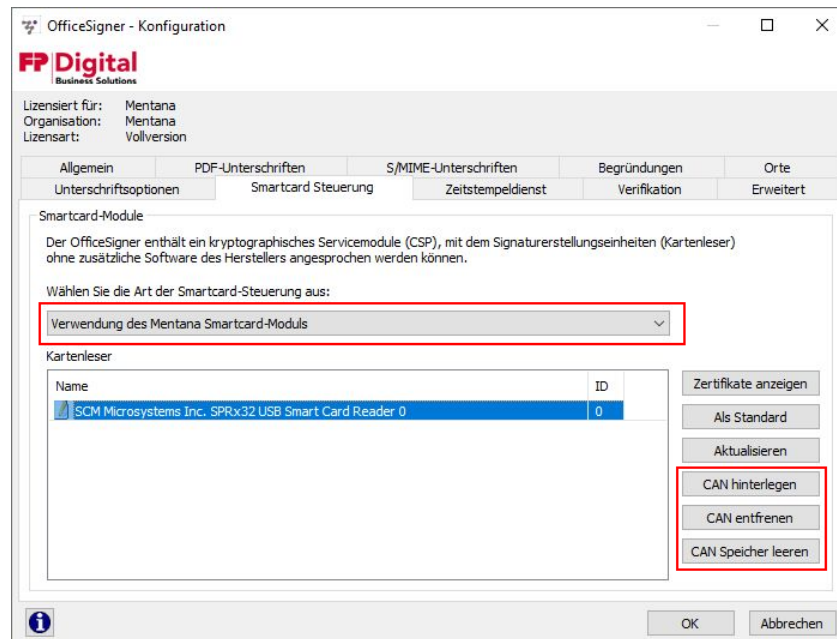


Abbildung 9 - CAN Cache

Befindest sich eine Signaturkarte im Kartenleser, dann können Sie durch Klick auf die Knop „CAN hinterlegen“, die Karten CAN im CAN Cache des FP OfficeSigners speichern. Benötigt die Karte die CAN Eingabe dann werden Sie zur Eingabe der CAN aufgefordert (siehe Abbildung 10). Ist das nicht der Fall, dann bekommen Sie eine entsprechende Meldung (siehe Abbildung 11).



Abbildung 10 - CAN Eingabe in der Konfiguration

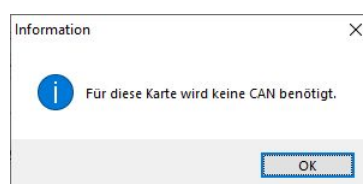


Abbildung 11 - keine CAN benötigt

Sie können die CAN der Karte im Kartenleser auch aus dem CAN Cache entfernen. Klicken Sie dazu auf den Knopf „CAN entfernen“. Ist zu der Karte ein CAN im Cache hinterlegt, wird noch eine Bestätigungsmeldung angezeigt (siehe Abbildung 12). Wurde zu der Karte eine CAN im Cache gefunden, erhalten Sie eine Meldung (siehe Abbildung 13).



Abbildung 12 - Karten CAN aus Cache entfernen

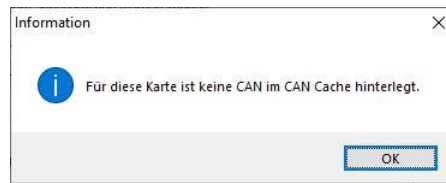


Abbildung 13 - Karten CAN nicht im Cache

Wollen Sie die gesamten CAN Cache leeren, dann klicken Sie auf den Knopf „CAN Speicher leeren“ und bestätigen Sie die darauf folgende Anfrage mit „Ja“ (siehe Abbildung 14).



Abbildung 14 - CAN Cache leeren

Der CAN Cache wird in der Konfiguration des FP OfficeSigners in der Unter-Sektion „pacepincache“ abgespeichert (siehe Abbildung 15).

```

87      <checktype>never</checktype>
88      <checkmethod>single</checkmethod>
89    </documentcheck>
90    <fileextensions>
91      <default-pkcs7-ext>p7s</default-pkcs7-ext>
92      <default-timestamp-ext>tsr</default-timestamp-ext>
93    </fileextensions>
94    <logging>
95      <logger>
96        <type>none</type>
97      </logger>
98    </logging>
99    <!-- PIN cache for smartcards with PACE support -->
100   <pacepincache>
101     <!-- Save PACE PIN to configuration: false, true -->
102     <savepin>true</savepin>
103     <!-- PACE PIN cache item -->
104     <pacepincacheitem>
105       <!-- Smartcard serial number -->
106       <cardserialnum>9276003212460001246F</cardserialnum>
107       <!-- Smartcard PACE PIN -->
108       <pacepin type="appkey">00E600E200F300B600170082</pacepin>
109     </pacepincacheitem>
110   </pacepincache>
111 </configuration>
112

```

Abbildung 15 - CAN Cache Sektion in der Konfigurationsdatei (configwx.xml)

## 5 Abbildungsverzeichnis

Abbildung 1 – D-Trust Card 5.1 Signaturkarte mit CAN.....	3
Abbildung 2 - Ausschalten des RFID Feldes des Kartenlesers .....	4
Abbildung 3 - Signatursitzung starten - Reader mit PACE.....	5
Abbildung 4 - CAN Eingabe - Reader mit PACE.....	6
Abbildung 5 - Signatursitzung starten - Reader ohne PACE .....	6
Abbildung 6 - CAN Eingabe - Reader ohne PACE .....	7
Abbildung 7 – Signatur-PIN Eingabe - Reader ohne PACE.....	7
Abbildung 8 - Einstellungen – Smartcard Steuerung .....	7
Abbildung 9 - CAN Cache .....	8
Abbildung 10 - CAN Eingabe in der Konfiguration .....	8
Abbildung 11 - keine CAN benötigt .....	8
Abbildung 12 - Karten CAN aus Cache entfernen .....	8
Abbildung 13 - Karten CAN nicht im Cache .....	9
Abbildung 14 - CAN Cache leeren .....	9
Abbildung 15 - CAN Cache Sektion in der Konfigurationsdatei (configwx.xml) .....	9

## 6 Tabellenverzeichnis

Tabelle 1 – PIN Eingabe bei Kombination von Smartcard und Kartenleser .....	4
-----------------------------------------------------------------------------	---