FP Digital
Business Solutions

FP Zertifikatsmanager

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 Zertifikatsmanagers. 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 Zertifikatsmanager) 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 Zertifikatsmanager) 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 Zertifikatsmanager die kontaktbehaftete Schnittstelle verwendet. Die Vorgehensweise ist in Abbildung 2 beschrieben.

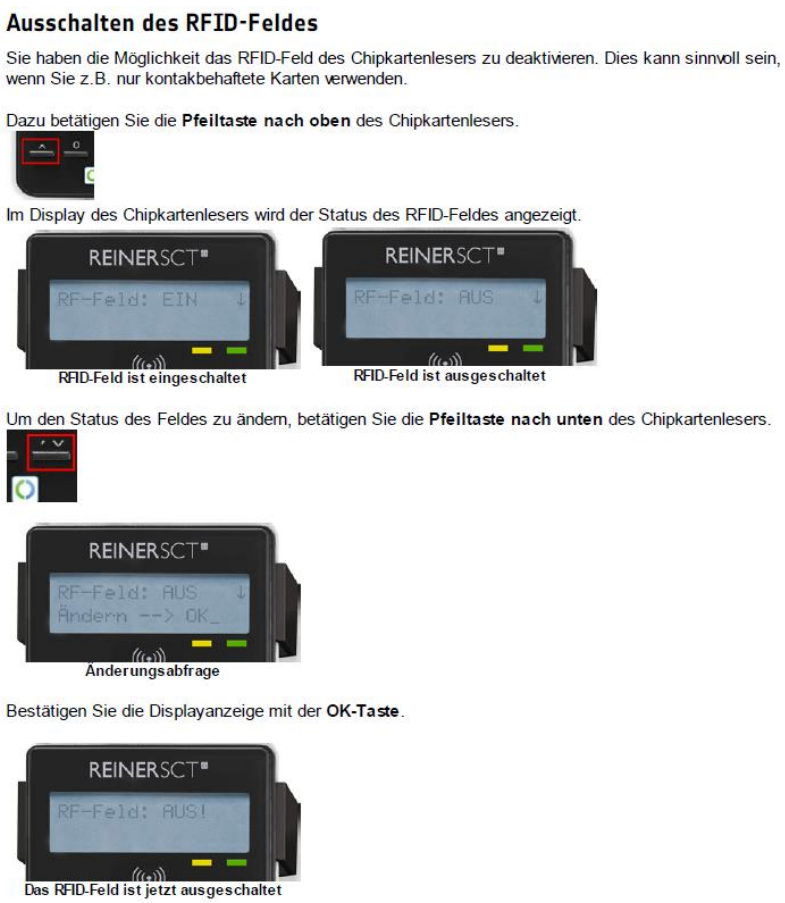

Abbildung 2 - Ausschalten des RFID Feldes des Kartenlesers

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

Es wird beschrieben, wie sich der FP Zertifikatsmanager 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 Zertifikatsmanager unterstützt.

4.1 FP Zertifikatsmanager

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. Haben Sie ein Zertifikat ausgewählt und die Signaturkarte benötig die CAN für den Aufbau einer gesicherten Kommunikation, dann werden Sie zur Eingabe der Karten CAN aufgefordert. Sie können die CAN auch speichern (siehe Abbildung 3 und Abbildung 4). 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.

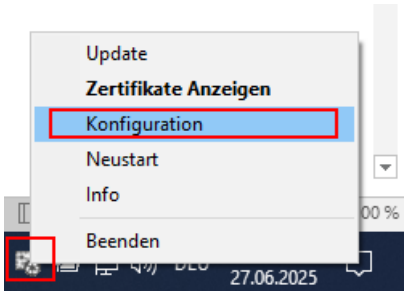

Abbildung 3 - Konfiguration der Zertifikatsmanagers

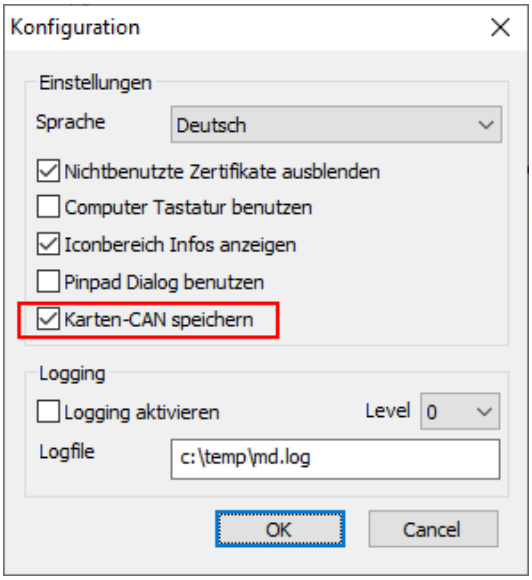

Abbildung 4 - Karten CAN speichern

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. Haben Sie ein Zertifikat ausgewählt und die Signaturkarte benötig die CAN für den Aufbau einer gesicherten Kommunikation, dann werden Sie zur Eingabe der Karten CAN aufgefordert. Sie können die CAN speichern (siehe Abbildung 3 und Abbildung 4). 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. Nach Eingabe der CAN müssen Sie nun den Signatur-PIN über die Tastatur des PC eingeben.

5 Abbildungsverzeichnis

6 Tabellenverzeichnis