

Anwenderdokumentation PersoSim

V1.4

Die nachfolgende Anwenderdokumentation soll dem Anwender bei der Installation und den ersten Schritten im Umgang mit PersoSim helfen.

Inhaltsverzeichnis

1	Komponenten & Installation	1
1.1	Simulator	2
1.2	Treiber	2
1.3	Editor	3
2	Benutzung des PersoSim Simulators	4
2.1	Benutzeroberfläche	4
2.2	Laden von Personalisierungen	5
2.3	Wechseln des verwendeten Lesertyps	5
2.4	Logging und Konsole	7
2.5	Smartphone als Kartenleser	7
3	Erstellen eigener Profile mit PersoSim Editor	10

1 Komponenten & Installation

Grundvoraussetzung für den Betrieb von PersoSim ist eine Java Laufzeitumgebung ab Version 1.8.

1.1 Simulator

Die Hauptanwendung PersoSim enthält den Karten-Simulator und gleichzeitig den virtuellen Kartenleser der vom Treiber (siehe unten) an das jeweilige Betriebssystem angebunden wird. Die Anwendung erfordert keine Installation im klassischen Sinne. Sie ist nach dem Entpacken der Zip-Datei bzw. des Tar-Balls sofort lauffähig.

Der Start erfolgt betriebssystemabhängig über die `PersoSim.exe` unter Windows bzw. `PersoSim` unter Linux oder MacOS. Nach dem Start erscheint die jeweilige GUI wie in Abbildung 1. Je nach Anwendungsfall (z.B. bei einer Anbindung per RemoteIFD) kann der Simulator jetzt unmittelbar genutzt werden.

1.2 Treiber

Um den virtuellen Kartenleser (und damit die simulierten Ausweise) regulär nutzen zu können stehen betriebssystemspezifische Treiber zur Verfügung. Diese binden PersoSim als Kartenleser im jeweiligen PCSC-Stack ein und erlauben damit den Zugriff aus jeder kompatiblen Anwendung.

Das Vorgehen für die Installation des Treibers ist betriebssystemabhängig. Im Folgenden wird die Installation für Windows, Linux und MacOS beschrieben.

Windows Für die Installation von PersoSim wird lediglich als Betriebssystem Windows 7 oder neuer vorausgesetzt.

Der Treiber erkennt selbständig um welche Version von Windows (Version 7, 8, 8.1 oder 10) es sich handelt und erkennt auch automatisch die Architektur (32 oder 64 Bit). Zur Installation des Treibers muss lediglich den Anweisungen des Installationsprogramms Folge geleistet werden. Im Gegensatz zu vorherigen Version des Treibers müssen keine Testzertifikate mehr separat installiert werden, allerdings kann es unter Windows 10 notwendig sein die Treibersignaturprüfung für die Installation zu deaktivieren. Nach erfolgreicher Installation erscheint der virtuelle Kartenleser ähnlich wie physische Kartenleser als "PersoSim Virtual Reader" im Gerätemanager unter Smartcard-Leser und kann dann genutzt werden.

Linux Die folgende Anleitung zur Installation des Treibers unter Linux wurde für Ubuntu 12.04 LTS erstellt und dort getestet. Sie ist aber grundsätzlich auch auf anderen Linux-Derivaten durchführbar.

Zusätzlich zur Ubuntu 12.04 LTS Standardinstallation werden die folgenden Pakete benötigt:

- `pcscd`
- `pcsc-tools`
- `libpcsclite-dev`

Diese können per `sudo apt-get install pcscd pcsc-tools libpcsclite-dev` installiert werden.

Nach dem Entpacken des Archivs liegt der Treiber im Quellcode vor und muss zunächst kompiliert werden. Dies geschieht mit Hilfe des Aufrufs `make` im Verzeichnis des entpackten Archivs. Die anschließende Installation erfolgt mit dem Aufruf `sudo make install`. Der Treiber wird beim nächsten Start des PCSC-Daemon (`sudo service pcscd restart`) automatisch geladen.

MacOS Um die notwendige Toolchain auf MacOS bereitzustellen muss Xcode installiert werden. Zusätzlich müssen die "command line developer tools" installiert werden. Das genaue Vorgehen hängt von der genutzten MacOS- und Xcode-Version ab. Für aktuelle Versionen sollte der Konsolenbefehl `xcode-select --install` zu einem Dialog für die Installation der Kommandozeilenwerkzeuge führen.

Nach dem Entpacken des Archivs liegt der Treiber im Quellcode vor und muss zunächst kompiliert werden. Dies geschieht mit Hilfe des Aufrufs `make` im Verzeichnis des entpackten Archivs. Die anschließende Installation erfolgt mit dem Aufruf `sudo make install`. Nach einem Neustart wird der virtuelle Treiber von MacOS erkannt und kann mit PersoSim genutzt werden.

1.3 Editor

Der PersoSim Editor erlaubt das Modifizieren bestehender Profile oder auch die Erzeugung völlig neuer Personalisierungen für den Simulator. Damit können Karten mit beliebigen Inhalten simuliert werden.

Analog des Simulators erfordert auch der PersoSim Editor keine Installation im klassischen Sinne. Installation und Start funktionieren identisch durch Entpacken des Archivs ausführen der enthaltenen Executable. Nach dem Start erscheint die GUI wie in Abbildung 6 in Kapitel 3.

2 Benutzung des PersoSim Simulators

2.1 Benutzeroberfläche

PersoSim stellt im Vordergrund die Benutzeroberfläche des eingebundenen virtuellen Kartenlesers dar (siehe Abbildung 1). Alle weiteren Funktionen sind über Tabs und Menüs erreichbar und werden im folgenden erläutert.

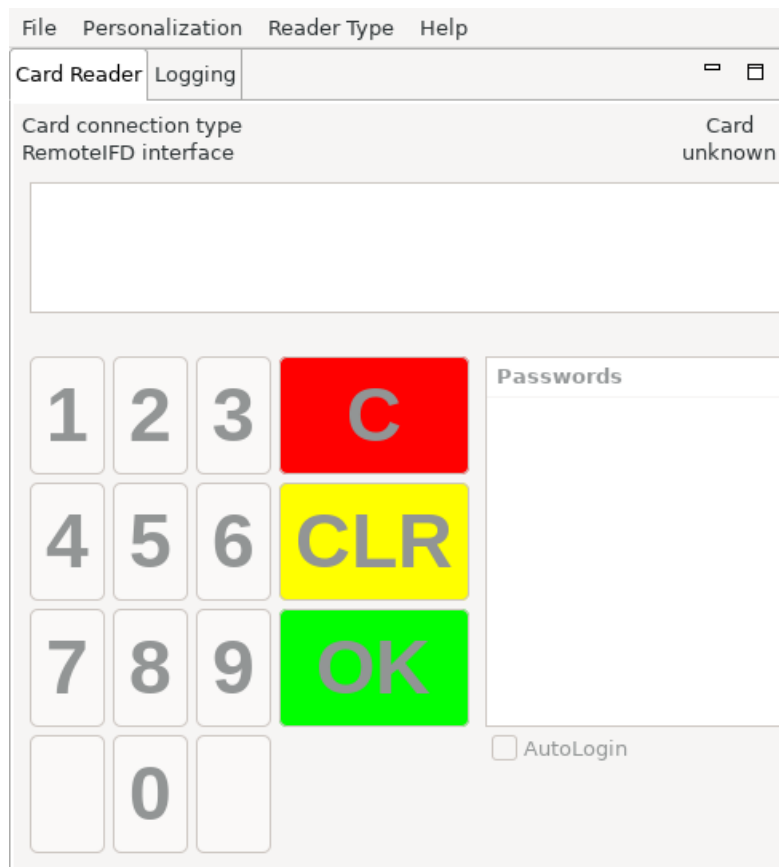


Abbildung 1: PersoSim Hauptfenster

2.2 Laden von Personalisierungen

Personalisierungen innerhalb von PersoSim lassen sich sowohl über die Kommandozeile als auch mit Hilfe von Menüpunkten über die grafische Benutzeroberfläche laden. Wird keine Personalisierung explizit ausgewählt so wird standardmäßig Profil 1 verwendet. Nach dem Laden einer Personalisierung ist diese sofort aktiviert. Dies entspricht dem Auflegen eines Ausweises auf einen Hardware-Kartenleser. Es stehen 16 vorgefertigte Standardprofile zur Auswahl. Hierbei handelt es sich um 11 Personalausweise sowie 5 Unionsbürgerkarten. Eine aktuelle Übersicht der verschiedenen Personalisierungen und der darin verwendeten Daten findet sich auf der PersoSim-Website im Bereich Downloads.

Laden von Personalisierungen über das Menü Die wohl komfortabelste Möglichkeit Personalisierungen zu laden ist das Anwendungsmenü. Der Menüpunkte "Personalization" bietet hierfür folgende Unterpunkte:

- **Select Perso from file** Öffnet einen Datei-Dialog und erlaubt die Auswahl einer beliebigen Personalisierung aus einer vorliegenden XML-Datei.
- **Select predefined Perso template** Erlaubt die direkte Auswahl der oben beschriebenen Standardprofile.
- **Remove card** entfernt die simulierte Karte von Leser.

Laden von Personalisierungen über die Kommandozeile Auch auf der Kommandozeile (siehe Abschnitt 2.4) lassen sich Personalisierungen einfach laden. Hierfür wird das Kommando `loadperso<Dateiname>` benutzt. Alternativ kann statt des Dateinamens auch eine Zahl angegeben werden, die als Abkürzung zu einem der angebotenen Standardprofile dient.

2.3 Wechseln des verwendeten Lesertyps

Der virtuelle Kartenleser, der im Rahmen von PersoSim genutzt werden kann, kann so konfiguriert werden, dass er sowohl einen Basis- als auch ein Standardleser simuliert. Die Auswahl des Lesertyps erfolgt über den Menüpunkt "Reader Type".

Basisleser besitzen in der Regel weder Display noch Tastatur. Entsprechend verfügt auch der PersoSim-Basisleser lediglich über die beiden Infelder im oberen Bereich, die anzeigen ob eine Karte simuliert wird und über welche Verbindung die Simulation bereitgestellt wird. (vgl. Abbildung 2)

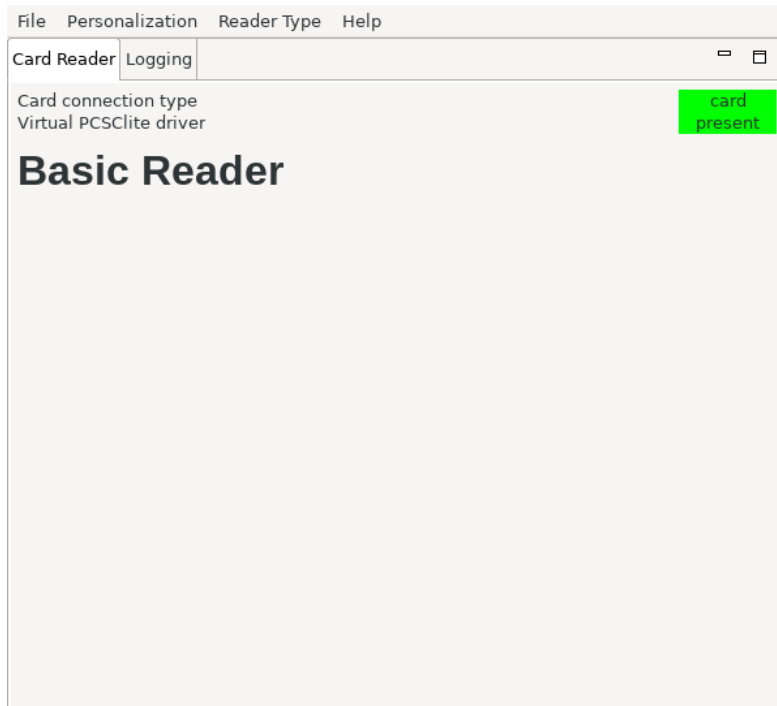


Abbildung 2: PersoSim als Basisleser

Standardleser verfügen über ein Display und eine Tastatur, über die z.B. Informationen gemäß BSI TR-03119 angezeigt und Passwörter eingegeben werden können. Entsprechend verfügt der PersoSim-Standardleser über ein Display in dem Anweisungen und die eingegebene Pin angezeigt werden, sowie ein Tastenfeld zur Eingabe der Pin. Unterhalb des Displays wird der zur Authentisierung übertragene CHAT angezeigt (wenn man mit der Maus darüber verweilt werden die einzelnen Bits menschenlesbar aufgeschlüsselt).

Zusätzlich erlaubt es der PersoSim-Standardleser im rechten Bereich häufig genutzte Passwörter zu speichern und per Doppelklick direkt zu nutzen. Gerade bei der Durchführung von mehreren Tests kann die Eingabe eines Passworts (PIN, CAN oder PUK) relativ zeitaufwendig werden. Aus diesem Grund gibt es die Möglichkeit, ein automatisches Logon in PersoSim zu aktivieren. Abbildung 3 zeigt diese Funktion exemplarisch: hier sind als Passwörter sowohl '123456' (PersoSim default PIN) als auch '500540' (CAN für default PersoSim-Profil) hinterlegt. In diesem Fall ist die '123456' ausgewählt und wird automatisch als PIN eingegeben.

Beim Programmstart wird automatisch der Standardleser aktiviert.

Es gilt zu beachten, dass die Eingabeelemente auf dem Pinpad des Standardlesers nur dann und solange aktiviert sind wie sie im Rahmen einer Kommunikation mit dem simulierten Ausweis benötigt werden. D.h. zu Programmstart sind diese zunächst ohne

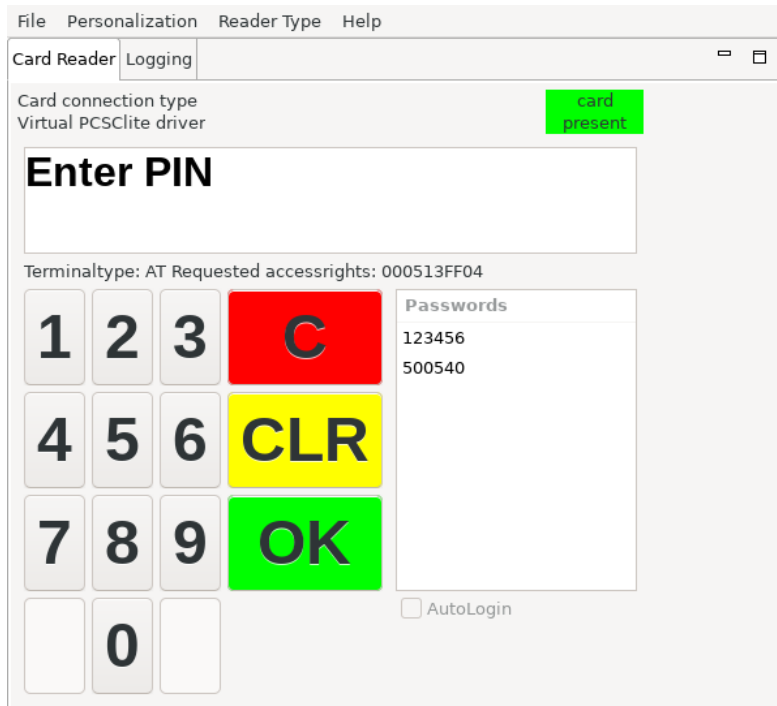


Abbildung 3: PersoSim als Standardleser

Funktion. Sobald eine Eingabe erforderlich ist, erscheint ein entsprechender Hinweis auf dem Display.

2.4 Logging und Konsole

Über den Tab "Logging" erreicht man die Konsole in der Log-Informationen über sämtliche Kommandos an den Simulator sowie dessen Rückmeldungen protokolliert werden (siehe Abbildung 4). Hier können über das Kontextmenü sowohl Einstellung zum Logging-Verhalten vorgenommen als auch der Log-Inhalt in eine Datei geschrieben werden.

Außerdem bietet diese Konsole die Möglichkeit den Simulator direkt mit Kommandos in der Kommandozeile zu steuern. Eine Liste der verfügbaren Kommandos lässt sich mit dem Kommando `help` aufrufen.

2.5 Smartphone als Kartenleser

Die BSI TR-03112-6 sieht die Funktion "Remote IFD" vor, auch bekannt unter dem Namen "Smartphone als Kartenleser". Mit dieser Funktion lässt sich ein NFC-fähiges

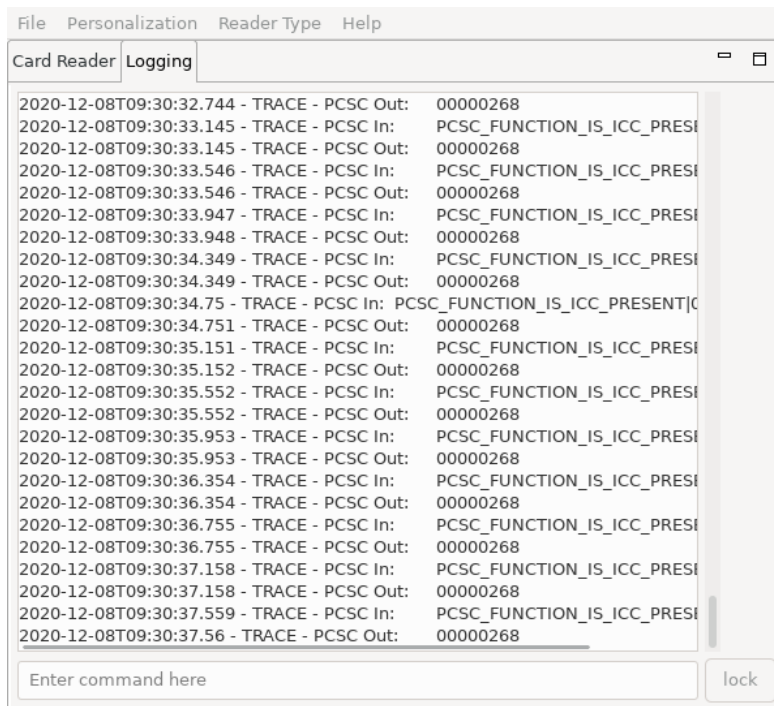


Abbildung 4: PersoSim Konsole

Smartphone als Kartenleser im Kontext des Personalausweises nutzen. Auch PersoSim unterstützt diese Funktion sowohl in der Desktop-Anwendung als auch in der Android-App und kann so von einem eID-Client per Netzwerk angesprochen werden.

Um diese Funktion zu nutzen muss zunächst die Anbindung im Menüpunkt "Reader Type" → "UseRemote IFD" entsprechend umgestellt werden. Der aktive Verbindungstyp wird stets im oberen Bereich der Kartenleser-Oberfläche (oberhalb des PinPads) angezeigt.

Damit ein eID-Client mit PersoSim per Remote IFD kommunizieren kann, müssen die beiden Geräte/Programme miteinander gekoppelt werden. Der entsprechende Dialog ist im Menü "ReaderType" → "Configure RemoteIFD" erreichbar (Abbildung 5).

Im oberen Bereich werden bereits gekoppelte Anwendungen angezeigt. Bei Bedarf können diese hier per Kontextmenü entfernt werden.

Im mittleren Bereich kann der Kopplungsvorgang durch Klick auf "Start pairing" initiiert werden. Dies unterbricht vorhandene Verbindungen für die Dauer des Koppelvorgangs und zeigt den notwendigen Kopplungscode an. Mithilfe dieses Kopplungscode kann sich ein entsprechender eID-Client dann mit PersoSim verbinden (siehe hierzu auch die Dokumentation des eID-Clients). Nach einer erfolgreichen Kopplung erfolgt die gegenseitige



Abbildung 5: Konfiguration Remote IFD

Authentisierung zertifikatsbasiert, sodass keine weitere Kopplung mehr notwendig ist.

Zu guter Letzt lässt sich im unteren Bereich der Name dieser PersoSim-Instanz konfigurieren. Dieser wird von eID-Clients zur Kopplung und zum Wiederverbinden genutzt, damit der Benutzer die entsprechende Gegenstelle auswählen kann.

3 Erstellen eigener Profile mit PersoSim Editor

Zusätzlich zu den mitgelieferten Profilen innerhalb von PersoSim besteht die Möglichkeit, eigene Profile zu erstellen. Profile bestehen aus einem XML-File, das alle relevanten Informationen für die Simulation enthält. Damit der Anwender aber nicht im XML-File editieren muss, gibt es ein zusätzliches Werkzeug zum einfachen Editieren der Profile. Abbildung 6 zeigt die Oberfläche des Editors, der genauso wie der Simulator auf der Website zum Download bereitsteht.

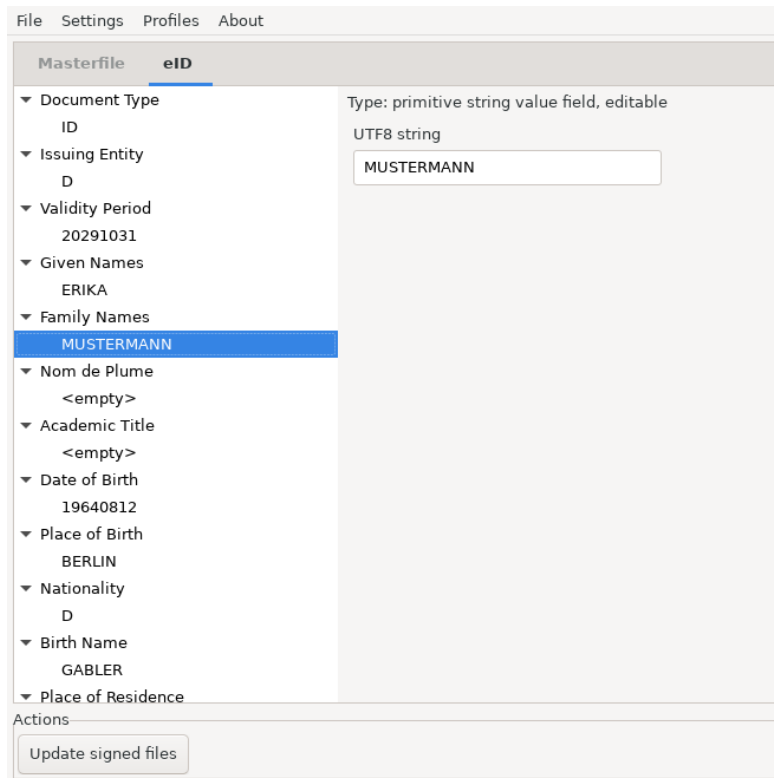


Abbildung 6: PersoSim Editor

Der Editor unterstützt den Anwender bei der Eingabe neuer Profile, indem er auf fehlerhafte Eingaben aufmerksam macht. So weist der Editor beispielsweise darauf hin, sobald der Anwender einen falschen Ländercode eingibt. Als Basis für eigene Profile kann der Anwender natürlich auch die mitgelieferten Profile nutzen.

Unter den Signatur-Einstellungen kann der Anwender ein DS-Zertifikat inkl. DS-Schlüssel eintragen, um das neue Profil auch final zu signieren. Die dazu notwendigen Dateien EF.CardSecurity und EF.ChipSecurity werden dabei neu erstellt, um das Profil zu vervollständigen. Erstellt man ein Profil 'from the scratch' kann man auch ein dazugehöriges EF.CardAccess erstellen lassen. Diese personalausweisspezifischen Dateien enthalten die

Standardparameter für Kryptografie und Protokolle, die durch die BSI TR-03110 und BSI TR-03127 für den deutschen Personalausweis vorgegeben werden. EF.CardAccess, EF.CardSecurity und EF.ChipSecurity lassen sich nicht mit dem Editor neu generieren und nicht manuell bearbeiten.