

HANDBUCH MOBILEKEY.NFC

Stand: Juli 2012

HANDBUCH MOBILEKEY.NFC

1.0	PRODUKTBESCHREIBUNG	3
1.1	BESTELLCODE	3
2.0	BENUTZERHINWEIS	3
2.1	SICHERHEIT UND SYSTEMVORAUSSETZUNGEN	3
2.2	EMPFEHLUNG	3
3.0	SIMONSSVOSS MOBILEKEY-APPLIKATION	3
4.0	ABLAUFDIAGRAMM	4
5.0	INSTALLATION	5
6.0	KONFIGURIEREN DER APPLIKATION MIT DEM „CONFIGURATOR“ TOOL	6
7.0	SIMONSSVOSS-APP	13
8.0	TAGESBETRIEB	13

HANDBUCH MOBILEKEY.NFC

1.0 PRODUKTBESCHREIBUNG

Software zur Nutzung der SimonsVoss SmartCard-Technologie im Zusammenhang mit Smartphones → NFC. Bestehend aus drei Softwareteilen.

Publisher: Läuft als „Dienst“ und hat eine Internetverbindung zum OTA-Server (Over The Air).

MobileKey Configuration Utility: Hat eine Verbindung zur LSM-Datenbank und verwaltet alle, in der LSM angelegten G2-Karten (Mifare Classic, DESFire in Vorbereitung)

SimonsVoss APP: Für iOS (iPhone 4) und Android Betriebssystem (Samsung Galaxy SII, SIII in Vorbereitung). Zum Download der SimonsVoss MobileKey-APP.

1.1 BESTELLCODE

MOBILEKEY.NFC → zum freien Internet Download: WWW.SIMONS-VOSS.COM

2.0 BENUTZERHINWEIS

Es sind umfangreiche Kenntnisse der Anwendungssoftware LSM erforderlich, um einen sicheren und störungsfreien Betrieb zu gewährleisten.

2.1 SICHERHEIT UND SYSTEMVORAUSSETZUNGEN

Siehe LSM-Handbuch

2.2 EMPFEHLUNG

MOBILEKEY.NFC sollte nur im Zusammenhang mit der LSM-Business/ Professional verwendet werden! LSM Basic sollte nur zu Vorführungszwecken verwendet werden!

3.0 SIMONSSVOSS MOBILEKEY-APPLIKATION

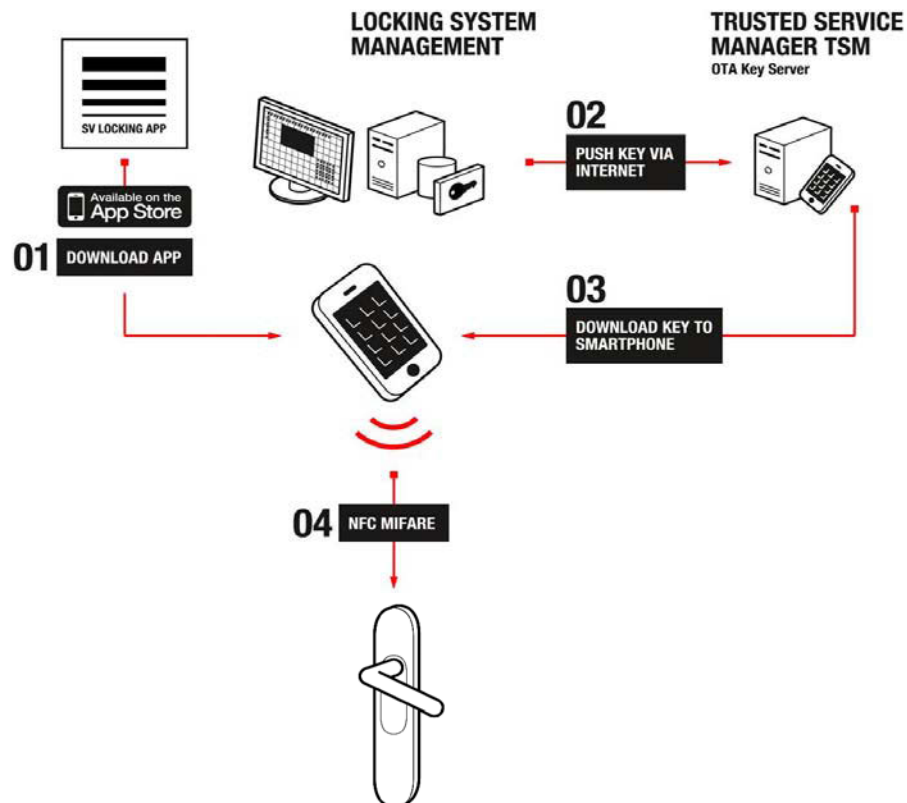
Die MobileKey-Applikation ermöglicht eine zentrale Administration digitaler Schließsysteme (digitale SmartCard-Schließzylinder | -SmartHandle | -SmartRelais2, CompactReader).

Idee dabei ist, statt den Schließungskomponenten, die Identmedien (Smartphone) zu vernetzen. Die Vernetzung mit der zentralen Administrations-SW (LSM) erfolgt dabei über existierende mobile Netzwerke.

HANDBUCH MOBILEKEY.NFC

4.0 ABLAUFDIAGRAMM

Die SimonsVoss-Lösung dazu arbeitet wie folgt:



1. Der Endanwender lädt die SimonsVoss MobileKey-App auf sein Smartphone.
2. Nachdem der Schließanlagenverwalter in seiner Systemoberfläche mit Hilfe des „Configurator“ Tools alle Identmedien (G2-Karten) markiert hat, die als Smartphone arbeiten sollen, und zusätzlich einen Dienst („Publisher“) gestartet hat, werden immer dann, wenn sich an den Schließberechtigungen der jeweiligen Smartphone-User etwas ändert, automatisch neue Berechtigungsdatensätze generiert und auf einen zentralen Server (OTA Key Server) hinterlegt.
3. Der Endanwender kann sich über Mobilfunknetzwerke seinen aktuellen Schlüssel vom OTA (Over The Air) abholen, indem er in seiner MobileKey- App die Taste „Schlüssel erneuern“ berührt und eine PIN eingibt.
4. Anschließend kann er – NFC-basiert, d.h. das Smartphone verhält sich wie eine Mifare-Karte – mit seinem aktualisierten „Schlüssel“ all die Türen öffnen, die der Schließanlagenverwalter für ihn freigegeben hat.
Interessant dabei ist, dass der Schließanlagenverwalter präzise Zeitfenster vorgeben kann, in denen der Anwender zutrittsberechtigt ist. Danach verfällt sein „Schlüssel“ und er muss sich erneut einen aktualisierten Schlüssel herunterladen.

HANDBUCH MOBILEKEY.NFC


SimonsVoss arbeitet derzeit mit einem sogenannten NFC-Attachment/ micro SD-Karte, einer Brückentechnologie, in der die komplette NFC-Technologie (13,56 MHz RFID Interface, sowie das sogenannte Secure Element mit sicherem Karten-Datenspeicher und sicherer Programmausführungsumgebung) in einem modularen Adapter, der iCarte integriert ist. Dieser Adapter wird an das iPhone gesteckt und fungiert zusätzlich als iPhone Schutzhülle.

5.0 INSTALLATION


Die MobileKey-Applikation von SimonsVoss besteht kundenseitig aus drei Komponenten:

- Die MobileKey-App für den User mit der eigentlichen Schlüsselfunktion (Smartphone). Download der „SimonsVoss-App
- Ein „Configurator“ Tool, mit dem der Schließanlagenadministrator in seiner LSM Benutzeroberfläche diejenigen Identmedien selektieren kann, die als MobileKeys verwaltet werden sollen
- Ein „Publisher“ Dienst, der im Hintergrund läuft und automatisch Sorge trägt, dass immer aktualisierte Schlüsseldatensätze auf dem zentralen OTA Key Server liegen



Unter „Dienste“ sollte nach der Installation überprüft werden, ob der „Publisher“ gestartet ist!

 SimonsVoss MobileKey Publisher Performs LSM DB monitoring and publishing of the mobile keys to the OTA Server. Gestar...

In diesem Ordner befinden sich die Installationsdateien mit Versionsnummer – kann unterschiedlich sein.

 setup-1.0.911

Bitte „setup.exe“ ausführen.

 ISSetupPrerequisites
 setup.exe

Bitte der Installationsroutine folgen. Nach Fertigstellung finden Sie die installierten Dateien unter: C:\Programme\SimonsVoss\MobileKey

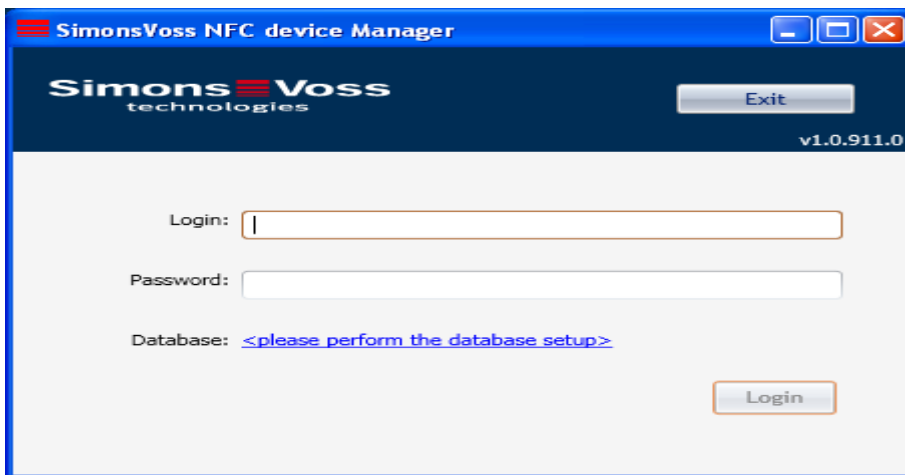
Ordner	Name	Größe	Typ
	Configuration		Dateiordner
	Publisher		Dateiordner
	SimonsVoss.MobileKey.LanguageSettings.exe	37 KB	Anwendung
	WPFToolkit.Extended.dll	338 KB	Programmbibliothek

HANDBUCH MOBILEKEY.NFC

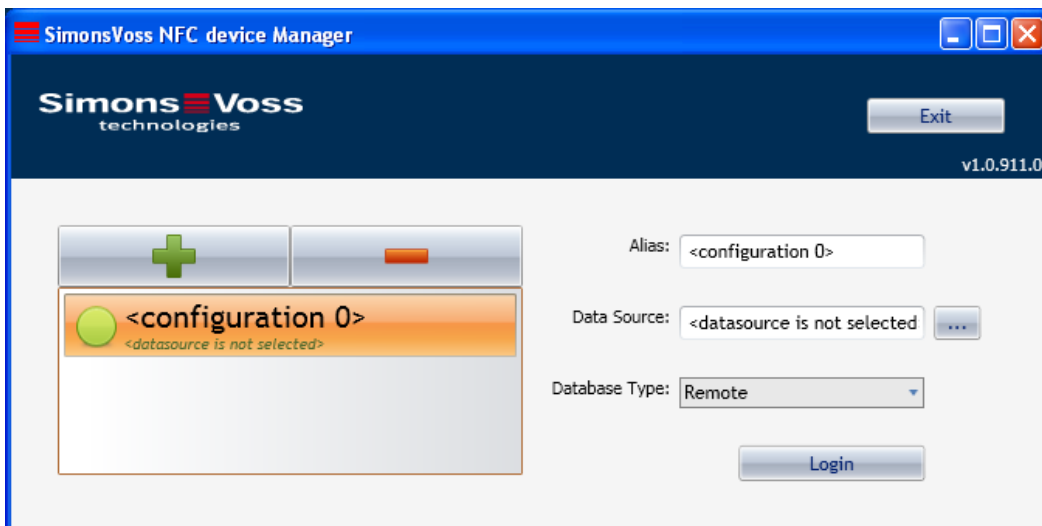
6.0 KONFIGURIEREN DER APPLIKATION MIT DEM „CONFIGURATOR“ TOOL

Achtung: Der Configurator setzt auf eine existierende Schließanlage/ Datenbank auf. Alle Identmedien, die im Configurator als Smartphone gekennzeichnet werden sollen, müssen im richtigen Format (MIFARE Classic [später auch MIFARE DESFire]) angelegt sein. (Siehe Schließanlage Eigenschaften → Kartenmanagement G2).

Starten Sie die „ MobileKey Configuration Utility“



1. Stellen Sie die Verbindung zur SV-Datenbank her → „Database“



HANDBUCH MOBILEKEY.NFC

Alias: Namensgebung

Data Source: Pfadangabe zur SV-Datenbank

Defaultpfad ist:

C:\Dokumente und Einstellungen\AllUsers\Anwendungsdaten\
SimonsVoss\Repository**Name Database**\smbd.add

Database Type: „Remote“ zu wählen bei Server-Client Struktur LSM Business
„Lokal“ zu wählen bei z.B. LSM Basic

Mit dem + (Plus)-Symbol können neue bzw. andere Datenbankverbindungen hinzugefügt werden.

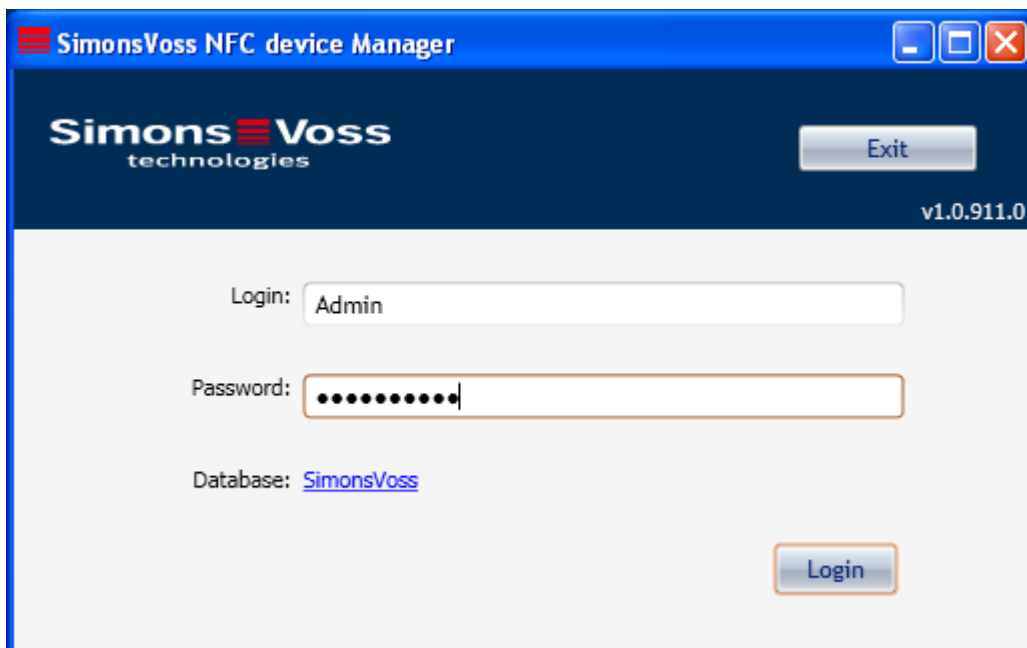
Mit dem – (Minus)-Symbol können angelegte Datenbankverbindungen gelöscht werden.

Login: Betätigen, um die eingestellte Datenbankverbindung herzustellen.

2. Login : Benutzername (default: Admin) → für SV-Datenbank

Password: Passworteingabe (default: system3060) → für SV-Datenbank

Achtung: Wenn Sie ein anderes „Login“ bzw. „Password“ benutzen (empfohlen!), dann verwenden Sie dieses.



Betätigen Sie „Login“.

Unter „Database“ wird die zuvor ausgewählte Datenbank (bzw. Ihr Alias) angezeigt.

Bitte beachten Sie, dass die Spracheinstellungen von NFC Device Manager und LSM-Benutzeroberfläche identisch sind. Sie können dies im Bedarfsfall mit der „SimonsVoss.MobileKey.LanguageSettings.exe“ korrigieren.

HANDBUCH MOBILEKEY.NFC

Nach erfolgreicher Anmeldung erscheint folgendes Fenster:

Achtung: Bei erstmaliger Anmeldung müssen Sie als erstes auf das Zahnrad unten rechts (Change Settings) klicken, um die Verbindung zum OTA-Server herzustellen (vgl. nächste Seite).

Name: Verwendete Schließanlage

Number of PIN tries: Anzahl der zulässigen Falscheingaben bei Benutzung der SimonsVoss-APP zum Download der Schlüsseldatensätze.

Dynamic Time Frame: Wurden Datensätze auf dem OTA-Server hinterlegt, können sie mit dieser Einstellung zeitlich eingeschränkt werden. Entweder beginnt die zeitliche Befristung nach der Übermittlung auf den OTA-Server → Number of Hours (z.B. 168), oder man hinterlegt eine generelle Uhrzeit → Time of the Day (z.B. 24 Uhr). Diese Einstellungen gelten zunächst global für alle Nutzer. Sie können diese Einstellungen auch individualisieren. Siehe dazu die Beschreibung zu „Transponder List“ weiter unten.

Key Description: Eine Beschreibung kann auf alle NFC-Geräte (Smartphone) hinterlegt werden.

Publish Keys: Vorgenommene Änderungen werden zum OTA-Server übermittelt.

Save Configuration: Speichern der Konfiguration.

HANDBUCH MOBILEKEY.NFC

Change Settings (Zahnrad unten rechts): Zur Anmeldung am OTA-Server auf das Symbol klicken. Folgendes Fenster öffnet sich:

Address: Softwareport, über die der Device-Manager mit der Schließanlagen-Datenbank kommuniziert.

OTA-Server: URL für den verwendeten Server.

Operator Name: Wird von SimonsVoss angelegt und dem jeweiligen Benutzer bekannt gegeben. Eine Änderung des Namens kann vorgenommen werden.

Operator Password: Wird von SimonsVoss angelegt und dem jeweiligen Benutzer bekannt gegeben. Eine Änderung des Passwortes kann vorgenommen werden.

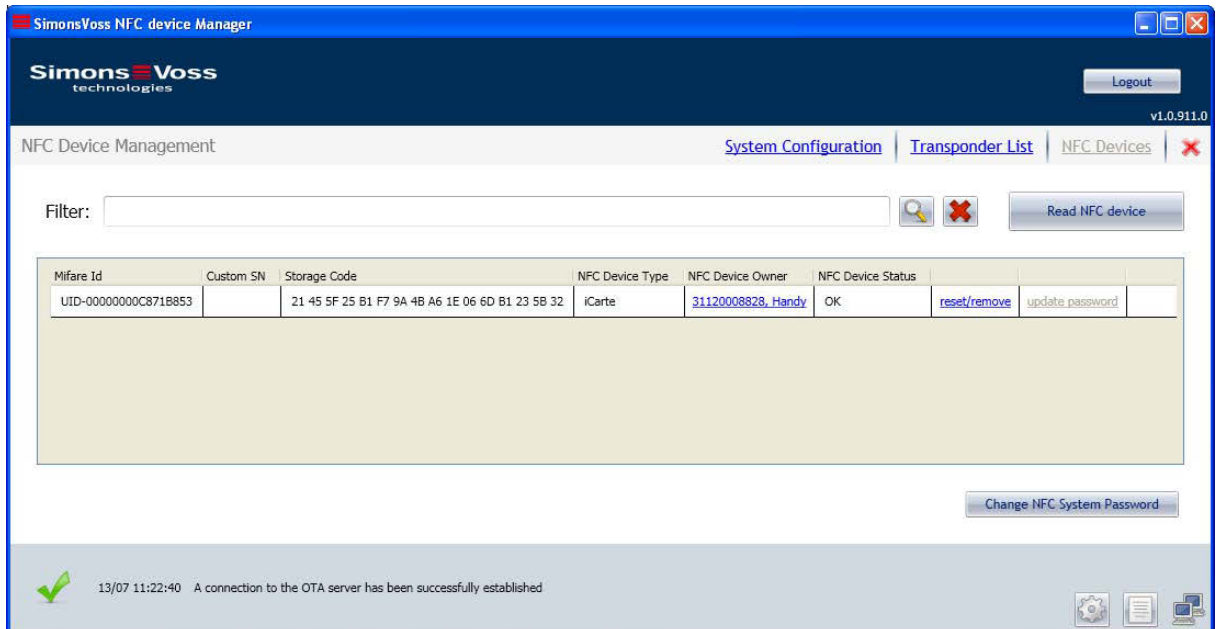
Export Settings to Publisher: Vorgenommene Änderungen werden zum OTA-Server übermittelt.

Ein grüner Haken (links unten) zeigt an, dass die Verbindung zum OTA-Server hergestellt ist.

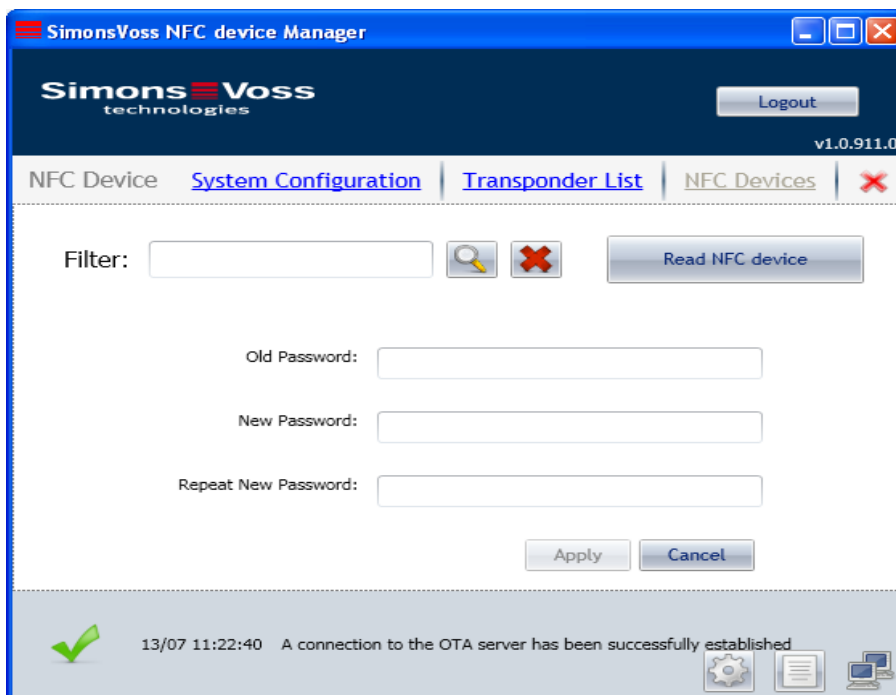
System Configuration: Betätigen Sie „System Configuration“ und das Ausgangsfenster wird wieder sichtbar.

HANDBUCH MOBILEKEY.NFC

NFC-Devices: Betätigen, folgendes Fenster wird sichtbar:



Change NFC System Password: Hier muss ein Passwort vergeben werden. Damit werden die versendeten Daten gegen Manipulation geschützt! Bei der Erstvergabe muss kein „altes Passwort“ eingegeben werden.



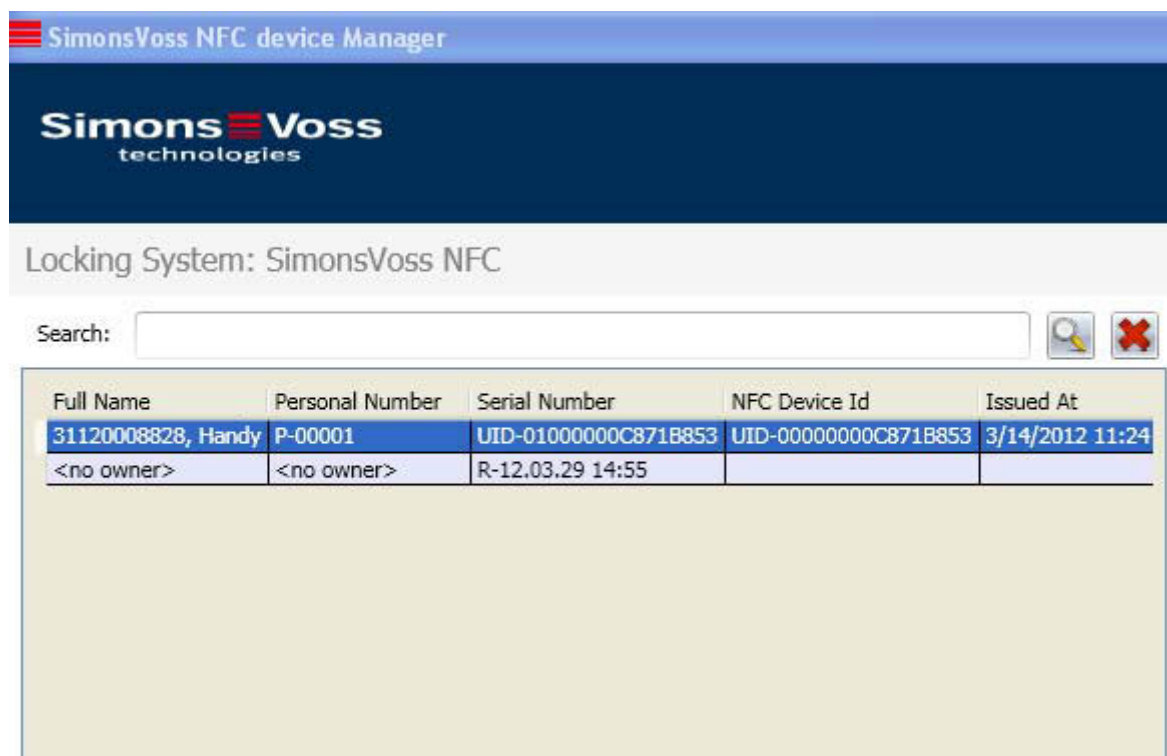
HANDBUCH MOBILEKEY.NFC

Read NFC device: Das Smartphone **mit** Attachment oder microSD-Karte **und** gestarteter SimonsVoss-APP auf das SimonsVoss-Programmiergerät (SMARTCD.HF) legen und danach „Read NFC device“ betätigen. Die Daten werden vom Attachment bzw. microSD-Karte an den OTA-Server übermittelt (Internetverbindung nötig!) und in einer Tabellenform sichtbar gemacht. Dieser Vorgang muss je nach Anzahl wiederholt werden. Danach sind alle benötigten Daten am OTA-Server vorhanden.

Reset/ remove: Nicht mehr benötigte oder auch verlorene Attachments bzw. microSD-Karten können hierüber vom OTA-Server entfernt werden. Warnmeldung beachten!!!

Transponder List: Betätigen, um die Administration der „vernetzten Schlüssel“ vornehmen zu können. Folgendes Fenster wird sichtbar:

(Hier nur der linke Teil des Fensters dargestellt:)



The screenshot shows the 'SimonsVoss NFC device Manager' window. The title bar reads 'SimonsVoss NFC device Manager'. Below the title bar is the SimonsVoss technologies logo. The main content area is titled 'Locking System: SimonsVoss NFC'. There is a search field with the label 'Search:' and a magnifying glass icon. Below the search field is a table with the following data:

Full Name	Personal Number	Serial Number	NFC Device Id	Issued At
31120008828, Handy	P-00001	UID-01000000C871B853	UID-00000000C871B853	3/14/2012 11:24
<no owner>	<no owner>	R-12.03.29 14:55		

Alle zuvor in der LSM angelegten G2-Karten werden hier angezeigt.

Initialise MobileKey anklicken.

HANDBUCH MOBILEKEY.NFC

Folgendes Fenster wird sichtbar (hier nur die rechte Seite dargestellt):

The screenshot shows a web application window titled "System Configuration" with a "Logout" button and version "v1.0.911.0". The "NFC Devices" tab is active. The form contains the following fields and controls:

- Card Owner: <no owner>
- Personal #: <no owner>
- Serial #:
- Temporary Disable MobileKey Publishing
- NFC device Id: <please add NFC devices> (dropdown menu) with a [read NFC device](#) link.
- Custom SN (optional): [text input field]
- PIN: [text input field]
- Description: [text input field]
- Dynamic Time Frame: The number of hours since the last key issue (dropdown menu)
- Number of Hours: 168 (text input field) with a note "(acceptable values: 1h - 255h)"

At the bottom, there are three buttons: "Save", "Publish", and "Reset".

Temporary Disable MobileKey Publishing: Wird der "Haken" gesetzt, werden keine Daten zum OTA-Server übertragen.

NFC device ID: Hier werden alle UID-Seriennummern aufgelistet.

Read NFC device: Für die Zuordnung einer Person zu einem Attachment/ microSD-Karte, legen Sie diese bitte mit gestarteter SimonsVoss-APP auf das Programmiergerät (SMARTCD.HF) und markieren einen Eintrag einer G2-Karte = Person und betätigen „read NFC device“. Jetzt ist das Attachment/ microSD-Karte einer Person zugeordnet. Dieser Vorgang kann sich je nach Anzahl wiederholen.

Detach NFC device: Zum Trennen von Person und Attachment/ microSD-Karte markieren Sie bitte den jeweiligen Eintrag und betätigen Sie „detach NFC device“.

Custom SN (optional): Hier kann optional die Seriennummer vom Attachment eingetragen werden. (Diese finden Sie unter dem Barcode auf der Innenseite des Attachments).

PIN: Wenn eine PIN hinterlegt wird, muss die jeweilige Person diese PIN in der SimonsVoss-APP, vor dem Download neuer Schlüsseldaten eingeben.

Description: Es können zusätzliche Information für den jeweiligen Nutzer gesendet werden.

Dynamic Time Frame: In diesem Drop-Down Menü können Gültigkeits- und Verfalls-eigenschaften der Datensätze User individuell eingestellt werden. Entweder beginnt die zeitliche Befristung nach der Übermittlung auf den OTA-Server → Number of Hours (z.B. 168), oder man hinterlegt eine generelle Uhrzeit → Time of the Day (z.B. 24 Uhr).

HANDBUCH MOBILEKEY.NFC

Des Weiteren finden Sie hier unter Set fixed valid from/expiry dates:

Activation Date: Kann ab sofort sein oder auch in der Zukunft liegen.

Expiration Date: Es sollte **immer** ein Verfallsdatum im Schlüsseldatensatz enthalten sein. Nach dem Ablauf des Verfalldatums können keine SimonsVoss Schließungen mit dem Smartphone geöffnet werden – erst nach einem erneuten Download.

Save: Alle Daten werden gespeichert.

Publish: Nur die **markierten** Einträge aus der Tabelle werden an den OTA-Server übermittelt und sind für die Personen nutzbar.

Reset: Markierte Einträge werden zurückgesetzt.

Logout: Trennt Verbindung zur Datenbank.

7.0 SIMONSVOSS-APP

Schlüssel erneuern: Betätigen, um neue Daten vom OTA-Server herunterzuladen.

PIN: Muss in der SimonsVoss-APP eingegeben werden, wenn der Administrator eine PIN hinterlegt hat. So können Unbefugte, die das Smartphone im Besitz haben, keine „Schlüsseldaten“ herunterladen.

8.0 TAGESBETRIEB

Wenn sich in der LSM Schlüssel- bzw. Kartendaten ändern, dann können diese mittels der MobileKey Software zum OTA-Server übertragen und vom Nutzer heruntergeladen werden. Halten Sie das Attachment/ microSD-Karte vor den SimonsVoss Kartenleser – die MobileKey-APP muss gestartet sein.

