MOBILEKEY.NFC
MANUAL

Version: July 2012

SimonsVoss technologies

MOBILEKEY.NFC MANUAL

SimonsVoss Technologies GmbH
Feringastr. 4
85774 Unterföhring
Germany

This product fulfills essential requirements of CE-Conformity.
The declaration of conformity can be found at
www.simonsvoss.com

MOBILEKEY.NFC MANUAL

1.0 PRODUCT DESCRIPTION

Software for using SimonsVoss SmartCard technology together with smartphones → NFC, consisting of three software components.

Publisher: operates as a 'service' and has internet connection to the OTA server (OTA = **O**ver **T**he **A**ir).

MobileKey configuration utility: has a connection to the LSM database and manages all G2 cards added to the LSM database (Mifare Classic, DESFire in the pipeline)

SimonsVoss App: for iOS (iPhone 4) and Android operating system (Samsung Galaxy SII, SIII in the pipeline). Used to download the SimonsVoss MobileKey app.

1.1 ORDER CODE

MOBILEKEY.NFC → free Internet download: WWW.SIMONS-VOSS.COM

2.0 USER INFORMATION

Extensive knowledge of the LSM application software is required to ensure reliable, problem-free operation of the app.

2.1 SECURITY AND SYSTEM PRE-REQUISITES

See LSM Manual

2.2 RECOMMENDED

MOBILEKEY.NFC should **only** be used in conjunction with **LSM Business / Professional**. LSM Basic should be used for **demonstration purposes only**.

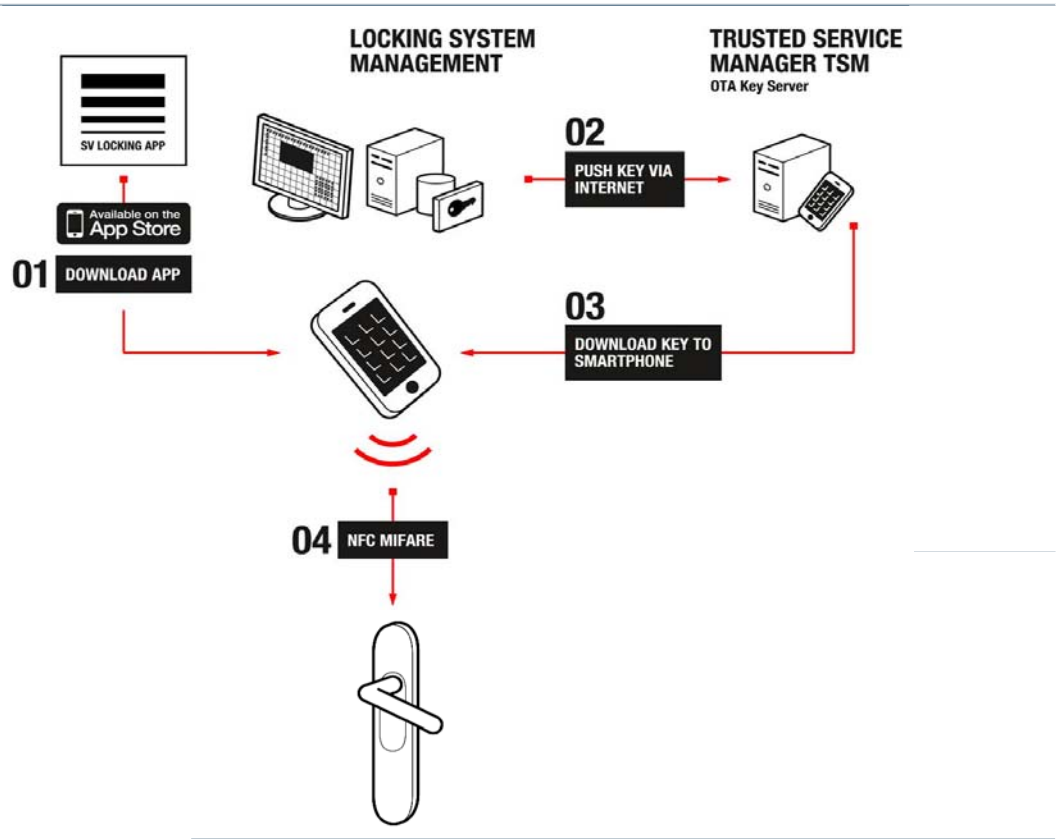
3.0 SIMONSVOSS MOBILEKEY APPLICATION

The MobileKey application provides central administration of digital locking systems (digital SmartCard locking cylinders | -SmartHandle | -SmartRelais2, CompactReader).

The idea is to network ID media (smartphones) instead of locking components. Networking to the central administration software (LSM) is achieved via existing mobile networks.

4.0 OPERATION SEQUENCE DIAGRAM

The SimonsVoss solution functions as follows:



1. The end user downloads the SimonsVoss MobileKey app onto their smartphone.

2. After the locking system administrator has used the 'Configurator tool' on their system interface to select all ID media (G2 cards) which are to function as a smartphone and has also started a service ('publisher'), new authorisation data sets are automatically generated whenever there is a change to locking authorisations for the respective smartphone user and saved to a central server (OTA Key Server).

3. The end user can retrieve their current key from the OTA server via mobile phone networks by pressing 'Renew key' button on their MobileKey app and entering a PIN.

4. They are then able to use their updated key to open all doors which the locking system administrator has authorised them to open using the NFC-based solution, i.e. the smartphone acts like a Mifare card.

   The interesting feature here is that the locking system administrator can specify exact time windows when the user is authorised to enter. After this time period, the user's 'key' expires and they need to download an updated key once more.

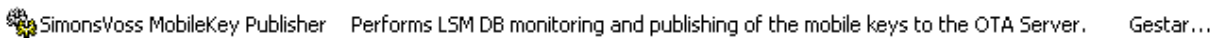
SimonsVoss currently works with an NFC attachment/ micro SD card, a bridge technology, in which the full NFC technology (13.56 MHz RFID interface and what is called the Secure Element with a secure card data memory and a secure program execution environment) is integrated into a modular adapter, the iCard. This adapter is plugged into the iPhone and also acts as an iPhone protective cover.

5.0 INSTALLATION

The SimonsVoss MobileKey application consists of three components for the customer:

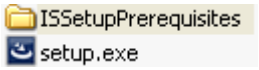
- The MobileKey app for the user with the actual key function (smartphone). 'SimonsVoss app' download
- A 'configurator' tool which the locking system administrator can use on their LSM user interface to select ID media which are to be administrated as Mobile Keys
- A 'Publisher' service which runs in the background and automatically ensures that constantly updated key datasets are located on the central OTA Key Server

After installation, you **must** check under 'Services' to ensure that the 'Publisher' has been launched.

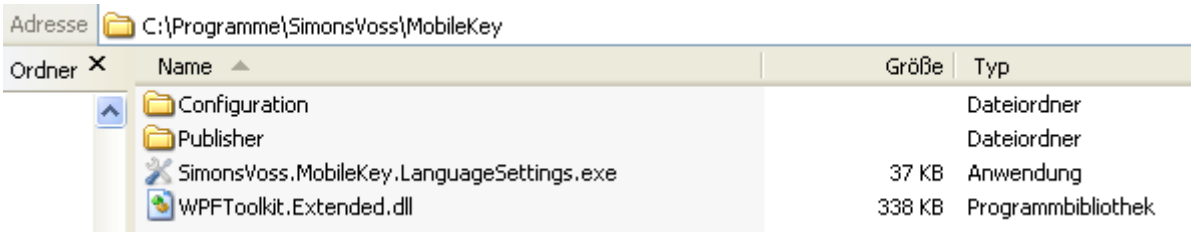


This file contains the installation files with version numbers – may vary.

Please run 'setup.exe'.



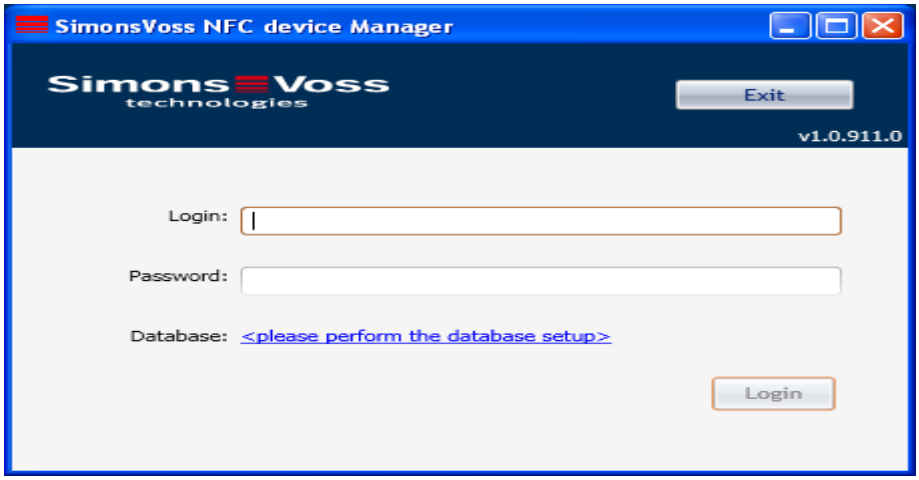
Follow the installation routine. Once complete, you will find the installed files at: C:\Programs\SimonsVoss\MobileKey



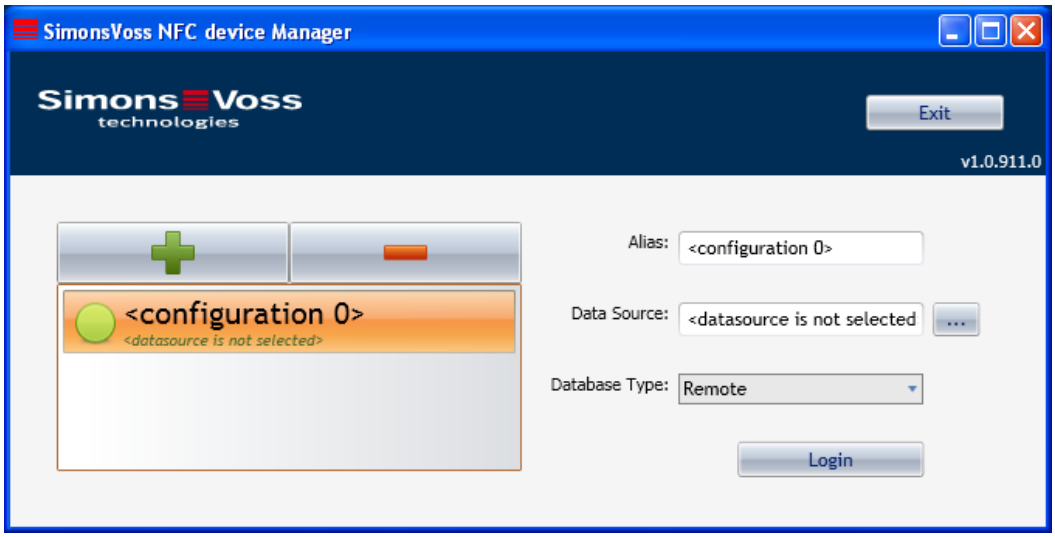
6.0 CONFIGURING THE APPLICATION USING THE 'CONFIGURATOR' TOOL

Warning: the Configurator uses an existing locking system/ database. All ID media which are to be identified as smartphones in the configurator must be created in the right format (MIFARE Classic [also MIFARE DESFire at a later date]). See Locking system properties → Card management G2.

Start the 'MobileKey Configuration Utility'



1. Establish the connection to the SV database → 'Database'



Alias: name
Data source: path to SV database

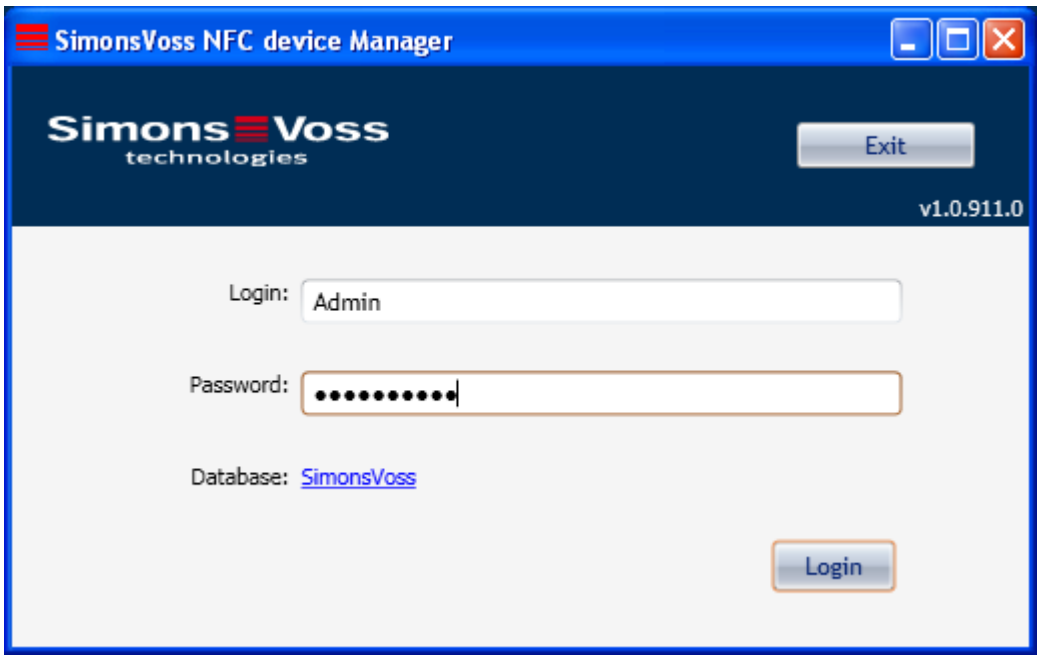
Default path is:
C:\Documents and Settings\AllUsers\Application data\
SimonsVoss\Repository***Name Database***\lsmdb.add

Database type: select 'Remote' in LSM Business server client structure.
Select 'Local' for LSM Basic, for instance.

New or other database connections can be added using the + (plus) symbol.
The – (minus) symbol can be used to delete existing database connections.
Login: activate to establish the pre-set database connection

2. Login: user name (default: Admin) → for SV database
   Password: enter password (default: system3060) → for SV database

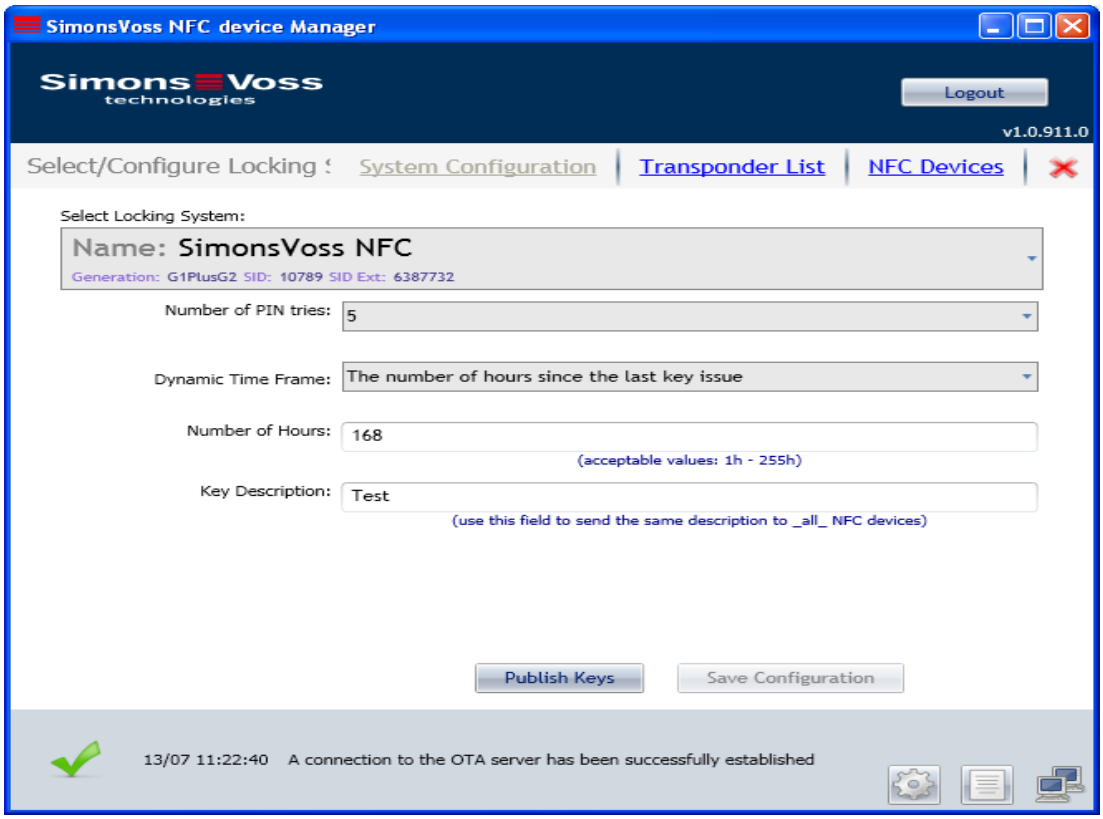
Note: If you use a different 'Login' or 'Password' (**recommended**), then use the different one.



Activate the 'Login'.
The selected database (or your alias) will be displayed under 'Database'.

Please note that language settings in NFC Device Manager and on the LSM user interface are the same. If required, you can modify this setting using 'SimonsVoss.MobileKey. LanguageSettings.exe'.

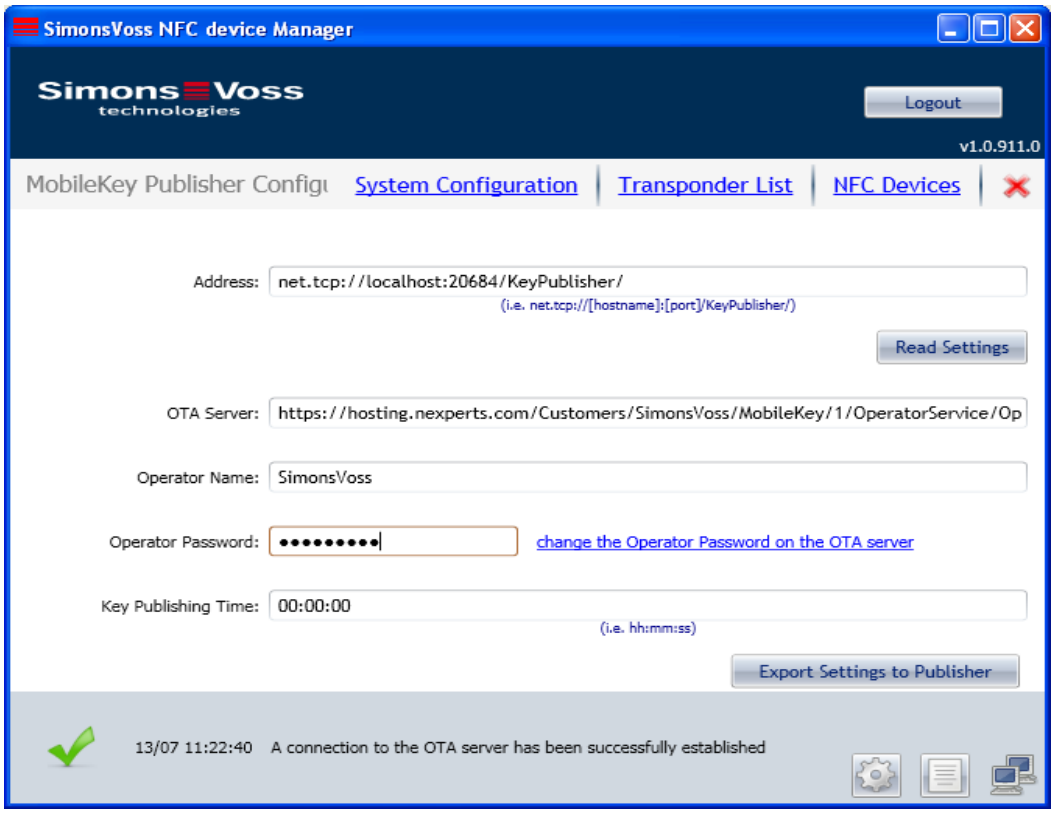
The following window will appear after a successful login:



Note: when logging on for the first time, you will first need to click on the cog wheel (Change Settings) in the bottom right-hand corner to establish the connection to the OTA Server (compare with next page).

Name: locking system used
Number of PIN tries: Number of permitted incorrect PIN entries when using the SimonsVoss app to download key datasets.
Dynamic Time Frame: if datasets have been saved on the OTA server, this setting can be used to establish a time restriction. The time limit either begins after transmission to the OTA Server → Number of hours
(e.g. 168), or a general time is entered → Time of day (e.g. 24.00 hours). These settings apply to all users initially, but you can also customise these settings. See the description of the 'Transponder list' further below.
Key description: a description can be saved to all NFC devices (smartphones).
Publish keys: any changes made are transmitted to the OTA server.
Save configuration: saving of the configuration.

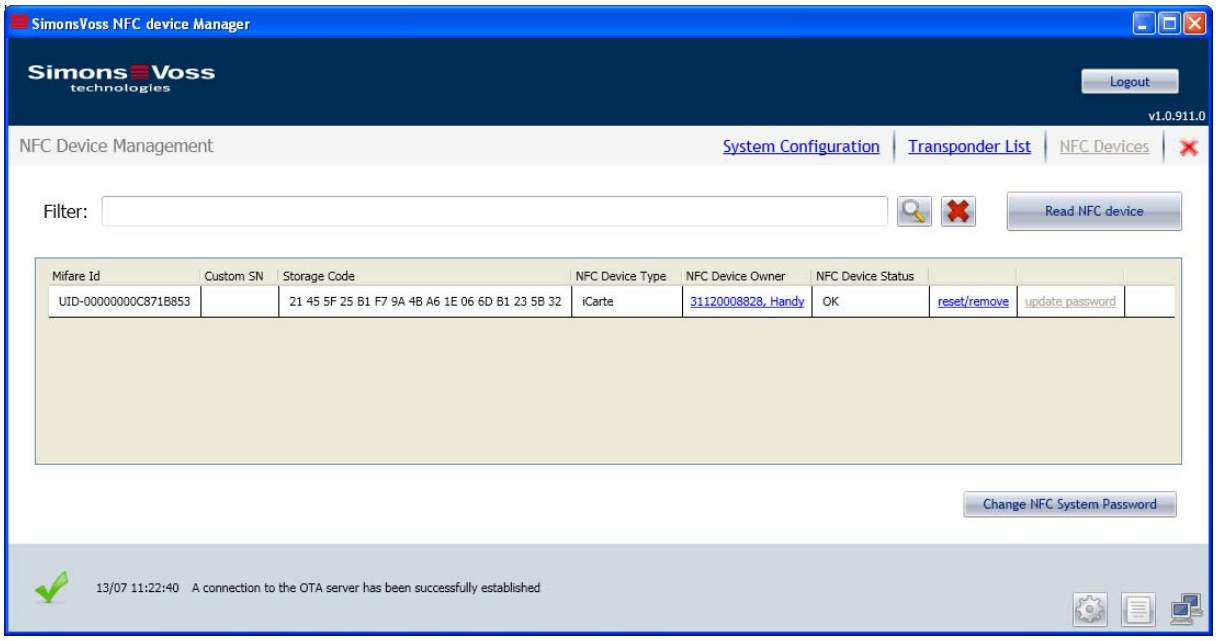
Change settings (cog wheel at bottom right-hand side): click on the symbol to log on to the OTA server. The following window will open:



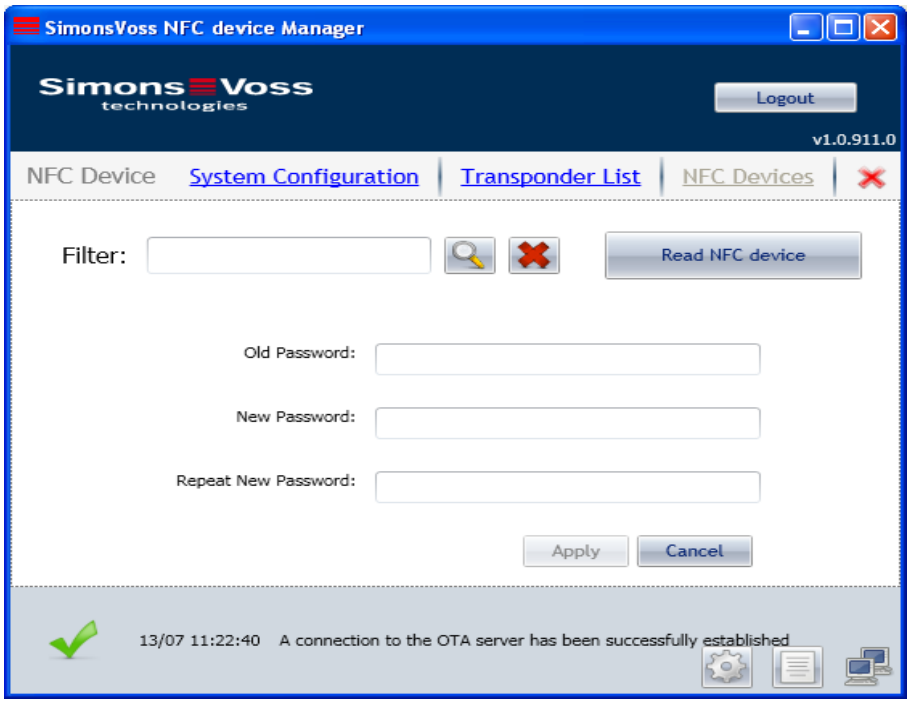
Address: software port which the device manager uses to communicate with locking system database.
OTA server: URL for the server used.
Operator name: created by SimonsVoss and given to the respective user. The name can be changed.
Operator password: created by SimonsVoss and given to the respective user. The password can be changed.
Export settings to publisher: any changes made are transmitted to the OTA server.

A green check mark (bottom, left-hand corner) shows that a connection to the OTA server has been established.
System configuration: click on 'System configuration' and the initial window will appear again.

NFC devices: click on link and the following window will open:



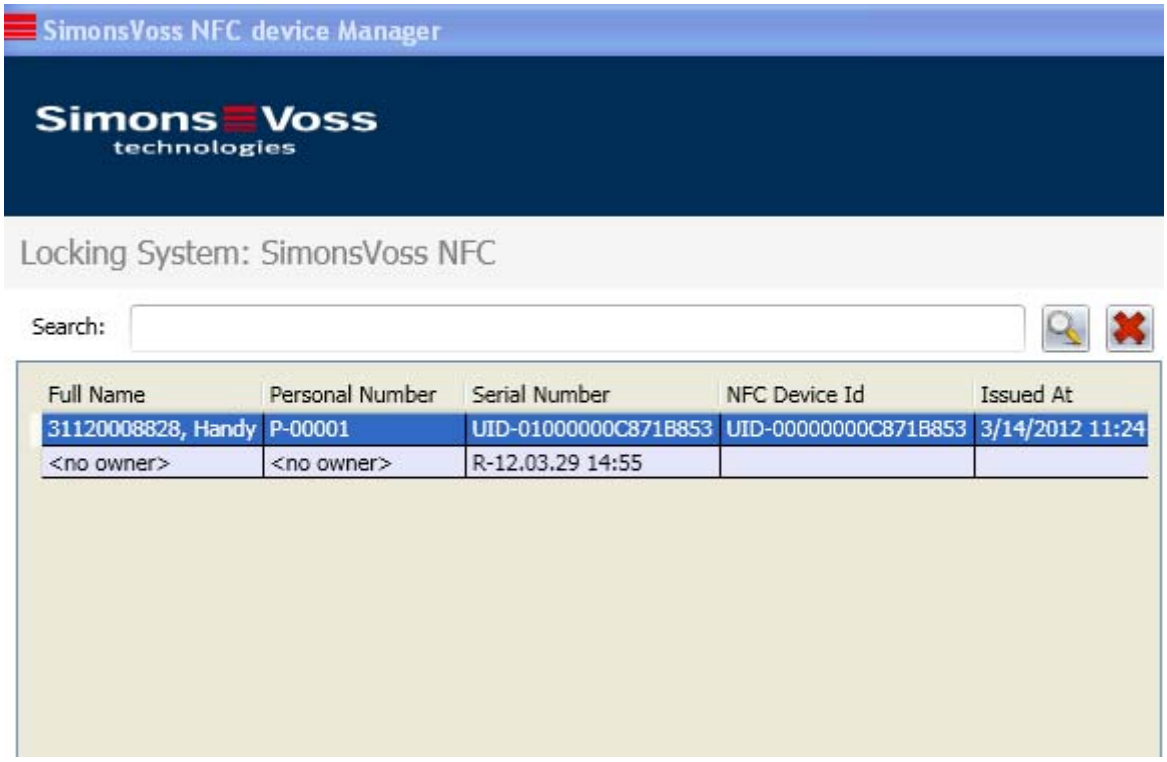
Change NFC system password: you need to allocate a password here, so that the transmitted data is **protected against manipulation**. You must not use an 'old password' the first time that you allocate a password.



Read NFC device: place the smartphone **with** the attachment or microSD card **and** with the SimonsVoss app launched onto the SimonsVoss programming device (SMARTCD.HF) and then press 'Read NFC device'. The data are then transmitted from the attachment or microSD card to the OTA server (**internet connection required**) and made visible in table format. This process must be repeated for each device. All required data are then available on the OTA server.
Reset / remove: this function can be used to remove lost attachments or microSD cards or those no longer needed from the OTA server. Observe **warning message**.

Transponder list: press on this link to administer 'networked keys'. The following window will open:

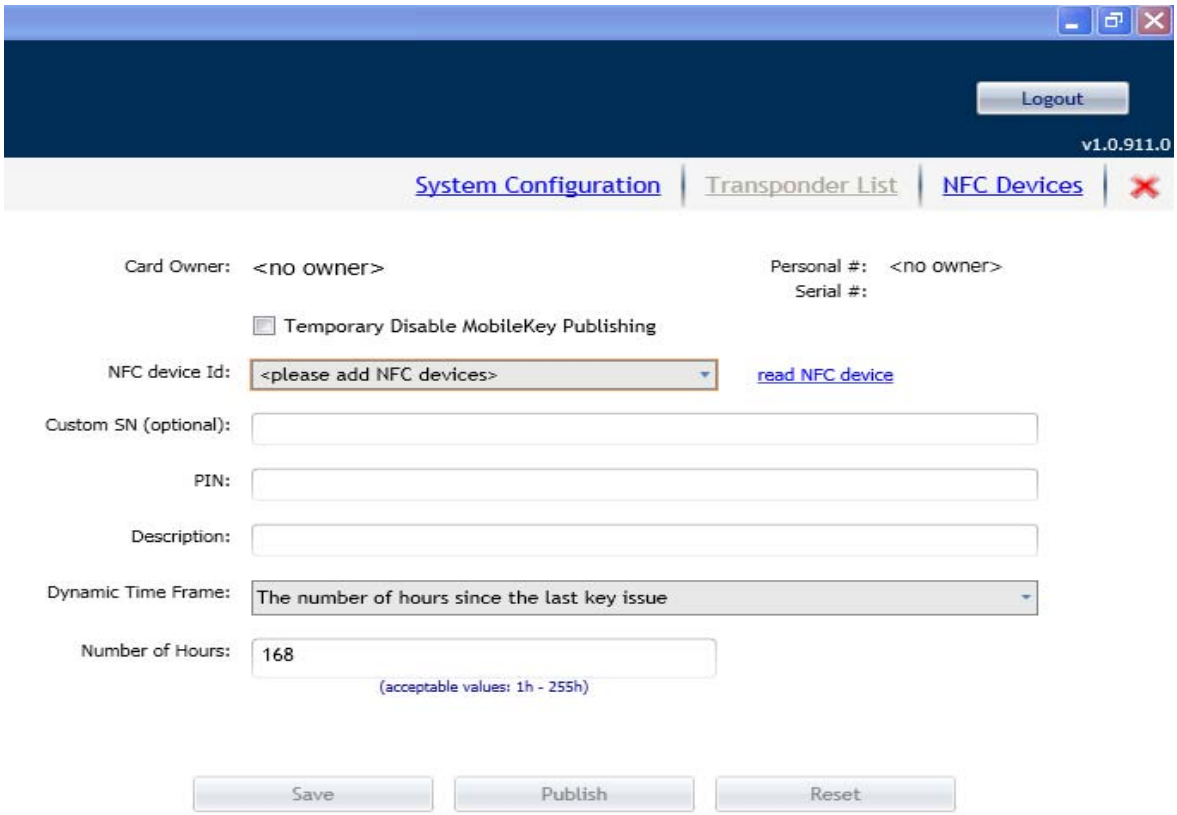
(Only the left-hand side of the window is shown here)



All G2 cards previously added to the LSM are shown in this window.

Click on 'Initialise MobileKey'.

The following window will appear (only the right-hand side of the window is shown here):



Temporary Disable MobileKey Publishing: no data are transmitted to the OTA server if this box is checked.
NFC device ID: all UID series numbers are listed here.
Read NFC device: to assign a person to an attachment or microSD card, place the attachment or the card with the SimonsVoss app launched onto the SimonsVoss programming device (SMARTCD.HF), select a G2 card entry = Person and then press 'Read NFC device'. The attachment/ microSD card is now assigned to a person. This process must be repeated for each person.
Detach NFC device: to disassociate a person from an attachment/ microSD card, select the respective entry and press 'Detach NFC device'.
Custom SN (optional): this is where the attachment serial number can be entered as an option. (You can find this number under the barcode on the inside of the attachment).
PIN: if a PIN is added, the respective user must enter this PIN in the SimonsVoss app before downloading new key data.
Description: additional information can be sent for the respective user.
Dynamic Time Frame: this drop-down menu is used to configure validity and expiry details of datasets on an individual basis for users. The time limit either begins after transmission to the OTA Server → Number of Hours (e.g. 168), or a general time is entered → Time of day (e.g. 24.00 hours).

You will also find Set fixed valid from/expiry dates here:
Activation Date: can be activated with immediate effect or also for the future.
Expiration Date: a key dataset should **always** contain an expiry date. Once the expiry date is reached, the smartphone cannot be used to open SimonsVoss locks. The user cannot open locks until a dataset is downloaded again
Save: all data are saved.
Publish: only the **selected** entries in the table are transmitted to the OTA server and can be used for people.
Reset: selected entries are reset.
Logout: breaks connection to the database.

7.0 SIMONSVOSS APP

Renew key: press to download new data from the OTA server.
PIN: must be entered into the SimonsVoss app if the administrator has created a PIN. This ensures unauthorised users who have taken the smartphone are unable to download 'key data'.

8.0 DAY-TO-DAY OPERATION

If key or card data are modified in the LSM, such data can be transmitted to the OTA server using the MobileKey software and then downloaded by the user. Hold the attachment/ microSD-card in front of the SimonsVoss card reader. You need to launch the MobileKey app in order to do so.