SUPPORT INFORMATION

Access

2020-05-22

Setup of SiPass integrated 2.75 with fingerprint reader SIGMA Lite+Multi from Idemia (Safran Morpho)

This document describes the setup of biometric SIGMA range reader of Idemia (SAFRAN Morpho) to work in SiPass integrated 2.75. The communication between the reader and RIM of SiPass integrated is via OSDP (RS485 interface).

Before rollout on site it is recommended to verify the results with the local setup.

The setup was performed using Mifare DESFire EV1 cards.
This setup is limited to particular reader configurations. As a big variety of configuration setups with SIGMA Lite+Multi reader is possible only the described configuration has been tested.

VANDERBILT

Table of content

1. SOFTWARE & HARDWARE MODULES 3

2. SETUP 3

2.1 INSTALLATION OF SIPASS INTEGRATED SOFTWARE 3
2.2 FIRST READER CONFIGURATION VIA MBTB 3
2.3 CONNECTION OF SIGMA LITE+MULTI READER TO SIPASS INTEGRATED RIM 4
2.4 SIGMA READER CONFIGURATION VIA MORPHOMANAGER SOFTWARE 6
2.4.1 Creating a new Wiegand Profile 6
2.4.2 Creating a new Biometric Device Profile 7
2.4.3 Adding a device to MorphoManager 9
2.4.4 Adding a client to MorphoManager 9
2.4.5 Create a new User Policy for Card plus finger template stored on card 10
2.4.6 Card Enrolment (Card CSN + fingerprint stored on card) 11
2.4.7 Compatibility of SiPass integrated with SIGMA fingerprint reader from Idemia and VRx0S-MF/ VRx0M-MF reader from Vanderbilt on one site 13
2.4.7.1 Creating a new Wiegand Profile (for reversed CSN sent via OSDP) 13
2.4.7.2 Enrolment of reversed CSN in MorphoManager and in SiPass integrated software 15
2.4.8 Customized Key Policy 16
2.4.9 Card Only parallel to Card + Fingerprint Template mode 19
2.4.9.1 Configuration of new User Authentication Mode and User Policy 19
2.4.9.2 Card Enrolment (Card CSN) 21
2.5 SUMMARY 23

1. Software & Hardware modules

This setup was tested with the following software modules and hardware unit:

Description	Version
SiPass integrated Software	2.75.10.0001
MBTB (MorphoBioToolBox) Software	3.4.9.0
MorphoManager Software	13.1.5.5

Description	Serial number
SIGMA Lite+Multi (Model: MPH-AC001B) in MA5G native mode	1724SML0000768

2. Setup

2.1 Installation of SiPass integrated Software

Install SiPass integrated as described in SiPass integrated installation manual.

2.2 First reader configuration via MBTB

Install MBTB on SiPass server PC and connect the reader via network cable to the PC.

Using MBTB tool several reader settings can be configured:

- Network settings of the reader should be configured (*Quick Configuration -> Authorized IP* address menu). It is also possible to configure the settings using web browser (see Quick User Guide of the reader).
  Default SIGMA reader IP address is set to 192.168.1.10.
- Configuration of reader communication with Access Control System via OSDP:
  Key Configuraiton → *Manage Configuration Keys* menu → three parameters should be set to:

  comm_channels_state.serial = 1
  OSDP.channel = 1
  OSDP.device_serial_address = 1.

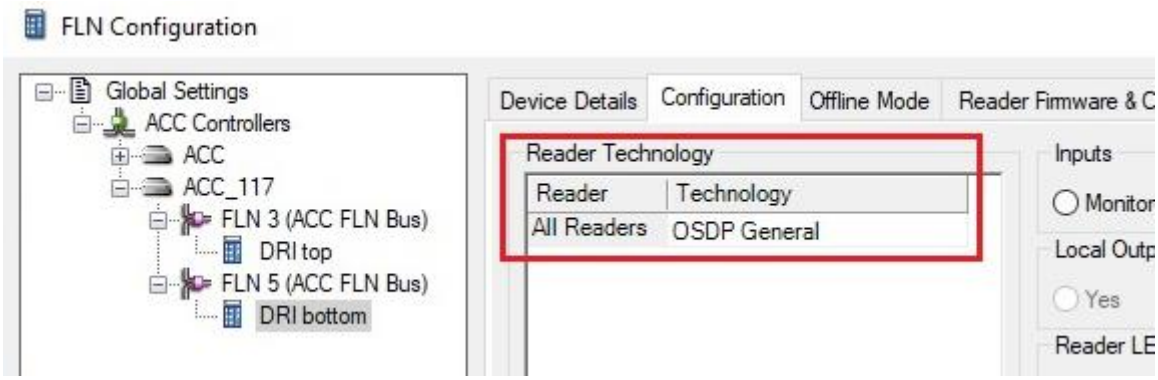
Remark:
The SIGMA reader address (**OSDP.device_serial_address**) is to be set dependent on connected RIM hardware (Reader Interface Module) of SiPass. If the reader is connected to ADD5100 (DRI) the address can be set to 1 - 2. If the reader is connected to ADE5300 (ERI) the address can be set to 1 - 8.

- In Quick Configuration → Communication Configuration there the Type is to be set to **Half Duplex** and the Baud Rate to be configured to **9600**.

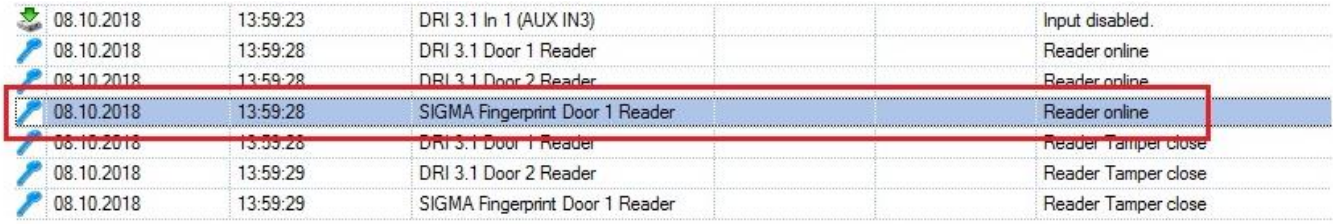
2.3 Connection of SIGMA Lite+Multi reader to SiPass integrated RIM

RIM (DRI)	↔	SIGMA Lite+Multi
Tx/+	↔	RS485_A (blue)
Rx/-	↔	RS485_B (blue/red)
0V	↔	Power GND (black) + RS485_GND (black/red)
12V	↔	Power +12V (red)

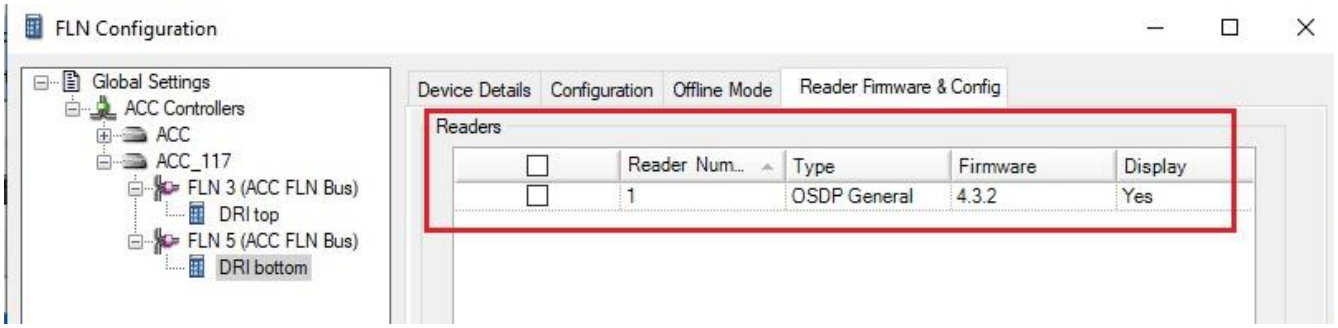
In SiPass integrated *Configuration client → FLN Configurator* select "**OSDP General**" for reader technology of the RIM where the SIGMA reader is connected to.



When the Sigma reader comes online via OSDP there is an audit trail message in SiPass integrated software showing that the reader is online:



Additionally in *FLN Configuration* dialog in tab *Reader Firmware & Config* there is the reader information available if it is online:



In case the SIGMA reader is online through OSDP the LCD screen changes from the standard one to the OSDP controlled screen.

Standard LCD screen **OSDP LCD screen**

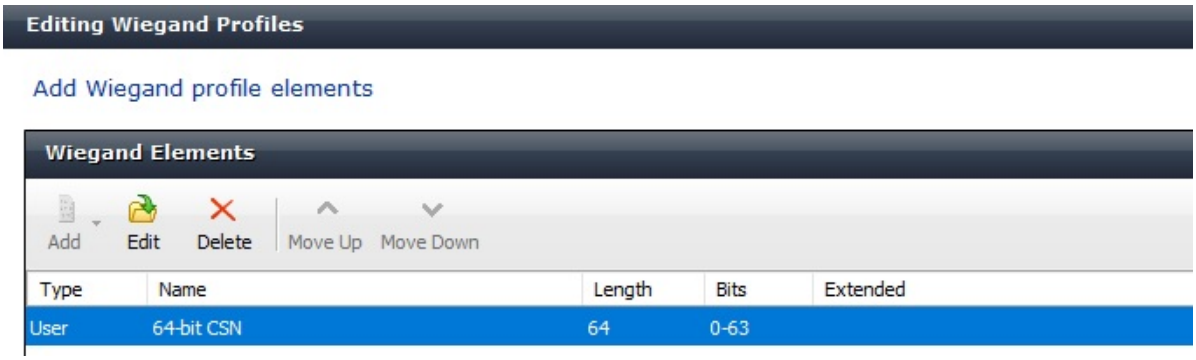
2.4 SIGMA reader configuration via MorphoManager Software

Install MorphoManager Software on SiPass server PC.
For the installation and the first configuration steps of MorphoManager Software please refer to *MorphoManager Quick Install Guide* document.

2.4.1 Creating a new Wiegand Profile

A new Wiegand Profile needs to be created to support a 64-bit CSN. This is due to the requirement of reading the CSN from the card. This Wiegand profile is used by the Biometric Device Profile to send the Id encoded on card via OSDP after the Biometric check has been performed.

In *Administration* → *Wiegand Profiles* click on ***Add***.
Give the Wiegand Profile a Name, e.g. *64-bit CSN* and set the Bit Length to 64, then click on ***Next***.
In the *Wiegand Elements* dialog click on ***Add*** and select ***User***, give the element the Name and set the Length to 64, then click on ***Next***.

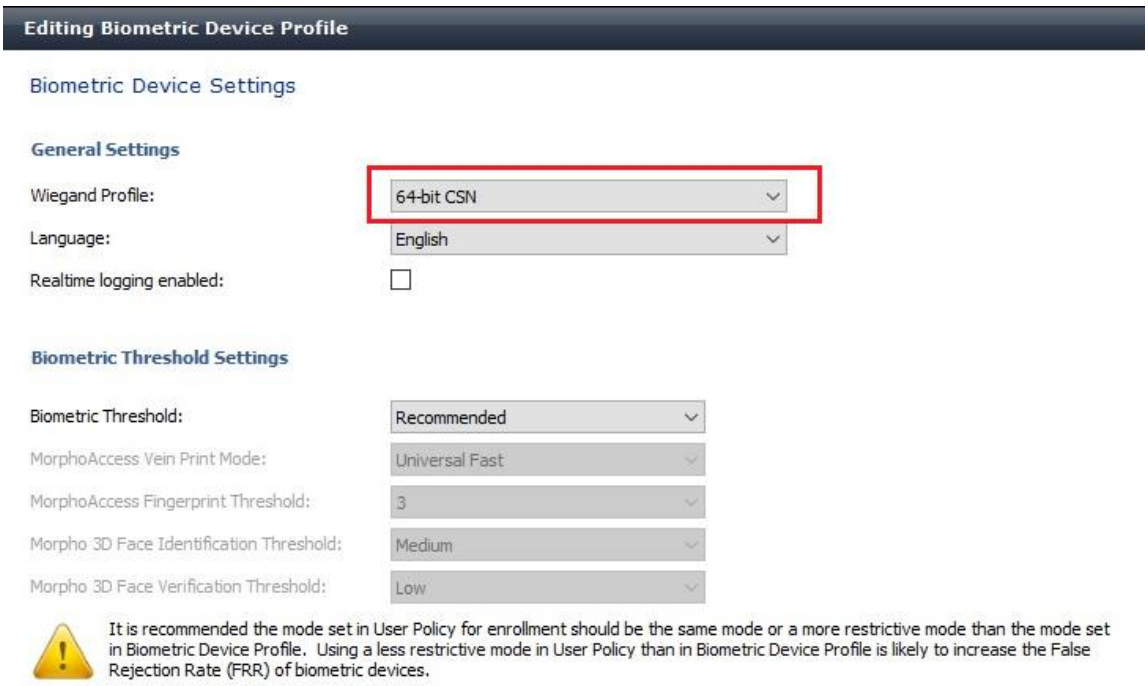


2.4.2 Creating a new Biometric Device Profile

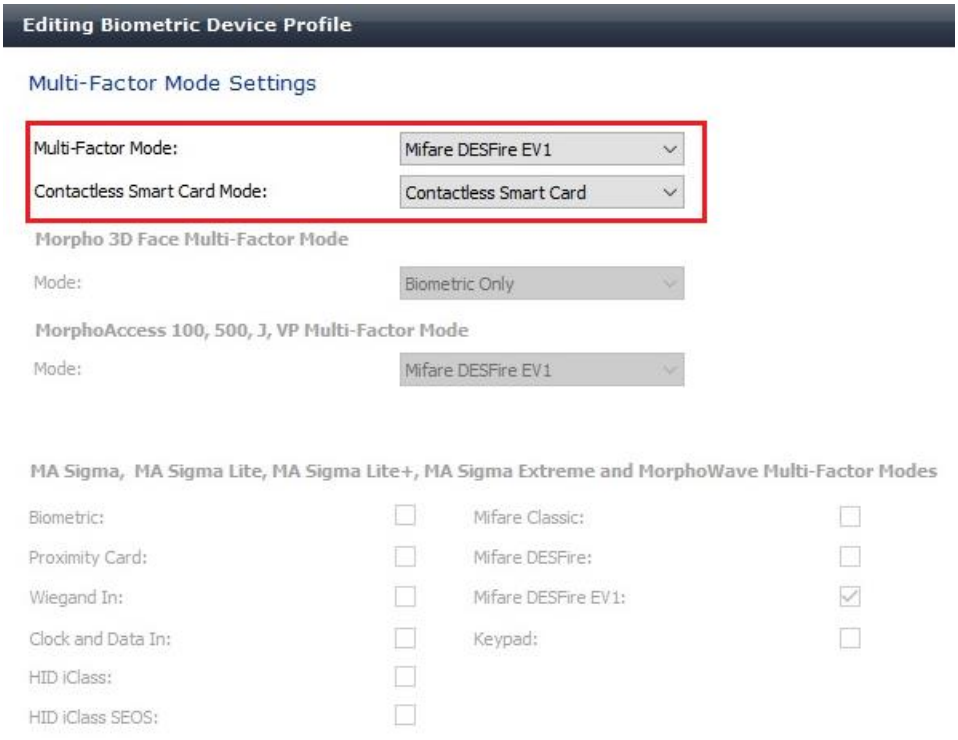
In *Administration -> Biometric Device Profile* select ***Add***. Give the new Biometric Device Profile (BDP) a Name, e.g. DESFire Ev1 CSN with OSDP. Then click on ***Next***.

Let the Key Policy by Default if no customized key for fingerprint encoding is needed. For Encoding with customized key see chapter **Fehler! Verweisquelle konnte nicht gefunden werden.**.

In *Biometric Device Settings* dialog change the Wiegand Profile to **64-bit CSN** profile you created before and then click on ***Next***.



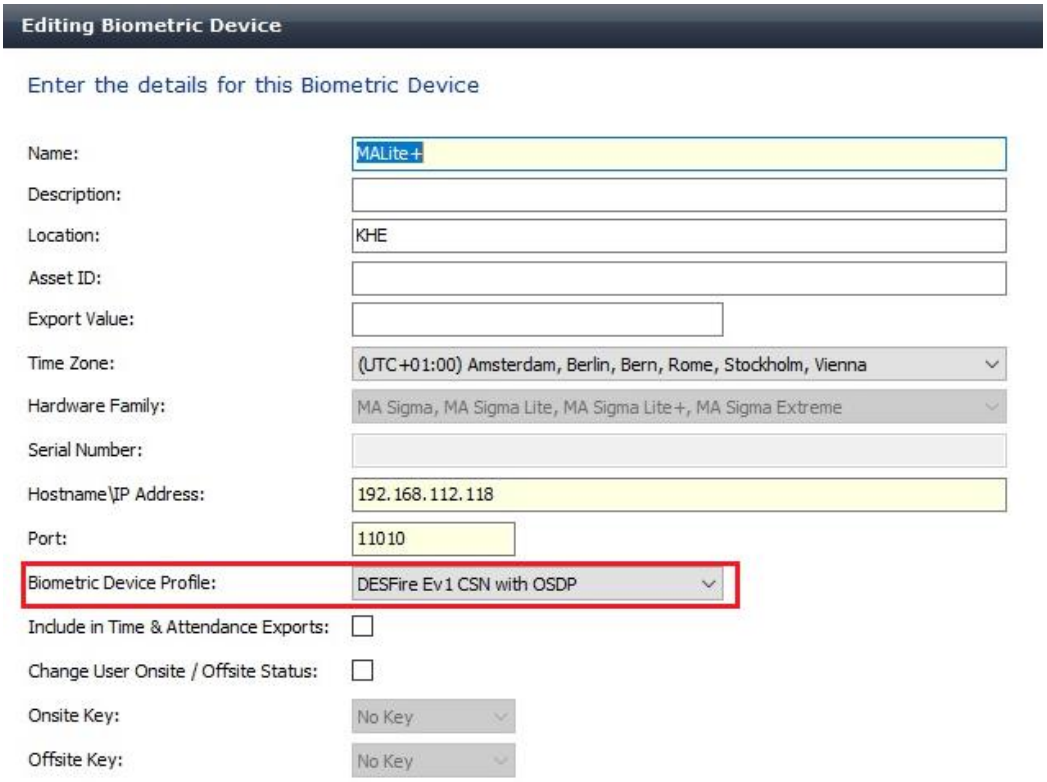
In *Multi-Factor Mode Settings* dialog the following settings are to be done:
- Multi-Factor Mode to ***Mifare DESFire EV1***.
- Contactless Smart Card Mode to ***Contactless Smart Card***.



The screen should show the above settings, click on ***Finish***.

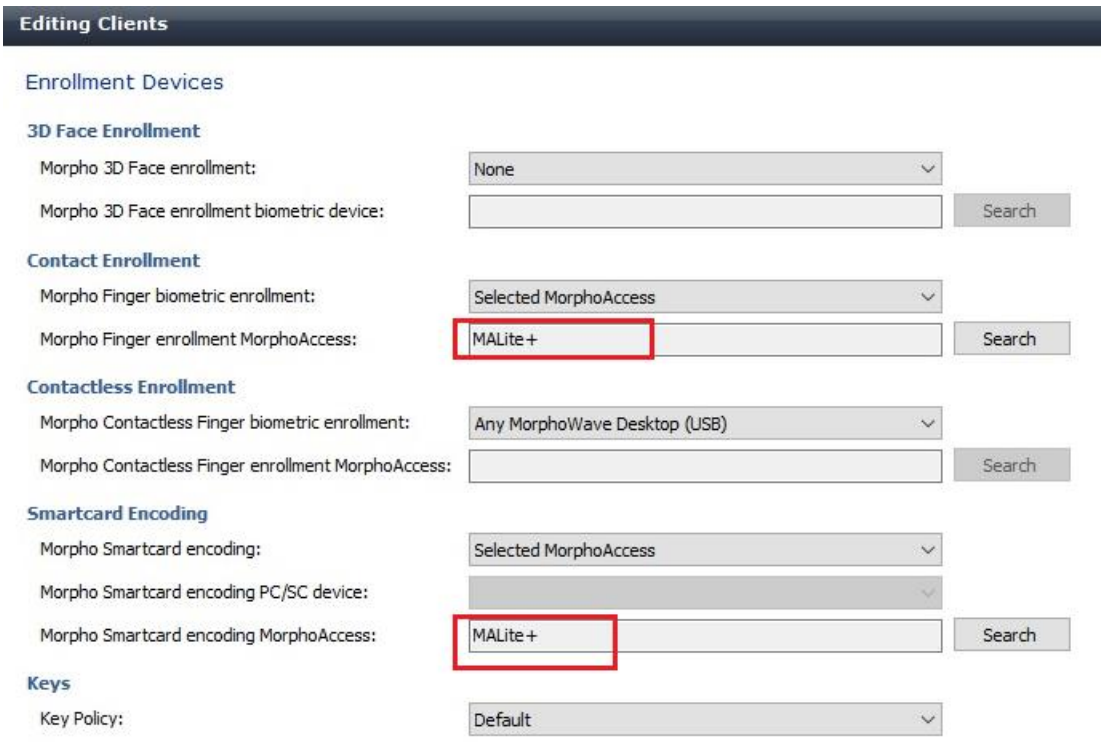
2.4.3 Adding a device to MorphoManager

When a device is added to MorphoManager the Biometric Device Profile created above can be used in the Biometric Device Profile drop down menu to configure the reader.



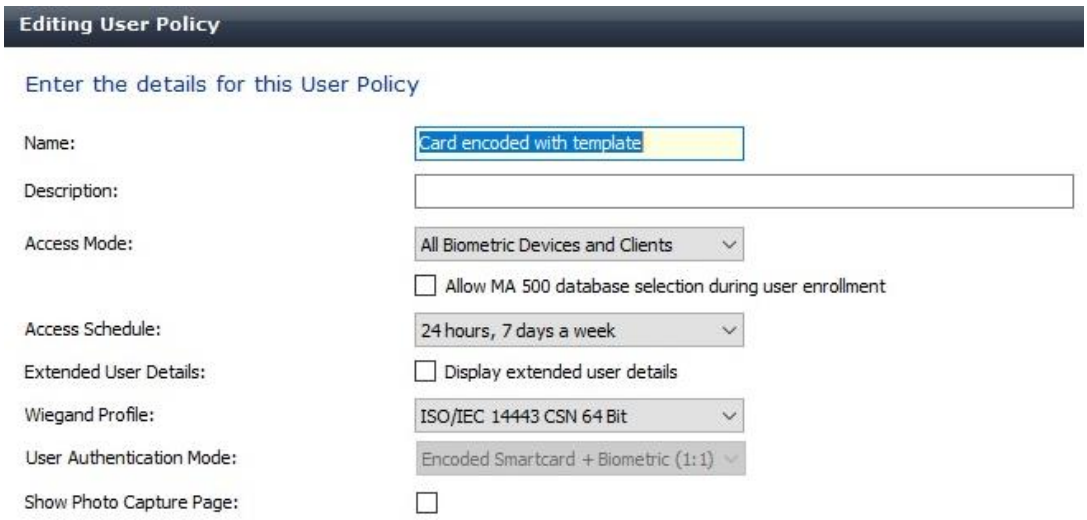
2.4.4 Adding a client to MorphoManager

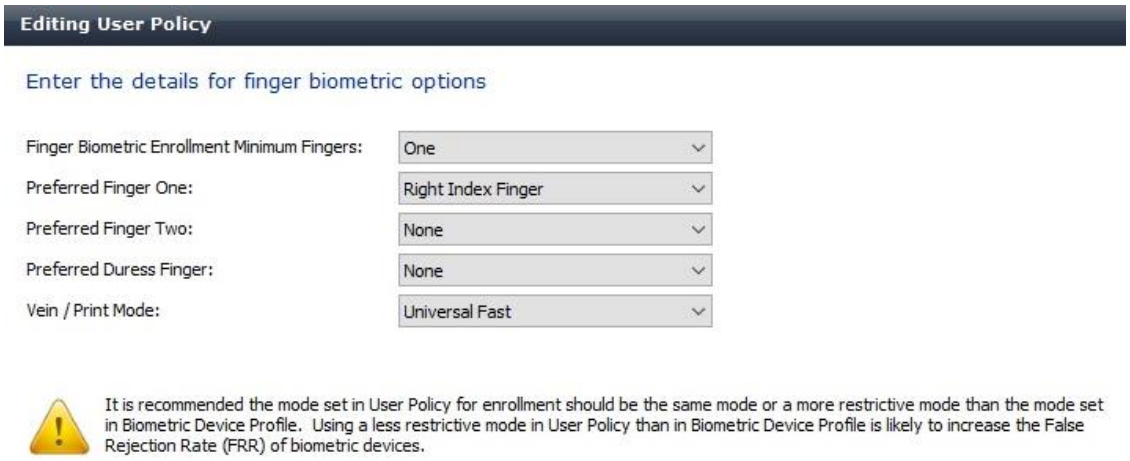
In *Administration -> Clients* select ***Add***. In this dialog your client PC will be added to MorphoManager.
Click to ***Next*** until the dialog *Enrollment devices* will appear.
During this test the card enrolment, encoding and access is done via the same SIGMA reader. That is why the MorphoAccess reader from the list is select by *Contact Enrollment* and *Smartcard Encoding*.



2.4.5 Create a new User Policy for Card plus finger template stored on card

In *Administration -> User Policy* select ***Add***. Give the User Policy a Name e.g. Card encoded with template.
Make the changes below for the new User Policy and then click on ***Finish***.





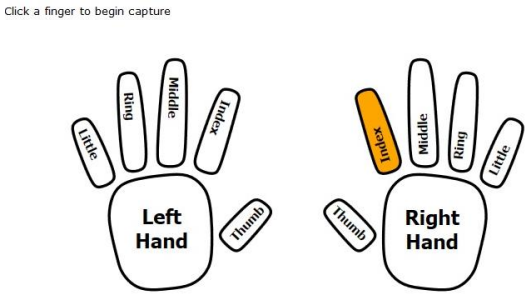
Remark:
The enrolling of two or more fingers is always suggested. Just in case some has to cover an injury with a plaster on their primary finger they can still gain access without needing to re-enrol.

2.4.6 Card Enrolment (Card CSN + fingerprint stored on card)

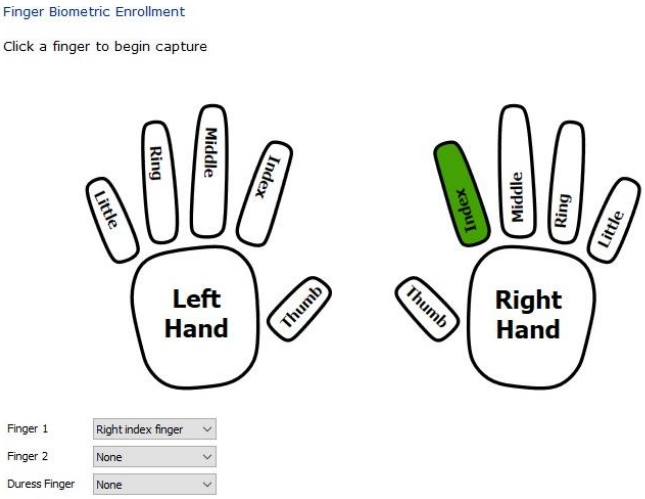
Enrolment will be done in *User Management* menu.
During enrolment process select the required user policy for the user from the drop-down dialog.

Enter the user details and click on ***Next*** for further user details.
In the *Wiegand Values* dialog click on ***Read CSN*** to read the CSN of the card.
Then click on ***Next***.

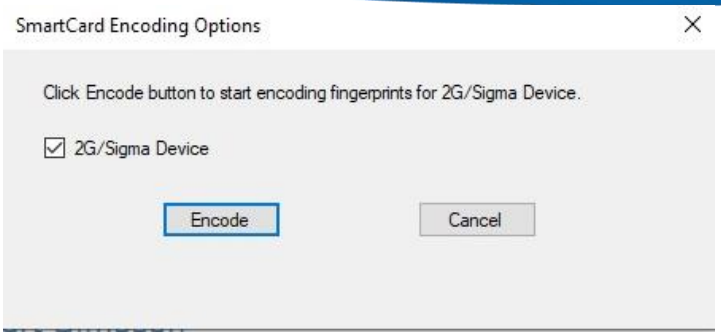
Now click on the finger you would like to enrol.



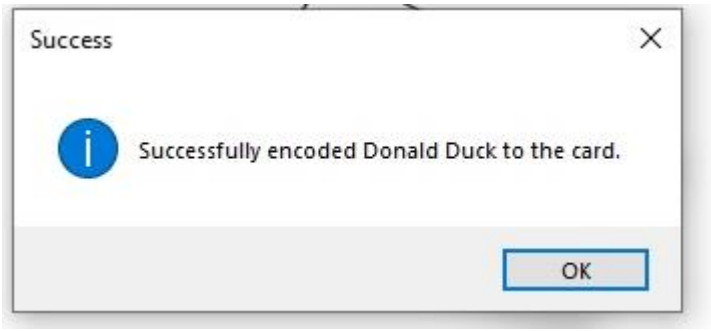
After the fingerprint is successfully enrolled click on ***Next***.



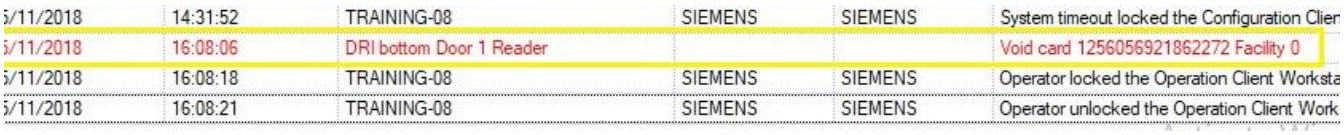
Now click to ***Encode*** to encode the CSN and fingerprint data on card.



During encoding you will be asked to present the card (in this test Mifare DESFire EV1) to encode the information on card.



After successful encoding of the card it is possible to present the card to the SIGMA reader and the card CSN will appear in SiPass integrated audit trail.



5/11/2018	14:31:52	TRAINING-08	SIEMENS	SIEMENS	System timeout locked the Configuration Clien
5/11/2018	16:08:06	DRI bottom Door 1 Reader			Void card 1256056921862272 Facility 0
5/11/2018	16:08:18	TRAINING-08	SIEMENS	SIEMENS	Operator locked the Operation Client Worksta
5/11/2018	16:08:21	TRAINING-08	SIEMENS	SIEMENS	Operator unlocked the Operation Client Work

The encoded CSN of the card can be now added to SiPass integrated system (creating a Cardholder with access rights).

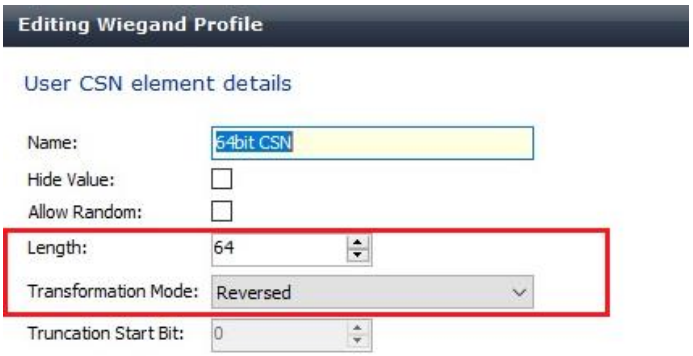
2.4.7 Compatibility of SiPass integrated with SIGMA fingerprint reader from Idemia and VRx0S-MF/ VRx0M-MF reader from Vanderbilt on one site

If there are SIGMA fingerprint readers and Vanderbilt readers VRx0S-MF/VRx0M-MF installed on one site, then the card CSN reading by the reader should be considered.
VRx0S-MF/VRx0M-MF reader reads the card CSN reversed in comparison to SIGMA reader. To get the same card number with SIGMA and Vanderbilt reader a new Wiegand profile with reversed CSN has to be created. This reversed Wiegand Profile has then to be assigned to the User Policy. This User Policy is to be selected during card enrolment.

2.4.7.1 Creating a new Wiegand Profile (for reversed CSN sent via OSDP)

In *Administration → Wiegand Profiles* click on ***Add***.

Give the Wiegand Profile a Name, e.g. *64-bit CSN reversed* and set the Bit Length to 64, then click on ***Next***.
In the *Wiegand Elements* dialog click on ***Add*** and select ***User (CSN)***, give the element the Name, set the Length to 64, select **Reversed** for Transformation Mode, and click on ***Next***.



In *User Profile* dialog select the Wiegand Profile for reversed CSN. Click on ***Finish***.

2.4.7.2 Enrolment of reversed CSN in MorphoManager and in SiPass integrated software

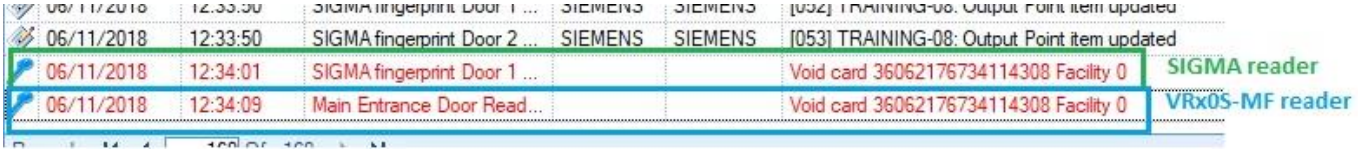
Enrol the user like in chapter 2.4.6 described.

During enrolment process in MorphoManager the CSN of the card is displayed as reversed and this reversed Id will be stored on the card.

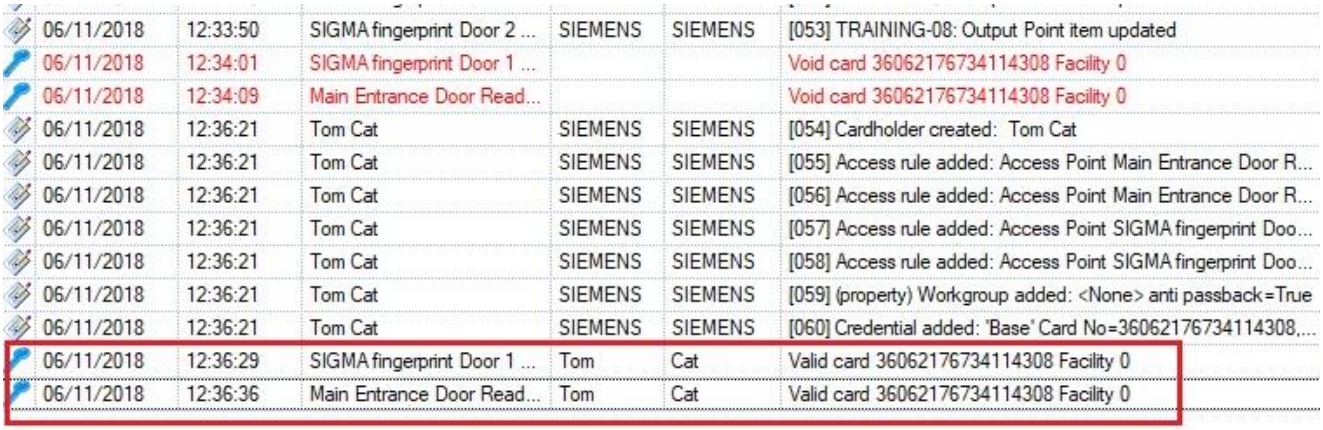
Reversed CSN

After successful card encoding it is possible to badge on the SIGMA reader that is connected to SiPass integrated. In SiPass Audit Trail the reversed CSN number is displayed.

After badging on VRx0S-MF/VRx0M-MF reader, that is connected via RS485 (OSDP) to SiPass, the card number is the same as the card number transmitted by SIGMA reader.



The cardholder can be configured in SiPass integrated software for access:



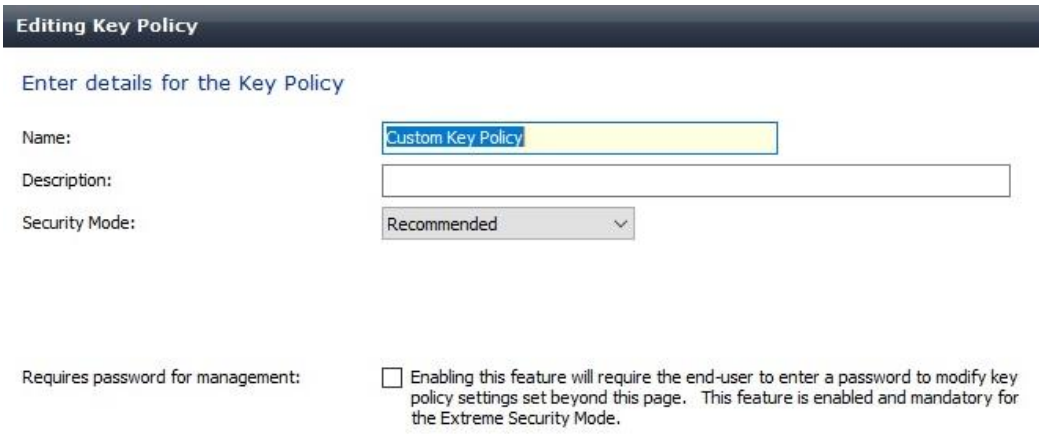
06/11/2018	12:33:50	SIGMA fingerprint Door 2 ...	SIEMENS	SIEMENS	[053] TRAINING-08: Output Point item updated
06/11/2018	12:34:01	SIGMA fingerprint Door 1 ...			Void card 36062176734114308 Facility 0
06/11/2018	12:34:09	Main Entrance Door Read...			Void card 36062176734114308 Facility 0
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[054] Cardholder created: Tom Cat
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[055] Access rule added: Access Point Main Entrance Door R...
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[056] Access rule added: Access Point Main Entrance Door R...
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[057] Access rule added: Access Point SIGMA fingerprint Doo...
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[058] Access rule added: Access Point SIGMA fingerprint Doo...
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[059] (property) Workgroup added: <None> anti passback=True
06/11/2018	12:36:21	Tom Cat	SIEMENS	SIEMENS	[060] Credential added: 'Base' Card No=36062176734114308,...
06/11/2018	12:36:29	SIGMA fingerprint Door 1 ...	Tom	Cat	Valid card 36062176734114308 Facility 0
06/11/2018	12:36:36	Main Entrance Door Read...	Tom	Cat	Valid card 36062176734114308 Facility 0

2.4.8 Customized Key Policy

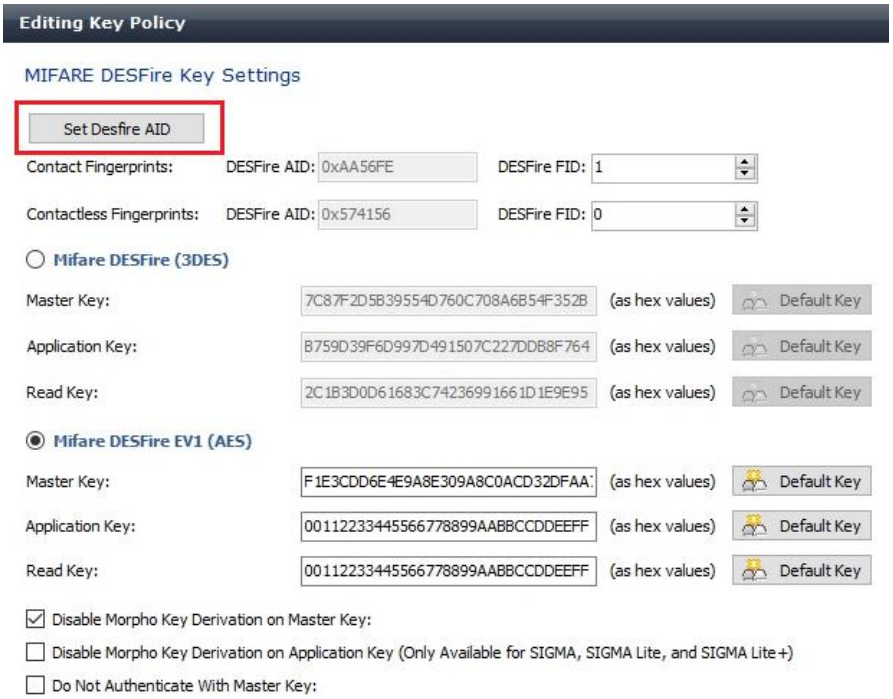
In MorphoManager it is possible to create customized key policy. This option allows the setting of Contactless Card keys and whether they are stored in an encrypted or unencrypted format.

As example the fingerprint of the user has to be stored on card in
AID (Application ID): AA56FE
FID (File ID): 1
Application key: 00112233445566778899AABBCCDDEEFF
Read key: 00112233445566778899AABBCCDDEEFF

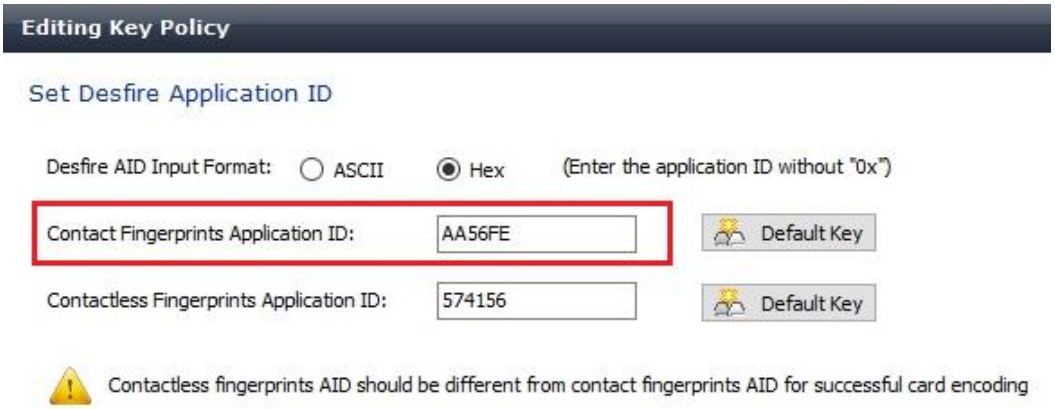
In *Administration* select *Key Policy* dialog and click to ***Add***.
Give the Key Policy a Name, e.g. Custom Key Policy and set the Security Mode to **Recommended** (for more information see MorphoManager User Manual document).



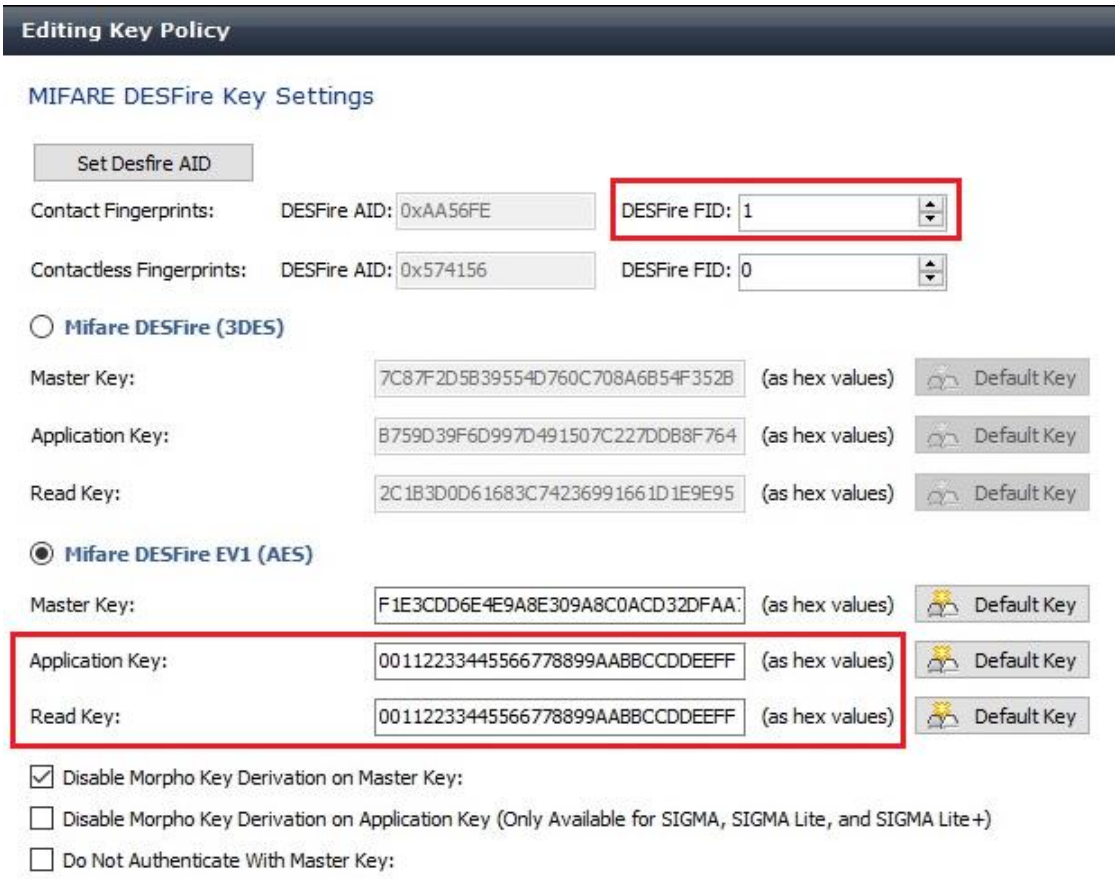
Click to ***Next*** until *MIFARE DESFire Key Settings* dialog appears.



Click the button *Set Desfire AID* and set there the AID to AA56FE:
Contact Fingerprint Application ID: AA56FE

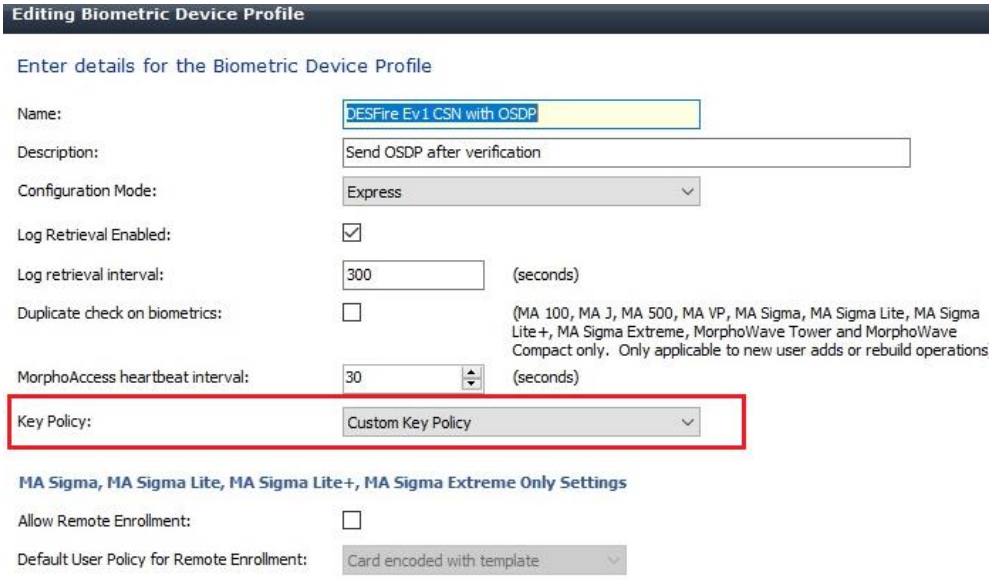


Select *Mifare DESFire EV1 (AES)* and put there the FID 1, the Application Key and the Read Key. Then click to ***Finish***.

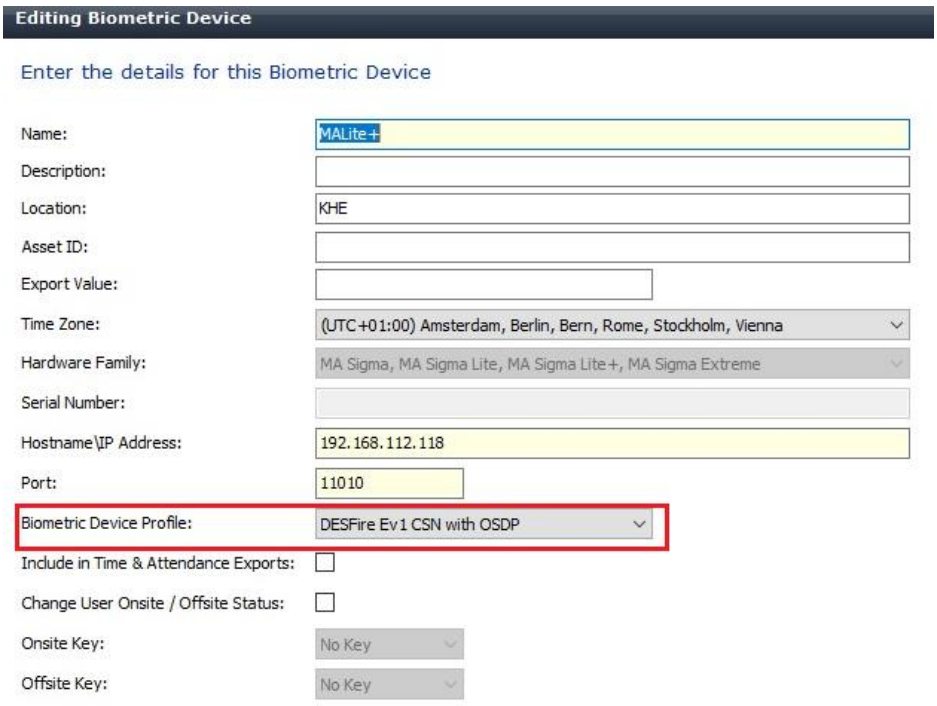


The new created Key Policy can be assigned to the Biometric Device Profile. And the Biometric device Profile will be assigned to the Biometric device. On this way the SIGMA readers will be customized configured to encode and read information with particular key.

In *Administration* go to *Biometric Device Profile* you created before and select there the above created Key Policy. Click to ***Finish***.



In *Administration* go to *Biometric Device* and select there the Biometric Device Profile that has assigned the Custom Key Policy to. Click on ***Finish***.



After this configuration it is possible to encode cards on the way described in chapter 2.4.6. Only the fingerprint will be encoded in AID AA56FE, FID 1 with customized key.

That means that these cards can also be read by this SIGMA fingerprint reader that has these settings assigned to (key policy). The cards encoded for the same AID with another key will not be read by this reader.

2.4.9 Card Only parallel to Card + Fingerprint Template mode

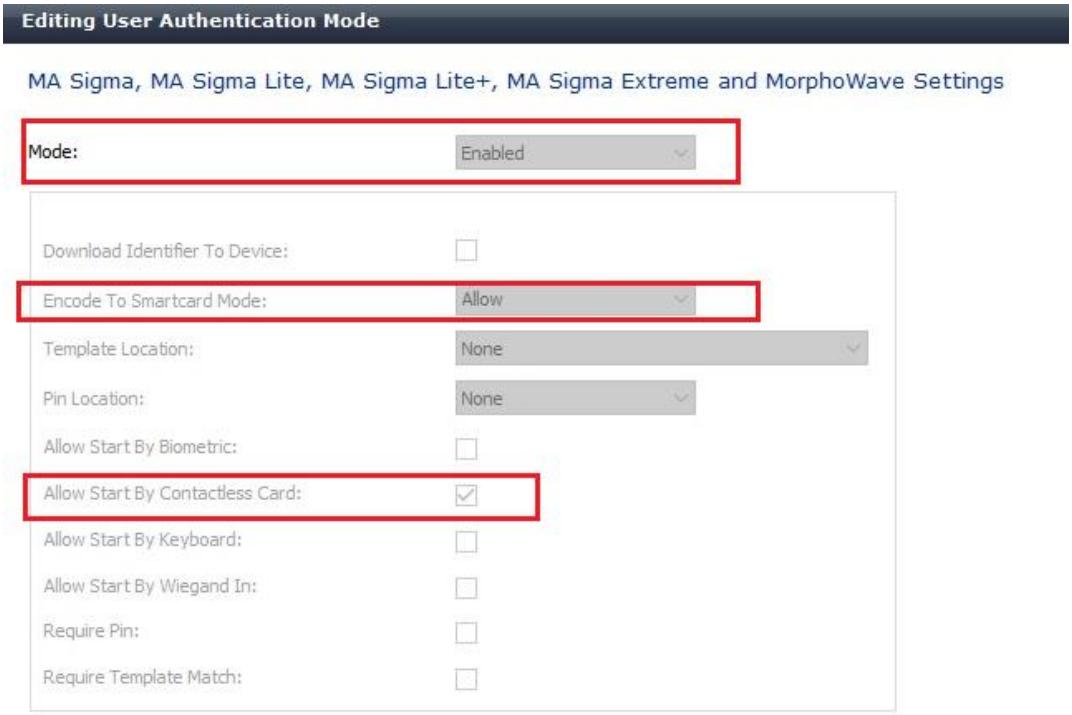
It is also possible to badge with the card only on the SIGMA reader.
For the *Card Only* a new User Authentication Mode and User Policy has to be created.

2.4.9.1 Configuration of new User Authentication Mode and User Policy

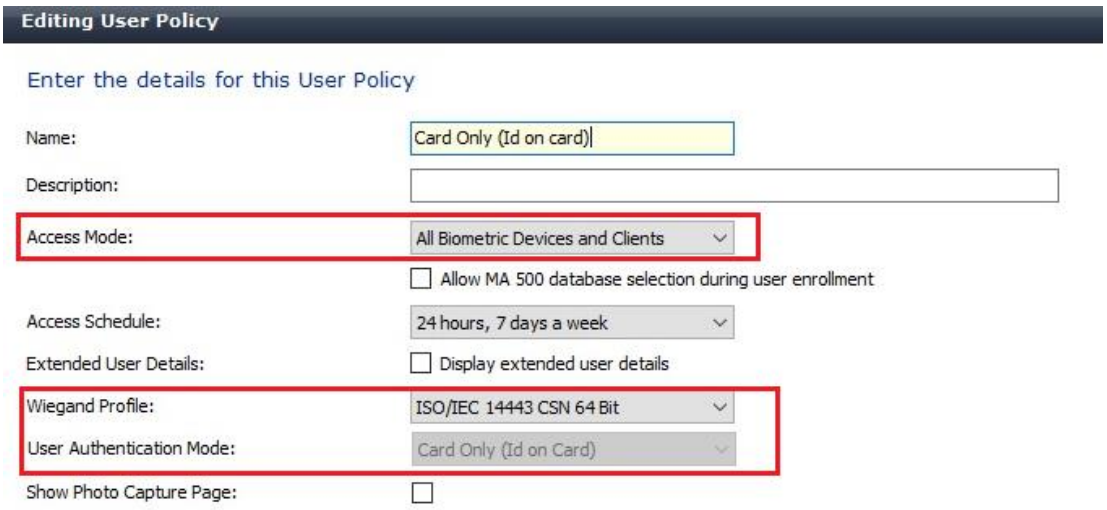
In *Administration* in *User Authentication Mode* click on ***Add***. Give the authentication mode a Name, e.g. *Card Only (Id on card)* and click on ***Next***.

Make the settings like shown below and click on ***Finish***.

Mode: Enabled
Encode to Smartcard Mode: Allow
Allow Start By Contactless Card: activated



The above created User Authentication Mode has to be applied to the new User Policy.
In *User Policy* click to ***Add*** and give a new policy a Name, e.g. *Card only (Id on card)*. Make the settings shown below and click on ***Finish***.



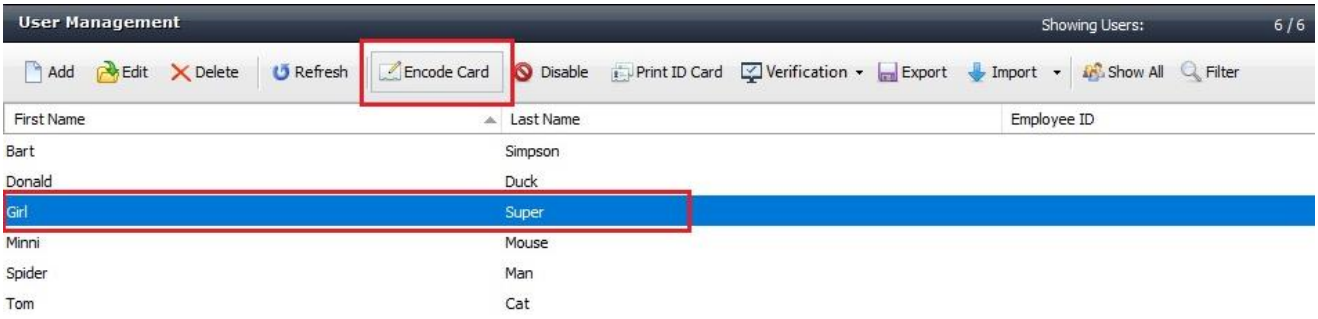
Here the User Policy will encode a card with the CSN of the card but no template. The reader should support Card + Fingerprint Template & Card Only at the same time.

2.4.9.2 Card Enrolment (Card CSN)

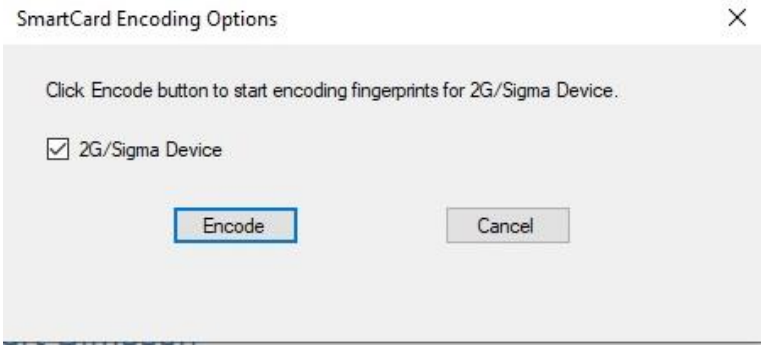
In *User Management* menu ***Add*** a user, select the above created user policy (Card only (Id on card)), enter the user details and click on ***Next***.

In the *Wiegand Values* dialog click on ***Read CSN*** to read the CSN of the card.
Then click on ***Finish***.

Select the enrolled user again and click on the button ***Encode Card***.



Click to ***Encode*** to encode the CSN on card.



If the encoding of card is successful it is possible to badge with this card on the SIGMA fingerprint reader connected to SiPass integrated system. As no fingerprint template is stored on card the card CSN will be enough for access control in SiPass system.

2.5 Summary

The SIGMA fingerprint reader can work properly with SiPass integrated system via RS485 interface (OSDP protocol).
The tested modes are **Card CSN Only** and **Card CSN + Fingerprint Template** (stored on card).
If the customer would like to use SiPass integrated access control system with SIGMA fingerprint readers like tested, then the recommendation is to have an enrolment client PC with MorphoManager software running on it. This enrolment station can be e.g. on the SiPass Client PC. With help of MorphoManager software the cards/users can be enrolled/encoded to be used within SiPass integrated system. According to test results it is possible to use SIGMA readers parallel to Vanderbilt readers VRx0S-MF/VRx0M-MF on site.

SUPPORT INFORMATION

If you have any questions, please contact our Technical Competence Centre.
Contact details can be found on our website.

Vanderbilt International GmbH

Borsigstrasse 34
65205 Wiesbaden
Germany