

SIEMENS



User manual for Configuration Card Creation Tool

Liefermöglichkeiten und technische Änderungen vorbehalten.
Data and design subject to change without notice. / Supply subject to availability.

© 2013 Copyright by Siemens AB

Wir behalten uns alle Rechte an diesem Dokument und an dem in ihm dargestellten Gegenstand vor. Der Empfänger erkennt diese Rechte an und wird dieses Dokument nicht ohne unsere vorgängige schriftliche Ermächtigung ganz oder teilweise Dritten zugänglich machen oder außerhalb des Zweckes verwenden, zu dem es ihm übergeben worden ist.

We reserve all rights in this document and in the subject thereof. By acceptance of the document the recipient acknowledges these rights and undertakes not to publish the document nor the subject thereof in full or in part, nor to make them available to any third party without our prior express written authorization, nor to use it for any purpose other than for which it was delivered to him.

Contents

1	Introduction	4
2	Creating configuration cards.....	5
2.1	Installing the 3CT software and the OmniKey reader	5
2.2	Starting the 3CT program	5
2.3	Creating a new configuration card	5
2.3.1	MIFARE DESFire EV1	7
2.3.2	MIFARE Classic/Plus SL1 in Classic Mode	7
2.3.3	MIFARE Plus SL2	8
2.3.4	MIFARE Plus SL3	8
2.4	Writing the settings on the configuration card.....	8
2.5	Transferring the settings to the card reader.....	8
2.6	Creating additional configuration cards	9
2.7	Viewing and editing the settings saved on configuration cards	9
2.8	Erasing settings from configuration cards.....	9
2.9	Saving settings to a file on disk.....	9
2.10	Opening and editing a saved file from disk.....	9
2.11	Export configuration to SiPass integrated.....	10
2.12	Changing password	10

1 Introduction

The Configuration Card Creation Tool (3CT) is a program which enables required settings to be used for the card readers AR10S-MF, AR11S-MF, AR40S-MF and AR41S-MF. The settings for key and buzzer volume, display time and light frame time amongst others can easily be adjusted to personal preferences and transferred via the programmed configuration card to one or several card readers.

The 3CT kit is delivered with:

- A CD with the software for 3CT.
- An OmniKey reader device which writes the required data to the configuration cards.
- MIFARE DESFire EV1 cards, pre-programmed for the purpose.



Information

Please note that the configuration cards created with 3CT may contain information which is vital to the system security – ensure that they are stored in a safe place.

2 Creating configuration cards

2.1 Installing the 3CT software and the OmniKey reader

1. Install the 3CT software and the OmniKey reader by inserting the CD and follow the instructions in the wizard.
2. Connect the OmniKey reader to the computer with the USB cable.

2.2 Starting the 3CT program

1. Open the program **3CT** from the **Start Menu**. The window 3CT opens.
2. In the dialog window, select one of the new types of cards which can be created:
 - **Standard configuration card** – for using all possible settings.
 - **Set Reader Address only** – the reader address but no other information is displayed in the window New card.
 - **Restore Reader to factory settings** – the configuration card will reset the card reader to factory settings.
 - **Open file** – opens a configuration saved to file on disk.
 - **Read card** – reads configuration from a configuration card.
3. Ensure that the correct OmniKey reader is installed by opening **Card>Select reader**. The pop-up window 3CT Reader selection opens.
4. In the dropdown menu, ensure that the **OMNIKEY CardMan 5x21-CL 0** is selected. Click **OK**.

2.3 Creating a new configuration card

Follow the instructions for the respective card type:

- **Set Reader Address only** and **Restore Reader to factory settings**, continue on section 2.4 *Writing the settings on the configuration card on page 8*.
- **Standard configuration card**, follow these instructions:
 1. In the tab **New Card**, enter a **Description**. This description can be used to distinguish between different configuration card settings.
 2. Click the tab **Behaviour**.
 3. In the field for **Keyboard Backlight**, select one of the following:
 - **Always on**
 - **On when active for xx seconds**
 - **Off**.
 4. In the field for **Buzzer volume**, select the settings for:
 - **Key press feedback** – the sound which the card reader will give when a key is pressed.
 - **Card Read feedback** – the sound which the card reader will give when a card is read.

- **System sounds** – the sounds which are programmed in the system which the card reader is connected to.
- 5. In the tab for **Visual and Display options**:
 - Select the appropriate for each colour of **Light frame follows LED indicators** if the light frame of the card reader should act as the light settings of the specific LED indicator.
- 6. Select the seconds for **Message duration**, 1 – 60.
- 7. In the drop down menu following **Alphabet**, select the required alphabet:
 - **Latin1** for Western European languages
 - **Cyrillic** for Russian
- 8. Click the tab **Communication**.
- 9. Tick **Include Card reader address on Configuration Card** and select 0 – 8 in the dropdown menu, should the configuration card set this address. Address 0 is default and will make the ERI/DRI set the address to the next free address on the reader bus.
- 10. In the field **OSDP Communication**, select one of three choices if the card reader should:
 - **Keep current setting for OSDP communication**
 - **Activate secure OSDP communication**, enter the **OSDP Encryption Key** in the field
 - **Deactivate secure OSDP communication**

Please note that secure OSDP communication is only supported in SiPass integrated with version 2.65 or higher. Please read more in section 2.11 Export configuration to SiPass integrated on page 10.
- 11. Select **Flash yellow LED on lost communication** if the card reader should indicate accordingly.
- 12. Click the tab **Card Types**.
- 13. Select how this configuration card should configure the reader card types:
 - **Read UID on all card types (factory default)**
 - **Keep card type configuration in reader**
 - **Configure the reader to use the following card types** - For this option select card types according to the access cards which will be used for the card reader the reader should support.
- 14. A tab for each selected access card opens. Please refer to the respective access card to continue:
 - **MIFARE DESFire EV1** on page 7
 - **MIFARE Classic/Plus SL1 in Classic Mode** on page 7
 - **MIFARE Plus SL2** on page 8
 - **MIFARE Plus SL3** on page 8

2.3.1 MIFARE DESFire EV1

1. In the field for **Card data**, select the data for:
 - **Read UID**
 - **Read Memory**
 - **Report card data to system**
 - **As read from card**
 - **Reverse bits**
 - **Reverse bytes**
2. In the field for **Memory Definition**, fill out the data for:
 - **Application ID**
 - **File ID**
 - **Start bit**
 - **Number of bits**
3. Select the **Communication between the card and card reader**:
 - **Send card data in plain text**
 - **Send card data enciphered**
4. To update and/or set the key, tick the box for **Include Key settings on Configuration Card**:
 - Fill out the data for **Key**.
 - Select **Key number**.
5. In the menu, open **File** and **Save** the settings.

2.3.2 MIFARE Classic/Plus SL1 in Classic Mode

1. In the field for **Card data**, select the data for:
 - **Read UID**
 - **Read Memory**
 - **Report card data to system**
 - **As read from card**
 - **Reverse bits**
 - **Reverse bytes**
2. In the field for **Memory Definition**, fill out the data for:
 - **Sector**
 - **Block**
 - **Start bit**
 - **Number of bits**
3. To update and/or set the key, tick **Include Key settings on Configuration Card**:
 - Fill out the data for **Key**.
 - Select **KeyA** or **KeyB**.
4. In the menu, open **File** and **Save** the settings.

2.3.3 MIFARE Plus SL2

1. In the field for **Card data**, select the data for **Report UID to system**:
 - **As read from card**
 - **Reverse bits**
 - **Reverse bytes**
2. In the menu, open **File** and **Save** the settings.

2.3.4 MIFARE Plus SL3

1. In the field for **Card data**, select the data for **Report UID to system**:
 - **As read from card**
 - **Reverse bits**
 - **Reverse bytes**
2. In the menu, open **File** and **Save** the settings.

2.4 Writing the settings on the configuration card

1. Place the configuration card in the plastic slot on the reader. In the user interface, click **Write**.
2. A pop up window will confirm that the data is written on the configuration card. Click **Ok**.

Please note that any authentication key written to the card cannot be read by 3CT. To save an authentication key for later use in 3CT, the configuration should be saved on a password protected file.

2.5 Transferring the settings to the card reader

1. Bring the configuration card to the card reader.
2. Turn off the card reader.
3. Place the configuration card in close proximity to the card reader.
4. Turn on the card reader.
5. The light frame will flash green and a sound will confirm that the card reader has registered the settings.

2.6 Creating additional configuration cards

1. Open **File>New**. The pop up window **New Configuration Card** is displayed.
2. Select one of the new types of cards which can be created:
 - **Standard configuration card** – for using all possible settings.
 - **Set Reader Address only** – the reader address but no other information is displayed in the window New card.
 - **Restore Reader to factory settings** – the configuration card will reset the card reader to factory settings.
3. Continue to follow the instructions for *Creating a new configuration card* on page 5.

2.7 Viewing and editing the settings saved on configuration cards

1. Place the configuration card on the OmniKey reader.
2. Open **Card>Read**. The settings are displayed in a tab in the user interface.
3. For editing the settings, follow the instructions for *Creating a new configuration card* on page 5.

2.8 Erasing settings from configuration cards

In order to erase saved settings from configured cards:

1. Place the configuration card on the OmniKey reader.
2. Select **File>Erase**.
3. In the pop up window, confirm that the settings are to be erased by clicking **OK**.

2.9 Saving settings to a file on disk

1. Select **File>Save** to save the configuration settings on disk. If there are authentications keys these will only be saved to file if a password is entered upon request. If entered, the password will be used to encipher the authentication keys to preserve integrity.
2. The selection **File>Save As** can be used to save the current file to a new file.

2.10 Opening and editing a saved file from disk

1. To read and edit a file saved on disk, select **File>Open**. If the file contains authentication keys, a password needs to be entered in order to decipher these. If the password is not entered, all other parts of the file can still be read.
2. For editing the settings, follow the instructions for *Creating a new configuration card* on page 5.

2.11 Export configuration to SiPass integrated

SiPass integrated version 2.65 SP1 and higher can send configuration data created in 3CT over the reader bus to the card reader. To accomplish this, the configuration data is exported to a file which can be imported into SiPass integrated. Please refer to the SiPass integration documentation on how to do the import. To preserve the integrity of the configuration data, the exported file is enciphered using a password. The OSDP settings for the reader bus are carried out in the SiPass integrated user interface. Thus, the OSDP settings are not saved in the 3CT exported file.

1. To export configuration data for SiPass integrated select **File>Export for SiPass integrated**.
2. Enter a **Password** to use for enciphering the file. This password will be needed when importing the file into SiPass integrated.

2.12 Changing password

1. To change the password used for enciphering of authentication keys and/or export to SiPass integrated, select **File>Set password**.
2. Enter a **Password** to use for enciphering the file. The new password entered will be used when saving a file to disk, and/or when exporting to SiPass integrated.

Issued by
Siemens AB
Security Products
International Headquarters
Englundavägen 7
SE-171 24 Solna
Tel. +46 8 629 0300

www.siemens.com/securityproducts

© 2013 Copyright by Siemens AB

Data and design subject to change without notice.
Supply subject to availability.

Document no. **A-100003-7**
Edition 10.2013