

Class 2 Smart Card Reader SPR532

User Manual



Table of Contents

1	INTRODUCTION.....	3
1.1	IMPORTANT NOTES	3
1.2	CERTIFICATION LABEL	3
1.3	STANDARDS	3
1.4	SYSTEM REQUIREMENTS	3
1.5	APPLICATIONS	4
2	INSTALLATION	5
2.1	DRIVER, FIRMWARE UPDATE (DFU).....	5
2.2	HARDWARE.....	8
2.2.1	<i>SPR532 Serial</i>	8
2.2.2	<i>SPR532 USB</i>	8
3	CONTROL ELEMENTS	9
3.1	KEYPAD	9
3.2	LED-STATUS AND ACOUSTIC SIGNALS (BUZZER)	10
4	PIN-ENTRY	11
5	SECURITY	11
5.1	SECURITY FUNCTIONS OF THE SPR532	11
5.1.1	<i>Secure PIN-entry</i>	11
5.1.2	<i>Clear memory</i>	11
5.1.3	<i>Secure firmware download</i>	11
5.1.4	<i>Tampering</i>	11
5.2	USAGE SECURITY RECOMMENDATIONS	12
5.2.1	<i>Secure environment</i>	12
5.2.2	<i>Verification of the firmware version</i>	12
5.2.3	<i>Verification of the seal</i>	12
5.2.4	<i>Secure handling of the PIN</i>	13
5.2.5	<i>HBCI- and signature cards</i>	13
6	TROUBLESHOOTING	14
6.1	DRIVER	14
6.2	SPR532 SERIAL	14
6.3	SPR532 USB	14
7	SUPPORT	15
7.1	LATEST DRIVERS AND FIRMWARE UPDATES	15
7.2	TECHNICAL SUPPORT	15
7.3	HOTLINE	15
7.4	ADDITIONAL INFORMATION	15
8	ABBREVIATIONS	16

1 Introduction

The SPR532 is available with hybrid RS-232 and USB interchangeable cable.

These operating instructions describe the installation of the SPR532 and give a detailed description of the adaptation on the appropriate interface.

1.1 Important notes

Before setting up the SPR532, please examine whether the housing and the seal on the lower surface are intact (see also Chapter 5.2.3). The hardware is developed in such a way that when opening the housing, the internal mounting plates break off and the seal is destroyed. Thus any kind of tampering can easily be recognized. In case of suspicion of tampering please refer to your dealer and/or to your local SCM Microsystems branch.

1.2 Certification label

The SPR532 with firmware version (V5.10) is certified and confirmed to be in accordance with the German signature law dated 16 May 2001 based on Common Criteria. Thus it allows you to use it for qualified digital signatures. Please verify the firmware version with the program FWV510_Check.exe, which is part of the installation software, before using the reader. Before updating the firmware please visit http://www.bsi.de/zertifiz/zert/index_en.htm to obtain information regarding the certification. If the firmware version is not contained in the list of the certified products, the reader must not be used for applications in accordance with the German signature law (SigG).

Certification to Common Criteria EAL3+ (high): BSI-DSZ-CC-0394
Confirmation in accordance with the German signature law from 16 May 2001 (SigG): BSI.02080.TE.XX.2006

Please read the security information in Chapter 5 before using the reader.

1.3 Standards

The SPR532 is a class 2 card reader, compatible with the software standards CT-API and PC/SC as well as the Microsoft USB CCID protocol. With this reader you can use all ISO7816- and EMV2000-compatible cards, e.g. the German HBCI card and GeldKarte as well as all signature-law-conformed smart cards. For further information about the different standards and protocols, please refer to Chapter 7.4 "Additional information".

1.4 System requirements

To install the SPR532 you need a PC with one of the following operating systems:

- Windows® 95
- Windows® 98
- Windows® 98 SE
- Windows® ME
- Windows NT®
- Windows® 2000
- Windows® XP

Please be aware that Windows® 95 and Windows NT® do not support USB. In this case, you must use the serial version of the SPR532. If you are using Windows® 98, it is recommended to install Windows® 98 Second Edition (SE) with extended USB support. In order to install the software you need a CD-ROM drive. For the serial version of the SPR532 you need both a COM and a PS/2 port. The USB version requires a free USB port. For further information refer to Chapter 2, "Installation".

1.5 Applications

The integrated keypad the SPR532 allows you secure PIN-entry and is therefore suitable for HBCI banking and signature-law-conformed applications in the home and office environment. Secure PIN-entry ensures that the PIN is only transmitted to the smart card and never leaves the reader or is transmitted to the PC (host). Contact your bank for further information regarding HBCI and the required smart card.

2 Installation

2.1 Driver, firmware update (DFU)

Insert the installation CD-ROM into your CD-ROM drive, the setup program will initiate automatically. If not, please double click on the file "setup.exe". Follow the instructions and restart the computer if necessary (USB version) or shut it down (serial version), before you attach the smart card reader.

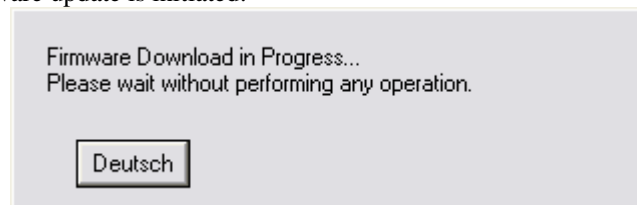
The setup automatically checks the firmware version of the connected SPR532 reader. If the firmware version is lower than the actual version V5.10, it will update the firmware version. This step guarantees that SPR532 readers (in particular readers with firmware version V4.15 - part number 903391, certification label CC:TUVIT-DSZ-CC-9209, SigG:TUVIT.09370.TE) as well as readers with the firmware version V5.09 – part number 904712, certification label CC:BSI-DSZ-CC-0363, SigG:BSI.02072.TE.XX.2006) are compliant to industry software requirements including:

- PC/SC 2.0 part 10 PIN handling,
- ZKA-Sig-API (German banking signature API),
- SASCIA (German signature alliance API) and
- OpenSource CCID driver.

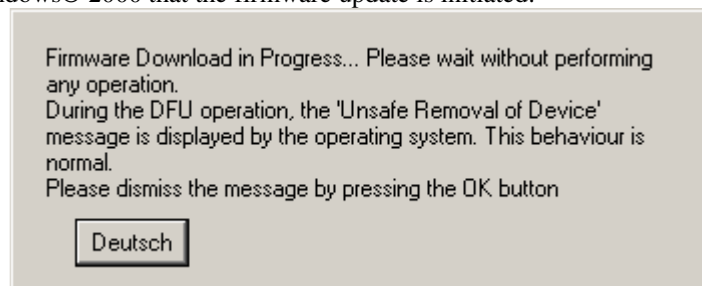
Certified and confirmed, as well as uncertified firmware versions are available for download. Certified and confirmed versions are explicitly marked under indication of the certifying and confirmation ID. This ID is shown on the Internet page of the German federal net agency "Bundesnetzagentur" under the subject telecommunications, electronic signature. If the user is downloading uncertified firmware, he or she will be informed about this fact.

After the installation you may also set the firmware update manually to update further SPR532 readers. For that purpose, the firmware update tool DFUWrapper.exe (under Windows® 98/ME/2000/XP) has to be initiated over the appropriate program group or from the installation directory.

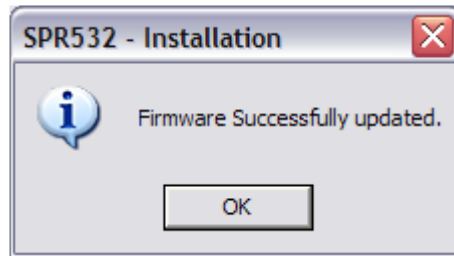
Information that the firmware update is initiated:



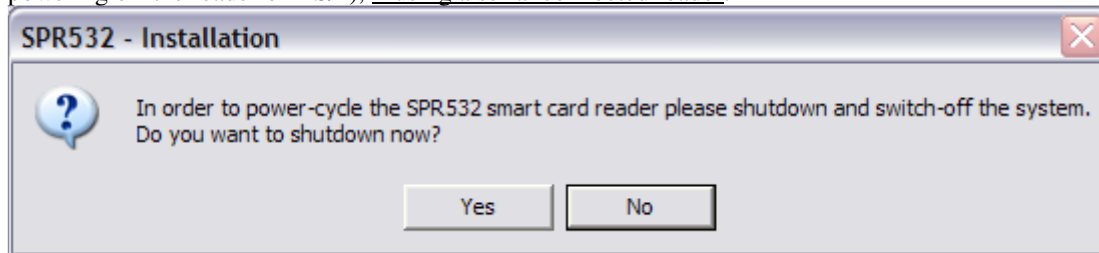
Information under Windows® 2000 that the firmware update is initiated:



Information about the successful firmware download:

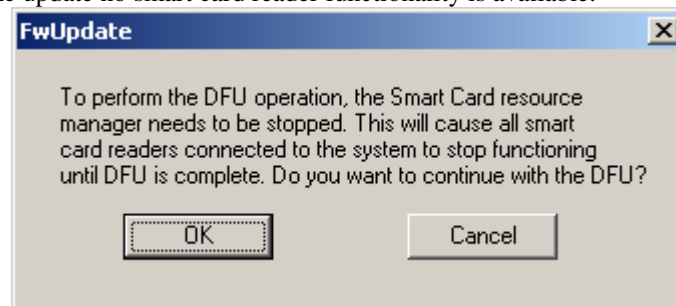


After checking for and installing firmware updates, you must shut down and switch off the computer (including powering off the reader on PS/2), if using a serial connected reader:

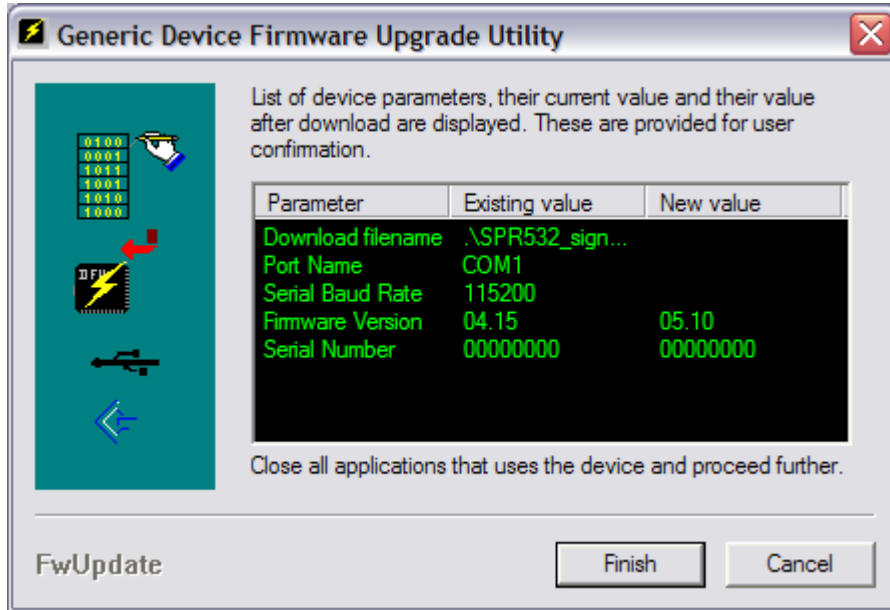


Under Windows NT4® the firmware update tool fwupdate.exe has to be initiated over the appropriate program group or from the installation directory. During the firmware update the following screens must be confirmed with "OK", "Finish" and "Close".

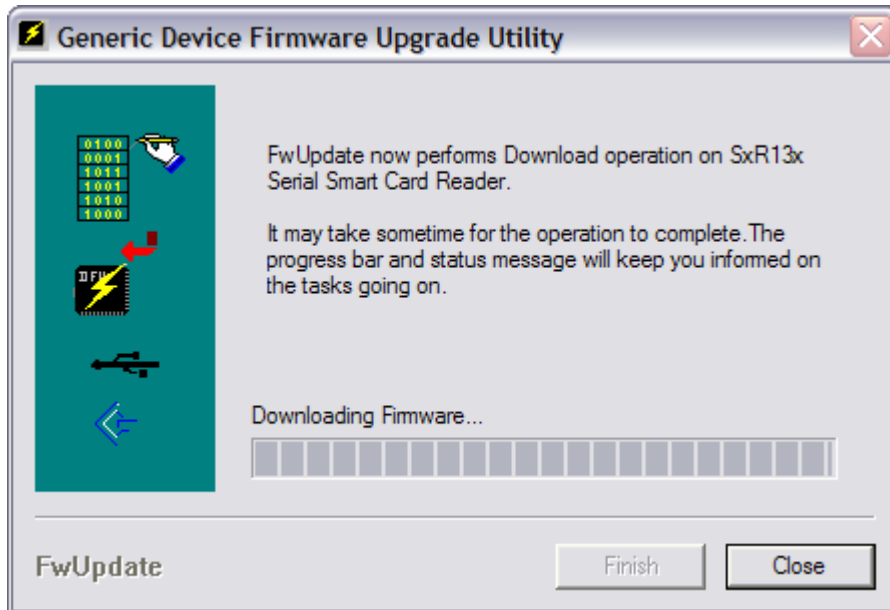
Reference that during the update no smart card reader functionality is available:



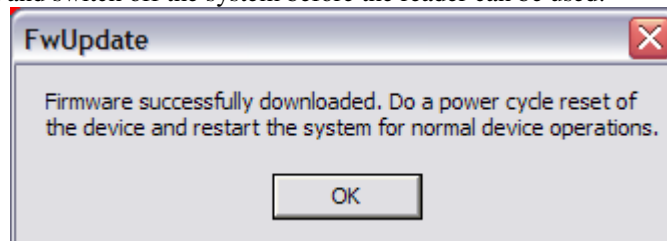
Information about the firmware on the smart card reader and the firmware that can be loaded:



Information about the successful firmware download:



Instruction to shut down and switch off the system before the reader can be used:



2.2 Hardware

The SPR532 is delivered with a hybrid connector, which enables you to attach the reader to the serial or USB interface by plugging in the appropriate cable. The serial as well as the USB adaptor must be connected to the reader before attaching it to the PC. The adaptor cable must not be exchanged when the device is connected to the PC.

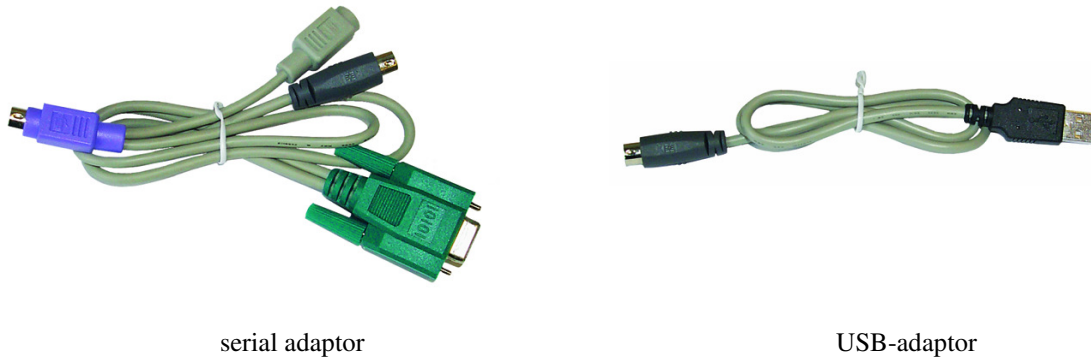


Fig. 2.1: adaptor cable

2.2.1 SPR532 Serial

If you are working with the serial version of the SPR532, shut down and switch off the computer before attaching the smart card reader. Never attach or remove the device during operation as it may cause permanent damage of your PC or SPR532.

Connect the SPR532 hybrid cable with the serial cable supplied with your smart card reader. Attach the serial plug of the cable to the serial interface (COM port) of your PC. Put the PS/2 plug between the keyboard and the PC. This connector is required to power the smart card reader. If you now start the PC, Windows® will recognize the SPR532 automatically and load the appropriate driver.

2.2.2 SPR532 USB

Connect the SPR532 hybrid cable with the USB cable supplied with your smart card reader. Plug the black USB type A connector into one of the PC's free USB connectors. Windows® will recognize the SPR532 automatically and load the appropriate driver. If your PC has no more USB ports available, you can use a USB hub to extend the number of USB ports. Please note that active hubs require their own power supply.

3 Control elements

3.1 Keypad

The SPR532 is equipped with an integrated keypad that allows you to securely enter your PIN:



Function

Numeric keypad	Numeric keys 0 - 9
C	Clear
x	Cancel
✓	Confirmation

Fig. 3.1: SPR532 keypad

3.2 LED-status and acoustic signals (buzzer)

The SPR532 has two LEDs and a buzzer to indicate the actual operating mode or possible malfunctions. Always install the SPR532 in such a way that you can see both LEDs. Together with the buzzer, they indicate the following states:

Status	LED1 (green)	LED2 (orange)	Buzzer	
Power on, DFU* completed	Off	Off	740 Hz/25 ms	
Reader active	On 0.5 s Off 4.5 s	Off	Off	
Smart card active	On	Off	Off	
Smart card communication	On 0.5 s Off 0.5 s	Off	Off	
Secure PIN-entry active	On	On 0.5 s Off 0.5 s	0-9	2400 Hz/25 ms
			C	1100 Hz/25 ms
			✖	1100 Hz/25 ms
			✓	1100 Hz/25 ms
			PIN-entry successful	900 Hz/100 ms 1200 Hz/100 ms
			PIN-entry failed	300 Hz/100 ms
PIN-entry successful, smart card active	On	On	Off	
PIN-entry successful, smart card communication	On 0.5 s Off 0.5 s	On	Off	
Smart card communication failure	On 100 ms Off 100 ms	Previous state	Off	
Self-test failed during boot	On 100 ms Off 100 ms	Previous state	Off	
DFU* running	Off	On	Off	
DFU* failed	Off	On 32 ms Off 32 ms	Off	
BootROM Mode	On	On	Off	

* Device firmware upgrade

4 PIN-entry

By using the integrated keypad, the SPR532 guarantees secure PIN-entry. This feature must be supported by the application being used.

Secure PIN-entry is only guaranteed when using the numeric keypad. During the entry, you can verify secure PIN-entry mode by checking the LED-status of the SPR532 (table "LED-status and acoustic signals"). Confirm the PIN with [✓] or cancel the entry with [✖]. You can erase and re-enter the PIN by pressing the [C] key.

Important: The PC keyboard is not suitable for secure PIN-entry. Always use the integrated keypad of the smart card reader. Detailed information about the security functions is covered in Chapter 5 "Security".

5 Security

5.1 Security functions of the SPR532

5.1.1 Secure PIN-entry

The SPR532 is a class 2 card reader. Therefore the PIN verification is performed between the smart card reader and the smart card. As the PIN never leaves the smart card reader or is transmitted to the PC it is impossible for other applications (e.g. spy software) to get knowledge of the PIN.

5.1.2 Clear memory

To guarantee a maximum level of security, the PIN is erased from the SPR532 memory immediately after it is not needed anymore.

PINs are erased from the reader's memory in the following instances: during the power-on procedure, after transmission of the command to the smart card, after pulling the card, in case of an abort by the user, with a timeout during the PIN input and after defined resetting commands from the host.

5.1.3 Secure firmware download

The verification of a signature of the firmware with the hash algorithm SHA-1 and the asymmetrical RSA algorithm with a bit length of 1024 guarantee the integrity and authenticity of the firmware while loading the firmware into the smart card reader.

5.1.4 Tampering

On its bottom casing, the SPR532 is equipped with a falsification-safe seal. This allows you to recognize if someone opened the housing to perform any manipulations of the hardware. Please verify regularly if the seal is still intact (Chapter 5.2.3) before using the reader. Also make sure that the SPR532 is directly attached with the respective interface (USB/serial port). There must be no other devices between the PC and the smart card reader with the exception of a USB hub, when needed.

5.2 Usage security recommendations

To get the optimal security functions of the SPR532, please read the following recommendations carefully. Aside from keeping the PIN secret and a secure installation environment, the user is also responsible for a regular examination of all security functions of the SPR532.

Before using the SPR532, make sure that no security-relevant changes were made with the smart card reader by checking the intactness of the security seal (see Chapter 5.2.3). In case of suspected tampering, the user takes full responsibility for continued use of the device as such tampering may have affected the security features. It is recommended to discontinue use and to contact your dealer or your local SCM Microsystems branch.

The SPR532 is exclusively designed for home and office usage and therefore not suitable for any kind of publicly accessible areas.

5.2.1 Secure environment

It is recommended that you install the SPR532 in an area where access by unauthorized individuals is avoided and an unobserved PIN-entry is guaranteed.

5.2.2 Verification of the firmware version

Verify the firmware version regularly. This allows you to ensure that the smart card reader is always operating with the certified firmware (V5.10). To check the firmware version, please use the "FWV510_Check.exe" utility provided with your smart card reader. You can run the program directly from the CD-ROM. By doing that you ensure that the application has not been modified. When updating the SPR532 firmware, you will also receive a new version of the FWCheck utility, since it is explicitly designed for a specific firmware version. In case the FWCheck utility indicates a deviation of the firmware version, you can always check the firmware certification status on the following website: http://www.bsi.de/zertifiz/zert/index_en.htm. Without a certified firmware the smart card reader must not be used for applications following the German signature law (SigG).

5.2.3 Verification of the seal

The SPR532 is equipped with a falsification-safe seal on its bottom side with four predetermined breaking points. Any attempts to remove it will result in an irreversible damage of the seal. A damaged seal exhibits a regular hexagon structure, which can be best recognized by a lateral view of the foil (Fig. 5.1). The integrated hologram prevents the seal from being copied. In order to detect any unauthorized manipulations of the device, please regularly verify if the seal is still intact.



Fig. 5.1: Seal on bottom of the SPR532

5.2.4 Secure handling of the PIN

Your PIN allows you to access your smart card securely. Therefore it is important that no one but you knows your PIN. Always ensure that your PIN is entered unobserved. Never write the PIN down on the smart card or in any other places that are accessible by other people. Do not enter the PIN via the keyboard of the PC. Always use the keypad of the SPR532.

During PIN-entry, please ensure that the SPR532 is working in "Secure PIN-entry mode". You can verify this by checking the LED status (table "LED-status and acoustic signals").

5.2.5 HBCI- and signature cards

When using the SPR532 with home banking, other finance software or digital signature applications, remove your smart card immediately after finishing the transaction or signature. Also keep your smart card in a safe place.

For secure finance and digital signature applications use only processor smart cards which meet the specifications according to DIN ISO7816 and/or EMV2000, in order to ensure the protection of the personal identification data (PIN).

When using the SPR532 in accordance with SigG/SigV, both signature applications and smart cards which have been evaluated and confirmed in SigG context should be used.

6 Troubleshooting

If you encounter any problems using the SPR532 or if your smart card is not recognized, this chapter will give you some advice on how to solve the most common issues. In case you are not able to solve the problem, please refer to Chapter 7, "Support".

6.1 Driver

Usage of the SPR532 requires proper driver installation. Normally you see this by the fact that the smart card reader is recognized automatically after the driver installation. If the application has problems communicating with the smart card reader, open the device manager and look for exclamation or question marks. If the reader is listed correctly under smart card readers and you still encounter problems, uninstall the driver by initiating the uninstaller (program group SPR532 in the start menu) and perform a reinstallation.

6.2 SPR532 Serial

Verify that both connectors (serial and PS/2) are attached to the PC. The data communication between the PC (host) and the SPR532 is done via the COM port (RS-232), the PS/2 connector supplies the required power.

6.3 SPR532 USB

Please note that Windows® 95 and Windows NT® do not support USB. To use the USB version of the SPR532 with Windows® 98 it is recommended to install Windows® 98 Second Edition (Windows® 98 SE), which provides extended USB support.

In case you are using a USB hub, ensure that the hub is working properly. Please note that active hubs need external power supply. Verify the USB connector with other devices such as a USB mouse or a scanner.

7 Support

7.1 Latest drivers and firmware updates

Please visit our website <http://www.scmmicro.com/> for the latest drivers and firmware updates. Here you will also find the latest news and support issues as well as information about other products from SCM Microsystems.

7.2 Technical Support

For technical support please send an email to:

support@scmmicro.com (USA)
support@scmmicro.de (Germany, Europe)

7.3 Hotline

SCM Microsystems telephone support is available from Monday to Friday 9.00 to 13.00 (CET):

☎ 01805 666830 (0,12 €/min)

If you want to reach us from outside Germany, please call this number: **+49 89 9595 5000**

7.4 Additional information

http://www.tuvit.de/	CT-API specification, information about the German signature law (SigG)
http://www.bsi.de/zertifiz/zert/index_en.htm	Information about certification
http://www.pcscworkgroup.com/	PC/SC specification
http://www.microsoft.com/	Information about the CCID protocol
http://www.usb.org/	USB specification
http://www.iso.org/	Information about ISO standards
http://www.emv2000.info/	Information about EMV2000
http://www.scmmicro.com/	Latest drivers and firmware updates

Further information regarding application programming:

http://www.pcscworkgroup.com/	PC/SC
http://www.ct-api.de/	CT-API
http://www.teletrust.de/	MCT: CT-API and CT-BCS

8 Abbreviations

BSI	Bundesamt für Sicherheit in der Informationstechnik
CC	Common Criteria
CCID	Integrated Circuit(s) Cards Interface Devices
CT-API	Card Terminal - Application Programming Interface
DFU	Device Firmware Upgrade
HBCI	Home Banking Computer Interface
ID	Identifier
LED	Light Emmitting Diode
PC	Personal Computer
PC/SC	Personal Computer / Smart Card Interface
PIN	Personal Identification Data
SASCIA	Signature Alliance Application Programming Interface
SigG	German Signature Law
USB	Universal Serial Bus
ZKA-Sig-API	Signature Application Programming Interface of the German ZKA (Zentraler Kreditausschuss der deutschen Kreditwirtschaft)

All company and product names mentioned are registered marks of the respective manufacturers.