

cgSecurePlatform for BlackBerry 10

User Guide

Version 1.2

12.05.2016

Document History

Version	Date	Autor	Notes
1.0	25.11.2014	certgate	-
1.1	16.07.2015	certgate	certgate PC/SC Driver Installation updated
1.2	12.05.2016	certgate	cgCard Type 4 Specification added

Content

1	About this Guide	1
2	System Overview	3
2.1	Hardware	3
2.2	Software	4
3	Installation	6
3.1	Installation Requirements	6
3.2	Installation of the PC Software	6
3.3	Installation of the Mobile Device Software	10
3.4	Update and Uninstall of the Software	11
4	Using Scenarios	12
4.1	Email Security	12

List of Figures

Figure 1: cgCard Specification 4
Figure 2: System Architecture 5
Figure 3: Create Token Profile Example..... 10

1 About this Guide

The cgSecurePlatform for BlackBerry 10 Manual contains all essential information for the administrators and users to use the certgate microSD Smartcard in BlackBerry 10 systems. This manual includes a description of the certgate hardware and certgate software components for BlackBerry 10.

This document is divided into the following chapters:

About this Guide – The first chapter is a short statement of the purpose and scope of this document.

System Overview – This chapter gives a description of the certgate hardware and software components for BlackBerry 10.

Installation – This chapter will give step by step instructions on how to install and configure the certgate software components.

Using Scenarios – This chapter provides a description of the main using scenarios of a smart-card on the BlackBerry 10 devices.

Who Should Use It

This guide is intended to assist users who want to use the certgate Smartcard microSD (cgCard) as a certificate store in his own BlackBerry10 device.

Typographical Conventions

The following kinds of text formatting and icons identify special information in the document:



Warning

Warnings mark situations where loss of data or misconfiguration of the device is possible if the instructions are not obeyed.



Note

Notes provide additional information on a topic, and emphasize important facts and considerations.



Tip

Tips provide best practices and recommendations.



Code

Code Examples

Menu, Buttons

Items you must select, such as menu options, com-mand buttons, or items in a list. Example:
Go to the **System** tab.

Parameters

Parameter and attribute names.

Note



To understand this document you need a knowledge of IT security. You should be familiar with the following concepts: (digital) certificates, private, public, and secret keys, digital signature, PKI, etc.

2 System Overview

Smartcards provide one of the most reliable and secure mechanism for storing digital certificates (identities) on a dedicated hardware modul which is specifically designed with security in mind. **cgCard**, in combination with our software component **certgate Smartcard Driver for BlackBerry 10**, provides you with the possibility to benefit from this great technology on your BlackBerry 10 device.

2.1 Hardware

cgCard

cgCard is the first microSD Card which integrates smartcard technology with regular flash memory.

It represents the most efficient way to use a certified Secure Element (EAL 5+) beyond desktop operating system on mobile device such as smartphones, laptops and tablets without the need of any additional equipment.

Almost every mobile device has a microSD card slot. Meaning, almost every device available on the market can benefit from cgCard and its embedded, certified secure element. It has never been easier to create public-key pairs for encryption, generate secure random numbers or store existing digital certificates on a dedicated secure element. cgCard provides hardware based, tamper-proof, yet easy to use security to all sorts of applications. Just like any other smart card, only smarter.

Some of the functionality provided by cgCard is as follows:

- EAL 5+ certified micro controller
- Platform independent secure element for Windows, Linux, Android or BlackBerry
- Hardware based certificate store for up to 12 certificates (depending on the used cardlet)
- On-Card cryptographic key pair (RSA, etc.), signature (RSA, PKCS#15) or random number generation

Furthermore, additional advantages in using cgCard are:

- Supports every PKI and two-factor authentication
- Hardware based, dedicated secure element
- Easy to use, portable certificate store
- On-card signature generation (the private key never leaves the secure element)
- No need for additional hardware: cgCard can be used in every microSD card slot
- Flash memory for storing additional data


	
Java Card Operating System	jTOP ID Common Criteria level EAL5+ certified
SD Specification	3.0
Java Card Version	3.0.4 Classic
Global Platform	2.2.1
Smart Card Chip	Infineon SLE 78 Common Criteria EAL 5+ certified, RNG AIS31, FIPS-140
Smart Card Chip Storage	ca. 80 kByte EEPROM
Available Flash Memory	8 GB

Figure 1: cgCard Specification

2.2 Software

Windows Driver- cgCard

The **certgate PC/SC Driver** delivered with the smartcards, facilitates the interoperability necessary to allow cgCard to be effectively utilized in the PC environment.

Applets and Smartcard Administration Tool- cgSecurePlatform for Windows

The certgate BlackBerry 10 software is based on the cryptovision applets. The cgCard is empty and must be initialized and personalized before you use it in the BlackBerry 10 device.

By installing the administrator version of **cv act sc/interface**, you can perform all sorts of administration tasks like profile creation, PIN change, unlock smartcard, generation or import of keys and more.

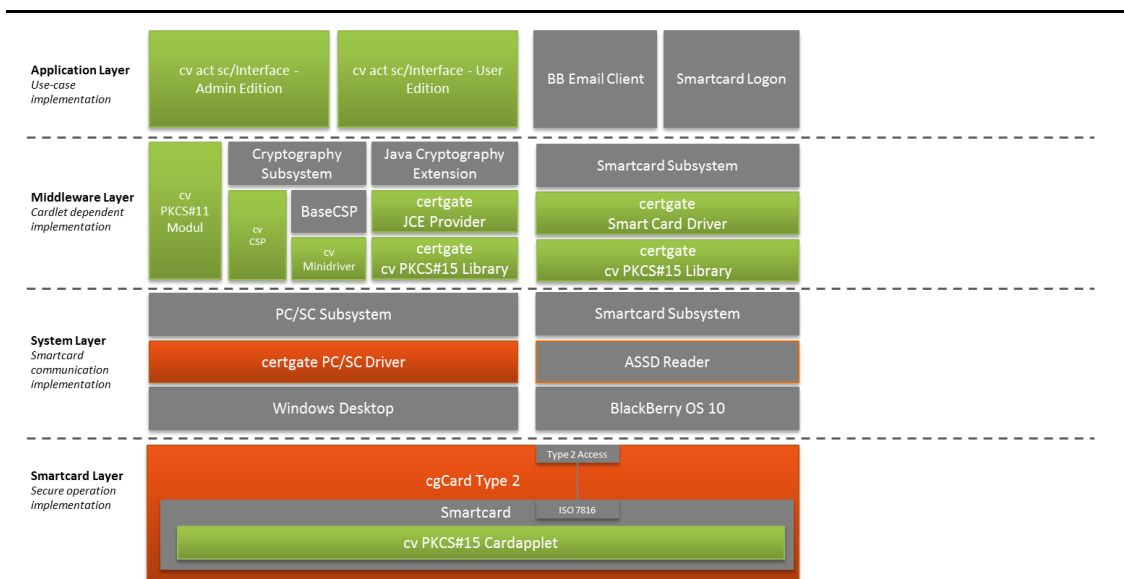
After them the certgate smartcard is ready for using in the BlackBerry 10 device.

certgate BlackBerry 10 Middleware- cgSecurePlatform for BlackBerry 10

Following components are delivered with the **cgSecurePlatform for BlackBerry 10** package:

- **certgate-smartcard-driver-bb10-x.x.bar**
This .BAR has to be installed on the BlackBerry 10 device in order to support and manage the certgate microSD Smartcard
- **cgSecurePlatformforBlackBerryOS10.pdf**
This documentation describes how to personalized and use the certgate microSD Smartcard in the BlackBerry 10 devices

The following illustration shows the architecture of the certgate components and the standard system components:



Legend:

Grey= OS components

Green= cryptovision applets dependent components

Orange= cgCard Type 4 specific components

Figure 2: System Architecture

3 Installation

The desktop software components, certgate PC/SC Driver and the cv act sc/interface, are easily to install using the .msi packages. The BlackBerry 10 software which is to install on the devices is delivered as .BAR file.

The requirements for installing these modules are specified in the next chapter.

Use this checklist if you are performing an initialization and personalization of the cgCard on Desktop:



- Install the corresponding certgate PC/SC driver for cgCard
- Install the cryptovision cv act sc interface Manager “cgSecurePlatform-windows_x.x\cv_act_scinterface_x.x\cv act scinterface xx\installation_admin”. Please select “Smart Card Minidriver (required for use with Cryptography API: Next generation, recommended for use with automated Software Distribution)”
- Use the cv act sc/Interface Manager

3.1 Installation Requirements

certgate PC/SC Driver

The certgate PC/SC Driver Installer supports following operating systems:

- Windows 7 (32bit and 64bit)
- Windows 8 (32bit and 64bit)

cv act sc/Interface Manager

The successfully with cv act sc/interface tested Microsoft Operating Systems are:

- Windows 7 with Service Pack 1
- Windows 8.1
- Windows Server 2008 R2 with Service Pack 1
- Windows Server 2003 with Service Pack 3
- Windows Vista with Service Pack 2
- Windows Server 2008 with Service Pack 2

certgate BlackBerry 10 Components

The certgate Smartcard Driver for BlackBerry 10 is general for all BlackBerry 10 Versions (up Version 10.2) designed and implemented. The compatibility with new BlackBerry OS Versions will be tested by certgate.

3.2 Installation of the PC Software

certgate PC/SC Driver

You find the latest certgate PC/SC Driver Installer under:

“.\cgCardV4-windows...\pcsc-v4-driver-windows...”

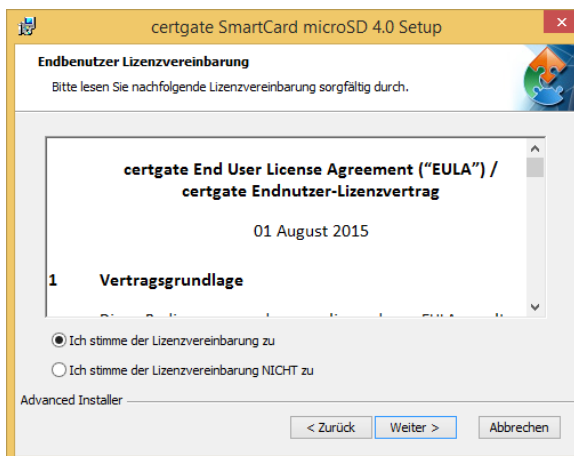
Please choose the appropriate version (32bit or 64bit) to be installed on your computer.

The next paragraphs will detail the procedure for installing the PC/SC driver for cgCard Type 4 on a Windows 8.1 x64 computer. The outlined procedure is almost the same for every other Windows operating system and other types of cgCard.

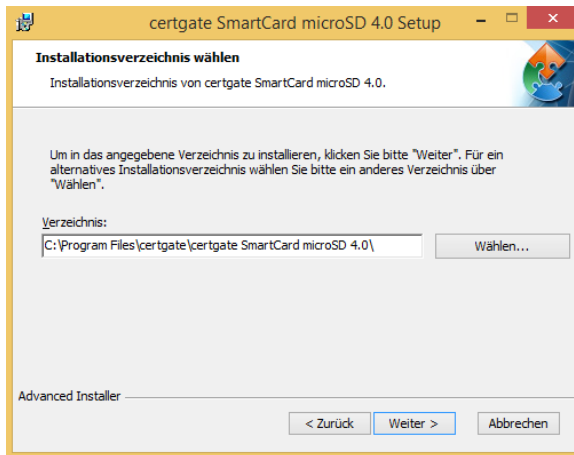


Run the corresponding setup file (32bit or 64bit) needed for your system to open the **“certgate SmartCard microSD 4.0 Setup”** which will guide you through the installation process.

Click on **“Next”**.



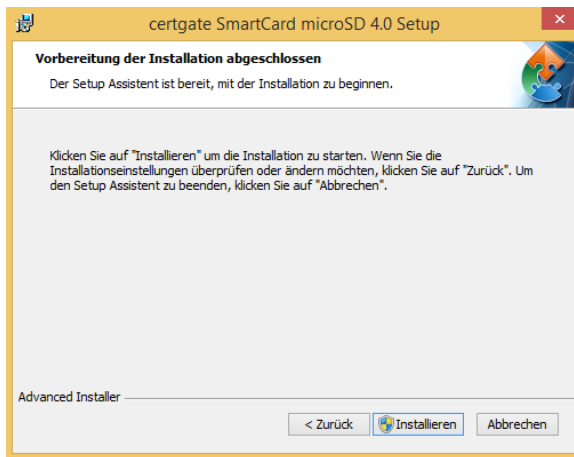
Read the license agreement and if you agree to the terms and conditions, click **“I accept the terms in the license agreement”** and proceed the installation with **“Next”**.



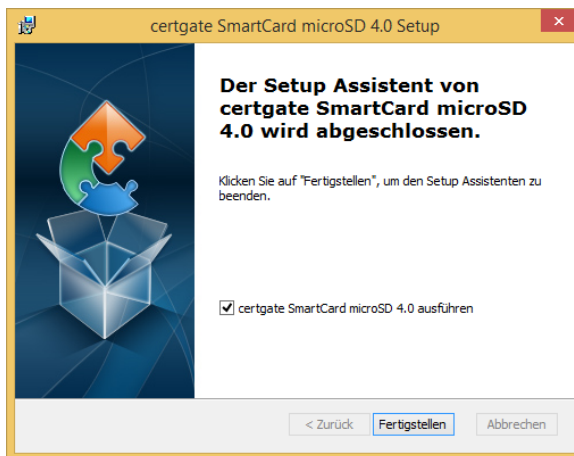
On the **Select Installation Folder** page, use the selected default directory or click **Browse** to change the installation folder.

The default directory is **"C:\Program Files\certgate\certgate SmartCard microSD 4.0\"**

Click **"Next"**.







On the **Confirm Installation** page, click **"Install"** to install the certgate PC/SC Driver.



Finish the installation by clicking **"Close"**.

The installation process creates a shortcut **cgPCSCVxTray** for the **Programs** menu under **Auto-start**.

The **cgPCSCV4Tray**  icon is displayed on the bottom right side of your taskbar and displays the status of your smartcard. The status can be as follows:

- No card inserted 
- Card inserted 
- Card in use 

General Information (e.g. Version) about the **cgPCSCV4Tray** can be displayed via **Info**.

The **Exit** button closes the **cgPCSCV4Tray**.

Now the **certgate microSD Smartcard** is ready to be used (e.g. ready to load and install card applets).

cv act sc/interface Manager

To initialize and personalize the cgCard please install the cryptovision cv act sc/interface Manager. Therefore start the file SETUP.EXE under "**cgSecurePlatform-windows_x.x\cv_act_scinterface_x.x\cv act scinterface xx\installation_admin**" as a user with administrator rights. Follow the on screen installation instructions as guided by the setup wizard.

Please select "**Smart Card Minidriver (required for use with Cryptography API: Next generation, recommended for use with automated Software Distribution)**".

The installation process creates a shortcut for the Program menu called **cv cryptovision** and you will find the following files under it **cv act sc interface Manager** and the **cv act sc interface Manual**.

Here a short description of the initializing and personalizing process of a card:

The cgCards that you received are empty. In order to prepare a smartcard for use, a profile must be created on the smartcard. These profiles can be setup with the Manager menu item "**Create Token Profile**" and select "**PKCS#15 Profile**"

The "**Token Label**" as well as "**SO-PIN**", "**User-PIN**" and "**Serial Number**" are your free choice, although we recommend using the Hardware SN as Serial Number.

We recommend to create a "**Minidriver compatible**" profile because this is the most thoroughly tested configuration.

Therefore a 48 digit Challenge Response PIN is necessary, but since this cannot be used with the cgSecurePlatform there is no need to keep a record of the used value.

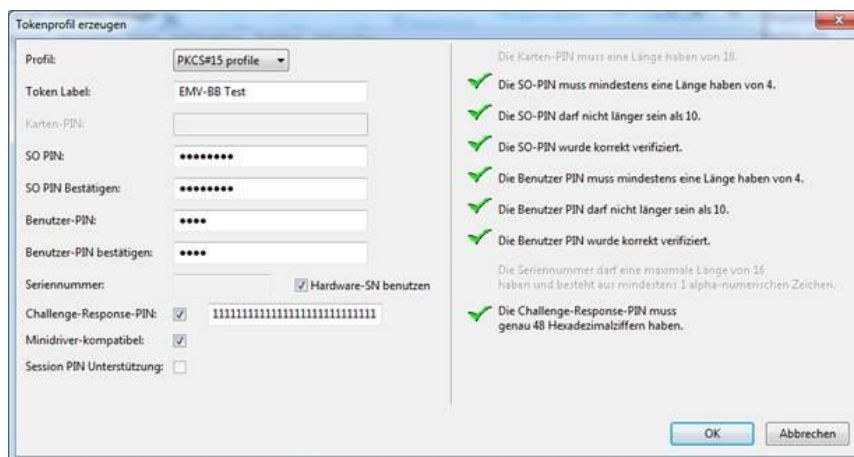


Figure 3: Create Token Profile Example

After the profile is created you can now load certificates and keys onto the card if this is necessary for your use-case.

To do this you “**Login**” using the “**Token**” menu. After this you can either Import a Key Pair and corresponding certificate from a .pfx or .p12 file using the “**Key Pair**” menu or you can import a single certificate without keys using the “**Certificate**” menu.

Imported RSA Keys and certificates can then be used on Windows Desktop, BlackBerry or Android devices.



Tip
More information about the cryptovision software you will find in the **cv act sc interface Manual**.

3.3 Installation of the Mobile Device Software

The **certgate Smartcard Driver for BlackBerry 10** is available as .BAR file. The installation files can be found in the folder

cgSecurePlatform-for-BlackBerry10-x.x\certgate-smartcard-driver-bb10-x.x

The .BAR files can be installed over the BlackBerry Enterprise Server.



For more information about how to install and manage software on your BlackBerry 10 device please read the documentation provided by BlackBerry (e.g. “Advanced Administration Guide-BlackBerry Device Service”)

After installing the certgate Smartcard Driver for BlackBerry you will find a shortcut **cgSmartcard Manager** on your work space.

This application allows you to:

- Show the certgate driver version
- Change smartcard PIN
- Show logfiles

Displays the version of the certgate Smartcard Driver



You can change the default PIN for your certgate Smartcard before you use it.

It's quick and easy to do this in the **cgSmartcard Manager PIN Change**

You have to type the old PIN first, and then the new PIN twice.



Display Logfiles

3.4 Update and Uninstall of the Software

Desktop Software

The cryptovision sc Interface Manager can be removed using the well-knowing uninstall process for Windows software (**Control Panel-> Programs and Features-> Uninstall**).

An update of the software is possible, the installed version will be overwritten.

BlackBerry 10 Software

The installed certgate .BAR can be removed using the familiar mechanism.

A new version of the certgate driver can be installed over the BES.

4 Using Scenarios

The certgate microSD Smartcard serves as a secure storage for private keys and certificates. After the certificates are imported from the cgCard in the BlackBerry certificates store, these are available for all BlackBerry applications.

BlackBerry application that use certificates is e.g. S/MIME email client .

The prerequisites for using the certgate Smartcard in your BlackBerry 10 Device for S/MIME scenario is:

- extended messaging security for the BlackBerry Device Service in BlackBerry Enterprise Service 10 to permit BlackBerry smartphone users to send S/MIME-protected email messages on BlackBerry 10 smartphones
- installed certgate Smartcard Driver for BlackBerry 10
- complete setup of a Work Account



More information about how to enable S/MIME in a BlackBerry Enterprise Service 10 you will find in the BlackBerry article [KB34437](#).

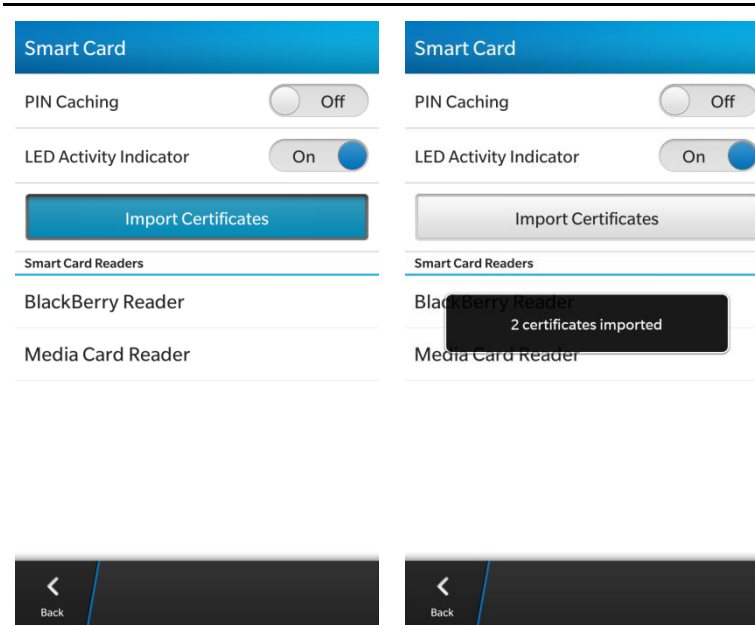
How secure e-mail with smartcard based certificates works you will find in the next chapter.

4.1 Email Security

You can digitally sign or encrypt messages if you use a work email account that supports S/MIME-protected messages on your BlackBerry 10 device. Therefore you don't have to install additional software on device.

At first you must import the key pairs from the certgate Smartcard on the BlackBerry device. Therefore, please follow the steps below:

The screenshot shows the BlackBerry 10 System Settings application. The 'System Settings' menu on the left includes options like Screen lock, Language and Input, Voice Control, BlackBerry Link, BlackBerry ID, BlackBerry Protect, Security and Privacy (highlighted), Media Sharing, Date and Time, Software Updates, and Search. The 'Security and Privacy' menu on the right includes Application Permissions, Device Password, SIM Card, Smart Card (highlighted), Encryption, Parental Controls, Diagnostics, Security Wipe, and Certificates. To the right of the screenshot, the text reads: 'Open the **System Settings**. Then go to **Security and Privacy**.'



Then select **Smart Card**.
Now you select **Import Certificates** and all certificates stored on the card will be imported on your BlackBerry device.

The imported certificates are displayed under **System Settings/ Security and Privacy**.

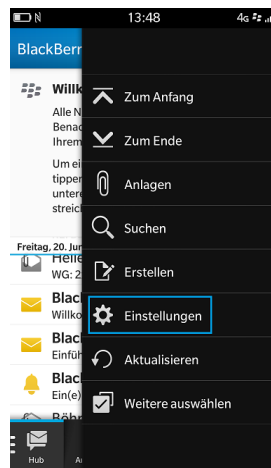
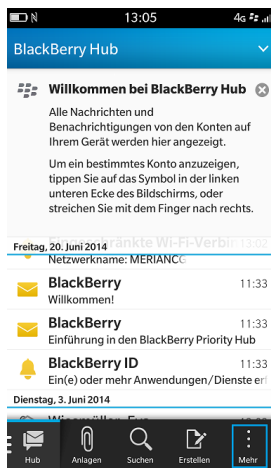


How to distribute CA certificates to devices please read the **BlackBerry Device Service Advanced Administration Guide** .

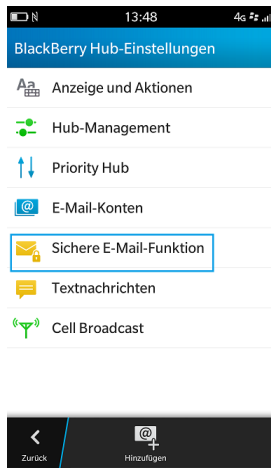
Now the certgate Smartcard is ready to use and the smartcard certificates are imported to the key store on your Blackberry device, and also ready to use. The private keys remain on the smartcard. As a result, private key operations such as signing and decryption use the smartcard, and public key operations such as verification and encryption use the public key stored on your device.

4.1.1 S/MIME Settings

You can configure now the S/MIME preferences on device in the BlackBerry Hub settings, including choosing certificates.



Open the **BlackBerry Hub**.
Then go to **More/ Settings**.

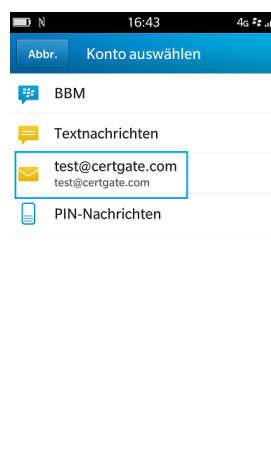
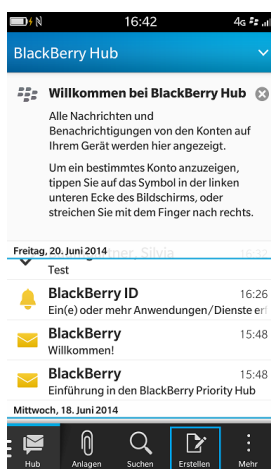


Under **Secure E-Mail-functions** you can configure the following S/MIME profile settings:

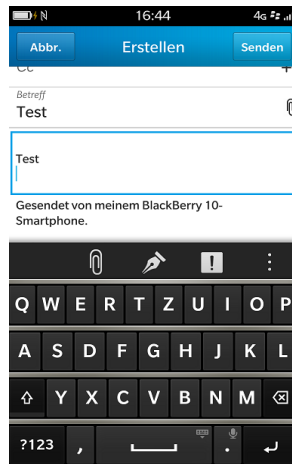
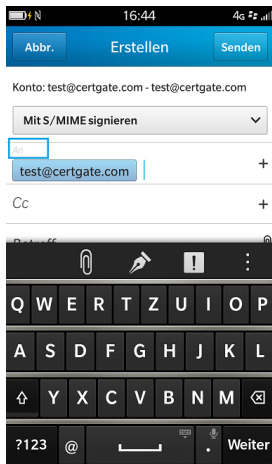
You can enable the S/MIME on device, ...

... select the certificates you want to use for encryption and signing.

4.1.2 Signing E-Mails

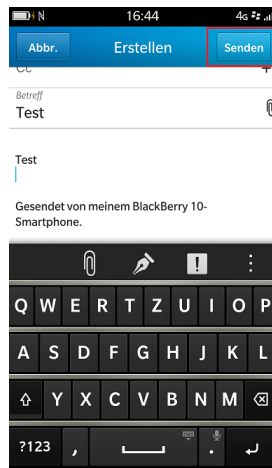
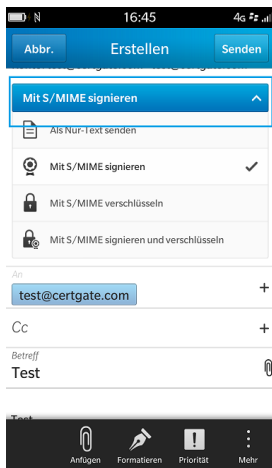


Go to **BlackBerry Hub** select **Compose** and select your e-mail account .



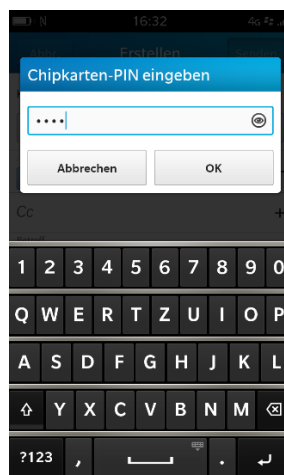
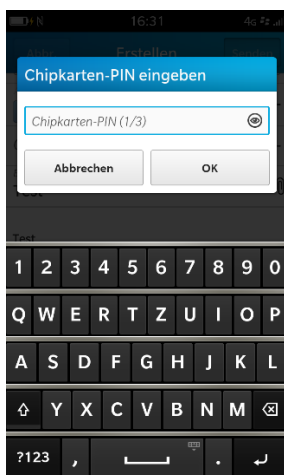
Now write your e-mail.

You can enable the S/MIME on device, ...

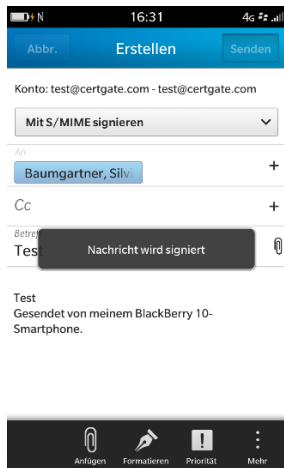


Select the option Sign to send a signed e-mail.

Click on sent.



Now you are asked to enter your smartcard PIN. Thereafter go on with a click to OK.



Wait a few seconds.

The e-mail will now be signed with the certificate you chose at S/MIME Setup.