Application Notes ANCT17

PGP Desktop

Purpose of Application: Using the CrypToken for data protection and encryption/signing
Version: PGP Desktop 10.1.1 (Win32/64), CrypToken Kit 1.50 or higher
Last Update: 16 October 2013 by Steffen Kaetsch
Target Operating Systems: Windows 8/7/Vista (32 & 64 bit), XP
Target Processor Platforms: Intel x86
Applicable for Product: CrypToken® MX2048 JCOP, CrypToken M2048 MULTOS

Using the CrypToken with PGP Desktop

PGP Desktop Home is easy-to-use data encryption software that can secure an individual's most valuable and confidential information. The CrypToken adds professional Two-Factor-Authentication to PGP allowing to store keys and certificates on a small and portable device.

CrypToken®

- Runs on all operating systems with CCID support without separate driver
- Multiple keys and certificates can be stored in one token
- Certified smart card chip meets highest security standards according to Common Criteria
- Multi-platform support: Windows, Linux, Mac OS X
- Existing JavaCard or MULTOS applications for smart cards run without modification
- Ability to load customer-specific applications and algorithms
- Solid metal casing

PGP Desktop

Table of Contents

1. CrypToken® Installation

1.1 SafeSign Installation

To install SafeSign open the folder \SafeSign\Windows on the "CrypToken Kit" CD. There are two .exe files:

SafeSign-Identity-Client-admin.exe - Administrator Installation (for System Administrators)
SafeSign-Identity-Client-user.exe - User Installation (for normal Users)

The Administrator Installation installs an extended Token Administration Utility (TAU) which does not only allow to configure the CrypToken, it also provides administrative tasks which will be performed automatically when the Token is inserted (e.g. checking the validity of installed certificates). A detailed description can be found on the CrypToken CDROM at folder \Documentation\Application Notes (AET):

TAU_Guide_SafeSign-IC-Standard_v2.1.pdf - description of the Token Administration Utility
TMU_Guide_SafeSign-IC-Standard_v2.1.pdf - description of the Token Management Utility (User)

Start the SafeSign installation by double-clicking the suitable .exe file. On the Welcome screen, click "Next", then confirm the License Agreement and select the installation folder. At the next screen the desired program features can be selected (see Fig. 1.1). There is no need to change anything here: If you leave the default settings, all necessary components for accessing the CrypToken on your PC will be installed automatically. The most important component for PGP Desktop is PKCS#11 which is mandatory for the CrypToken to work with PGP Desktop.

After the SafeSign installation was completed successfully, click the "Finish" button.

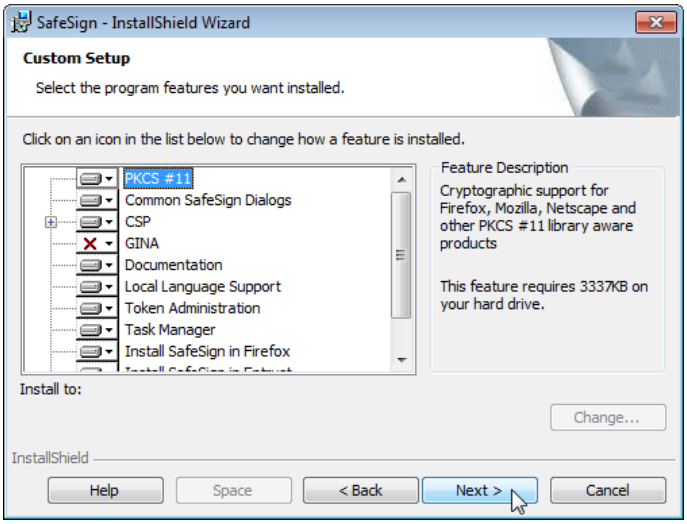

Fig. 1.1: SafeSign installation

1.2 CrypToken driver installation

Attach the CrypToken to a USB port. Windows will recognize a new device and opens the "Found New Hardware Wizard" (see Fig. 1.2). You can click on the balloon icon in the lower right corner to get more details. If your computer is connected to the Internet, Windows 7/Vista will automatically obtain the driver from Windows Update.

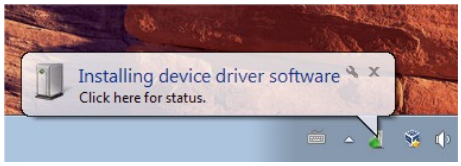

Fig. 1.2: CrypToken Driver Installation

Under Windows XP, you will be asked if Windows should connect to Windows Update and search for the driver (see Fig. 1.3). Select the "Yes, this time only" radio button and click next. If you have no internet connection, or you want to install the driver manually, put the "CrypToken Kit" CD in your CDROM drive and let Windows browse for drivers at the location of your CDROM drive (for instance E:\). You may also download the latest CrypToken drivers at www.cryptoken.com ⇨ Support ⇨ Download Area.

Fig. 1.3: CrypToken Driver Installation under Windows XP

Windows will notify you when driver installation was finished successfully (see Fig. 1.4).

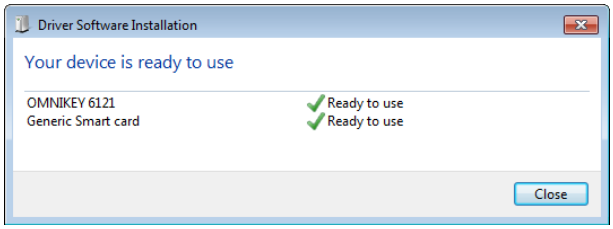

Fig. 1.4: Finishing CrypToken Driver Installation

If Windows 7/Vista tells you that the "Generic Smart card" driver cannot be found, then you most probably did not install SafeSign yet. Please refer to chapter 1.1 for SafeSign installation.

2. Initializing the CrypToken

The CrypToken needs to be initialized prior to use it for storing certificates and keys within PGP. To do so, attach the CrypToken to the USB port and start the Token Administration Tool under:

Start - Programs - SafeSign Standard - Token Administration (Administrator Installation, see 1.1)

or

Start - Programs - SafeSign Standard - Token Management (User Installation, see 1.1)

The following information will be displayed:

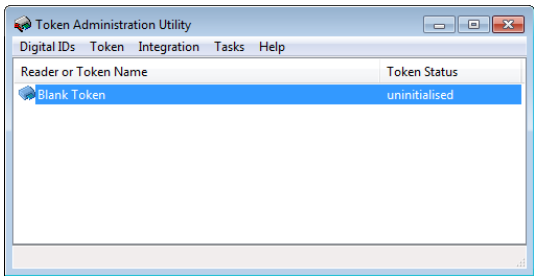

Fig. 2.1: Token Management: uninitialized CrypToken

Select the menu point "Token" and "Initialize Token". Choose a Token label, specify PIN and PUK for the attached CrypToken and confirm them. Then click "OK".

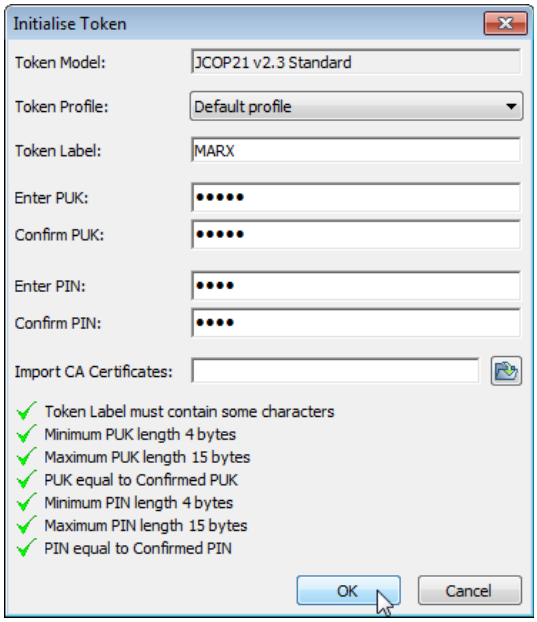

Fig. 2.2: Initializing the CrypToken

Wait until you received the message that the initialization was successful and click "OK" to finish. The CrypToken is now operable.

You can change PIN and PUK of the CrypToken later, if required. Choose the menu point "Token" and "Change PIN" resp. "Change PUK" to do so. If you entered the wrong PIN 3 times, the CrypToken will be blocked. Choose "Unlock PIN" from "Token" menu in that case to unlock the PIN (PUK is required for this operation). If wrong PUK was entered 3 times, the token is blocked completely!

3. Using the CrypToken with PGP Desktop

3.1 Storing a key on the CrypToken

Make sure that PGP Desktop is properly installed on your computer and the CrypToken is plugged into the USB port.

Open PGP Desktop and go to "File" ⇨ "New PGP Key". A Wizard will come up.

If SafeSign was installed properly and the CrypToken was initialized successfully (as described in chapter 1 and 2), PGP will recognize the CrypToken and automatically offers to generate the key on it (see Fig. 3.1).

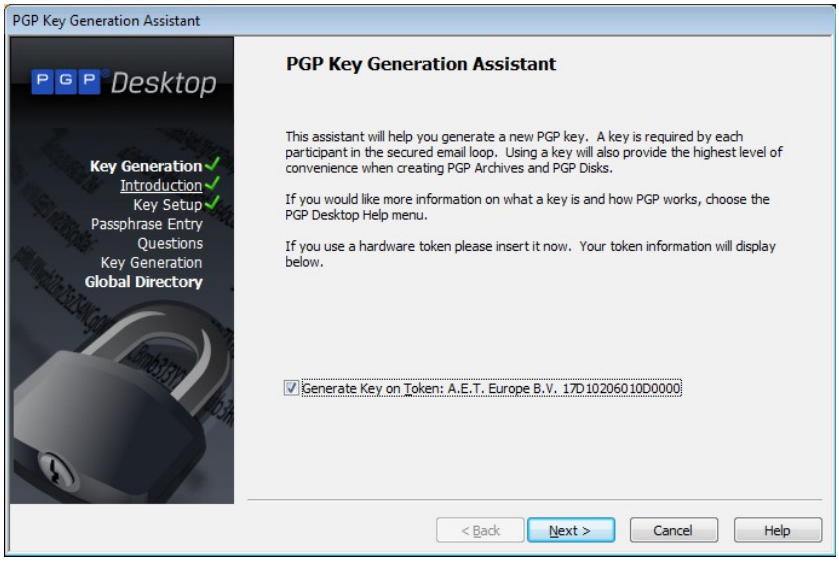

Fig. 3.1: Generating a key on the CrypToken

Next you will be asked for your Email address. Furthermore, there is an "Advanced" option available on this screen:

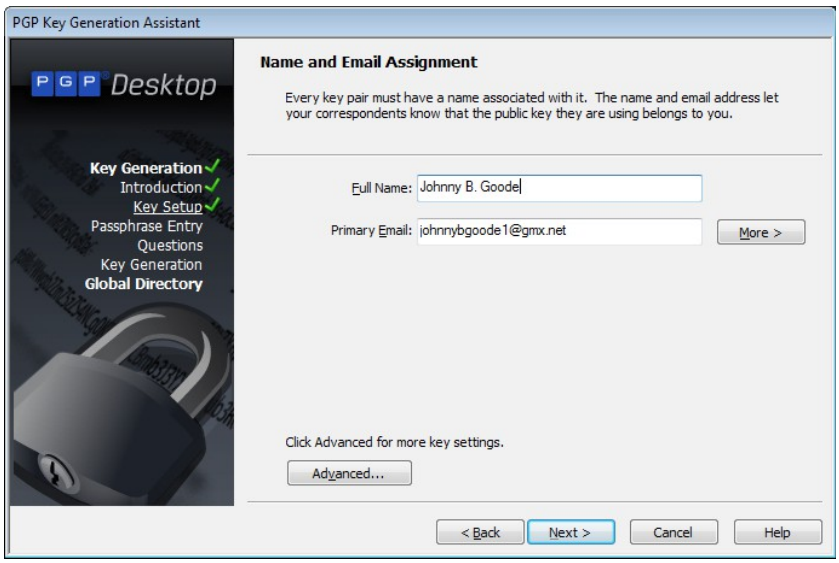

Fig. 3.2: Generating a key on the CrypToken

When clicking on "Advanced", you will get more information on key settings and lenght. If you have a CrypToken M2048, you will see that the RSA key length is set to 1024 bit (Fig. 3.3). This is because of a limitation of SafeSign together with the CrypToken M2048 which allows a maximum key lenght of 1024 bit. For the CrypToken MX2048 JCOP the maximum key length is 2048 bit.

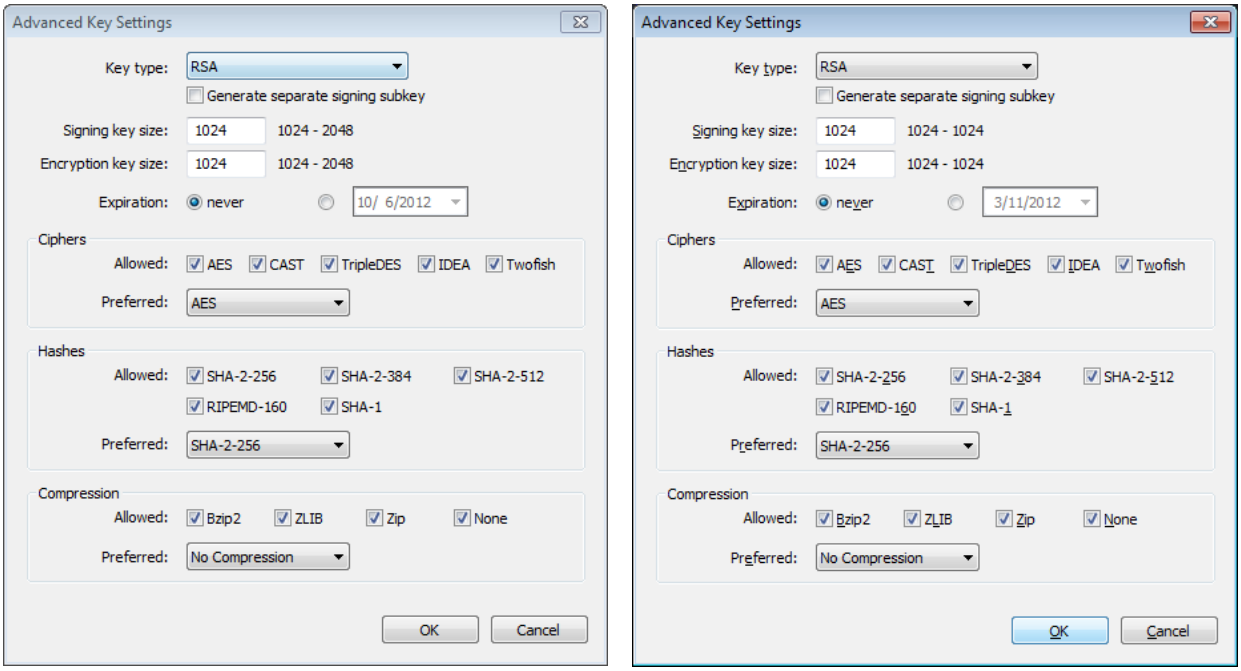

Fig. 3.3: Advanced key settings for the CrypToken MX2048 JCOP (left) and the M2048 MULTOS (right)

As the next step you have to provide the PIN of your CrypToken. Now it will take a while to generate the key pair.

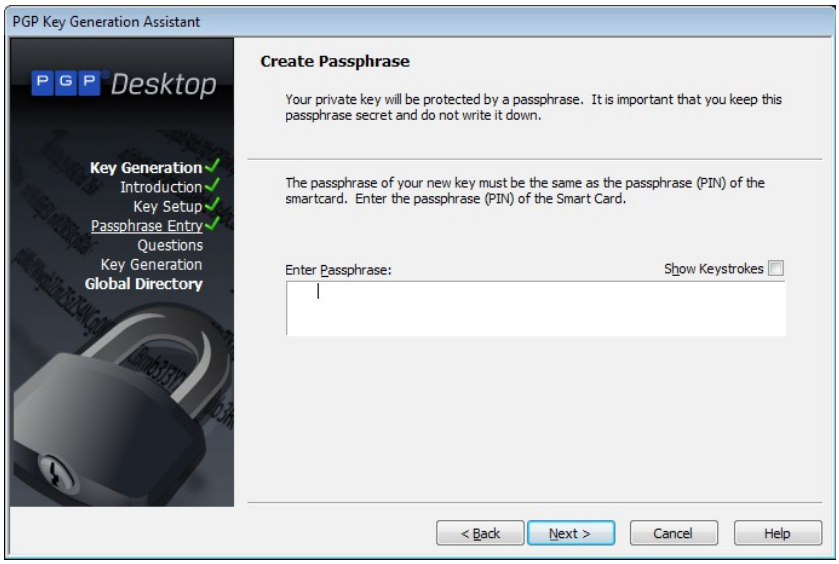

Fig. 3.4: Entering the passphrase (CrypToken PIN)

After everything was finished successfully, you will see a Token Symbol with description "Smartcard Keys" on the PGP Desktop including key information:

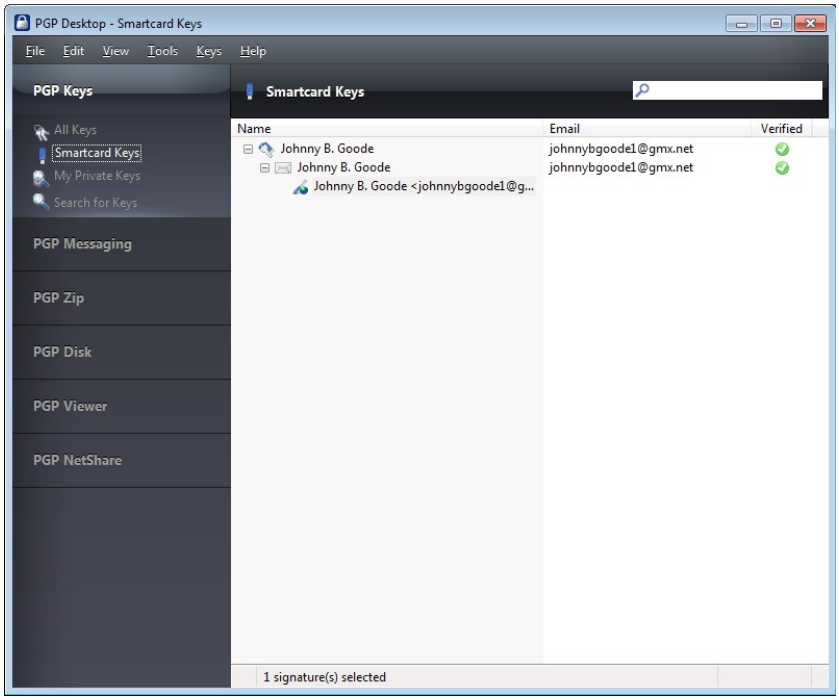

Fig. 3.5: Information about keys stored on the CrypToken

When you click on "Tools" ⇨ "Options" ⇨ "Keys" you will see information about key synchronization with the CrypToken. PGP will detect the CrypToken (configured for SafeSign) automatically:

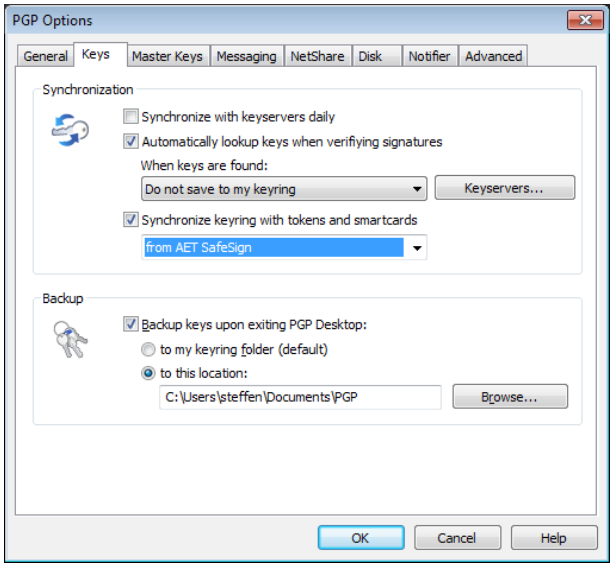

Fig. 3.6: Keyring synchronization

3.2 Check Token content with SafeSign Administration Tool

The SafeSign Administration Tool allows to check the content of the CrypToken, and to add or remove certificates if required. Start the SafeSign Administration Tool (see chapter 2) and click on "Token" ⇨ "Show Token Objects":

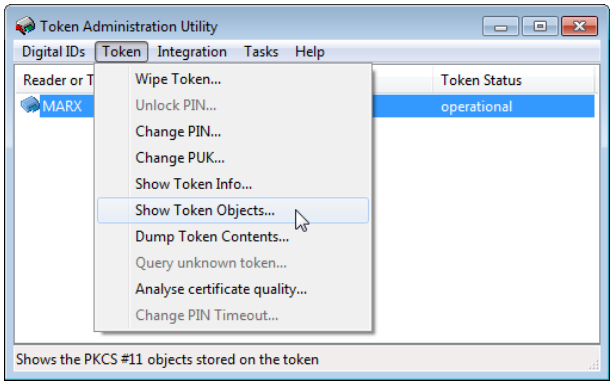

Fig. 3.7: Display objects stored in the CrypToken

To view Private objects, click on "Show Private Objects" and put in the CrypToken PIN.

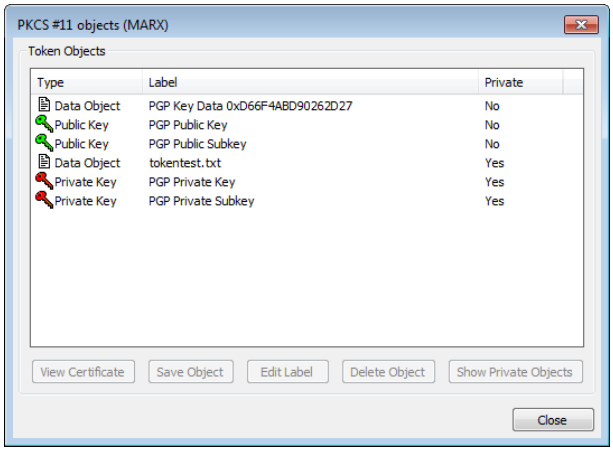

Fig. 3.8: Display private objects stored in the CrypToken

MARX cryptotech authentication done right™

Application Notes ANCT17

PGP Desktop

CrypToken Data Sheet

	CrypToken M2048	CrypToken MX2048
Supported Standards	PKSC#11, Microsoft CSP	PKSC#11, Microsoft CSP, Minidriver
Operation System	MULTOS	JCOP
Smart Card Chip	Infineon SLE66CX	SmartMX/JCOP41
Smart Card Chip Certifications	EAL 5+, EMV, ISO 7816	EAL 4+, EMV, ISO 7816, JavaCard 2.4.1, Global Platform
Controller Chip	Atmel/Omnikey	Atmel/Omnikey
Controller Chip Certifications	WHQL, USB CCID, PC/SC, HBCI, EMV2000	WHQL, USB CCID, PC/SC, HBCI, EMV2000
Memory (total)	64 KByte	80 KByte
Ability to Load Customer Specific Applications	yes	yes
Tamper-Proof Hardware	yes	yes
Secure Against External Interception	yes	yes
Operating Systems Supported	Windows, Linux, Mac OS X	Windows, Linux, Mac OS X
Data Retention Time	minimum 10 years	minimum 10 years
Write Cycles	>500.000	>500.000
Default Middleware Configuration	SafeSign	SafeSign
Available w/o Middleware	Yes	Yes
Electrical Certificates	FCC, CE, RWTÜV	FCC, CE, RWTÜV
Dimensions	15 x 8 x 36 mm	15 x 8 x 36 mm
Weight	9.5g	9.5g
Temperature	0°C to +60°C / 32°F to 140°F	0°C to +60°C / 32°F to 140°F
Humidity	0% to 95% relative humidity	0% to 95% relative humidity

CrypToken Certifications

CrypToken Developer's Kit

www.cryptoken.com/cryptoken-kit

MARX Data Security GmbH
Vohburger Strasse 68
85104 Wackerstein, Germany
Phone: +49 (0) 8403 / 9295-14
Fax: +49 (0) 8403 / 9295-29
contact-de@cryptotech.com

MARX CryptoTech LP
3355 Annandale Lane, Suite 2
Suwanee, GA 30024 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
contact@cryptotech.com

www.cryptoken.com