

Email Encryption and Digital Signature w/X.509 certificates CrypToken® as secure and portable container for Certificates



Described Version: The BAT! 3.80.06

Also applicable for: The BAT! 3.0 and up

Target platforms: Windows Vista/XP/2000

MARX hardware: CrypToken M2048 / MX2048 JCOP



Private Communication in a Public World!

Emails are like post cards. Everybody can read through them and change something on the way between sender and receiver. Encryption and digital signing creates a secure envelope around your emails. With traditional email encryption solutions, the certificate is stored on your harddisk - a potential target for eavesdroppers and intruders.

The CrypToken is a secure storage device for all your certificates and passwords. Your most confidential information is never exposed to the file system.

- Convenient email encryption and digital signing
- Easy implementation into Microsoft Outlook, Outlook Express, Thunderbird, The BAT!, David, PGP Mail, ...
- Authentication with X.509 certificates (S/MIME) or PGP keys
- Safe against phishing and password theft

Table of Contents

- 1. System Requirements.....2**
- 2. CryptToken® Installation.....2**
 - 2.1 CryptToken driver installation under Windows XP.....2
 - 2.2 SafeSign Installation.....3
 - 2.3 Initializing the CryptToken.....4
- 3. Managing Certificates.....5**
 - 3.1 Storing Certificates on the CryptToken.....5
 - 3.2 About Certificates.....5
- 4. The Bat! Configuration.....6**
- 5. Encrypting and Signing Emails.....7**
- 6. Receiving Encrypted and Signed Emails.....8**

1. System Requirements

- Microsoft Windows Vista, XP, 2000
- Installed Ritlabs The Bat!
- CrypToken MX2048 JCOP / M2048 MULTOS with SafeSign

2. CrypToken® Installation

2.1 CrypToken driver installation under Windows XP

Attach the CrypToken to a USB port. Windows will notify a new device and opens the Found New Hardware Wizard. If your computer is connected to the Internet, simply install the driver using Windows Update: select the "Yes, this time only" radio button and click next (see Fig. 2.1). If you want to install the driver manually, put the "CrypToken Kit" CD in your CDROM drive and follow the instructions as described in Fig. 2.1 and 2.2. You may also download the latest CrypToken drivers at www.cryptoken.com ⇒ Support ⇒ Download Area.

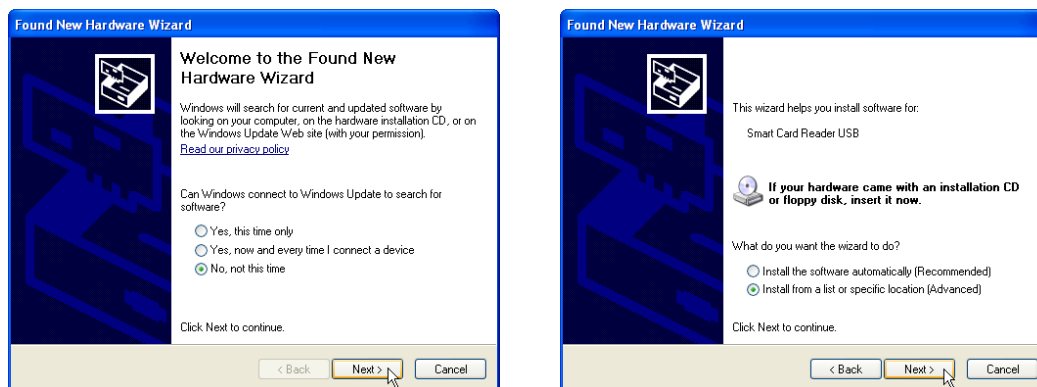


Fig. 2.1: Found New Hardware Wizard (Step 1 and 2 - Windows XP)

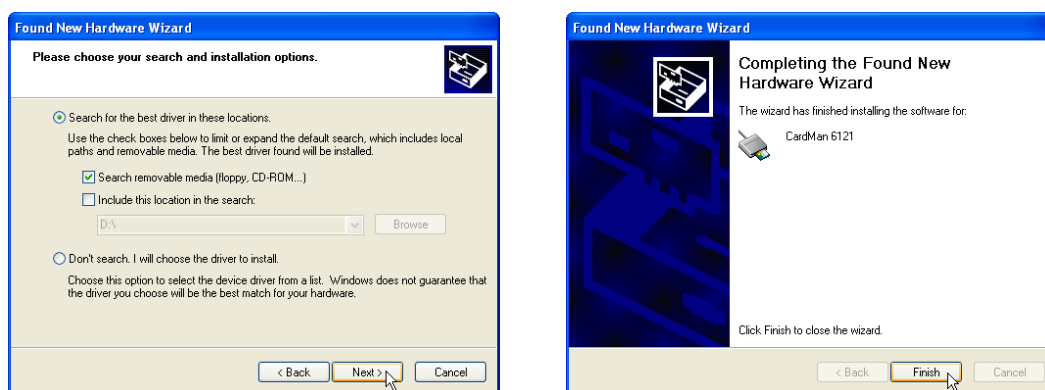


Abb. 2.2: Found New Hardware Wizard (Step 3 and 4 - Windows XP)

After the wizard has finished you will get a notification that the driver was installed successfully.

2.2 SafeSign Installation

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

SafeSign-Identity-Client-admin-eval.exe - Administrator Installation (for System Administrators)

SafeSign-Identity-Client-user-eval.exe - User Installation (for normal Users)

The difference between these two versions: 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 CrypToken is inserted (e.g. checking the validity of installed certificates). A detailed description can be found on the "CrypToken Kit" CDROM at folder \Documentation\Application Notes (AET):

TAU_Guide_SafeSign-IC-Standard_v2.1.pdf - description of the Token Administration Utility (Administrator Installation)

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

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. 2.3). There is no need to change anything here: If you leave the default settings, all necessary components for integrating the CrypToken under Outlook/Outlook Express and Internet Explorer will be installed automatically. After the installation has completed, click the "Finish" button.

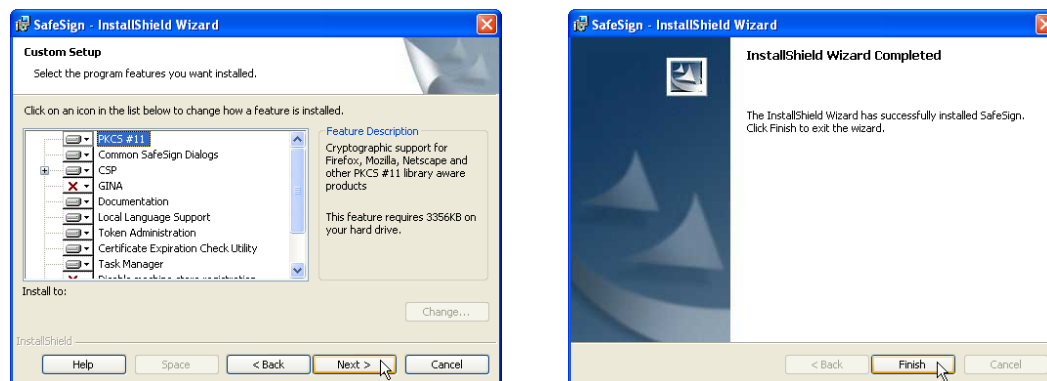


Fig. 2.3: SafeSign installation

2.3 Initializing the CrypToken

The CrypToken needs to be initialized prior to use it for storing certificates and keys. 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 2.2)

OR

Start - Programs - SafeSign Standard - Token Management (User Installation, see 2.2)

The following information will be displayed:

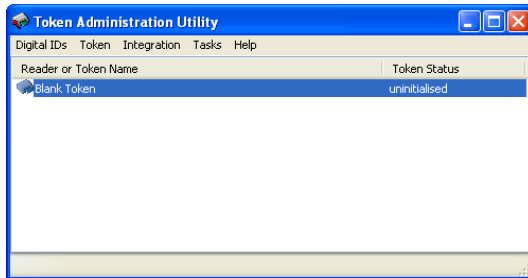


Fig. 2.4: Token Management: uninitialized CrypToken

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

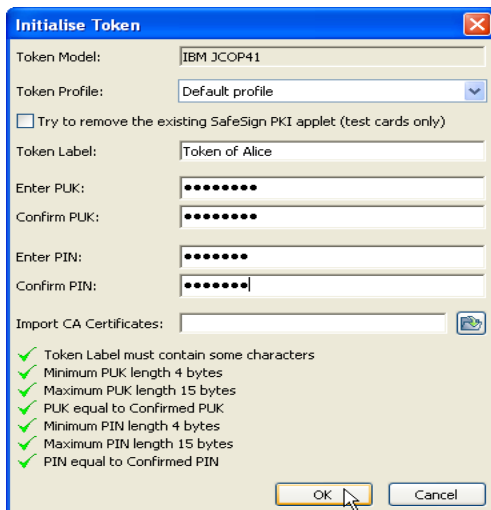


Abb. 2.5: Initializing the CrypToken

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

3. Managing Certificates

3.1 Storing Certificates on the CrypToken

Attach the CrypToken to the USB port of the computer and start the Token Administration Tool under: **Start - Programs - SafeSign Standard - Token Administration** (Administrator Installation, see 2.2) or

Start - Programs - SafeSign Standard - Token Management (User Installation, see 2.2)

Select the menu point "Digital IDs", then "Import Digital ID" or "Import Certificate", depending on the type of your existing certificate:

Choose "Import Digital ID" for the following file types:

- .pfx
- .p12

resp. bzw. "Import Certificate" for the file types:

- .cer
- .der

Browse for the ID/certificate you want to install on the CrypToken.



Digital IDs/Certificates for encryption and signing of Emails can be obtained from different Certificate Authorities (CA), for example:

www.cacert.org

www.comodo.com/products/certificate_services/email_certificate.html

www.verisign.com

For testing purposes, you may also obtain Demo certificates from our webpage:

www.cryptoken.com/ctwebutils/phpki/

Select the certificate on your hard disk you want to import. Enter the password which was used to protect the certificate file. At the next step you will be asked for the PIN of the CrypToken (see Fig. 3.1). Wait until you receive the confirmation that the certificate was imported successfully to the CrypToken.

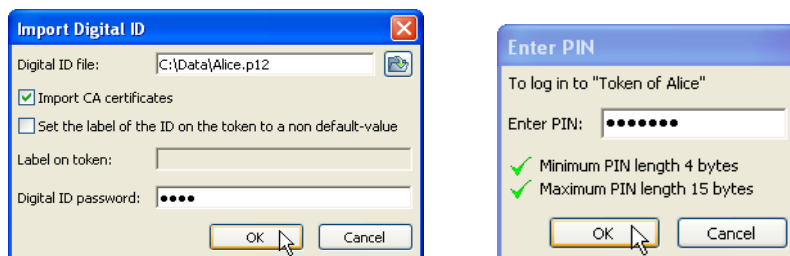


Fig. 3.1: Import Digital ID

3.2 About Certificates

After applying for a certificate (see 3.1) you will receive an encrypted file which contains the all necessary information. Such digital certificate comprises a public part containing a public key signed by the CA which has issued the certificate, and an accompanying private key. The certificate does not work without the private key. That is why it is vital to take good care of the private key.

Certificates stored on the CrypToken cannot be copied back to the hard disk or to another CrypToken anymore. MARX recommends to copy the certificate file to a removable media (CD, USB storage drive etc.) and keep it in a safe location. This allows you to restore the certificate from the backup, should the CrypToken be lost or deleted.

4. The Bat! Configuration

Start The Bat! and go to "Options" ⇒ S/MIME" (Fig. 4.1).



Fig. 4.1: Open S/MIME Preferences

Change S/MIME Preferences according to Fig. 4.2. Select "RaakSign Standard Cryptographic Service Provider" for CrypToken M2048 (RaakSign) or "MARX CSP Provider" for CrypToken M2048 (MARX Middleware) or CrypToken 2000.

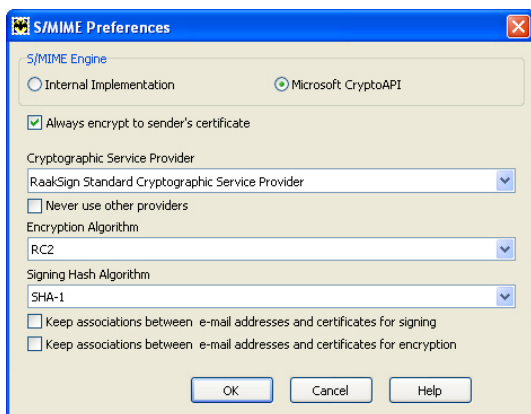


Fig. 4.2: S/MIME Preferences

5. Encrypting and Signing Emails

Attach the CrypToken to your computer and start The Bat!. Click on "Message • New" to write a new email. Afterwards go to "Privacy" (Fig. 5.1) and check "Enable S/MIME". To sign and/or encrypt check "Sign when Completed" and/or "Encrypt when Completed". To send encrypted emails you will need the public key of the receiver.

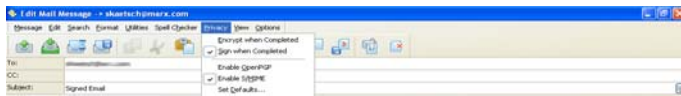


Fig. 5.1: Change message options

After clicking on the "Send" button, The Bat! will ask you to select a certificate that is used to sign/encrypt the email (Fig. 5.2).

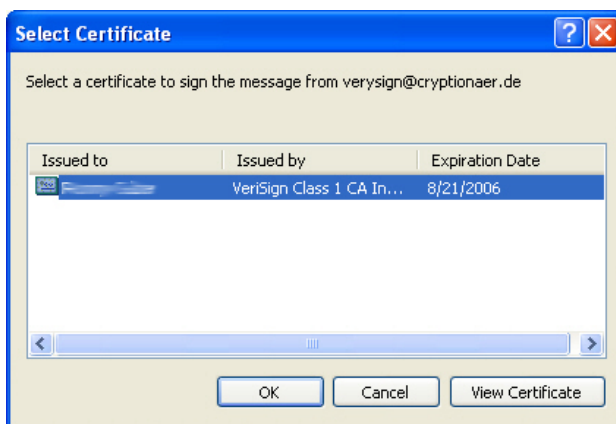


Fig. 5.2: Select a certificate

6. Receiving Encrypted and Signed Emails

Attach the CrypToken to your computer and start The Bat!. If you received a signed or encrypted email The Bat! will show a symbol within the email header (Fig. 6.1).



Fig. 6.1: Receiving a signed message

Following symbols are used to show the email status:



Fig. 6.2: Symbol for signed messages with trusted CA



Fig. 6.3: Symbol for signed messages with untrusted CA



Fig. 6.4: Symbol for encrypted messages

If you received a encrypted email The Bat! will show the content upon request. To decrypt the email click on the symbol for encrypted messages (Fig. 6.4) within the email header.

It's our business to protect yours

The CrypToken is ideal for...

- Online Banking: Secure Internet banking and financial transactions.
- VPN: Virtual Private Network control from remote locations.
- eGovernment: Access control to confidential information.
- Email: Encryption and digital signature of confidential emails.
- eCommerce: Secure B2B/B2C authentication.
- RAS and network logon: Access for authorized users only.
- WebSecurity: Secure web portal and internet and intranet identification.
- DataSecurity: Encryption of sensitive information.



Get your CrypToken Evaluation Kit:

www.cryptoken.com/eval
0049(0)8403 9295-14

Comparison table CrypToken M2048 and CrypToken MX2048

Features	M2048	MX2048
Token operating system	MULTOS	JavaCard
Operation	Driverless, if CCID OS used	
Certification smart card chip	EAL 5+ EMV, ISO7816	EAL 4+, EMV, ISO7816, JavaCard 2.3.1, GlobalPlatform 2.1.1
Controller chip certification	WHQL (Microsoft), HBCI (Home Banking Computer Interface), EMV, ISO7816	
Smart card chip	Infineon SLE66xx series	SmartMX/JCOP21
Cryptographic standards supported	PKCS#11v2.01, MS-CAPI	
Operating systems supported	Windows Vista/XP/2000, Linux, MacOS X	Windows Vista/XP/2000, Linux, MacOS X
Memory (total)	64 KByte	72 KByte
Casing & LED	Metal Designer Case, LED (duo color green/red, for „stand by/activity“), eye for key ring/lanyard	
Electrical certifications	FCC, CE, RWTUEV	FCC, CE, RWTUEV
Dimensions	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)	0.51" x 0.32" x 1.38" (13 x 8 x 35 mm)
Weight	0.326 oz (9,25g)	0.326 oz (9,25g)

CrypToken certifications



All trademarks used in this document are property of their respective owners.

MARX CryptoTech Germany

Vohburger Strasse 68
D-85104 Wackerstein
Phone: +49 (0) 8403 9295-14
Fax: +49 (0) 8403 929529
contact@cryptoken.com

MARX CryptoTech LP

4485 Tench Road #310
Suwanee, GA 30024 U.S.A.
Phone: (+1) 770 904 0369
Fax: (+1) 770 904 3893
info@cryptotech.com

www.cryptoken.com