

SSL Client Authentication Client Side Configuration CrypToken® as secure and portable container for Certificates



Described Version: Firefox 3.0.10

Also applicable for: Firefox 1.0 and up

Target platforms: Windows Vista/XP/2000, Linux, MacOS

MARX hardware: CrypToken M2048 / MX2048 JCOP



Upscale perimeter security!

Today's eBusiness solutions, financial transactions, and subscription services require reliable user authentication and secure transmission channels. This can be achieved with the combination of certificate based client authentication and SSL transmission.

To achieve a high level of security it is necessary to have a trusted storage container for all of your certificates. The CrypToken M2048 and MX2048 JCOP ensures that your certificates and other important pieces of information are safe from tampering and prying eyes.

- Easy implementation into existing web portals
- Strong access control for internet and intranet
- Authentication with X.509 certificates (S/MIME) or PGP keys
- Safe against phishing and password theft
- Client: all browsers with PKCS#11 or MS-CAPI support
- Server: all SSL compliant servers (e.g. IIS and Apache)



Download the latest Application Notes:

www.cryptoken.com/AN

Table of Contents

1. System Requirements.....	2
2. CrypToken® Installation.....	2
2.1 CrypToken driver installation under Windows XP.....	2
2.2 SafeSign Installation.....	3
2.3 Initializing the CrypToken.....	4
3. Managing Certificates.....	5
3.1 Storing Certificates on the CrypToken.....	5
3.2 About Certificates.....	5
4. Firefox Configuration.....	6
5. Establishing a SSL connection.....	7

1. System Requirements

- Microsoft Windows (Vista, XP, 2000)
- Mac OS – This document only contains a windows sample
- Linux – This document only contains a windows sample
- Installed Mozilla Firefox Version 3.x or above (www.mozilla.org)
- 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.

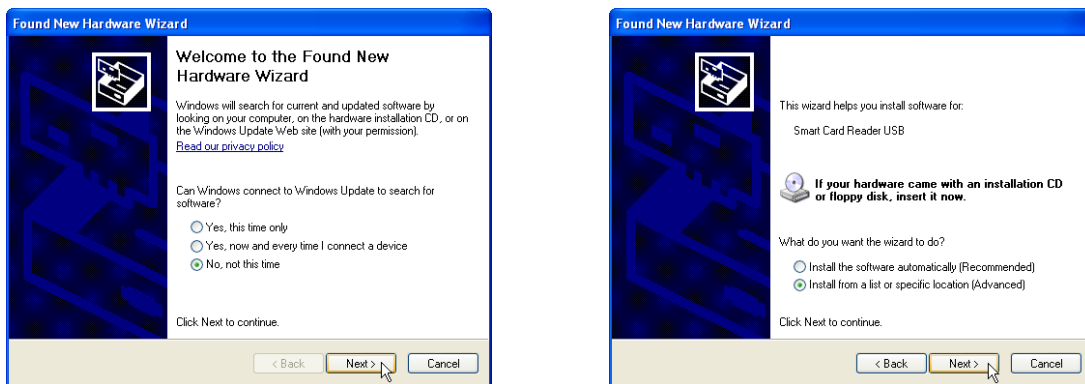


Fig. 2.1: Found New Hardware Wizard (Step 1 and 2 - Windows XP)

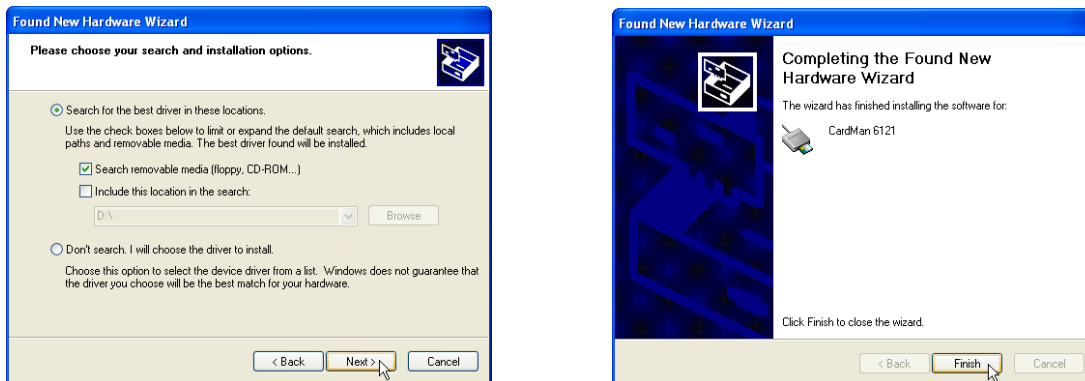


Fig. 2.2: Found New Hardware Wizard (Step 3 and 4 - Windows XP)

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
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. 2.3). 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. If you have installed Mozilla Firefox already installed on your PC, you will be asked if you want the SafeSign PKCS#11 Module to be installed for accessing the CrypToken within Firefox (see Fig. 2.4). Click the "Install" button to do so. Firefox will be opened, and you need to confirm the installation of the PKCS#11 module with "OK". You will receive a message that the installation was done. Click "OK" and close Firefox to continue with the SafeSign installation.



If you did not select to install the SafeSign PKCS#11 Module in Firefox during SafeSign setup, you can do it later manually. Read more about manual installation in chapter 4.1.

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

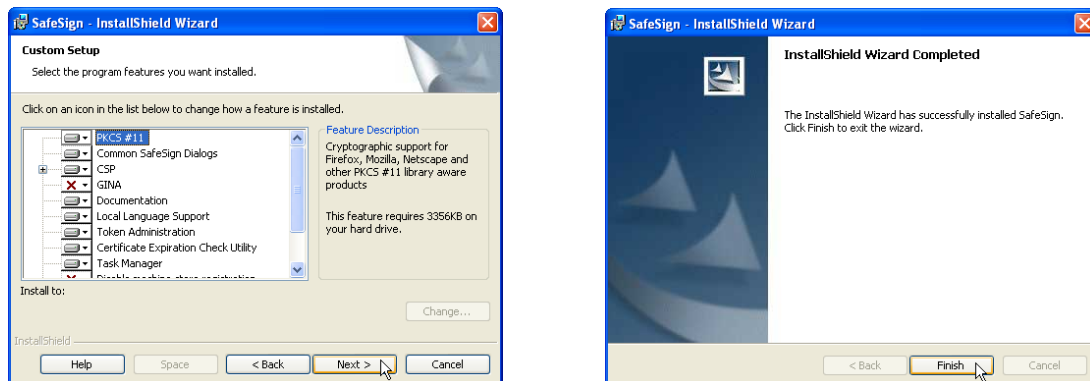
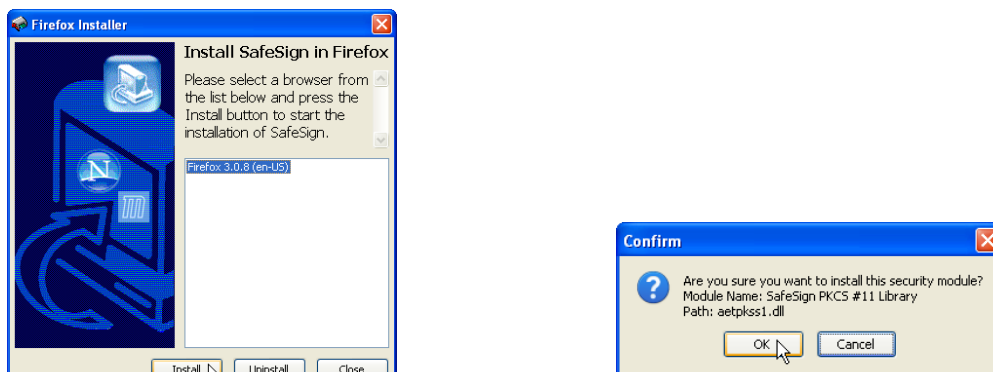


Fig. 2.3: SafeSign installation



2.4: Installing PKCS#11 Module in Firefox

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:

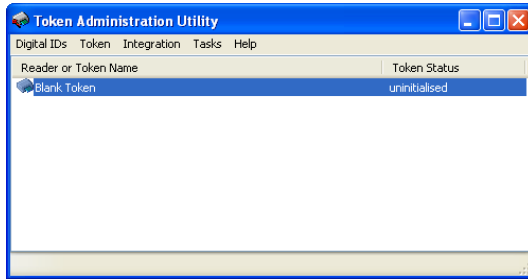


Fig. 2.4: Token Management: uninitialized CrypToken

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".

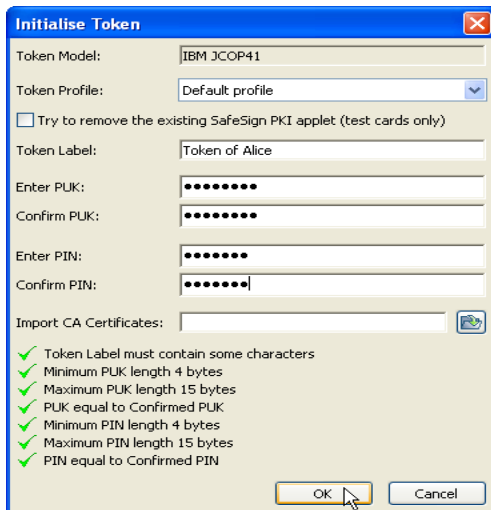


Abb. 2.5: Initializing the CrypToken

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.

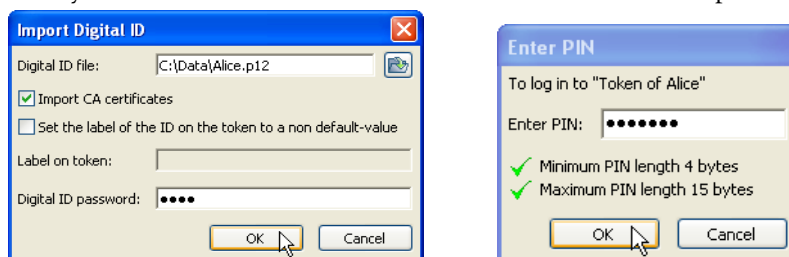


Fig. 3.1: Import Digital ID

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. Firefox Configuration



This step is necessary only if you did not install the SafeSign PKCS#11 Module for Firefox during SafeSign installation (see chapter 2.2), or if you want to check if the PKCS#11 Module was installed correctly. Otherwise please continue reading in chapter 5.

The configuration is described for Firefox Version 3.0.9.

Attach CryptToken, start Firefox and go to "Tools ⇒ Options".

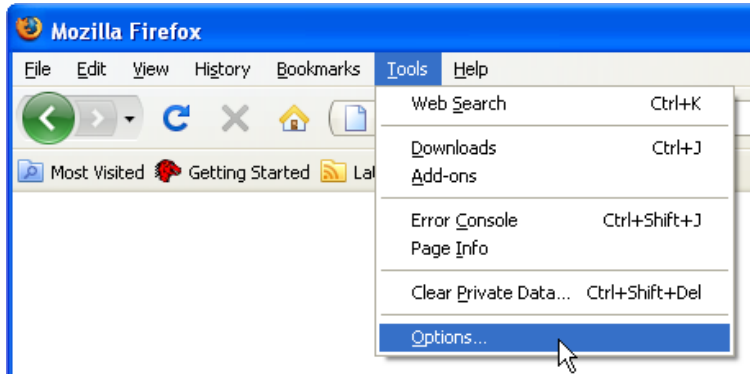


Fig. 4.1: Tools ⇒ Options

Select "Security Devices".

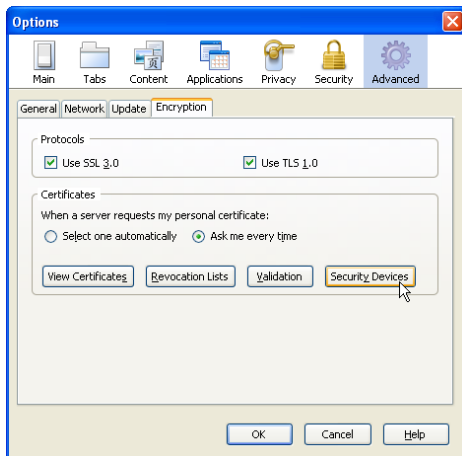


Fig. 4.2: Advanced ⇒ Encryption ⇒ Security Devices

Load the SafeSign PKCS#11 Module for the CryptToken. To do so click on "Load", enter a Name for the Security Module (e.g. "CryptToken PKCS#11 Module") and browse to C:\Windows\System32\Aetpkcs1.dll.

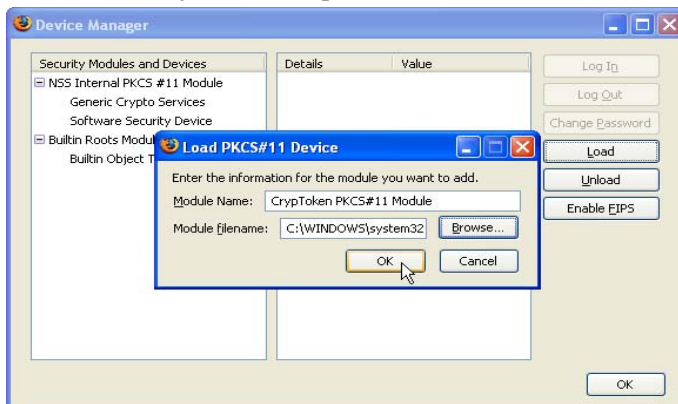


Fig. 4.3: Load PKCS#11 Device

Afterwards please confirm that you want to install this security module. Firefox will notify you that the security module has been installed successfully. You can check if the CrypToken was installed correctly by clicking on the Security Module. The screen output has to be similar to this:

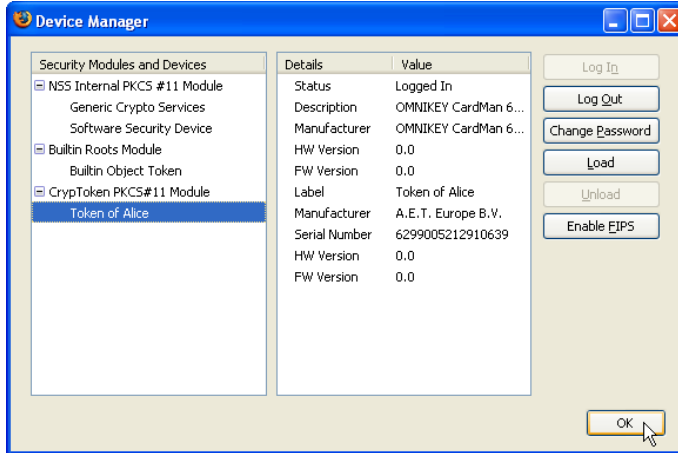


Fig. 4.4: Check communication with the Token

5. Establishing a SSL connection

When a browser points to a secured domain (e.g. <https://www.cryptoken.com>), a SSL handshake authenticates server and client (with the client certificate that is stored on the CrypToken). Afterwards an encrypted transmission channel is established that utilizes a unique session key. The secure SSL connection is indicated by a lock symbol in the lower right corner of Firefox (see Fig. 5.1). Additionally the HTTP address turns into HTTPS and the page logo is shown with blue background (see Fig. 5.2). If the website uses an Extended Validation (EV) certificate, the logo will be shown with a green background and will additionally display the name of the company.



Fig. 5.1: Lock symbol during SSL connection



Fig. 5.2: Firefox address bar during SSL connection (with normal and EV certificate)

To view servers certificate click in the lock symbol in the lower right corner.


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 / intranet identification.
- DataSecurity: Encryption of sensitive information.

Email Encryption
Outlook, Outlook Express, Mozilla, Thunderbird, Netscape and PGP.

eBusiness Client Applications
SSL v3 compatible for Public Key Authentication.


PKI Support
Secure storage of Microsoft, VeriSign, RSA Keon and other CA certificates.



Network- and PC Security
VPN, secure logon, data encryption.

MULTOS/JavaCard on-board
Certified SmartCard OS for high security.

CrypToken Evaluation Kit:
www.cryptoken.com/eval
+49 (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 / 9295-29
contact@cryptoken.com

www.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

Download the latest Application Notes: www.cryptoken.com/AN