Cryptoplus Card Manager v. 1.1.31
USER GUIDE
Customised version for ČSOB a.s. - English

August 2003
# Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contents</td>
<td>2</td>
</tr>
<tr>
<td>1. Foreword</td>
<td>3</td>
</tr>
<tr>
<td>2. CryptoPlus – How to Start</td>
<td>4</td>
</tr>
<tr>
<td>2.1 HW and SW preconditions</td>
<td>4</td>
</tr>
<tr>
<td>2.2 Licence Restrictions</td>
<td>5</td>
</tr>
<tr>
<td>2.3 Language Support</td>
<td>5</td>
</tr>
<tr>
<td>2.4 Types of readers supported by CryptoPlus</td>
<td>5</td>
</tr>
<tr>
<td>3. CryptoPlus Installation – Basics</td>
<td>6</td>
</tr>
<tr>
<td>3.1 Start Installation</td>
<td>6</td>
</tr>
<tr>
<td>3.2 Reader Driver Installation</td>
<td>8</td>
</tr>
<tr>
<td>3.3 CryptoPlus SW Installation</td>
<td>10</td>
</tr>
<tr>
<td>3.4 Reinstall, Uninstall CryptoPlus</td>
<td>14</td>
</tr>
<tr>
<td>4. Basic Functions and Control of CryptoPlus</td>
<td>19</td>
</tr>
<tr>
<td>4.1 CSP Parameters</td>
<td>22</td>
</tr>
<tr>
<td>4.2 Change PIN/PUK</td>
<td>23</td>
</tr>
<tr>
<td>4.3 Data Objects</td>
<td>25</td>
</tr>
<tr>
<td>5. Advanced Functions of CryptoPlus</td>
<td>27</td>
</tr>
<tr>
<td>5.1 Installation of CryptoPlus to be used in Netscape or Mozilla</td>
<td>27</td>
</tr>
<tr>
<td>5.2 Uninstall CryptoPlus used in Netscape or Mozilla</td>
<td>29</td>
</tr>
<tr>
<td>5.3 Internet Explorer 5.x Settings</td>
<td>31</td>
</tr>
<tr>
<td>5.4 MS Outlook 2000 Configuration</td>
<td>31</td>
</tr>
<tr>
<td>5.5 Outlook Express 5 Configuration</td>
<td>32</td>
</tr>
<tr>
<td>5.6 Netscape Communicator Configuration</td>
<td>34</td>
</tr>
<tr>
<td>6. Product Update</td>
<td>40</td>
</tr>
<tr>
<td>7. Smart Card Reader Installation</td>
<td>41</td>
</tr>
<tr>
<td>GemPC410, GemPC413, GemPC Twin serial, CardMan2011</td>
<td>41</td>
</tr>
<tr>
<td>GemPC430, GemPC433, GemPCTwin USB, CardMan 2020, CardMan 3121</td>
<td>42</td>
</tr>
<tr>
<td>GemPC400, CardMan 4000</td>
<td>42</td>
</tr>
<tr>
<td>8. Index and Basic Terminology</td>
<td>43</td>
</tr>
<tr>
<td>8.1 How is the certificate used in Windows?</td>
<td>45</td>
</tr>
<tr>
<td>8.2 Does the certificate always have to be on the card?</td>
<td>45</td>
</tr>
<tr>
<td>8.3 What is the difference between using the card in IE and Netscape Communicator?</td>
<td>45</td>
</tr>
</tbody>
</table>
1. Foreword

Dear Customer,

You have purchased a product whose primary task is to increase the security of electronic communication on the Internet. The basic component of the system is a cryptographic smart card that can reliably keep any secret confided in it – a private cryptographic key. Apart from this secret, the card also stores your X.509 certificate, i.e. a public block of data describing your identity (e-mail, address, job position, etc.), and the certification authority certificate, as well.

However, the aim of this document is not to acquaint you with the security principles used, but it is to help you with the first configuration of CryptoPlus, Internet Explorer and program for sending e-mail messages so that they co-operate with the smart card.

CryptoPlus Manager is equipped with detailed Help, the instructions and options how to work with the program are displayed continuously. Therefore the User Guide, which you are reading just now, describes only basic procedures, it does not deal with all the dialogs and possible error statuses.

We would like to thank you for your interest in our CryptoPlus product and wish you all the best.
2. CryptoPlus – How to Start

2.1 HW and SW preconditions

**HW Requirements**

- HW with the performance necessary to run the operating systems Windows 95, version OSR 2.1, Windows 98, Windows ME, Windows NT 4 SP6, Windows 2000, Windows XP.
- Free serial (or USB, PCMCIA) port to connect a smart card reader (connection requirements are defined by their manufacturers).

*It is necessary to use DIN/PS2 – PS2/DIN reduction, particularly with older types of PC that do not use PS/2 type to plug in a keyboard or mouse.*

- You can also use other readers than the ones recommended by the companies Gemplus or Omnikey. However, such readers have to be fully PC/CS compatible and their manufacturers have to supply them with recent drivers.

**SW Requirements**

The current version of CryptoPlus is natively integrated into a cryptographic subsystem of the operating system Microsoft Windows (it was tested with the versions Win95 OSR 2.1, Win98, WinME, NT4.0 SP6, Win2000 and WinXP). It means that any application using this cryptographic subsystem can co-operate with CryptoPlus smart card, too.

The applications are as follows:

*Attention!*  
- Microsoft Internet Explorer (version 5.0 and higher)
- Microsoft Outlook Express (version 5.0 and higher)
- Microsoft Outlook (version 2000 and higher)

Cryptoki module is supplied for Netscape, which is designed for versions 7.x and higher. As far as Mozilla is concerned, it is designed for versions 1.2 and higher.
2.2 Licence Restrictions

Licence terms and conditions for PC/SC interface of smart card readers and CryptoPlus – card manager are displayed on the screen during the installation. Since the reader driver files are in an original form stipulated by the reader manufacturer, the licence terms and conditions are in English language.

2.3 Language Support

There are several language mutations of CryptoPlus software in order to communicate in a user’s mother tongue. The selection of a language that the modules mutually communicate is controlled by the settings of regional support in the Windows operating system. If there is language support in CryptoPlus for the region of a user, the modules will use it. If the language is not available for the given region, the modules will use their preset language to communicate.

Note: The region of a user means currently selected regional support, which does not have to correspond with the Windows version. Some users can work with the English version of Windows with the region set for Slovak. CryptoPlus modules will communicate in Slovak with such users.

Recent CryptoPlus version supports the following languages: English, Czech, German, Slovak, Hungarian. The language support selection is performed during the installation, the language selection can be changed later with CryptoPlus application – card manager without reinstallation.

2.4 Types of readers supported by CryptoPlus

Gemplus and Omnikey original drivers (i.e. without any adjustments) are embedded in the Installer. The readers are standard part of CryptoPlus supplies. They are as follows:

- Serial port readers:
  - **Gemplus**: GemPC410, GemPC413, GemPCTwin,
  - **Omnikey**: CardMan 2011

- USB readers:
  - **Gemplus**: GemPC430, GemPC433, GemPCTwin,
  - **Omnikey**: CardMan 2020, CardMan 3121

- PCMCIA readers:
  - **Gemplus**: GemPC400
  - **Omnikey**: CardMan 4000
3. CryptoPlus Installation – Basics

The installer is designed to make work for an ordinary user as easy as possible. When installing, it detects various statuses and through synoptic summaries and hypertext links it offers the user the next steps.

If the installer finds some components already available on your PC, it will leave them unchanged and it will use them for its operation. For instance, a functional PC/SC reader is installed on your PC. If the installer detects it correctly, it will announce the fact on the opening screen and it will offer the next step to continue the installation (it will not offer the reader installation).

PC/SC support for communication with a reader is installed simultaneously with reader drivers. If PC/SC support is part of an operating system (from Windows 2000 and higher) or it is available on PC as the result of the previous installation, this step is also skipped.

3.1 Start Installation

As the installer restarts PC during the installation, we recommend closing all the applications running on your PC to avoid unsaved data loss.

Get the reader ready, but do not connect it to PC for the time being! Insert the installation CD into the drive. Use the File Explorer to start it manually (file Install.exe) unless the installation program starts automatically.

After the program starts, the opening screen displays the installation diagnostics. At first the installation guide detects the installed components, it offers the next recommended installation step in the part “How to continue?”. If you need to carry out other steps than the suggested ones, click on link “Other possibilities>>” to list the menu.

In fact, the installer can be started any time, without any impact on the current installation in PC.

1. No other applications can be running during the installation!
2. The installation in Windows NT4, Windows 2000 a Windows XP requires the system administrator permission!

The application Install.exe starts the installation.

After the installation starts, the language, in which the installation will be done, is selected. You can choose from Czech, Slovak, German, English, and Hungarian languages. Preset language corresponds to regional settings in Windows.
After the language is selected, CryptoPlus Installation Guide starts. The Installation Guide provides the user with detailed information about the installation status and it proposes problem solutions.
Screen Item Description:

- **PC/SC** – Windows communication interface, the interface is not installed in W9x operating systems as a standard, the installation is performed automatically during the reader installation.

- **No. of readers available** – the figure informs about the number of the readers with which the installer communicates through PC/SC interface correctly.

- **Installation package** – it shows the version of the installation package you are going to install.

- **CSP** – Cryptographic Service Provider – a dynamic library that implements cryptographic standards and algorithms. The item informs about the installation status and it displays the version of the installed CSP.

- **PKCS#11** – a standard interface for the devices that keep confidential information and perform cryptographic operations.

- **Card Manager** – informs about the version of already installed CryptoPlus – Card Manager.

- **Language** – informs about the language selection. The language selection will also be reflected in the Card Manager.

- **Operating system** – informs about the version of the operating system.

### 3.2 Reader Driver Installation

Unless your smart card reader is installed, click on “**Install smart card reader**”. The option will be displayed even if the reader is installed and connected, but due to the communication error the installer cannot detect it.

The following installer window displays a list of supported readers and their photos. Check the bottom side of your reader for type specification and select the appropriate type from the list. Be careful with the reader selection – when installing a different type, communication errors can occur.
The following instructions must be obeyed when installing the reader:

- Connect the reader after the installer has asked you.
- Do not install drivers without the installer (errors in PC/SC function can occur).
- Do not disconnect the reader upon the reader connection and installation, keep it connected permanently.
- Install the reader only on a functional port without any conflict.
- Do not share the port for reader connection with any other interface. Upon communication interrupt, PS/CS interface cannot establish the connection with the reader unless PC is restarted.

Some systems (Win95/98) do not provide the support to communicate with readers and smart cards – so called PC/SC – as a standard. If the support is not found on your PC, the program will install it prior to the reader installation. Before PC/SC is installed, it is necessary to agree with
the licence terms and conditions (written in English). If you click on the link *I agree*, the installation continues, otherwise the installation returns one step back.

Upon reader driver installation

![Figure 4.: Dialog window „Please wait...“](image)

you will be asked to restart your PC and to connect the reader only after you **enter to restart PC!!**

![Figure 5.: Dialog window „Connect the reader“](image)

See chapter 8 for detailed description of reader connection.

### 3.3 CryptoPlus SW Installation

If the reader is installed properly, you can select *Install CryptoPlus SW*.
User Guide

Installation Guide
CSOB CryptoPlus

Installation Guide helps CryptoPlus package to be applicable even to non-skilled user. Program digestedly notifies installation status, suggests problem solutions.

Up-to-date CryptoPlus installation status:

- At least one reader is accessible on the system. CryptoPlus software is not correctly installed. CryptoPlus (or same component) is not correctly installed and cannot be used.

What's the next step?
Install CryptoPlus software
- Install software for correct functionality of cryptographic subsystem based on smart cards.
- You must accept licence agreement before installation.

Tick boxes help you with adjusting the scope of the installation and file placement on hard disk.

Installation of CryptoPlus to be used in Netscape and Mozilla is described in Chapter 5.

Figure 6.: Dialog window „CryptoPlus software installation“

The next window shows license terms and conditions relating to CryptoPlus SW. After you have read the conditions, you must click on either “I agree” or “I do not agree” at the bottom of the screen. If you agree, the installation continues with setting the parameters for the installation.

Tick boxes help you with adjusting the scope of the installation and file placement on hard disk. Installation of CryptoPlus to be used in Netscape and Mozilla is described in Chapter 5.
It can happen in some cases that CryptoPlus SW has already been installed in a version customised for another provider (e.g., a different bank). CryptoPlus can be installed in more customised versions on one computer (each version is stored in a separate directory on a hard disk) and they can be used alternately. If more readers are used, they can be used even simultaneously! In such case the installer detects it automatically and offers a list of installed cards. The user has to tick the versions to be used simultaneously. If you are not sure about the registered cards, better leave them all.
When installing, a dialog window informing you about registered card collision can appear. If you are not going to use any of the listed cards, you can delete its registration.

If you are not sure, or if you use a card similar to another software, we recommend you not to delete the registration of the colliding cards, however, in such case it is most suitable to add these cards to the list of supported cards.

It is necessary to restart PC to run the reader and CryptoPlus properly. After PC restart, the installer runs once more to check for any error. If all the components are installed, you can select either “Terminate” the installation program, or “Run CryptoPlus – Card Manager”. If an error is found, the screen will display the next suggested step, which is the result of detection of separate needed functions. If you prefer not to terminate the Installation Guide, click on “other possibilities >>”.

If the Installation Guide does not start automatically after PC restart, start it manually (file install.exe).

![Installation Guide](image)

**Figure 10.: Dialog window „Terminate Installation Guide“**
3.4 Reinstall, Uninstall CryptoPlus

System administrator authorization is necessary to uninstall CryptoPlus in Windows NT4 and Windows 2000 XP!!

There are three ways to uninstall CryptoPlus:
1. Click on application module *UnInstall* in the menu *Start ➔ Programs ➔ CryptoPlus*.

*Figure 11.: Dialog window „Confirm CryptoPlus Uninstall,“*

*Figure 12.: Dialog window „System Settings Change – Computer Restart“*
Run Installation Program Install.exe

Procedure:

- Insert installation CD into CD ROM drive.
- Click on “Install SW CryptoPlus” in the main menu, or use File Explorer to run the installation file from CD ../Install.exe.

![Installation Guide](Image)

**Installation Guide**

**CSOB CryptoPlus**

Installation Guide helps CryptoPlus package to be applicable even to non-skilled user. Program digestsedly notifies installation status, suggests problem solutions.

**Up-to-date CryptoPlus installation status:**

At least one reader is accessible on the system; CryptoPlus software is installed. CryptoPlus is completely installed and ready for use.

**What’s the next step?**

Your CryptoPlus product has been installed properly. You can terminate the installation program. To register the certificate, run CryptoPlus - card manager.

[other possibilities >>]

**Detailed status of CryptoPlus installation**

<table>
<thead>
<tr>
<th>PC/SC</th>
<th>No. of readers available</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Installation package</td>
<td>1, 1, 29, 30724 CSOB Edition</td>
<td></td>
</tr>
<tr>
<td>CSP</td>
<td>[installed][2, 3, 989, 2807]</td>
<td></td>
</tr>
<tr>
<td>PKC5#11</td>
<td>[installed][pkcs5.dll[1, 0, 32, 3107] ]</td>
<td></td>
</tr>
<tr>
<td>Card manager</td>
<td>[installed][1, 3, 2, 2907]</td>
<td></td>
</tr>
<tr>
<td>Language</td>
<td>EN</td>
<td></td>
</tr>
<tr>
<td>Operating system</td>
<td>Microsoft Windows 2000 Professional Service Pack 4 (Build 2195) [2, 5, 0, 2195]</td>
<td></td>
</tr>
<tr>
<td>MS Internet Explorer</td>
<td>[6, 0, 2600, 1106]</td>
<td></td>
</tr>
</tbody>
</table>

**Accessible smart card readers**

Gemplus USB Smart Card Reader 0 | [works fine]

![Figure 13.: Dialog window „Installation Guide“](Image)

Click on „other possibilities >>“ to display alternatives to CryptoPlus installation.

**The following functions are involved:**

- **Repair current CryptoPlus installation**

  This option displays if the installer detects an installed version. After the earlier installation is detected, it is repaired, i.e. the missing parts of the recent installation are added.
**Install smart card reader**
The option enables you to install a reader from the list of supported readers. You can use this option to update the system with another reader or to repair faulty reader installation.

**Installation status**
A function to find out quickly if the CryptoPlus installation has been completed successfully. In particular, it is useful for notebook users where external peripheries are frequently plugged in and unplugged. Its aim is to check the current status of CryptoPlus installation.

**Restart computer** – after PC restart all the modification, carried out during the installation, are activated. CryptoPlus cannot be correctly used without restart. When selected, the installer is launched and the installation status is displayed.

**Uninstall CryptoPlus software**
Upon click on „Uninstall CryptoPlus software“, CryptoPlus will be uninstalled without any further warning.

It is necessary to uninstall the software in the following cases:
- CryptoPlus re-installation
- If the previous installation has been interrupted or any other error has occurred.
- Prior to the installation of new CryptoPlus version

**CryptoPlus software update**
If the installer detects an existing version of CryptoPlus, it evaluates whether it is older. If it is older, update is offered. In such case, it is displayed on the main screen of the installer.

**Forced reinstallation of CryptoPlus**
The option is available if any CryptoPlus version is installed. Use it to reinstall the software if the attempts to correct errors failed. The option does not solve reader communication errors.

**Uninstall PC/SC**
The option allows uninstalling Windows PC/SC interface. When installing the reader, PC/SC interface is installed again. With PC/SC reinstallation you can avoid possible problems with reader functionality. The option is displayed only if PC/SC has been installed and only on W9x and WNT4, WME. PC/SC interface cannot be uninstalled on other operating systems. Correction is carried out with standard means of Windows.

**Support Request Form**
If problems with CryptoPlus software installation occur, you can use this form to ask support technicians for help.
Alternative suggestions for CryptoPlus installation

If the recommended step (after repeating) hasn’t made correct installation, try to use some of the offered alternatives. Read suggestion list carefully and use the most suitable hint. None of the offered suggestions can cause irreversible changes of operating system or computer destruction. All of them are created to be used by non-skilled users:

- **Repair current CryptoPlus installation**
  "1. 2. 29. 30.724 Code Edition" version is installed on your computer. All its components will be overwritten with the same version. Useful in case the CryptoPlus used to work OK but suddenly it is malfunctioning.

- **Install smart card reader**
  Select and install smart card reader.
  On some operating systems (Win95/98) smart card support (PC/SC) is not installed by default. If smart card support is not found on the computer, Installation Guide will install it before reader installation. You must accept PC/SC licensing agreement before installation.
  Use this option to install more readers. It’s not possible to use more than one reader on some operating systems (Win95/98).

- **Installation status**
  You can re-check status of installation. It can be useful when administration tasks (installation of system software, file manipulation...) was performed during Installation Guide run.
  New test is also recommended after automatic restart of Installation Guide. It is possible installation Guide may be started before some drivers and services and consequently the results of the intuitive test can be inaccurate or distorted.

- **Restart computer**
  Turning on and off the computer should remove possible collisions in the computer settings, start the necessary procedure and register the libraries.
  When the system starts again, the Installation Guide should start automatically. If it does not, run it manually.

- **Uninstall CryptoPlus software**
  Uninstall CryptoPlus software from the computer.
  You can install CryptoPlus again in the future.

- **Perform uninstallation of CryptoPlus**
  Uninstall software without view to the previous installation. It is strongly recommended to use this in extreme case only.
  You must accept licence agreement before installation.

- **Support request form**
  If you have any problems with installation of CryptoPlus, please fill out this form and send it to helpdesk.

- **Terminate Installation Guide**

---

Figure 14.: Dialog window "Alternative suggestions for CryptoPlus Installation"

Upon click on "**Uninstall CryptoPlus software**", you will uninstall CryptoPlus software, you will also be asked to restart the computer.
Installation Guide
CSOB CryptoPlus

Installation Guide helps CryptoPlus package to be applicable even to non-skilled user. Program digestedly notifies installation status, suggests problem solutions.

**Up-to-date CryptoPlus installation status:**

At least one reader is accessible on the system. CryptoPlus software is not correctly installed.

CryptoPlus (or some component) is not correctly installed and cannot be used.

**What's the next step?**

**Restart computer**

Turning on and off the computer should remove possible collisions in the computer settings, start the necessary procedure and register the libraries.

When the system starts again, the installation guide should start automatically. If it does not, run it manually.

[Other possibilities >>](#)

---

**Detailed status of CryptoPlus installation**

<table>
<thead>
<tr>
<th>PC/SC</th>
<th>works fine</th>
</tr>
</thead>
<tbody>
<tr>
<td>No. of readers available</td>
<td>1</td>
</tr>
<tr>
<td>Installation package</td>
<td>1.1.20.36724 CSOB Edition</td>
</tr>
<tr>
<td>CSP</td>
<td>not installed</td>
</tr>
<tr>
<td>PKCS#11</td>
<td>not installed</td>
</tr>
<tr>
<td>Card manager</td>
<td>not installed</td>
</tr>
<tr>
<td>Language</td>
<td>EN</td>
</tr>
<tr>
<td>Operating system</td>
<td>Microsoft Windows 2000 Professional Service Pack 4 (Build 2195) [2.5.0.2195]</td>
</tr>
<tr>
<td>MS Internet Explorer</td>
<td>[6.0.2800.1106]</td>
</tr>
</tbody>
</table>

---

**Accessible smart card readers**

*Figure 15.: Dialog window „Restart computer“*
4. Basic Functions and Control of Cryptoplus

If you want to use a smart card to encrypt and sign e-mail messages, or to authorize with secure connection with web server, several conditions must be obeyed:

1. CryptoPlus software support must be installed.
2. The smart card must contain your private key with the relevant certificate.
3. Cryptographic system MS Windows must know your X509 certificate.

Your certification authority should help you fulfill the last two conditions.

If you receive CryptoPlus card that contains the certificate, it is sufficient to register the certificate in Windows through the utility of CryptoPlus – Card Manager (part of CryptoPlus installation package).

Active card operations (e.g. electronic signature calculation) are protected with PIN (Personal Identification Number).

Use the utility of CryptoPlus – Card Manager to unblock or change the PIN.

From the security point of view it is most important that the card owner is the only person to know PIN, or PUK. PIN or PUK disclosure to another person brings a risk of card abuse – the card is your electronic identity!

CryptoPlus – Card Manager is CryptoPlus smart card management program. This utility is equipped with special functionality that detects various problems and tries to solve the way to solve them.

See the program itself and “Help” for complete description of utility functions of CryptoPlus – Card Manager.

1. Insert the smart card into the reader.
2. Run Cryptoplus – Card Manager utility (upon standard installation, you can find it in desktop or in the menu Start → Programs → CryptoPlus → CryptoPlus.)
3. After Card Manager start it is necessary to download the card data first. “Solution suggestions” and “No data read from the card” displays in the main window. Insert the card into the reader and click on the underlined word “refresh”, or select Show → Renew from the program menu (use F5 as the hot key).
If another problem is displayed in the main window, e.g. reader connection or installation error, use program Install.exe to solve (detect) the problem. This program contains mechanisms to detect current installation status, it can give advice on how to solve the problem.

4. After the card data is downloaded, the automatic problem detector should list the unregistered certificates.
   Click on register to register every certificate you want to use actively.
Note 1: When registering the root certificates, the system offers you to add the certificate to the root certificate list. Before you approve of the operation, check the values of SHA-1 hash certificate displayed by CryptoPlus utility and the dialogue asking for a permission to add the root certificates. They should be the same.

Note 2: The certificate registered in this way is withdrawn from the “trouble” certificates immediately.
The certificate registration can also be performed by selecting the certificate you want to register in the left window and by selecting the function *Certificate → Register* in the Menu.

5. If the certificate is valid and registered in Windows, you can work with it in the applications that use cryptographic subsystem MS Windows. (Internet Explorer, Outlook Express, Office XP…)

### 4.1 CSP Parameters

CryptoPlus CSP use several parameters to modulate its functionality. The parameters are saved in the system registers and they are described in CSP documentation.

Some CryptoPlus CSP parameters can be displayed and changed through *CryptoPlus – Card Manager* program. They are as follows:

**CSP library version**

Information about currently installed CSP versions. *CryptoPlus – Card Manager* program cannot change this information, it changes automatically upon the installation of new CSP library version. Comparing the library versions, you can find out if the most recent version is installed. The number of the version can be significant information with CSP problems and possible hotline contact.

**Language**

Users can select languages to communicate with CryptoPlus applications.

**Dialog Timeout**

It sets timeout of CSP dialog window display in the range 30 – 600 seconds. If the user does not respond within the stipulated time to CSP window, the window closes automatically, as if the user has cancelled the action (Cancel). This setting does not apply to the PC/SC window for card opening. Alternative communications modules may not use this parameter.
Enable taskbar animation

If the user prefers not to display animation on the taskbar of the desktop, they can leave the field empty (no tick). CSP activity will then go on without accompanying animation. The animation symbolizes the course of the operations performed by CryptoPlus CSP. Turning on and off the animation does not have any impact on the way and security of CSP functioning.

Remember PIN by default

It influences the dialog initial setting to verify PIN. If the user has ticked Remember PIN by default, the field Remember for this session will always be ticked automatically when the dialog to verify PIN is displayed – and vice versa. The preset option can be changed after the dialog to verify PIN is displayed.

PIN time limit in the memory

It sets the maximum time interval for which CryptoPlus CSP can keep PIN value in the memory. The entered value can range from 5 minutes to 1440 minutes (= 24*60 = 1 day).

The option CSP Parameters displays the current parameter settings. The user can change the values and save them by the key “Save”. If the new values fail to be processed, the program generates error message. Upon successful saving, the new (current) values of the parameters will be displayed. The change of parameter settings becomes effective only upon the next start of the application using CryptoPlus card.

4.2 Change PIN/PUK

Active card operations (e.g. electronic signature calculation) are protected with PIN (Personal Identification Number).

⚠️ Attention! ⚠️ Three successive incorrect PIN entries will block the card. Only PUK (PIN unblock code) can unblock the card. Maximum four successive incorrect PUK entries are accepted. After the fifth successive incorrect entry the card is blocked irreversibly!

The initial PIN and PUK for cards will be received together with the card in a sealed envelope. If you need to change the initial PIN, or to unblock the card, use the CryptoPlus program and follow the guide below:

⚠️ Caution ⚠️ Due to security reasons it is most important that the card holder is the only person to know PIN and PUK. Disclosing PIN and PUK to another person brings a risk of card abuse – the card is your electronic identity.
Guide to Change PIN and PUK:

1. Insert the smart card into the reader.
2. Close all the applications that use CryptoPlus card.
3. Run CryptoPlus utility (after standard installation you can find it on the desktop or in the menu `Start → Programs → CryptoPlus → CryptoPlus`).
4. Read data about the card using the menu `Show → Renew`.
5. Select CryptoPlus card from the left window.

![Figure 19.: Window shown after the initial data download from the card](image)


![Figure 20.: Window with data about the card and Change PIN command](image)

Select the requested operation from the dialog window, enter necessary data and confirm with `OK`. The new PIN or PUK must have at least 4 digits and maximum 8 digits. Two parameters are checked to confirm the change: the length of the code and if the new value is the same as the re-entered one.
7. The card will use new PIN, or PUK, if the change was successful.

### 4.3 Data Objects

Data objects in CryptoPlus cards are user-defined data. They can be of various formats designed by the application that manages the data object. Data object values can be protected with PIN. Therefore, the data objects can be used to store sensitive data (passwords, codes, etc.). To access the data objects, PKCS#11 interface is used typically.

CryptoPlus – Card Manager utility shows detailed information about the data object selected in the information tree. The information about data objects include:

**Application**

The name of the application that is the data object manager. It is not compulsory.

**Name**

The name of the object.

**Protected with PIN**

Information whether the data object value is publicly accessible or its reading is subject to PIN entry.

**Data length**

Data value length, in bytes.
Data

Data value statement. 3 columns of information are displayed: data offset, data in hexadecimal and textual forms. If data reading is PIN protected and the data has not been read yet, the possibility to read the PIN protected value from the card is displayed.

Data object can be deleted

The possibility to delete the data object from the card is displayed.
5. Advanced Functions of CryptoPlus

The following chapter describes methods of installing and uninstalling CryptoPlus support for some other applications and how to configure the programs to make them use certificates as a security tool.

The dialogs displayed can differ from those you can see here; even the names of the menu items can be completely different. It is not possible to describe the configuration of a relatively wide range of applications that can be used by CryptoPlus cards. Therefore we suggest that you prefer the methods specified in the updated software documentation.

5.1 Installation of CryptoPlus to be used in Netscape or Mozilla

If Netscape or Mozilla viewer installation is detected, the possibility to register the module CryptoPlus Cryptoki to be used in these viewers is offered at the beginning of the installation.

![Figure 23.: Window for installation components](image)

![Figure 24.: Confirmation question prior to registration](image)
Figure 25.: Example of a window to register in Netscape browser

As soon as the registration is completed, part of CryptoPlus software utility installation is closed, the completeness of the installation so far is checked and if no errors have been found, the status is displayed on the screen.
5.2 Uninstall CryptoPlus used in Netscape or Mozilla

If Cryptoki module has been registered, the uninstaller offers you to unregister the module from Netscape (Mozilla).
Unregistering CryptoPlus Cryptoki.

With the help of this page you can unregister CryptoPlus support from your navigator. CryptoPlus Cryptoki Module can be registered.

Unregistered Cryptoki

Copyright © MCO.NET, s.r.o. All rights reserved.
CryptoPlus™ is registered trademark of the product.

Figure 30.: Example of a window to unregister in Netscape browser

Figure 31.: Dialog window „Confirm module uninstall”

Figure 32.: Dialog window „Information about module deletion”
5.3 Internet Explorer 5.x Settings

If the certificate is registered in MS Windows (see the chapter above) and it is valid, it can be used to client authentication for secure communication with a web server without any other explorer configuration. The certificate, however, must be issued for this purpose and the web server must recognize the certificates of your certification authority.

5.4 MS Outlook 2000 Configuration

1. Insert the smart card into the reader.
2. Run MS Outlook
3. Select Tools → Options in the application menu.

Algorithm” automatically. If they do not (e.g. you have more certificates), choose suitable certificates with “Select” key. Confirm the setting with „OK“.

![Change Security Settings](image)

**Figure 35.: Toolbar to change Outlook 2000 settings**

5. If needed, check in „Encrypt sent message text and enclosures“ and „Add digital signature to sent messages“ in „Options“ window (see point 4).

6. If your certificate is valid and contains relevant authorization, you can use it, together with CryptoPlus card, for electronic signature and incoming message decryption.

### 5.5 Outlook Express 5 Configuration

1. Insert the smart card into the reader.
2. Run Outlook Express
3. Click on **Tools → Accounts** in the application menu.
4. Select an account, with which you want to use CryptoPlus card, in bookmark **All** or **Mail**.
5. Click on *Properties*.

6. Select bookmark „Security” in the window for setting the account properties
7. Choose a certificate suitable for the given purpose and, where possible, select also preferred encryption algorithm (the stronger the level, the higher the security).

8. Confirm with **OK**.

### 5.6 Netscape Communicator Configuration

Contrary to standard “Microsoft applications”, Netscape Communicator does not require certificate registration in the system. It automatically works with the data stored in a smart card. CryptoPlus card can be used with this communicator only if CryptoPlus cryptographic module is registered. If Netscape Communicator is detected, the installer will offer you the registration automatically.
1. Proper CryptoPlus functioning requires CryptoPlus card to be inserted into the reader the moment Netscape is starting.

2. After CryptoPlus module is registered, Netscape start takes a little longer. The reason is that all the data is downloaded from the smart card just before the first window is displayed (if taskbar animation is allowed, you can see the separate steps).

Verification of cryptographic module registration in Netscape 4.7x

1. Run Netscape

2. Select **Communicator → Tools → Security Info (Ctrl+Shift+I)** in the menu.

![Example of the menu to select the function to configure the viewer](image)

Click on „**Cryptographic Modules**“ in „**Security Info**“ dialog. Apart from internal PKCS#11 module, there must also be CryptoPlus module (+ the name of the version) in the list of cryptographic modules.
3. Select CryptoPlus and click on *View/Edit* to open a window with more detailed information about the module. If you see data similar to the data in the following figure, the module should be working properly and the card should be ready for use.

Click on „*More Info…*“ to get further information about the slot (i.e. the reader) and the token (i.e. the smart card).
Certificate Configuration in Netscape Navigator (client authentication on SSL)

1. Run Netscape
2. Select **Communicator → Tools → Security Info (Ctrl+Shift+I)** in the menu.
3. Click on **Navigator** in **Security Info** dialog.
4. Select the most suitable option from the list of certificates **Certificate to identify you to a web site**.

1. If the name of the certificate begins with **CRYPTOPLUS**, it means that Cryptoplus card contains the given certificate along with the private key.

2. If there is a cluster of meaningless letters and digits, use CryptoPlus utility or click on **Yours** (below the title **Certificates**) directly in **Security Info** window and look at the corresponding certificates to get detailed certificate and key identity.

5. Confirm the settings with **OK**.

**Certificate Configuration in Netscape Messenger**

1. Run Netscape
2. Select **Communicator → Tools → Security Info** (Ctrl+Shift+I) in the menu.
3. Click on **Messenger** in **Security Info** dialog.

4. Select your certificate from the list of certificates **Certificate for your Signed and Encrypted Messages**.

   **Note 1:** If the name of the certificate begins with **CRYPTOPLUS**, it means that Cryptoplus card contains the given certificate along with the private key.

   **Note 2:** If there is a cluster of meaningless letters and digits, use CryptoPlus utility or click on **Yours** (below the title **Certificates**) directly in **Security Info** window and look at the corresponding certificates to get detailed certificate and key identity.

5. Confirm the settings with **OK**.
6. Product Update

Contact your supplier for more information about CryptoPlus or visit our web site:
http://helpdesk.cryptoplus.cz/csob

Electronic address for support and discussion: helpdeskEB@CSOB.cz

Free new software versions developed by CryptoPlus team can be downloaded from the web sites named above. To make an orientation easy, the name of installation package will include the number of the version, and a short list of changes compared with previous versions will also be attached. Updated user guide, in PDF format, will be available, too. To view the guide you need Adobe Acrobat Reader software (for free download refer to www.adobe.com).
7. Smart Card Reader Installation

Serial readers do not have their own power supply and they are supplied from PS/2 keyboard port (or mouse).

GemPC410, GemPC413, GemPC Twin serial, CardMan2011

Installation:

- Plug in the reader to free 9-pin PC serial port (port with green colour – if 25-pin port is the only available, you need reduction).
- Unplug the mouse or the keypad and plug in the purple connector from the reader (the mouse or keyboard must have PS/2 connector).
- Plug in the keyboard (or mouse) into the grey external connector of the reader.
- If the reader is connected properly, LED is flashing, if the reader is installed properly and the card is inserted in it, LED begins to light constantly (CardMan 2011 gives green light, when communicating apart from green light it flashes red).
- Mounting: slide the reader on the base (supplied with the reader)

Figure 43.: GemPC410 connection scheme
GemPC430, GemPC433, GemPCTwin USB, CardMan 2020, CardMan 3121

Installation:

- Plug USB connector of the reader in free USB port. After connection the reader is ready for use.

- GemPC430, GemPC433, GemPC Twin are equipped with USB cable, green LED diode. When it is supplied it flashes, when communicating it gives constant light.

- CardMan 2020 and CardMan 3121 give green light, when communicating apart from green light they flash red.

Figure 44.: Connection scheme of the reader with USB connector

GemPC400, CardMan 4000

Installation:

- Plug the reader in the free PCMCIA slot of your notebook.

- If you decide to leave the reader in the notebook, it has to be slid all the way to the slot end. Check if from time to time.
8. Index and Basic Terminology

**AID**
Application Identifier. A unique number of the application stored in a card. Systems working with a card can use AID to find the data for performing requested operations on a card.

**Asymmetric cryptography**
Type of cryptography that uses two different keys – public and private – to encrypt and decrypt data. The data encrypted with one of the keys can be encrypted only with the other from the keys.

The holder must be the only person to know the private key – it requires keeping on a safe place. On the contrary, the public key can be accessible to anyone. Encrypting e.g. e-mail with the public key of the addressee provides a certainty that only the addressee will read the message. On the contrary, if anyone signs a document with their private key, document receivers can verify the author authenticity with the public key.

The most common asymmetric algorithms are RSA and DSA.

**ATR**
Answer to reset (ATR) string of a card. The card uses the string to identify itself in the system after power supply connection.

**Authentication**
Process of verification of identity of a given subject (person, system, etc.).

**Certification Authority (CA)**
An authority which issues certificates. Prior to certificate issuing, CA verifies applicant identity. CA certificate is a root certificate.

**Certificate**
An electronically signed document containing the public key of the user and information about certification user. Therefore, the certificate ties up the information about the user with his public key.

The certificate is typically issued by a trustworthy certification authority (CA).

**Certification Path**
Every certificate is signed with the private key of the certificate issuer. (The exception is a root certificate that is signed with its own key.) Therefore if there is a certificate and an issuer certificate, we can verify cryptographically whether the explored certificate was issued by its supposed issuer. The repeated procedure can verify even the issuer certificate, its issuer, etc. up to the level of the root certificate. This verified string is called the certification path.

Some programs can use only those certificates in the system which all the superior certificates are registered – their certification path is verified completely.
Cryptographic Service Provider

A dynamically linked library. It implements cryptographic standards and algorithms. Win32 implements a standard, purely software version. There are versions of other manufacturers, to increase security, some implement cryptographic operations with hardware components (smart cards or cryptoadapters). The library is used for instance to encrypt/decrypt electronic mail; it is used for electronic signatures, etc.

CSP

See Cryptographic Service Provider

Key

See Private Key and Public Key.

Application Code

Application Identifier - see AID.

PC/SC

A standard Win32 interface to connect smart card readers.

PIN

Personal Identification Number. A numerical code to authorize some smart card operations. PIN is one of the protection means when working with smart cards. Without PIN no one can carry out any operation with a card which requires authorization. If an incorrect PIN is entered several times successively, its use is blocked. Only PUK can unblock PIN.

PKCS#11

A standard interface for devices keeping confidential information and performing cryptographic operations.

Private Key

One of a pair of keys used in asymmetric cryptography. The private key secrecy is one of the security presumptions. The private key is used for electronic signing of documents, for decrypting messages that have been encrypted with the matching public key.

PUK

Personal Unblocking Key. A numerical code to unblock PIN. If a card PIN is blocked upon repeated incorrect entry, entering PUK value can unblock it. Several successive incorrect entries of PUK block its use.

Public Key

One of a pair of keys used in asymmetric cryptography. Unlike the private key, the public key does not require secrecy. The public key is used to verify an electronic signature, to encrypt messages. The messages encrypted with the public key can be decrypted only with the matching private key.
8.1 How is the certificate used in Windows?

If you want the standard “Windows” application to be able to use the functions arising from X.509 certificate actively, the certificate must be registered in the system.

Note: “To use function actively” means generating electronic signature and data decryption.

When the certificate is being registered in the system, also the information necessary for the system to find the matching private key is stored with this certificate (i.e. the key that is used to generate electronic signature or to decrypt data).

The registered certificate can be described as follows:

The application that requires using the private key assigned to the certificate “looks through” information about the certificate registration to find out where to look for the needed private key. Then it asks the cryptographic Windows subsystem for access to this key and if it gains it, it can perform the requested operation.

8.2 Does the certificate always have to be on the card?

If you use the certificate in the applications using the cryptographic Windows subsystem, it does not have to be stored on the card. Registration in Windows is sufficient; i.e. the system knows where the relevant private key is.

If you use the certificate in Netscape Communicator, it has to be stored on the card.

8.3 What is the difference between using the card in IE and Netscape Communicator?

Internet Explorer (Outlook and Outlook Express as well) are programs integrated exclusively into Microsoft Windows. That is why they use standard cryptographic services of this system (by means of Crypto API that uses CSP cryptographic modules). To use the private key in these applications, it is necessary to have the private key together with the registered and valid X.509 certificate with information where to find the private key.
Netscape products are not bound to Microsoft Windows system only therefore they do not rely on their cryptographic subsystem but they use their own cryptographic modules. These modules are implemented according to PKCS (Publicly-Key Cryptography Standards), particularly PKCS#11. Each of these modules is responsible for storing complete electronic identity; i.e. it has to hold the public and private key and relevant X.509 certificate. If you like to use CryptoPlus smart card as the holder of your electronic identity also in Netscape Communicator, the relevant X.509 certificate must be stored on the card apart from the key.

Figure 45.: Registered Certificate

Correct installation procedure and faultless functioning of CryptoPuls requires the proper sequence of every steps of the installation. We recommend you to read carefully the information in the window “Current state of installation” and to control the installation according to the shown recommendations.

1. We recommend closing the running applications on your PC.

2. Čtečku zatím nepřipojíte k PC !!! (viz. poznámka pod čarou).
   Do not connect the reader to PC for the time being!!! (See the note below).
   Insert CryptoPlus installation CD into the drive. If the installation program does not start automatically, use the File Explorer to run the file Install.exe on CD manually.

3. Select the language of the communication during the installation.
   In the installer offer select Install smart card reader and enter the type of the reader you want to install.
   Be careful about selecting the proper reader type, the selection will affect the relevant driver!

4. Select Install CryptoPlus software in the installer offer.

5. The installer will ask you to turn off your PC. At the same time it will ask you to connect the reader to PC.

6. After restart the installer runs again and it displays: „Current state of CryptoPlus installation“. If the installation program does not start automatically, use the File Explorer to run the file Install.exe on CD manually.
   If the installation is completed, close the installer.

Note:
If you connect the reader to PC prior to running the installation, Plug&Play feature of the reader makes the operating system Windows detect the reader immediately and find an implicit driver for it. Although some recent versions of Windows have smart card reader driver embedded directly in installation drivers, these drivers do not have to treat CryptoPlus properly. Therefore cancel the operation when the OS Windows informs you that it has detected new hardware and is to look for a driver for this new hardware. Afterwards you can start the installation as described above.


CRYPTOPLUS ® is a registered trademark pursuant to Act no. 137/1995 of the Code.