

USER GUIDE FOR THE INTERNETBANKING of PPF banka a.s.

Part II: Certificates, OTP codes, SMS codes and working with Tokens

Contents:

1. Introduction	3
2. OTP codes and working with a Hardware OTP Token.....	3
3. SMS codes	4
4. Certificates and working with the Certification Token.....	5
4.1. Certification Centre	5
4.2. Downloading the SW for the correct operation of Internetbanking.....	6
4.3. Downloading the library for working with an electronic key (an applet for the encryption of data) 9	
4.4. Downloading drivers for the Certification Token.....	12
4.5. Downloading the SW for the administration of the Certification Token	15
4.6. Changing the PIN for the Certification Token.....	18
4.7. Generation of the Certificate.....	19
4.8. Renewing a Certificate	22
4.9. Deleting an invalid Certificate	25

1. Introduction

For greater clarity, the User Guide is divided into several parts, which are separate documents. This part describes work with Tokens and Certificates. The rest of the information relating to IB is provided in the other parts of the User Guide.

Where terms, abbreviations or phrases beginning with capital letters are used in this User Guide, their meaning will be as defined in the article "Definition of Terms" in the GBC and/or SBC, or, where applicable, as specified in the individual provisions of the GBC and/or SBC and/or this User Guide.

2. OTP codes and working with a Hardware OTP Token

An OTP code is a single-use numerical code (OTP = One-Time Password). OTP codes are continuously generated every 60 seconds and work on the basis of synchronisation between the Bank's authentication server and the User's OTP Token (they are so-called "time-based codes").

An OTP code is always valid only for a single operation (logging into IB, authorization of a Payment Order or request, creation of a notification etc.). The generated OTP code must be entered and confirmed for the operation performed within 10 minutes of its generation (**NOT of its being displayed!**).

OTP tokens display the currently generated OTP code – they do not generate this code only at the moment when it is displayed.

Only the Hardware OTP Token sold by the Bank may be used to generate and display OTP codes.

What is a Hardware OTP Token?

The Hardware OTP Token is an eToken PASS device produced by SafeNet Inc. It is a small electronic device resembling a miniature MP3 player. It is an OTP code generator which provides strong two-factor authentication.



Unlike a Certification Token, this solution is operating system independent, and Users do not have to install any supporting software or drivers - its advantage is therefore that it offers maximum mobility. It also eliminates the problems with generating Certificates.

The built-in battery has **a life of up to 7 years or 14,000 displayed OTP codes** – so that, for example, if ten codes are displayed per day the **Hardware OTP Token will have a life of around 5 years.**

To display the current OTP code, press the button on the right side of the Hardware OTP Token. The Hardware OTP Token will then show the currently generated OTP code on its LCD display. Copy this OTP code **into the relevant field in IB.**

**!!! NOTE !!!**

- The OTP code is shown on the display only for 30 seconds before the display goes off.
- It is also possible that during those 30 seconds a new OTP code will be generated and therefore displayed – OTP codes are generated continuously every 60 seconds regardless of whether or not the User is displaying them (see the introduction to section [2](#)).
- You must therefore give close attention to the OTP code displayed – if you will not be able to copy and confirm the displayed OTP code in time, it is better to wait for the next OTP code to be generated.
- If IB requires two OTP codes to be entered, this always means two different, consecutive OTP codes (as a particular example, when registering the Hardware OTP Token during your first login to IB). In these cases, after entering the first OTP code you will have to wait for another OTP code to be generated before entering it.

3. SMS codes

An SMS code is a single-use numerical code working on the OTP code principle – see section [2](#). However, SMS codes are not generated continuously, but only after a certain action is performed (they are so-called “event-based” or “challenge-response” codes).

An SMS code is also valid only for a single operation (logging into IB, authorization of a Payment Order or request, creation of a notification etc.). The generated SMS code is sent to the User’s mobile phone in an SMS and must be entered and confirmed for the operation performed within 10 minutes of its generation (**NOT of its being displayed!**).

The advantage compared to OTP codes is that Users do not need any special token, but can obtain SMS codes using only their mobile phones. This therefore eliminates the costs for purchasing the necessary device. In addition, the same advantage of maximum mobility applies in comparison to the use of a Certificate – this solution is operating system independent, and **Users do not have to install any supporting software or drivers** (i.e. the same as in the case of an OTP Token for OTP codes).

4. Certificates and working with the Certification Token

What is a Certification Token?

The Certification Token is a Borderless Security iKey 4000 USB Token produced by SafeNet Inc. It is a small USB PKI device similar to a flash disk, which provides strong two-factor authentication.



The Certification Token is compatible with USB 1.1 and above, and is secured by a PIN code. Support for encryption algorithms is directly integrated into the hardware of the Certification Token.

Software and drivers for administration of the Certification Token and a library for working with an electronic key must be installed on the PC on which the token will be used.

Only the Certification Token sold by the Bank may be used to generate and store Certificates.

To ensure its correct use, install the required technology and generate a Certificate as described in the sections below.

4.1. Certification Centre

The Certification Centre is accessible from the website <https://ibcc.ppfbanka.cz>. After entering this web address the following screen will be displayed:

Change the language (ENG) in the bottom right-hand corner. To ensure the correct generation of the Certificate it is necessary to follow these steps:

1. Download the SW for the correct operation of IB (Java) – section [4.2.](#) – **install this version of Java even if you already have Java installed on your PC;**
2. Download the library for working with an electronic key (an applet for the encryption of data) – section [4.3.](#);
3. Download the drivers for the Certification Token for the relevant operating system – section [4.4.](#);
4. Download the SW for Certification Token administration – section [4.5.](#);

5. **Restart the PC;**
6. Change the PIN for the Certification Token – section [4.6.](#);
7. Generate the Certificate – section [4.7.](#)

You can download the drivers and SW for the Certification Token and the applet for the encryption of data from the **Downloads** option. All the files which need to be downloaded to the PC for the Certification Token to function correctly will be displayed.

Downloads

Special software for work with Token

Java(TM) 2 Runtime Environment SE
Necessary to install for the correct running of Internetbanking application in your web browser. If you already have the latest version of Java installed on your PC, installation is not necessary.
1. [j2re-1_4_2_11-windows-i586-p.exe](#), 15,4 MB

BSC Applet PKCS11
Library for working with Electronic Signature with Certificate.
Necessary to install to your PC to be able to communicate properly with the Electronic Signature registered in PPF bank Internetbanking application.
2. [BSC Applet_PKCS11.exe](#), 497 KB

Token drivers for 32bit OS Windows
Necessary to install to your PC to be able to detect a USB Token iKey 4000
3. [iKeyDrv32_v1.exe](#), 4,1 MB

Token drivers for 64bit OS Windows (Some versions of OS Win. require installation of a compatible mode)
Necessary to install to your PC able to detect a USB Token iKey 4000
3. [iKeyDrv64_v1.exe](#), 1,5 MB

Administration Software for Token
We recommend you to install this software coming with a user interface for managing the Token iKey 4000 (including list of Certificates and their current validity, allows you to change the PIN for Token and other important functions)
4. [PPFBswToken_v1.msi](#), 8,7 MB

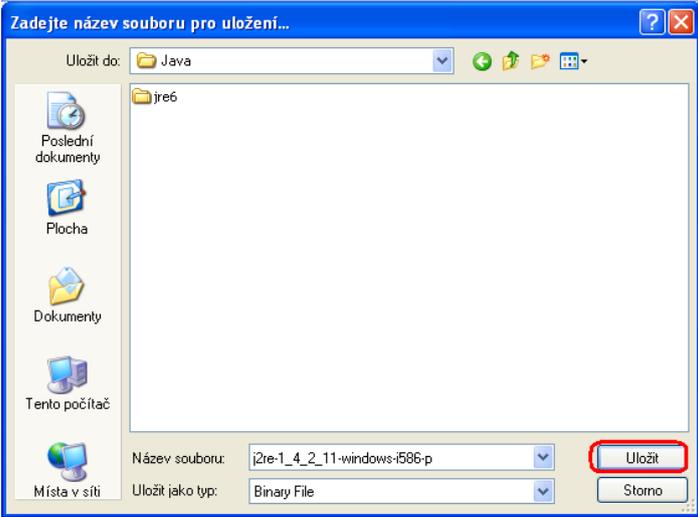
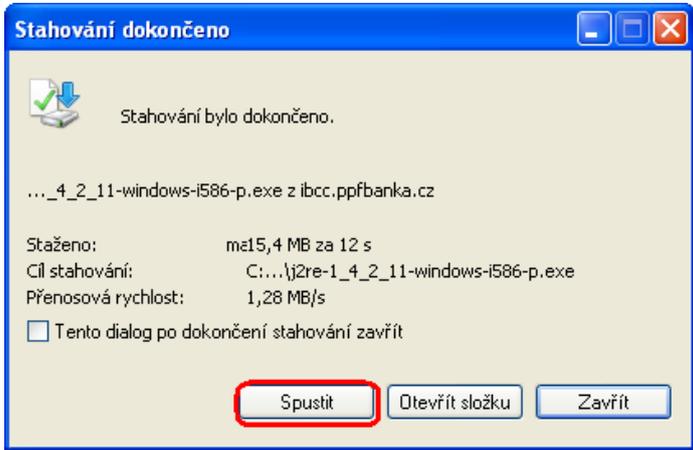
IMPORTANT NOTE:

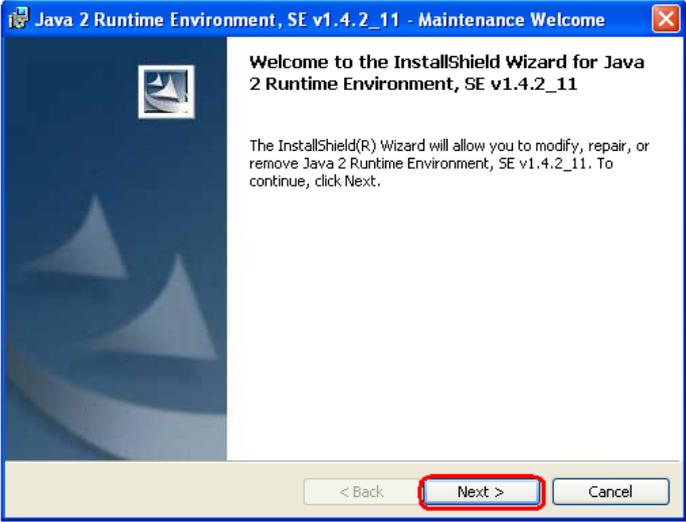
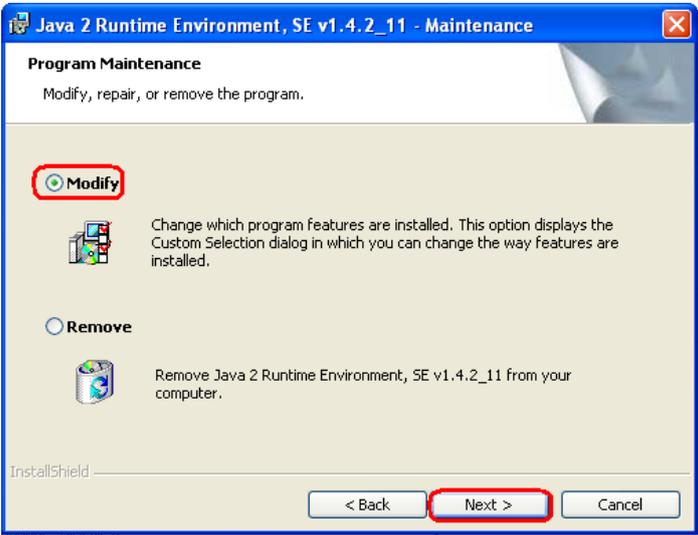
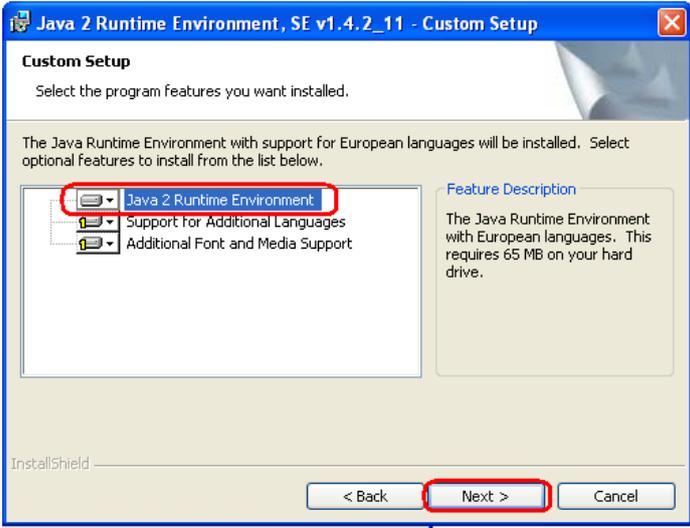
- In different browsers (Mozilla Firefox, Internet Explorer, Google Chrome etc.) the dialogue boxes displayed may slightly differ (for example instead of the *Save* button a *Save file* button may be displayed) or some extra dialogue boxes may be added.
- The language of the dialogue boxes depends on the settings of the operating system or the settings of the particular files – neither the Bank nor the User can influence this.
- If you are already using a Certification Token or a smart card (or other similar encryption technology) from another supplier or another bank, we recommend that you disconnect this technology at least while generating and saving the Bank’s Certificate (due to potential software conflicts during the generation of the Certificate). If you do not follow this recommendation, the Certificate for IB may not be saved to the Certification Token.

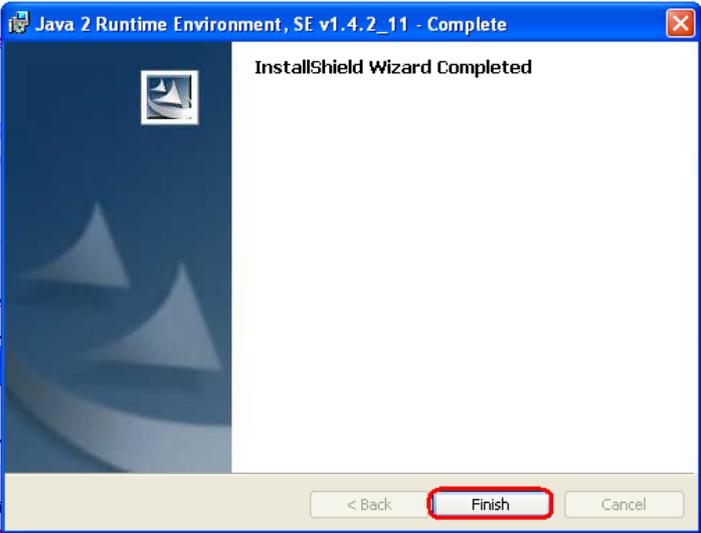
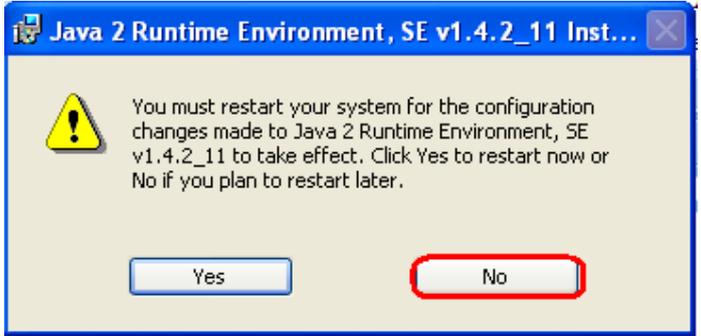
Installation is performed in the usual way, using Windows Installer.

4.2. Downloading the SW for the correct operation of Internetbanking

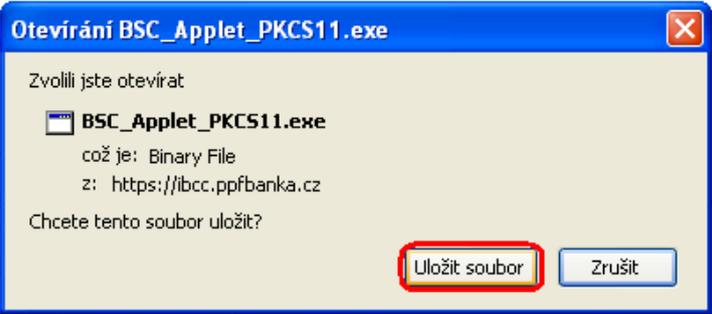
1.	First choose the file with the SW for the correct operation of IB. In the first dialogue box click on the Save (Uložit soubor) button.	
----	---	--

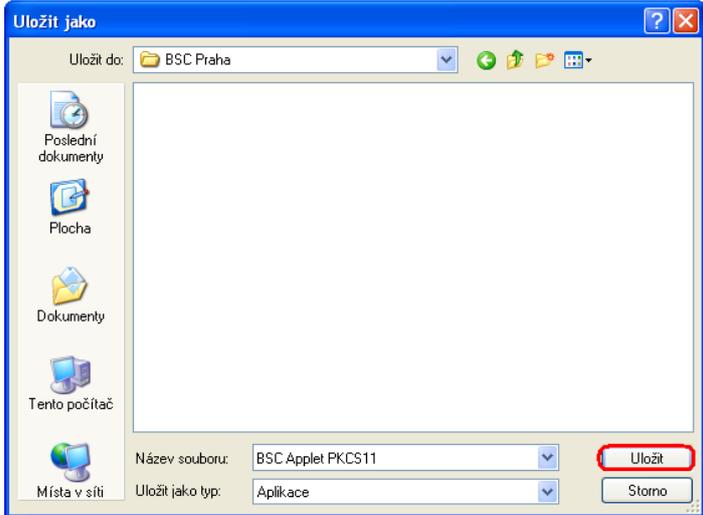
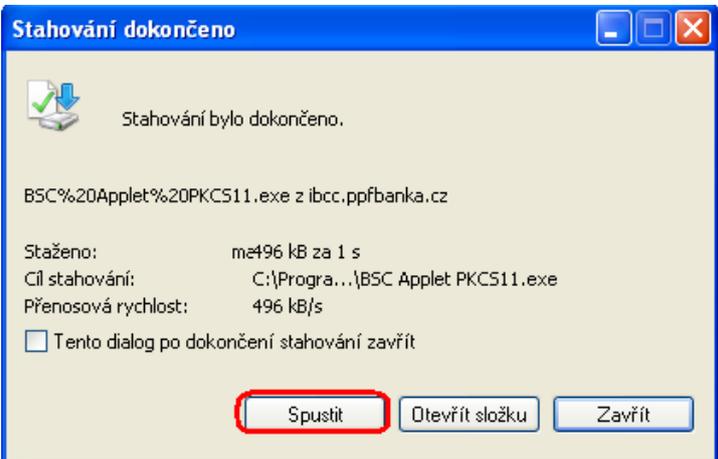
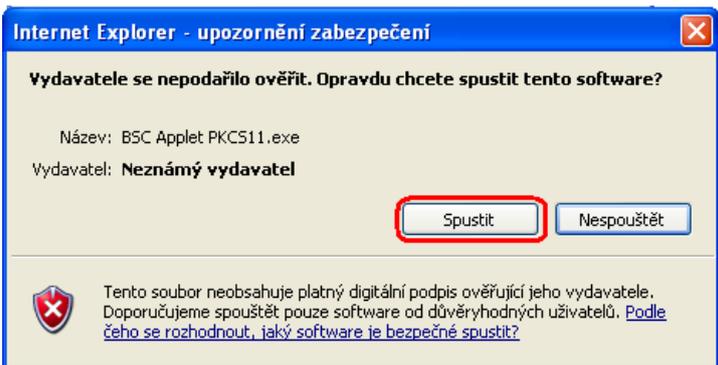
<p>2.</p>	<p>The program will ask you to select a directory for saving the file – select a directory and click on the Save (Uložit) button. Do not change the name or type of the file!!!</p>	
<p>3.</p>	<p>Information about the completion of the download will then be displayed – start the installation with the Run (Spustit) button.</p>	
<p>4.</p>	<p>The system will ask you if you wish to run the SW – confirm using the Run (Spustit) button.</p>	

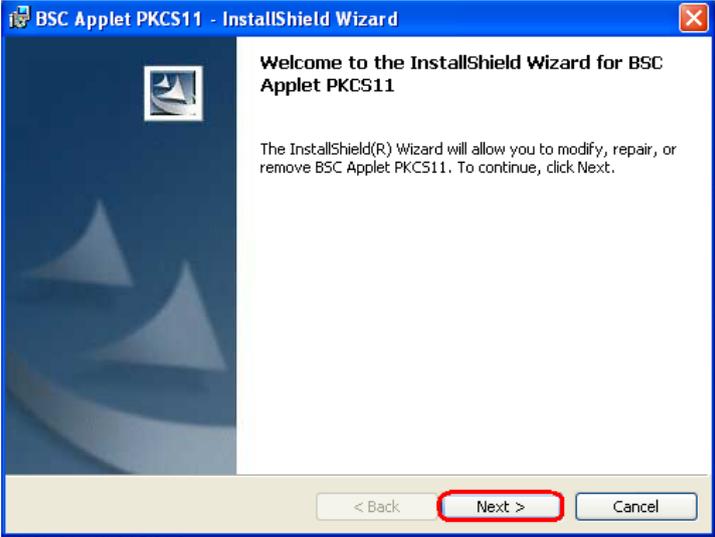
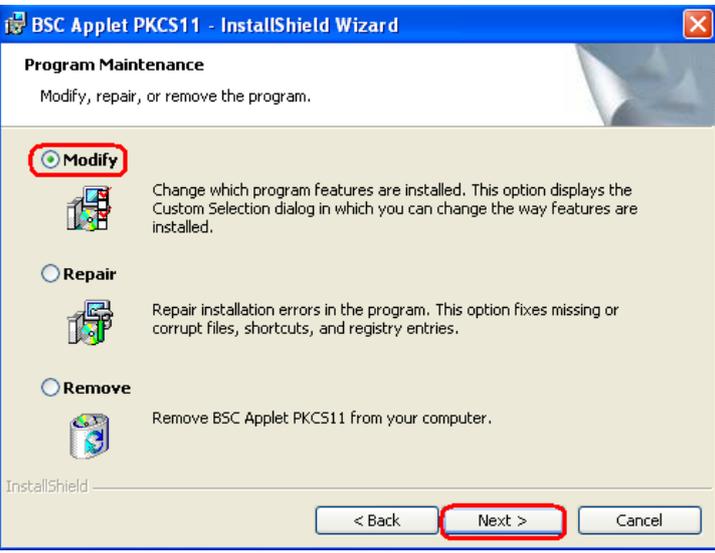
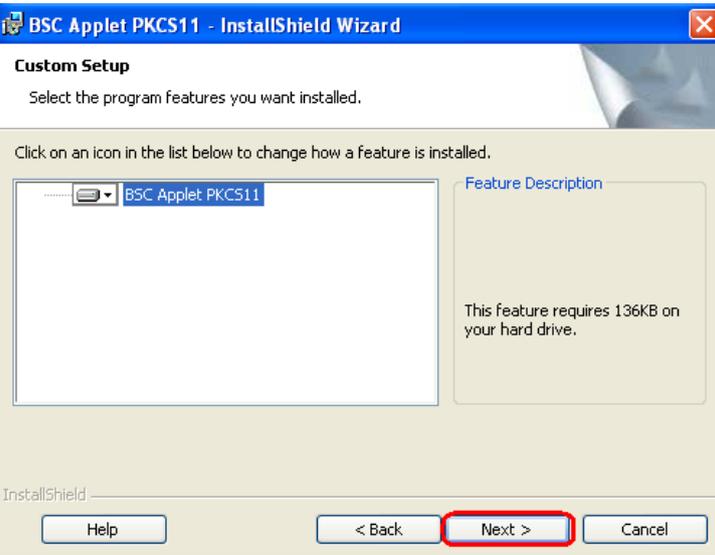
<p>5.</p>	<p>The installation wizard will be displayed. On the first screen of the wizard click on the Next button.</p>	
<p>6.</p>	<p>On the next screen leave the selected installation type (Complete, Modify or Typical) and click on the Next button.</p>	
<p>7.</p>	<p>On the next screen leave the selected Java 2 Runtime Environment option and click on the Next button.</p>	

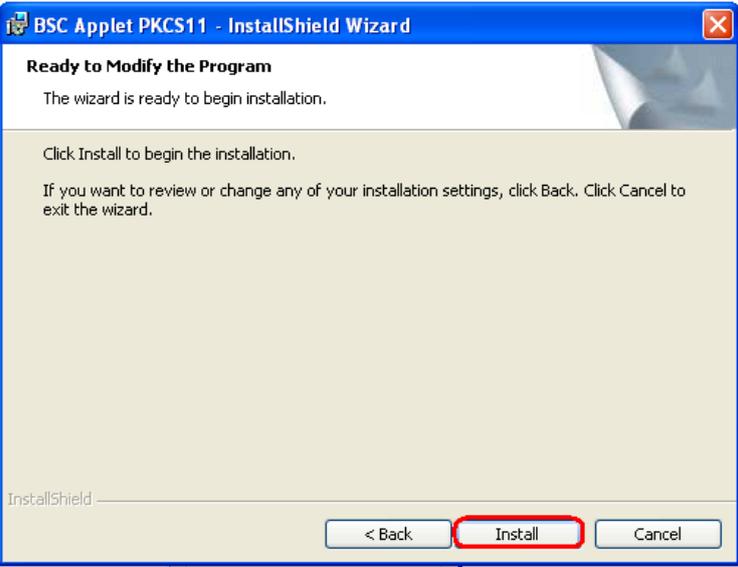
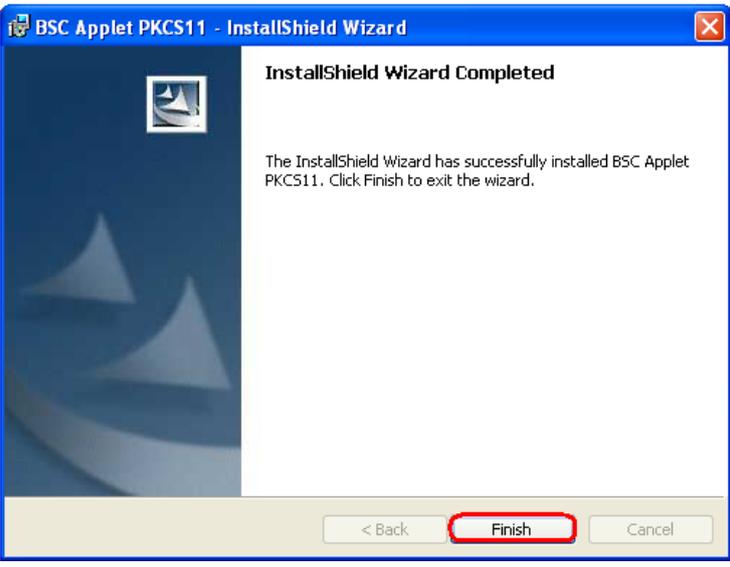
8.	After completing the installation click on the Finish button.	
9.	A box will then be displayed with information about the need to restart the PC – click on the No button (your PC will be restarted later after the installation of all the necessary SW).	

4.3. Downloading the library for working with an electronic key (an applet for the encryption of data)

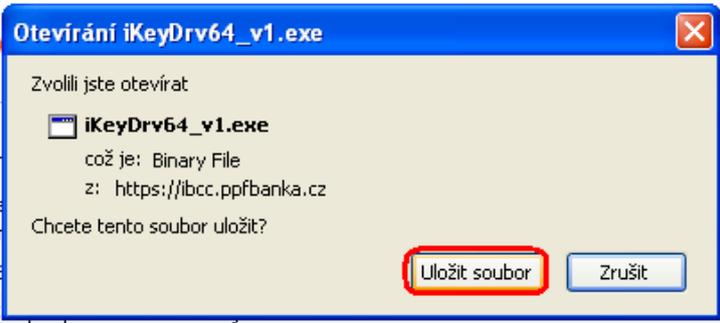
1.	Next, select the file with the applet for communication between IB and the Certification Token. In the first dialogue box click on the Save (Uložit soubor) button.	
----	--	--

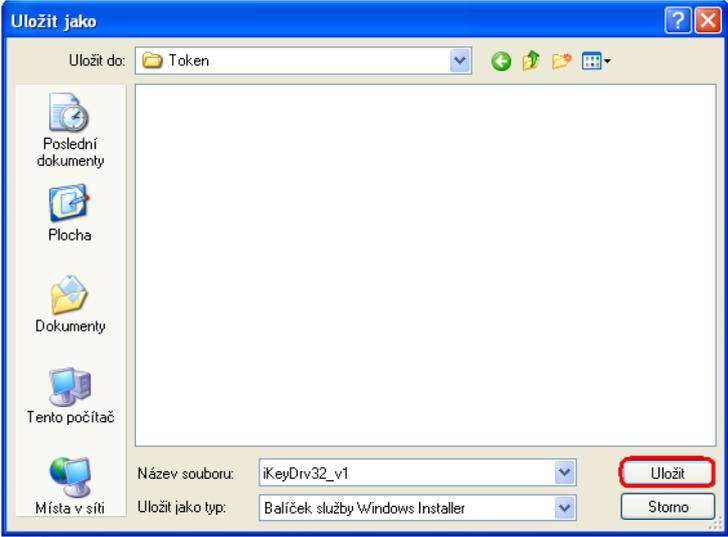
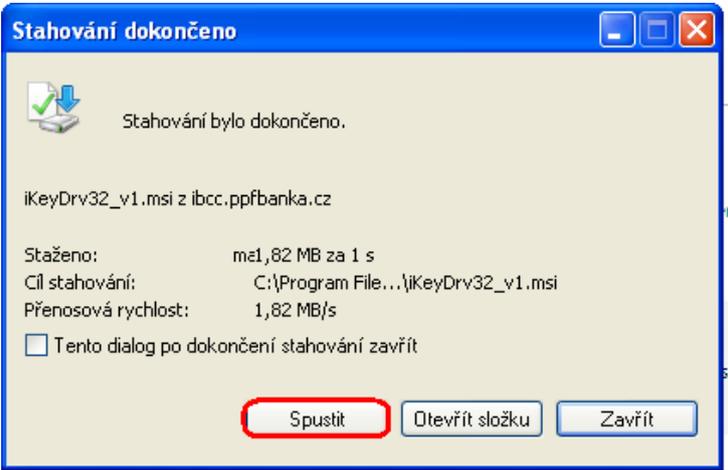
<p>2.</p>	<p>The program will ask you to select a directory for saving the file – select a directory and click on the Save (Uložit) button. Do not change the name or type of the file!!!</p>	
<p>3.</p>	<p>Information about the completion of the download will then be displayed – start the installation with the Run (Spustit) button.</p>	
<p>4.</p>	<p>The system will ask you if you wish to run the SW – confirm using the Run (Spustit) button.</p>	

<p>5.</p>	<p>The installation wizard will run. On the first screen of the wizard click on the Next button.</p>	
<p>6.</p>	<p>On the next screen leave the selected installation type (Complete, Modify or Typical) and click on the Next button.</p>	
<p>7.</p>	<p>On the next screen click on the Next button.</p>	

<p>8.</p>	<p>On the following screen, start the installation of the applet by clicking the Install button.</p>	
<p>9.</p>	<p>After completing the installation click on the Finish button.</p>	

4.4. Downloading drivers for the Certification Token

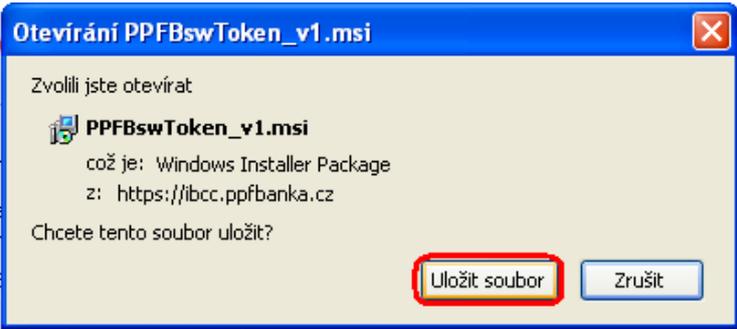
<p>1.</p>	<p>Next, select the file with the drivers for the Certification Token for your particular operating system. In the first dialogue box click on the Save (Uložit soubor) button.</p>	
-----------	--	--

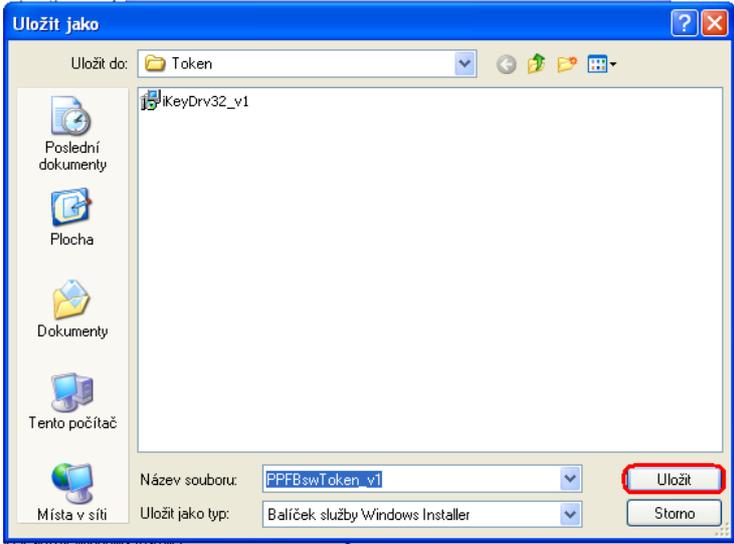
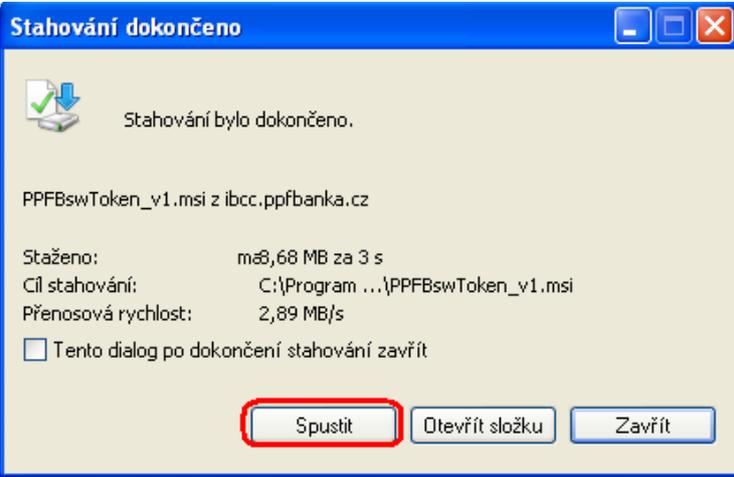
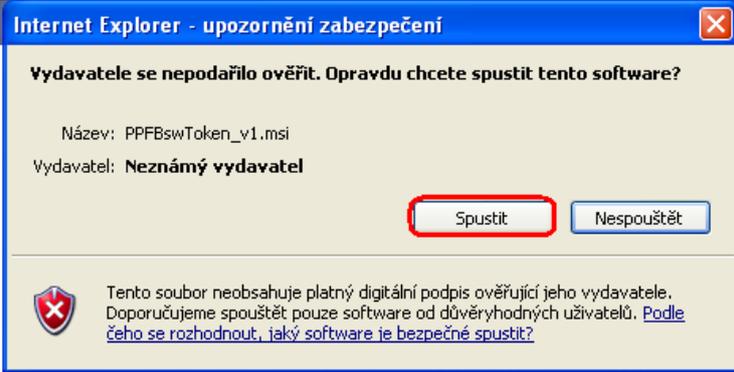
<p>2.</p>	<p>The program will ask you to select a directory for saving the file – select a directory and click on the Save (Uložit) button. Do not change the name or type of the file!!!</p>	
<p>3.</p>	<p>Information about the completion of the download will then be displayed – start the installation with the Run (Spustit) button.</p>	
<p>4.</p>	<p>The system will ask you if you wish to run the SW – confirm using the Run (Spustit) button.</p>	

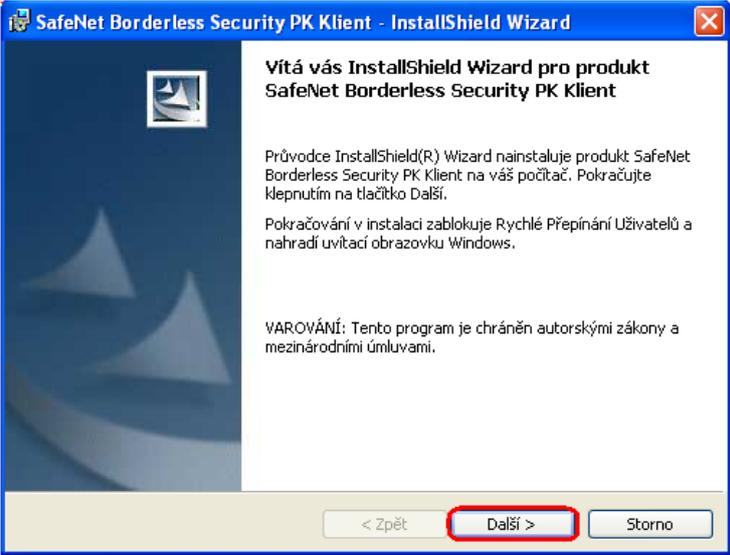
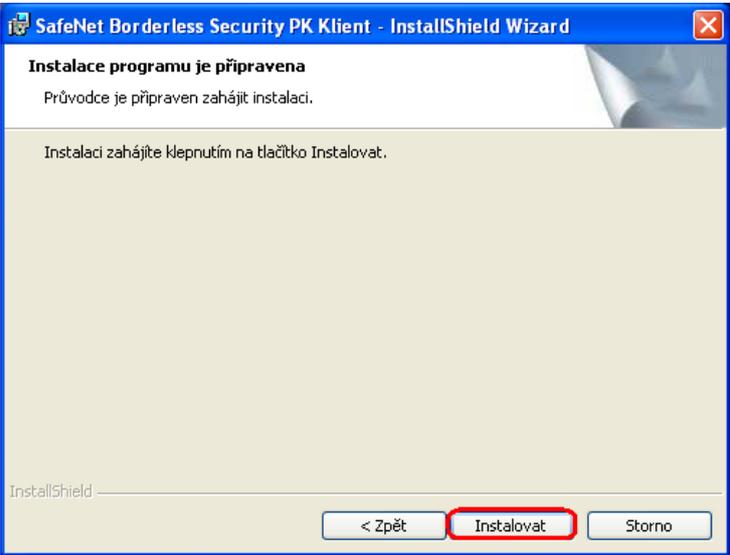
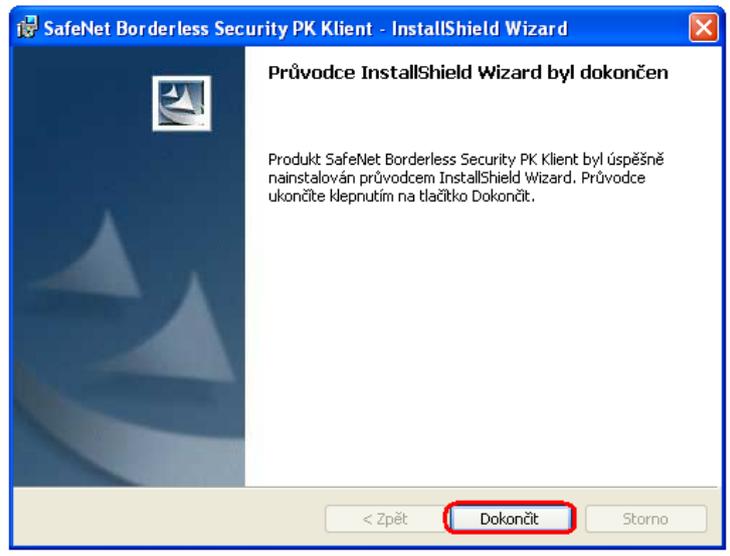
<p>5.</p>	<p>The installation wizard will run. On the first screen of the wizard click on the Next button.</p>	
<p>6.</p>	<p>The next screen displays a "License Agreement". Read this agreement, and if you agree select the option I accept the terms in the license agreement and click on the Next button. If you do not accept the "License Agreement" it will not be possible to install the drivers for the Certification Token and to generate the Certificate necessary for logging in and performing Authorization in IB.</p>	
<p>7.</p>	<p>On the following screen, start the installation of the drivers by clicking the Install button.</p>	

8.	The installation program will ask you to insert the Certification Token. Insert the Certification Token into the USB port and close the dialogue box by clicking the Close button.	
9.	After completing the installation click on the Finish button.	

4.5. Downloading the SW for the administration of the Certification Token

1.	Next, select the file with the SW for the Certification Token. In the first dialogue box click on the Save (Uložit soubor) button.	
----	---	--

<p>2.</p>	<p>The program will ask you to select a directory for saving the file – select a directory and click on the Save (Uložit) button. Do not change the name or type of the file!!!</p>	
<p>3.</p>	<p>Information about the completion of the download will then be displayed – start the installation with the Run (Spustit) button.</p>	
<p>4.</p>	<p>The system will ask you if you wish to run the SW – confirm using the Run (Spustit) button.</p>	

<p>5.</p>	<p>The installation wizard will run. On the first screen click on the Next (Další) button.</p>	
<p>6.</p>	<p>On the following screen, start the installation of the SW by clicking the Install (Instalovat) button.</p>	
<p>7.</p>	<p>After completing the installation click on the Finish (Dokončit) button.</p>	

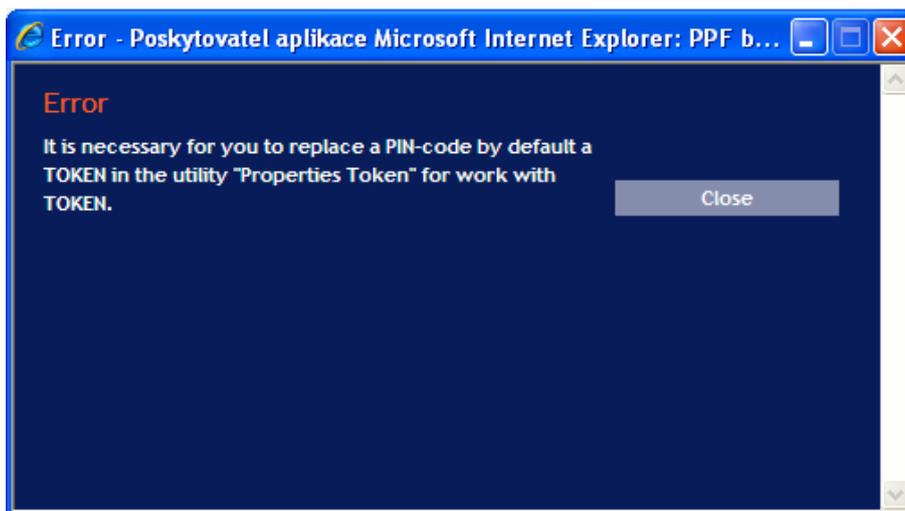
After successful installation a Certification Token icon will be displayed in the lower right-hand corner of the PC screen.



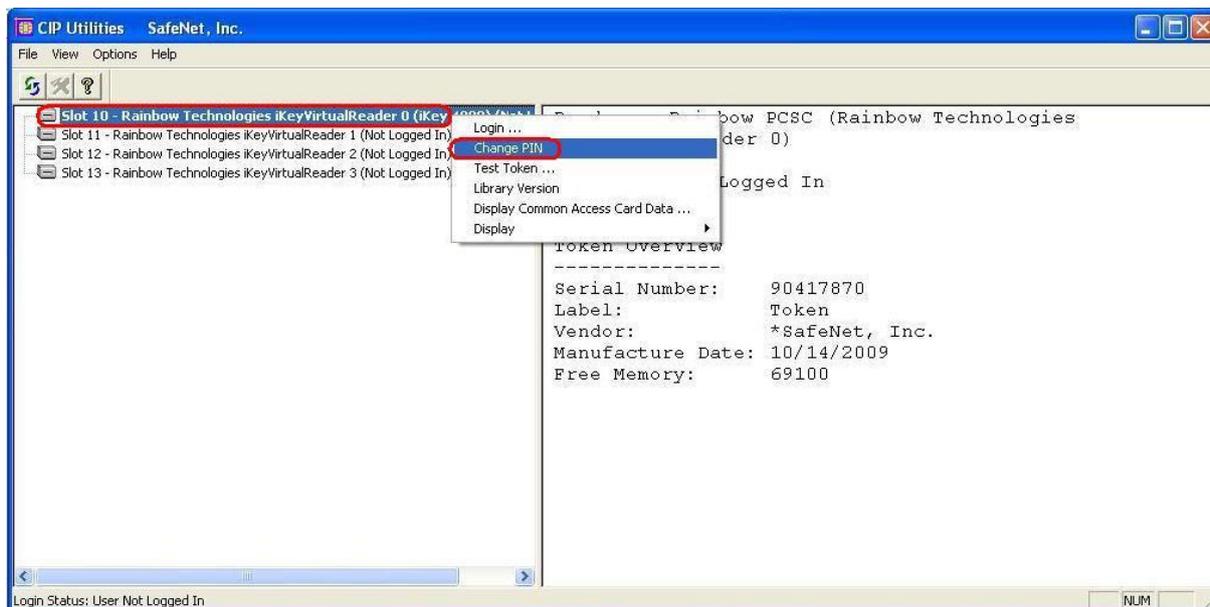
Now restart the PC.

4.6. Changing the PIN for the Certification Token

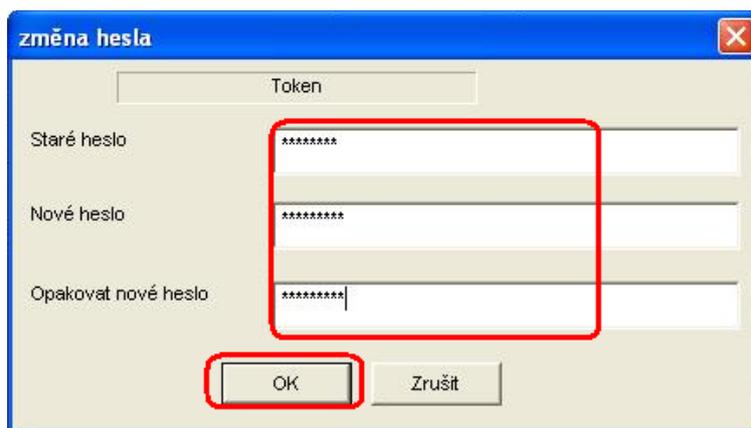
After restarting the PC, change the default PIN for access to the Certification Token. If you do not change the PIN you will not be able to generate the Certificate – when you attempt to generate the Certificate the Certification Centre will display this information:



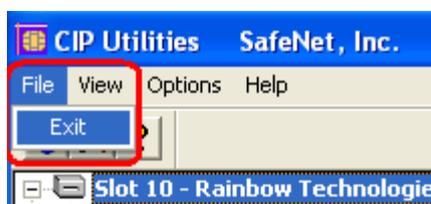
In order to change the PIN, insert the Certification Token into the PC and start the SW for the Certification Token (Start, Programs, SafeNet, Borderless Security PK, SafeNet CIP Utilities). After starting the SW, click with the right button of your mouse on the first line of the list. Click on the **Change PIN** option on the displayed menu.



Enter the default PIN into the **Old Password (Staré heslo)** field, then enter the new PIN into the **New Password (Nové heslo)** and **Repeat New Password (Opakovat nové heslo)** fields. A PIN must have between six and twenty characters, may contain only alphanumeric characters without diacritical marks, and must include at least one uppercase letter, one lowercase letter and one digit. Confirm the change with the **OK** button.



You can change your PIN again this way at any time – however a new PIN cannot be a repetition of an earlier one. Exit the program via the options **File** and **Exit**.

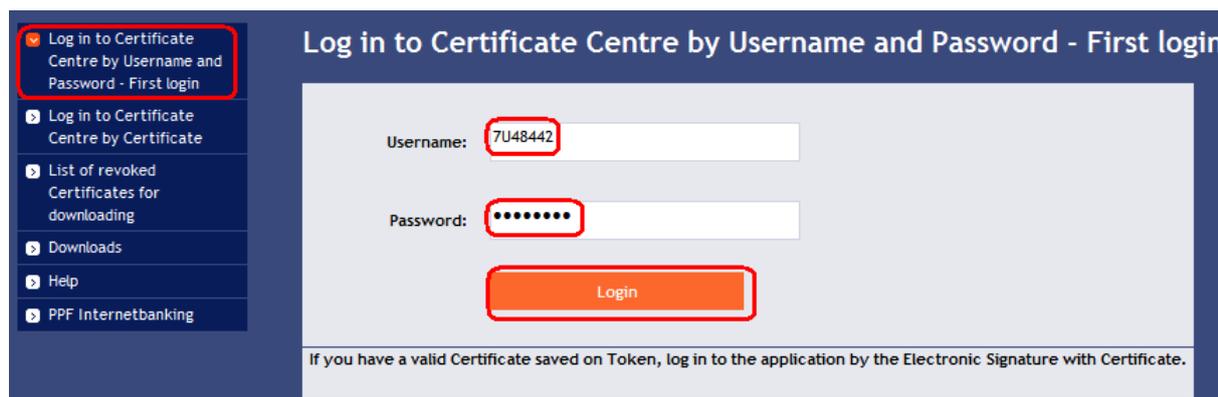


If you would like to use the Certification Token on a different computer, it is also necessary to install the drivers and SW for the Certification Token on that computer.

4.7. Generation of the Certificate

To generate a Certificate, go to the website of the Certification Centre again (<https://ibcc.ppfbanka.cz>), change the language (ENG) in the bottom right-hand corner and click on the option **Log in to Certificate Centre by Username and Password – First login**.

On the login screen enter your Certification Centre Login Name into the **Username** field (the envelope “**Certification Centre Login Name**”) and enter your Certification Centre Login Password into the **Password** field (the envelope “**Certification Centre Login Password**”). You received both of these envelopes after signing the contractual documentation. Confirm using the **Login** button.



The **New Certificate** option is automatically selected. The Certification Centre will display the name and the address of the User, and the User’s name will also be displayed in the upper left-hand corner of the application. The **Certificate name** field shows the default name under which the Certificate will be saved to the Certification Token. **We recommend changing this name** – the Certificate name must not include any diacritical marks or special characters (e.g. + * ? etc.). Enter the PIN for the Certification Token into the **PIN** field and click on the **Generate** button.

Saving of your Certificate

Name and surname: JANE DOVE
Address: 110 00 PRAHA 1
V CELNICI 1031/4

Save information
Certificate storage type: Electronic key(Token)

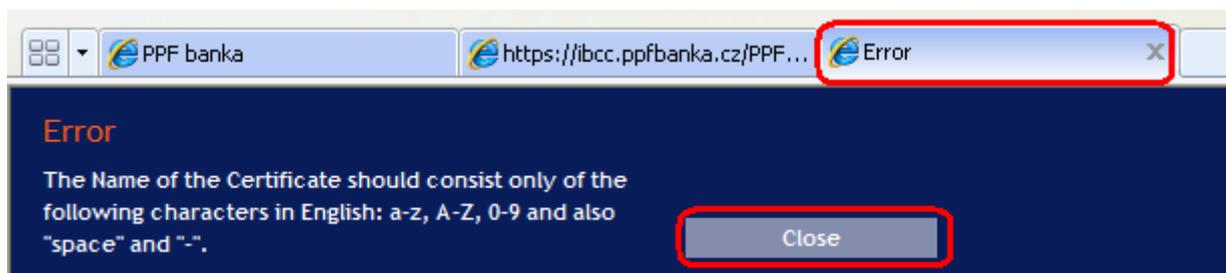
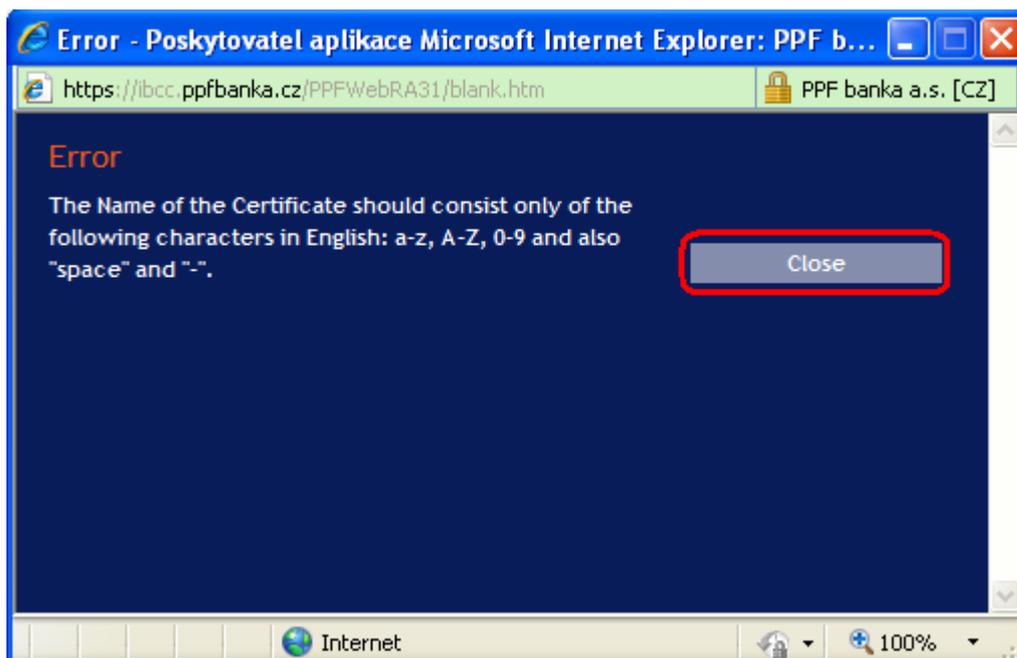
Certificate name: Jane 17 04 2012
PIN:

Generate

If you already use similar encryption device from another supplier or a bank, we recommend you to disconnect these equipments before generating and saving the certificate. If you do not do so, the certificate might not be installed successfully.

PIN of Token will be requested each time an electronic document is signed in the future. Remember it or store it in a place separately from Token in due to security reason. You can change PIN of Token using software application attached with your Token.

If the Certificate name contains unpermitted characters, the Certification Centre will display an error message in a window or tab with information about the permitted set of characters. Close this window by clicking on the **Close** button, correct the Certificate name, and click on the **Generate** button again.



The Certification Centre will generate the Certificate and display it. **!!! NOTE !!! Generation takes approximately 1 minute and while the Certificate is being generated system activity is shown by a graphic symbol in the form of flashing coloured squares. During the generation process do not leave the computer and do not perform any other activity in this browser window!!!**

To save the generated Certificate to the Certification Token, enter the PIN into the **PIN** field and click on the **Install** button.

Saving of your Certificate

Serial number: 2C5E (11358)

Issued by: EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ

Issued for: O=TESTOVACÍ KLIENT S.R.O. (IB),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid:48442,CN=JANE DOVE

Validity from: 17.04.2012 17:21

Validity to: 17.04.2013 17:21

Print: 71:B8:9D:71:4A:CA:AA:6F:09:F8:DA:88:B6:BF:32:D6

PIN:

Information about the successful saving of the Certificate will then be displayed.

Certificate saved successfully

Certificate no. 11358 was successfully saved in the system.
You can see parameters of the Certificate created on the screen "List of valid Certificates".

If you click on the **List of valid Certificates** option, the details of the Certificate will be displayed.

JANE DOVE

-
-
-
-

List of valid Certificates

Serial number: 2C5E (11358)

Issued by: EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ

Issued for: O=TESTOVACÍ KLIENT S.R.O. (IB),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid:48442,CN=JANE DOVE

Validity from: 17.04.2012 17:21:02

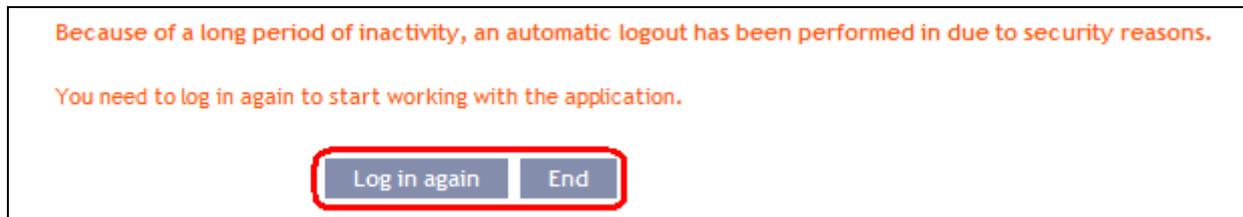
Validity to: 17.04.2013 17:21:02

Print: 71:B8:9D:71:4A:CA:AA:6F:09:F8:DA:88:B6:BF:32:D6

Here you can view the valid Certificate (e.g. to check when the Certificate expires so you can generate a new Certificate in time), invalidate the Certificate (by clicking on the **Revoke** button) or renew the Certificate (by clicking on the **Prolong** button). You can log out of the Certification Centre by clicking on the **Logout** button in the upper right-hand corner.

If you are inactive in the Certification Centre for a relatively long period of time you will be automatically logged out. If you wish to continue working in the Certification Centre, click on the **Log in**

again button. Perform a new login as described in section [4.8](#). If you do not want to continue working in the Certification Centre, click on the **End** button.

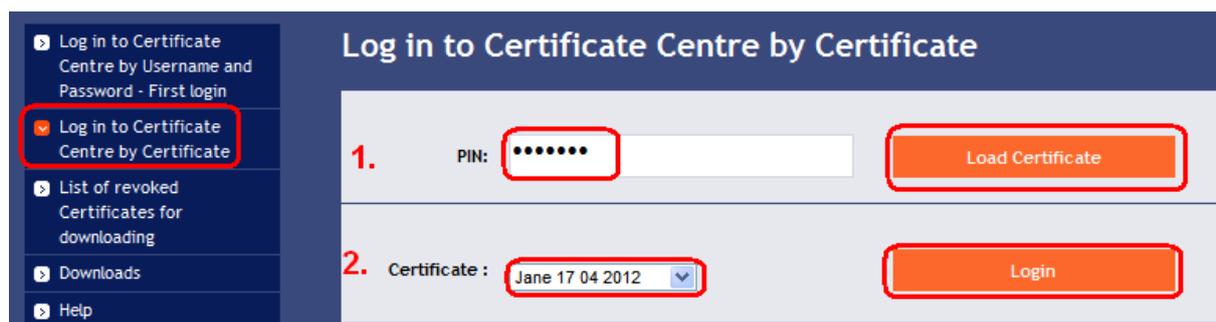


You can now log into IB, and after registering the Certificate (see Part I of the User Guide) you can start to use it.

Before the validity of the Certificate expires it is necessary to renew it as described in section [4.8](#). **If you do not renew the Certificate in time you will have to ask the Bank for new Certification Centre login data, as in the case of the first generation of the Certificate.**

4.8. Renewing a Certificate

Before the expiration of the validity of the Certificate you must generate a new Certificate. In this case, log into the Certification Centre (<https://ibcc.ppfbanka.cz>) and choose **Log in to Certificate Centre by Certificate**. Enter the PIN for the Certification Token into the **PIN** field and click on the **Load Certificate** button. Then choose a Certificate in the **Certificate** field and click on the **Login** button.



The **New Certificate** option will automatically be displayed, the same as in the case of generating a new Certificate (see section [4.7](#)). To renew the existing Certificate you can then simply enter the name of the new Certificate and the PIN and start the generation of the Certificate in the same way as in section [4.7](#). – the original Certificate will be automatically invalidated and will be replaced by the newly generated Certificate.

We recommend changing the name of the new Certificate so that it does not match the name of the now invalidated Certificate – if the names were the same you could have problems logging into IB or with the authorization of Payment Orders and requests for the Bank.

Saving of your Certificate

Name and surname: JANE DOVE
Address: 110 00 PRAHA 1
V CELNICI 1031/4

Save information
Certificate storage type: Electronic key(Token)

Certificate name: 48442
PIN:

Generate

If you already use similar encryption device from another supplier or a bank, we recommend you to disconnect these equipments before generating and saving the certificate. If you do not do so, the certificate might not be installed successfully.

PIN of Token will be requested each time an electronic document is signed in the future. Remember it or store it in a place separately from Token in due to security reason. You can change PIN of Token using software application attached with your Token.

After this, follow the same instructions as for generating the first Certificate (see section [4.7.](#)).

The second possibility for renewing the Certificate is to click on the **List of valid Certificates** option. After clicking on the **List of valid Certificates** option a list of valid Certificates will be displayed, along with the buttons **Revoke** and **Prolong**.

List of valid Certificates

Serial number: 2C5E (11358)
Issued by: EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ
Issued for: O=TESTOVACÍ KLIENT S.R.O. (IB),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid:48442,CN=JANE DOVE
Validity from: 17.04.2012 17:21:02
Validity to: 17.04.2013 17:21:02
Print: 71:B8:9D:71:4A:CA:AA:6F:09:F8:DA:88:B6:BF:32:D6

Revoke **Prolong**

Do not use the Revoke button!

To renew the Certificate, click on the **Prolong** button – a screen for generating the new Certificate will be displayed. Enter the name of the new Certificate into the **Certificate name** field, enter the PIN for the Certification Token into the **PIN** field, and click on the **Generate** button.

Renovation of your Certificate - step 1

Name and surname: JANE DOVE
 Address: 110 00 PRAHA 1
 V CELNICI 1031/4
 Certificate name:
 PIN:

Generate

If you already use similar encryption device from another supplier or a bank, we recommend you to disconnect these equipments before generating and saving the certificate. If you do not do so, the certificate might not be installed successfully.

PIN of Token will be requested each time an electronic document is signed in the future. Remember it or store it in a place separately from Token in due to security reason. You can change PIN of Token using software application attached with your Token.

Details of the generated Certificate will then be displayed. To save it, enter the PIN for the Certification Token into the **PIN** field and click on the **Install** button.

Saving of your Certificate

Serial number: 2C5F (11359)
 Issued by: EMAIL=info@ppfbanka.cz,CN=PPFBWEBRA,OU=InternetBanking,O=PPF banka a.s.,L=Prague,ST=Czech Republic,C=CZ
 Issued for: O=TESTOVACÍ KLIENT S.R.O. (IB),L=110 00 PRAHA 1,L=V CELNICI 1031/4,CN=uid:48442,CN=JANE DOVE
 Validity from: 17.04.2012 17:32
 Validity to: 17.04.2013 17:32
 Print: 15:52:E2:39:C5:98:8A:49:93:27:7F:86:BC:CE:94:99
 PIN:

Install

Information about the successful saving of the Certificate will then be displayed.

Certificate saved successfully

Certificate no. 11359 was successfully saved in the system.
 You can see parameters of the Certificate created on the screen "List of valid Certificates".

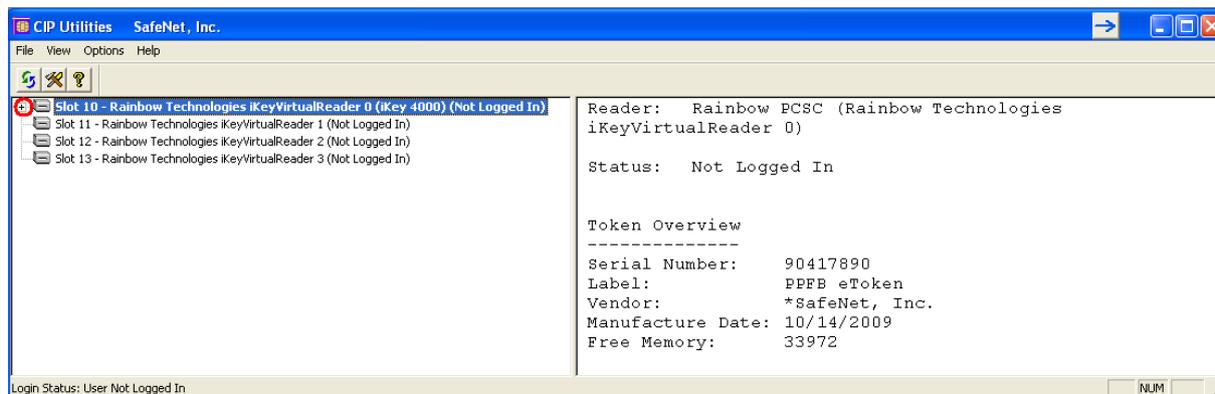
You can view the details of already invalidated Certificates in the **List of invalid Certificates** option.



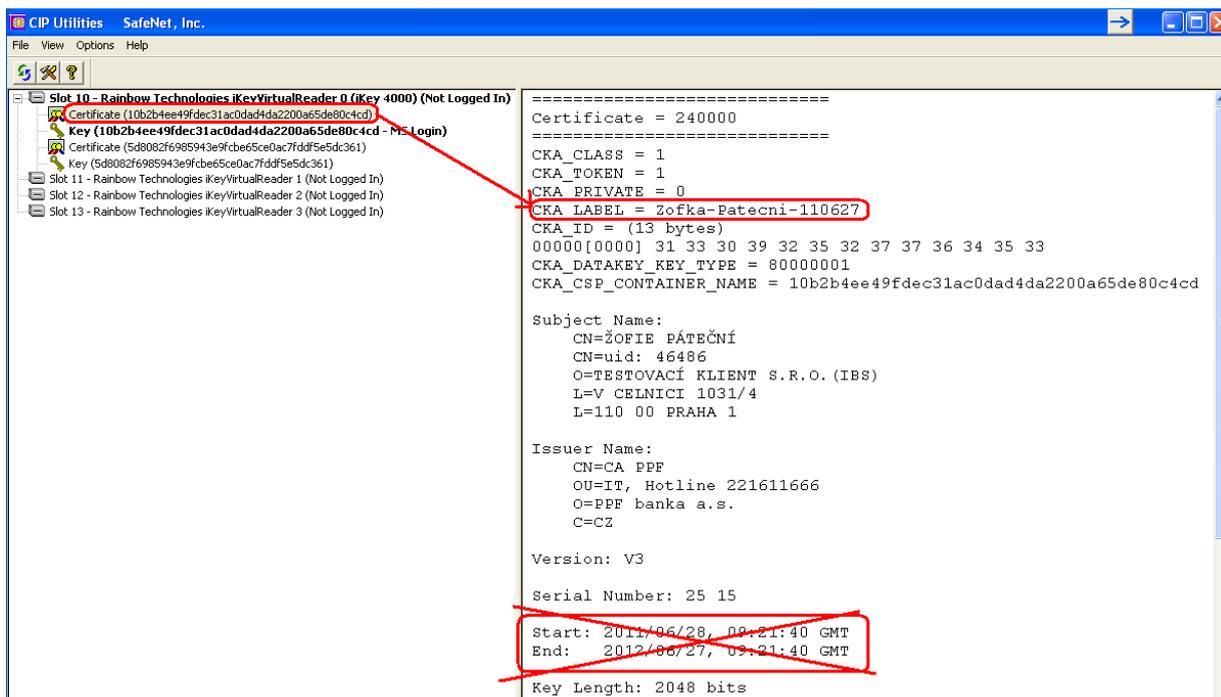
We recommend that you delete invalidated Certificates from the Certification Token – this will make sure that you do not use an invalid Certificate when logging into IB or during authorization.

4.9. Deleting an invalid Certificate

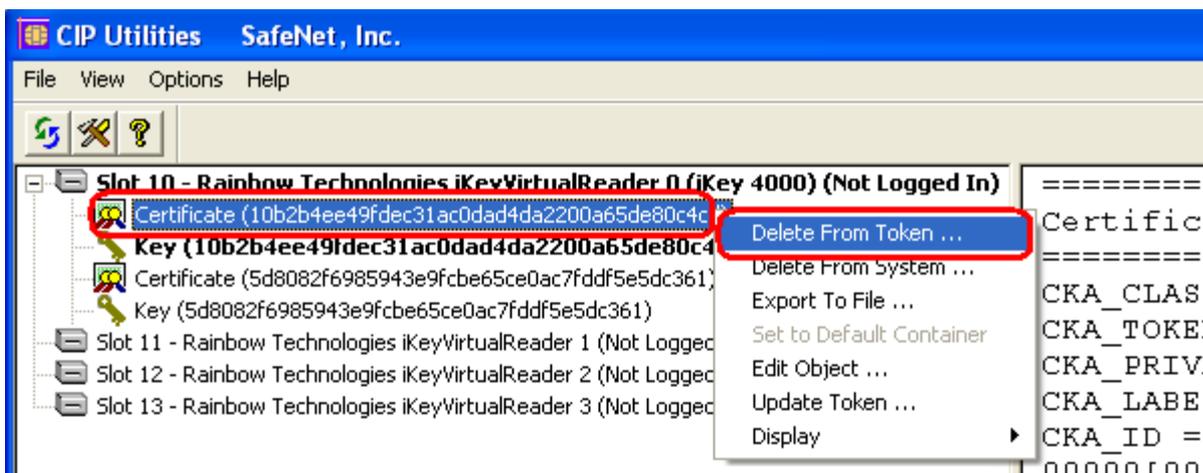
To delete an invalid Certificate, insert the Certification Token into the PC and start the SW for the Certification Token (Start, Programs, SafeNet, Borderless Security PK, SafeNet CIP Utilities). After opening the SW click on the cross at the beginning of the first row labelled “Slot...” on the left side of the screen. Each Certificate may be saved in a different Slot - a cross will then be displayed before each Slot in which a Certificate is saved, and to delete the invalid Certificate you will have to check through all the Slots marked with a cross.



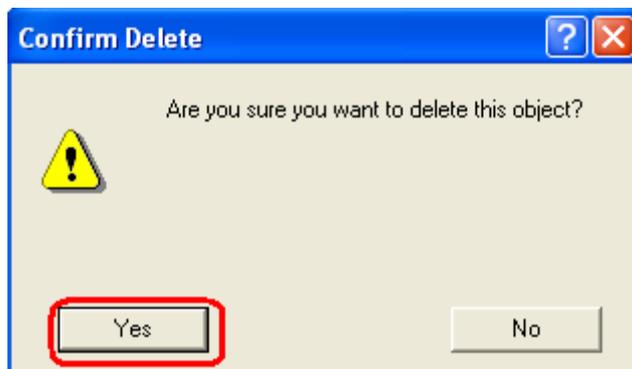
After clicking on the cross a list will expand showing all the Certificates saved on the Certification Token in the selected Slot (only two Certificates should be saved on the Certification Token – one valid and one invalid). Click on the line with the Certificate – its details will be displayed on the right side of the screen. When deleting an invalid Certificate always go by its name (in the **CKA LABEL** field), not by the information about the Certificate’s validity (in the **Start** and **End** fields) which is based on the date of the Certificate’s generation. In particular, the information about the end of the Certificate’s validity may not be up-to-date.



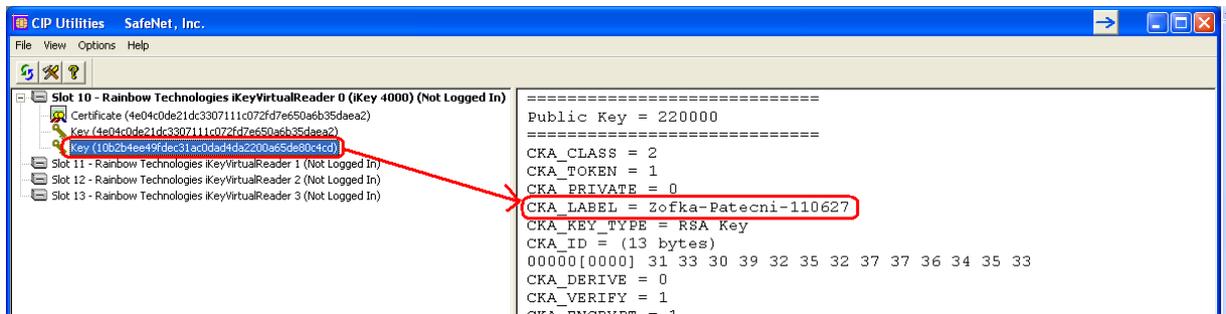
Select the invalid certificate, then click on it with the right button of the mouse. From the displayed menu, click on the **Delete From Token** option.



You will be asked if you are sure you want to delete the Certificate from the Certification Token – click on the **Yes** button.



!!! NOTE !!! Deleting a Certificate takes several seconds!!! Do not perform any other activities on your PC during its deletion. After the invalid Certificate has been deleted, the electronic key linked to the deleted Certificate is added under the electronic key linked to the valid Certificate.



Exit the program via the options **File** and **Exit**.

