In order to use cryptographic devices (smart cards or USB devices) in the BiznesPl@net system and to generate digital signatures, the following actions should be performed:

1. **Installation of Comarch SmartCard software to service cryptographic devices**
2. **Initialization of the card or USB device**

Please execute these actions in the above sequence. Please do not connect the card reader or USB device to the computer until the Comarch SmartCard software to service cryptographic devices is installed.

1. **Installation of Comarch SmartCard software to service cryptographic devices**

   The installation file: ComarchSmartCard.exe is available at BNP Paribas Bank website at the following address: [http://www.bnpparibas.pl/files/ComarchSmartCard.exe](http://www.bnpparibas.pl/files/ComarchSmartCard.exe). Download the ComarchSmartCard.exe and then run it. Once you have run the installer, follow the instructions appearing on the screen. An easy to use installation wizard will guide you through the process.

   **Please note:** To install the Comarch SmartCard software, you must have administrator rights on a given computer.

2. **Initialization of the card or USB device and key generation**

   Connect the USB device to your computer or connect a card reader and insert the smart card into the reader.

   Run the browser and log on to the BiznesPl@net system. In the field below, please enter the name under which the new key will be saved (you can give it any name without special or Polish characters) and choose Generate.

   ![Key generation](image)

   **Enter key name:** planet

   **Generate**  **Cancel**
If the cryptographic device (USB device or smart card) is new and has not been used yet, you need to initialize it, that is, to define a Personal Identification Number (PIN) to secure the device, and a Personal Unblocking Key (PUK).

Please define the following on the cryptographic device initialization screen now appeared:
- PIN (4 digits), and
- PUK (8 digits).

The **PIN** is a 4-digit code which secures the keys stored on a cryptographic device. The PIN prevents unauthorised and accidental use of your smart card or USB device, including execution of orders and instructions in your account, which require a digital signature. The PIN is strictly confidential and should be known only to you.

The **PUK**, or Personal Unblocking Key, is an 8-digit code which allows you to unblock the cryptographic device should it get blocked after your entered an invalid PIN five (5) times running. The PUK should be stored in a safe place and protected against loss.

Please note: Please remember that the PIN and PUK should not be kept together with a cryptographic device (USB device or smart card). This could result in unauthorized access to your account when your cryptographic device is lost or stolen.
Please note: If the cryptographic device (USB device or smart card) is blocked after you have entered an invalid PIN five (5) times running and you have forgotten the PUK, you may still use the device as long as it is reinitialized. However, all the keys saved on the cryptographic device will be deleted from its memory during the initialization process.

When you click "OK" to confirm, the system will offer you to print the PUK and then return to the new key generation process interrupted before. A window will appear requesting you to enter the PIN. Please enter the PIN that you have just defined and confirm by clicking "OK". Wait until the system generates the key and saves it in the chip memory on a smart card or USB device.