Information for Persons Receiving a Qualified Certificate on Smartcard, for Qualified Electronic Signature:

1. The trust service of issuing a qualified certificate is provided by Enigma Systemy Ochrony Informacji Sp. z o.o., (hereinafter referred to as "Enigma"), under the CenCert brand. The service is provided on the basis of Regulation (EU) No 910/2014 of the European Parliament and of the Council (eIDAS) and the Polish Act of 5 September 2016 on trust services and electronic identification.
2. The qualified certificate issued by Enigma is used to place and verify qualified electronic signatures.
3. The rules for using a qualified certificate, including the rights and obligations of Enigma and the Subscriber, are set out in the *Policy for Qualified Trust Services*, available on the CenCert website (www.cencert.pl). In particular, section 4.5.2 of the Policy describes the Subscriber's obligations related to securing the private key and the signature process, and section 9.8 specifies the limitation of CenCert's liability.
4. A qualified electronic signature has a legal effect equivalent to a handwritten signature (Article 25 (2) eIDAS). A qualified electronic signature based on a qualified certificate issued in one Member State is considered a qualified electronic signature in all other Member States (Article 25 (3) eIDAS).
5. An electronic card with a qualified certificate may only be used by the Subscriber (natural person) for whom the certificate was issued. Using someone else's card to place electronic signatures is a criminal act (Article 40 (1) of the Trust Services Act).
6. The subscriber may submit an application for certificate revocation at any time. If the company / institution's details are also entered in the certificate, the certificate may also be revoked by that company / institution. Details on the certificate revocation procedure are available on the CenCert website (www.cencert.pl). Pursuant to the eIDAS regulation, CenCert is required to revoke the certificate no later than within 24 hours of receiving a valid application.
7. The subscriber should revoke his certificate whenever the security of the certificate or related keys stored on the processor card is at risk (e.g. when he has lost the card or when an unauthorized person has access to the card).
8. The electronic card with the certificate is secured with the PIN and PUK code provided by the Subscriber. We strongly recommend that you SAVE YOUR PIN / PUK CODES IN A SAFE PLACE. **If an incorrect PIN code is entered three times, the code is blocked.** A blocked PIN can be unblocked and changed using the PUK code. If an incorrect PUK code is entered, this code will also be blocked. The number of allowed attempts for the PUK code depends on the card type and is specified in the e-mail with the activation code for the card. For security reasons, **CenCert does not have the Subscriber's PIN and PUK codes securing the signature key**. A blocked card is useless, and such a defect is not covered by the warranty.
9. The subscriber is obliged to check the data in the certificate before its first use. In the case of incorrect data - is obliged to immediately contact CenCert to revoke the certificate and receive a new one with the correct data. Signing with a certificate containing false data is a criminal act.

Attention! When you connect a new card (token) to your computer, the software present on your computer may display a window with the message: For security reasons you must change the Token Password.

This is normal, but it must not be done.

To activate the card, use only our *PEM-HEART Aktywacja kart* program from the *PEM-HEART Signature* package.

If you try to "change the PIN" for a card that has not yet been activated, it will take 3 tries irreversible damage (blockage) of the card.