Information for persons applying for the qualified certificate FOR ELECTRONIC SIGNATURE:

1. The trust service consisting in the issuance of 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 the Regulation of the European Parliament and of the Council (EU) No. 910/2014 (eIDAS) and the Polish Act of 5 September 2016 on trust services and electronic identification.

2. A qualified certificate issued by Enigma is to be used to create 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 limits of CenCert's liability.

4. A qualified electronic signature has a legal effect equivalent to a handwritten signature (Article 25.2 of eIDAS). A qualified electronic signature based on a qualified certificate issued in one EU Member State is considered a qualified electronic signature in all other Member States (Article 25.3 of eIDAS).

6. The subscriber may at any time submit a request for certificate revocation. If the certificate also includes the company's / institution's data, the certificate may also be revoked by this company / institution. Details of the certificate revocation procedure are available on the CenCert website (www.cencert.pl). Pursuant to the eIDAS regulation, CenCert is obliged to revoke the certificate no later than 24 hours after receiving the correct application.

7. The subscriber should revoke his certificate in every case when the security of the certificate or the related keys stored on the chip card is at risk (eg when the card is lost or when an unauthorized person has access to the card).

8. The rSign application on a mobile phone is secured with a code provided by the Subscriber PIN. WE SUGGEST STORING YOUR PIN CODE IN A SAFE PLACE. CenCert does not have a Subscriber's PIN code. Without knowing the PIN code, the mobile application cannot be unlocked, and such a defect is not covered by the warranty. It is then necessary to purchase a new certificate.

9. The subscriber is obliged to check the data in the certificate before its first use. In the event of incorrect data - is obliged to immediately contact CenCert in order to revoke the certificate and receive a new one with correct data. Submitting signatures with the use of a certificate containing untrue data is a punishable offense.

10. Requirements for a mobile device (e.g. a mobile phone) used to activate a signature:

a. The mobile device should be managed in accordance with the manufacturer's requirements, in particular the device cannot be "rooted" (Android rooting, iOS jailbreaking).

b. The device should be configured to lock the screen after a specified period of time. The screen should only be unlocked after the user has authenticated (e.g. fingerprint, password, etc.)

.....

Signature of the person applying for the certificate