Information for persons receiving a qualified certificate for ELECTRONIC SEAL IN REMOTE MODE:

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 is used to submit and verify qualified electronic seals. Seals are placed in remote mode, using HSM devices owned by CenCert, each time at the Subscriber's request. Seal requests are sent as part of an active sealing session. Establishment and extension of each such session requires, among others operations using a qualified signature of one of the persons authorized by the Subscriber.
3. The subscriber should, if necessary, manage changes on the list of authorized persons, notifying changes to CenCert in advance.
4. You will receive on the USB stick a file containing the encrypted "data used to activate the key for placing the seal". The key to decrypt this data will be sent to the e-mail address provided.
5. The received "data for activation of the key used for sealing" must be securely stored in a manner that guarantees their confidentiality and availability. CenCert does not have a copy of this data. Loss (deletion) of these data means the inability to submit the seal using the purchased certificate.
6. 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, chapter 4.5.2 of the policy describes the Subscriber's obligations related to securing the private key and the process of placing seals, and Chapter 9.8 sets out CenCert's liability limitations.
7. Authorized persons may submit an application for certificate revocation at any time. 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.
8. The certificate should be revoked whenever the security of the certificate or its associated keys is at risk (e.g. when access to the data activating the key has an unauthorized person).
9. The person using the seal is required to check the data in the certificate before its first use. In case of incorrect data - is obliged to contact CenCert immediately to cancel the certificate and receive a new one with the correct data. It is a punishable act to make a seal a certificate containing false information.

.....

Signature of the person receiving the data used to activate the key to make seals