KDPW | CCP

METHODS OF CONFIDENTIAL EXCHANGE AND PROCESSING OF ELECTRONIC DOCUMENTS (WITH PGP/GPG ENCRYPTION)

In order to keep electronic documents confidential, it is proposed to use PGP asymmetric encryption. It is a cryptographic standard that uses a simple public key infrastructure which creates a decentralized network of trust and is based on trust between cooperating persons. The simplicity of this solution makes it a popular tool that allows both secure exchange and secure storage of encrypted documents.

PGP encryption feature is supported by commercial software compliant with the OpenPGP standard created by IETF (*Internet Engineering Task Force – an organization designated to establish technical standards*) as well as by freeware software called GNU Privacy Guard (GPG). Both kinds of software are compatible and differ by additional features and licensing only.

A network of trust among stakeholders is established by using:

- a public key used for data encryption and electronic signature verification. This key may be transferred and made publicly available without the fear for the privacy of data encrypted with this key;
- a private key used for decryption of data (encrypted with the public key) and for data signature. A person that utilizes such a key must ensure its safety – the private key provides the basis for message authentication and confidentiality; its loss might be compared to losing a password.

To create a network of trust and to allow for safe exchange and processing of confidential documents, the following should be performed:

- Each party should generate their own pair of keys (a private key and a public key) following a manual that depends on the operating system installed on the workstation and the kind of software.
- Public keys should be exchanged between the parties exchanging documents. It can be achieved by sending the public key by e-mail or by uploading it to the website that allows stakeholders to download it (a file with .asc extension). A public key may be distributed without ensuring its confidentiality because it is not possible to decrypt a message (encrypted with a public key) using the same public key – it can be achieved with a private key from the same pair only.
- Remember to arrange a safe way to store the private key and allow access to only authorized persons. If the key is lost, encrypted documents will be inaccessible and if it is unintentionally disclosed, unauthorized persons might be able to access the documents.
- When working with confidential documents (encryption/decryption, document signing/ signature verification) a software manual provided by a software vendor should be consulted.

Confidential electronic documents, encrypted and signed in accordance with the PGP standard, can be openly sent in email, transferred on removable drives, stored in local filesystems or in a cloud, without jeopardizing their confidentiality or integrity.

KDPW | CCP

PGP/GPG Document exchange with KDPW_CCP using PGP/GPG encryption

In order to exchange confidential documents with KDPW_CCP in a safe way, based on PGP/GPG:

1. Generate a pair of keys (a private key and a public key) following the manual for the software used for PGP/GPG encryption.
2. Deliver your public key (a file with .asc extension) to a person working on KDPW_CCP side so that KDPW_CCP can encrypt documents to be transferred as well as verify electronic signature; also, develop a secure way to store your private key.
3. Receive a public key (a file with .asc extension) from a person working on KDPW_CCP side in order to encrypt documents meant to be sent to KDPW_CCP and to verify electronic signature of documents received from KDPW_CCP.
4. To send a confidential document to KDPW_CCP in a secure way, follow the PGP/GPG software manual to encrypt the document with KDPW_CCP's public key and to sign it electronically with your private key*. Next, send the encrypted document to KDPW_CCP using regular e-mail or ESDI/WEB**.
5. To read an encrypted confidential document received from KDPW_CCP, it should be decrypted with your private key (following the PGP/GPG software manual).

/* Encryption and signing of an electronic document are two distinct features that, depending on the software you own, might be performed in a different way. Usually, document signature is optional, depending on arrangements between parties.

/** ESDI/WEB is a secure channel of electronic communication used by KDPW and KDPW_CCP for electronic communication with participants. This solution provides confidentiality by encrypting the communication channel and by providing mutual authentication, unlike regular e-mail which by default has no security mechanisms implemented. Encryption of documents sent through ESDI/WEB by PGP/GPG ensures an additional level of confidentiality which specifically allows to decouple persons authorized to read particular information from another group of users who have access to the ESDI/WEB channel.