Klucze PGP - bezpieczna komunikacja i ochrona danych

PGP (Pretty Good Privacy) to standard kryptograficzny umożliwiający bezpieczne przesyłanie informacji poprzez ich szyfrowanie oraz cyfrowe podpisywanie. Opiera się na wykorzystaniu dwóch powiązanych kluczy: publicznego i prywatnego.

Klucz publiczny można swobodnie udostępniać innym. Służy on do szyfrowania wiadomości kierowanych do właściciela klucza oraz do weryfikacji jego podpisu cyfrowego.
Klucz prywatny pozostaje wyłącznie w rękach właściciela i służy do odszyfrowywania wiadomości oraz składania podpisów cyfrowych.

Dzięki zastosowaniu PGP możliwe jest:

- zachowanie poufności – tylko uprawniony odbiorca może odczytać wiadomość,
- potwierdzenie tożsamości nadawcy – odbiorca ma pewność, kto jest autorem,
- zapewnienie integralności danych – wiadomość nie została zmieniona w trakcie przesyłania.

Klucze PGP są szeroko wykorzystywane do zabezpieczania korespondencji e-mail, wymiany poufnych dokumentów oraz ochrony informacji przed nieuprawnionym dostępem.

W celu zapewnienia bezpiecznej i poufnej komunikacji Zespół CSIRT GOV zaleca szyfrowanie wiadomości z wykorzystaniem jednego z udostępnionych na stronie kluczy PGP, odpowiedniego dla wybranego adresu kontaktowego.

Pliki do pobrania

incydent@csirt.gov.pl - Klucz Publiczny txt, 3.96 KB

kwestionariusz@abw.gov.pl - Klucz Publiczny txt, 2.44 KB