KDPW CCP

METODA WYMIANY I PRZETWARZANIA ELEKTRONICZNYCH DOKUMENTÓW W SPOSÓB POUFNY (Z ZASTOSOWANIEM SZYFROWANIA PGP/GPG)

W celu zachowania poufności dokumentów elektronicznych proponowane jest zastosowanie szyfrowania asymetrycznego PGP. Jest to standard kryptograficzny wykorzystujący prostą infrastrukturę klucza publicznego, tworzącą zdecentralizowaną sieć zaufania i zbudowaną na zaufaniu pomiędzy współpracującymi osobami. Prostota rozwiązania sprawia, że jest to popularne narzędzie umożliwiające zarówno bezpieczną wymianę zaszyfrowanych dokumentów, jak i lokalne ich przetwarzanie.

Funkcjonalność szyfrowania PGP jest wspierana przez oprogramowanie komercyjne, zgodne ze standardem OpenPGP ustanowionym przez IETF (*Internet Engineering Task Force – organizacja zajmująca się wyznaczaniem standardów technicznych*), jak i oprogramowanie freeware, występujące pod nazwą GNU Privacy Guard (GPG). Oba rodzaje oprogramowania współpracują ze sobą, a różnią się jedynie dodatkowymi funkcjonalnościami oraz sposobem licencjonowania.

Sieć zaufania pomiędzy zainteresowanymi stronami uzyskuje się poprzez zastosowanie:

- klucza publicznego, służącego do szyfrowania danych i weryfikacji podpisu elektronicznego. Ten klucz może być przekazywany i udostępniany publicznie, bez obaw, że prywatność zaszyfrowanych nim danych zostanie naruszona;
- klucza prywatnego, służącego do odszyfrowywania danych (zaszyfrowanych kluczem publicznym) i podpisywania ich. Osoba, która się posługuje takim kluczem, musi szczególnie dbać o jego bezpieczeństwo – klucz prywatny stanowi podstawę do uwierzytelnienia wiadomości oraz zachowania jego poufności, a jego utrata jest porównywalna do utraty hasła.

W celu stworzenia sieci zaufania i umożliwienia bezpiecznej wymiany oraz przetwarzania dokumentów poufnych należy podjąć następujące działania:

- Każda ze stron powinna wygenerować własną parę kluczy (prywatny i publiczny), postępując zgodnie z instrukcją obsługi, zależną od systemu operacyjnego stacji roboczej i rodzaju oprogramowania.
- Należy dokonać wymiany kluczy publicznych pomiędzy stronami wymieniającymi się dokumentami. Można to zrobić przesyłając klucz publiczny mailem lub zamieszczając go na witrynie internetowej, w sposób umożliwiający pobranie go przez osoby zainteresowane (plik z rozszerzeniem .asc). Klucz publiczny można dystrybuować bez konieczności zachowania poufności, ponieważ nie jest możliwe odszyfrowanie wiadomości (zaszyfrowanej kluczem publicznym) przy użyciu tego samego klucza publicznego – można to zrobić jedynie kluczem prywatnym z tej samej pary kluczy.
- Trzeba pamiętać o zorganizowaniu bezpiecznego sposobu przechowywania klucza prywatnego, umożliwiając dostęp do niego jedynie upoważnionym osobom. Jego utrata spowoduje niedostępność dokumentów zaszyfrowanych, zaś niezamierzone ujawnienie stworzy możliwość uzyskania dostępu do zaszyfrowanych dokumentów przez osoby nieupoważnione.
- Pracując z dokumentami poufnymi (*szyfrowanie/deszyfrowanie, podpisywanie dokumentu /weryfikacja podpisu*) należy posługiwać się instrukcją obsługi oprogramowania dostarczoną przez jego producenta.

Poufne dokumenty elektroniczne, zaszyfrowane i podpisane zgodnie ze standardem PGP można w jawny sposób przesyłać pocztą elektroniczną, przenosić za pomocą nośników wymiennych, przechowywać w lokalnych systemach plików lub chmurze bez obawy ich ujawnienia lub naruszenia ich integralności.

Wymiana dokumentów z KDPW_CCP przy zastosowaniu szyfrowania PGP/GPG

Chcąc w bezpieczny sposób, w oparciu o szyfrowanie PGP/GPG wymieniać dokumenty poufne z KDPW_CCP, należy:

1. Wygenerować parę kluczy (klucz prywatny i klucz publiczny), postępując zgodnie z instrukcją obsługi oprogramowania wykorzystywanego do szyfrowania PGP/GPG.
2. Dostarczyć osobie współpracującej po stronie KDPW_CCP swój klucz publiczny (plik z rozszerzeniem .asc), służący do szyfrowania przez KDPW_CCP przesyłanych dokumentów oraz weryfikowania podpisu elektronicznego dokumentów odebranych przez KDPW_CCP, a także opracować bezpieczny sposób przechowywania własnego klucza prywatnego.
3. Odebrać od osoby współpracującej po stronie KDPW_CCP klucz publiczny KDPW_CCP (plik z rozszerzeniem .asc), służący do szyfrowania dokumentów przesyłanych do KDPW_CCP oraz weryfikowania podpisu elektronicznego dokumentów odebranych od KDPW_CCP.
4. Chcąc wysłać do KDPW_CCP bezpiecznie poufny dokument, należy postępując zgodnie z instrukcją obsługi oprogramowania PGP/GPG zaszyfrować go przy pomocy klucza publicznego KDPW_CCP oraz podpisać go elektronicznie przy pomocy własnego klucza prywatnego*, a następnie zaszyfrowany dokument przesłać do KDPW_CCP za pomocą zwykłej poczty elektronicznej lub ESDI/WEB**.
5. Chcąc odczytać zaszyfrowany dokument poufny odebrany od KDPW_CCP, należy odszyfrować go za pomocą własnego klucza prywatnego (postępując zgodnie z instrukcją obsługi oprogramowania PGP/GPG).

/* Szyfrowanie i podpisywanie dokumentu elektronicznego są to dwie rozłączne funkcjonalności, które zależnie od posiadanego oprogramowania mogą być realizowane w różny sposób. Podpisywanie dokumentu zazwyczaj stosuje się opcjonalnie, zależnie od uzgodnienia pomiędzy stronami.

/** ESDI/WEB jest to bezpieczny kanał komunikacji elektronicznej wykorzystywany przez KDPW i KDPW_CCP do komunikacji elektronicznej z uczestnikami. W rozwiązaniu tym poufność jest zapewniona poprzez szyfrowanie kanału komunikacyjnego oraz obustronne uwierzytelnienie, w odróżnieniu od zwykłej poczty elektronicznej, w której standardowo nie ma zaimplementowanych żadnych mechanizmów bezpieczeństwa. Szyfrowanie dokumentów przesyłanych za pomocą ESDI/WEB metodą PGP/GPG zapewnia zatem dodatkową ochronę poufności, w szczególności pozwalającą na uniezależnienie kręgu osób upoważnionych do odczytania danej informacji od grupy użytkowników mających dostęp do kanału ESDI/WEB.