



Co to jest PEM-HEART?

PEM-HEART to polskie oprogramowanie kryptograficzne rozwijane od 1993r. umożliwiające szyfrowanie i deszyfrowanie informacji, składanie i weryfikację podpisów elektronicznych, znakowanie czasem i weryfikowanie znaczników czasu, weryfikację ważności certyfikatów z wykorzystaniem protokołu OCSP lub w oparciu o automatycznie pobierane listy CRL.

PEM-HEART może pracować w trybie samoistnej aplikacji (GUI) albo usługowej biblioteki kryptograficznej integrowanej poprzez interfejs programistyczny (API).

Funkcjonalności oprogramowania PEM-HEART

- Wykorzystuje infrastrukturę PKI oraz najnowsze formaty certyfikatów (X.509 v3), list CRL, znaczników czasu i list TSL.
- Realizuje składanie i weryfikację podpisów elektronicznych
- Realizuje składanie i weryfikację podpisu pod plikiem dowolnego formatu.
- Realizuje składanie i weryfikację podpisów wielokrotnych i kontrasygnat.
- Realizuje składanie i weryfikację podpisów wewnętrznych i zewnętrznych.
- Realizuje znakowanie czasem dokumentów cyfrowych dowolnego formatu oraz dodawanie znaczników czasu do podpisów elektronicznych.
- Realizuje weryfikację statusu certyfikatu on-line protokołem OCSP (Online Certificate Status Protocol) oraz wyszukiwanie certyfikatów za pomocą usługi LDAP.
- Współpracuje z archiwum kluczy umożliwiając deszyfrację przesyłek pomimo upływu ważności kluczy i certyfikatów

Algorytmy, formaty i protokoły

- Realizuje szyfrowanie i deszyfrowanie dokumentów elektronicznych dowolnego formatu wg standardu CMS (Cryptographic Message Syntax) oraz S/MIME.
- Wspiera algorytmy SHA-1, SHA-2, RSA 2048-16384, RSA PSS, DSA, Krzywe Eliptyczne, AES, DES3
- Zapewnia obsługę protokołów TLS/SSL

Nośniki kluczy

- Karty kryptograficzne wykorzystując interfejsy PKCS#11 i CSP
- Urządzenia HSM wykorzystując interfejs PKCS#11
- Pliki dyskowe w formacie PKCS#12

Systemy operacyjne

PEM-HEART pracuje na wszystkich współczesnych systemach operacyjnych m.in. Windows, Linux, Mac OS, AIX, Free BSD, Unix.

PEM-HEART wersja 3.015 – wykorzystywany jest od prawie 15 lat w systemach NATO.

PEM-HEART wersja 3.9.7 – aktualnie certyfikowana wykorzystywana w systemach do ochrony informacji niejawnych



Dostawcą oprogramowania PEM-HEART jest Enigma Systemy Ochrony Informacji Sp. z o.o.

Enigma Systemy Ochrony Informacji jest producentem, dostawcą i integratorem zaawansowanych, dedykowanych rozwiązań w zakresie bezpieczeństwa systemów ze szczególnym naciskiem na bezpieczeństwo specjalne. Firma od 25 lat świadczy usługi w obszarze ochrony informacji, posiadając unikatową wiedzę na polskim rynku. Najważniejszym wspólnym elementem wszystkich oferowanych produktów i usług jest pełne bezpieczeństwo realizowanych systemów i przetwarzanych w nich informacji. Dotyczy ono zarówno rozwiązań sprzętowych i aplikacyjnych, jak i całego obszaru architektury i realizacji wdrożenia. Podstawą systemów tworzonych przez firmę Enigma są autorskie kryptograficzne rozwiązania sprzętowe i aplikacyjne.

ENIGMA SOI Sp. z o. o., ul. Jutrzenki 116, 02-230 Warszawa, tel. 22 570 57 10