SYSTEMY AUTOMATYCZNEJ IDENTYFIKACJI		
Dzień tyg. poniedziałek	Prowadzący mgr inż. Marek Gosławski	Studia stacjonarne
Kierunek Informatyka	Temat Oprogramowanie Open PGP Applet dla Basic / JavaCard	Grupa IP/ 2
Data oddania spraw. 05.06.2024	Wykonawca Paweł Kanclerzewski	Nr albumu 135314

1. Wstęp

W dzisiejszej erze cyfrowej, bezpieczeństwo danych w Internecie, w szczególności prywatnych wiadomości e-mail, staje się coraz bardziej istotne i krytyczne dla poprawnego funkcjonowania instytucji państwowych oraz prywatnych przedsiębiorstw. Incydenty takie jak masowy wyciek danych Yahoo, w którym w latach 2013 i 2014 ujawniono informacje z miliardów kont użytkowników, pokazują, jak wrażliwe i podatne na ataki mogą być nasze dane. Sytuacja ta miała poważne konsekwencje, wpływając nawet na wartość rynkową firmy w wysokości pół miliarda dolarów. Aby chronić naszą prywatność i bezpieczeństwo, niezbędne jest wdrożenie dodatkowych środków ochrony, takich jak szyfrowanie danych. Dzięki temu nasze informacje są lepiej zabezpieczone przed nieuprawnionym dostępem i potencjalnymi naruszeniami bezpieczeństwa, co minimalizuje ryzyko ich ujawnienia i wykorzystania przez niepowołane osoby. Możliwą do wykorzystania w tej dziedzinie technologią jest oprogramowanie Open PGP Applet. Głównym problemem dla wielu osób, które się są zaznajomione z tematem cyberbezpieczeństwa jest złudne przeświadczenie, że sami nie angażując w to dodatkowych środków nie są w stanie zadbać dodatkowo o zapewnienie dodatkowej ochrony swoich danych. W tym artykule przytoczone przeświadczenie te zostanie całkowicie zdementowane. Za pomocą przykładów darmowego oprogramowania przedstawione zostaną dodatkowe środki bezpieczeństwa dla wszystkich użytkowników urządzeń mobilnych, komputerów osobistych, chmur danych oraz poczt elektronicznych

2. Open PGP

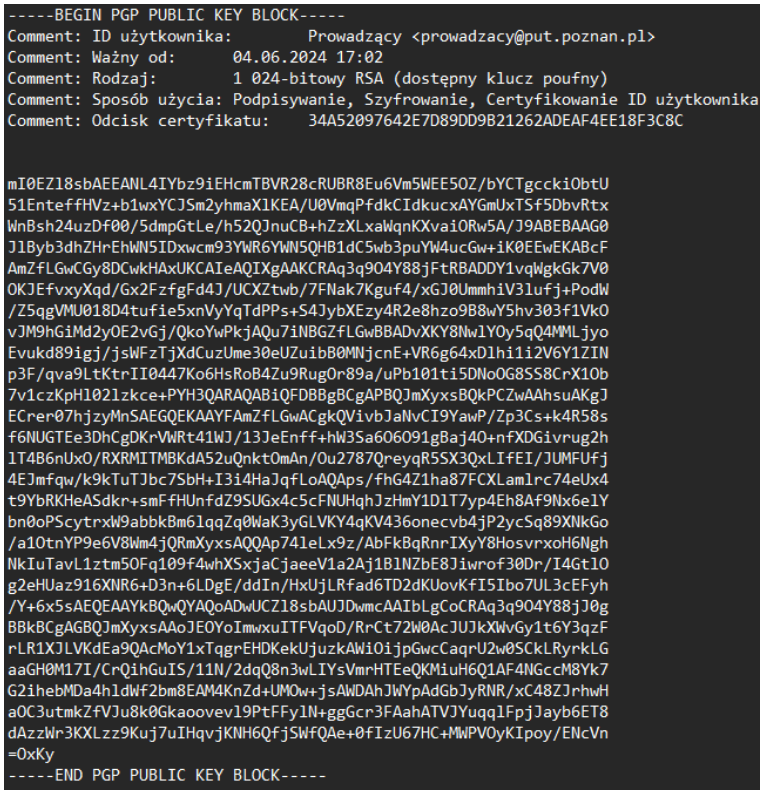
PGP (Pretty Good Privacy) to zaawansowany program kryptograficzny, który zapewnia prywatność i uwierzytelnianie danych, szczególnie w kontekście poczty elektronicznej. Wykorzystuje on hybrydowe podejście do kryptografii, łącząc szyfrowanie symetryczne i asymetryczne: szyfrowanie symetryczne służy do zabezpieczenia samej wiadomości, natomiast szyfrowanie asymetryczne do ochrony klucza sesji

symetrycznego szyfrowania. Dzięki temu połączeniu PGP oferuje wysokie bezpieczeństwo danych. PGP umożliwia także tworzenie podpisów cyfrowych, które gwarantują integralność i autentyczność wiadomości, umożliwiając odbiorcy weryfikację, czy wiadomość pochodzi od określonego nadawcy i czy nie została zmieniona. Standard OpenPGP pozwala na szyfrowanie i deszyfrowanie e-maili, co zapewnia bezpieczne przesyłanie poufnych informacji. Ponadto, PGP może być używane do podpisywania dokumentów cyfrowych oraz bezpiecznego logowania do systemów i usług, dzięki czemu tylko upoważnione osoby mają dostęp do poufnych danych. PGP stanowi niezawodne rozwiązanie w dziedzinie kryptografii, oferując kompleksową ochronę danych i prywatności w komunikacji cyfrowej.

3. Struktura klucza PGP

Struktura klucza PGP (Pretty Good Privacy) jest złożona i obejmuje klucz publiczny oraz prywatny, z których każdy pełni specyficzne funkcje w procesie szyfrowania i podpisywania wiadomości. Klucz publiczny, udostępniany innym użytkownikom, służy on do szyfrowania wiadomości oraz weryfikacji podpisów cyfrowych. Składa się on z nagłówka zawierającego metadane, unikalnego identyfikatora, informacji o algorytmie kryptograficznym, faktycznych danych klucza publicznego oraz dodatkowych informacji, takich jak data wygaśnięcia klucza czy dane właściciela. Klucz prywatny, trzymany w tajemnicy przez właściciela, służy do odszyfrowywania wiadomości zaszyfrowanych kluczem publicznym oraz do tworzenia podpisów cyfrowych. Zawiera on nagłówek, identyfikator, informacje o algorytmie kryptograficznym, faktyczne dane klucza prywatnego oraz dodatkowe informacje rozszerzające funkcjonalność klucza.

PGP umożliwia również tworzenie dodatkowych kluczy podpisów (subkeys), które mogą być używane do różnych celów, takich jak szyfrowanie, podpisywanie czy uwierzytelnianie. Podklucze te mają własne zestawy danych, w tym nagłówek, unikalny identyfikator, algorytm kryptograficzny oraz dane podklucza. Klucze PGP zawierają także metadane i certyfikaty, które pozwalają na weryfikację tożsamości klucza. Certyfikaty te to podpisy innych użytkowników potwierdzające autentyczność klucza publicznego, informacje o użyteczności klucza oraz ograniczenia czasowe, takie jak daty ważności klucza. Struktura klucza PGP jest zaprojektowana w celu zapewnienia najwyższego poziomu bezpieczeństwa, integralności i autentyczności danych, co umożliwia bezpieczne przesyłanie informacji oraz weryfikację tożsamości użytkowników.



Rys.1 Struktura klucza publicznego

4. Wiadomości zaszyfrowanej

Zaszyfrowane wiadomości za pomocą PGP stanowią bardzo dobrze spełniającą swoje zadanie tarczę ochronną dla prywatności komunikacji online. Proces szyfrowania gwarantuje, że treść wiadomości pozostaje nieczytelna dla osób nieuprawnionych, a jedynie osoba posiadająca klucz prywatny, będący swoistym kluczem do zamka, może odczytać jej zawartość. Ten klucz prywatny jest jak unikalny klucz do sejfu, który umożliwia dostęp do skarbnicy poufnych informacji. Ta jednostronna natura procesu gwarantuje, że nawet w przypadku przechwycenia zaszyfrowanej wiadomości przez osoby trzecie, treść pozostaje bezpieczna. W ten sposób PGP zapewnia nie tylko poufność, ale również integralność i autentyczność przesyłanych danych, co jest kluczowe dla bezpiecznej komunikacji online. Dzięki temu mechanizmowi, nadawcy mogą mieć pewność, że ich informacje pozostaną poufne, a odbiorcy mogą bezpiecznie odczytać treść wiadomości, wiedząc, że nie została ona naruszona przez osoby trzecie.

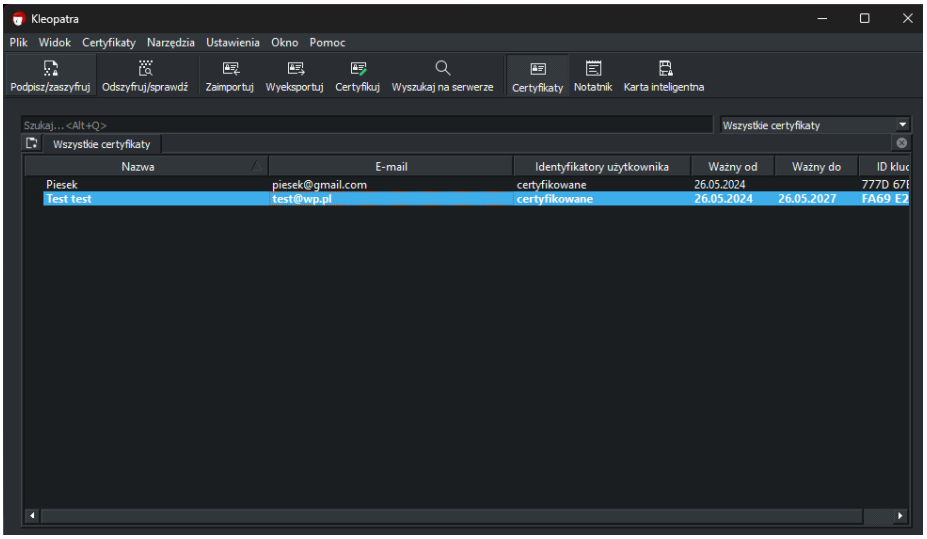
```
-----BEGIN PGP MESSAGE-----

hF4D/qIT1G8stUYSAQdARzsrkxvZFDuSHStyiHtog9vuCkqSGwrthUf4EBvwp1cw
nJjRfm4TkxTH04wp7ESFqpaoB8M1jRs1FcSMRwrjiryMPtMmGq6K7tIem93cJN90
1FwBCQIQg/sEUVGs/GyZDoFEfMRj3UxBptyN8wS1NGiKnRdDh8p5jmPERZG/K/oP
kgRCPCLQmahR+cBS6KYS4DA6CYCa8tL93P6tM34iDDrz1SD/krsiRW+E+vtssA==
=PcIm
-----END PGP MESSAGE-----
```

Rys.2 Struktura zaszyfrowanej wiadomości

5. Zastosowanie Open PGP w oprogramowaniu Kleopatra

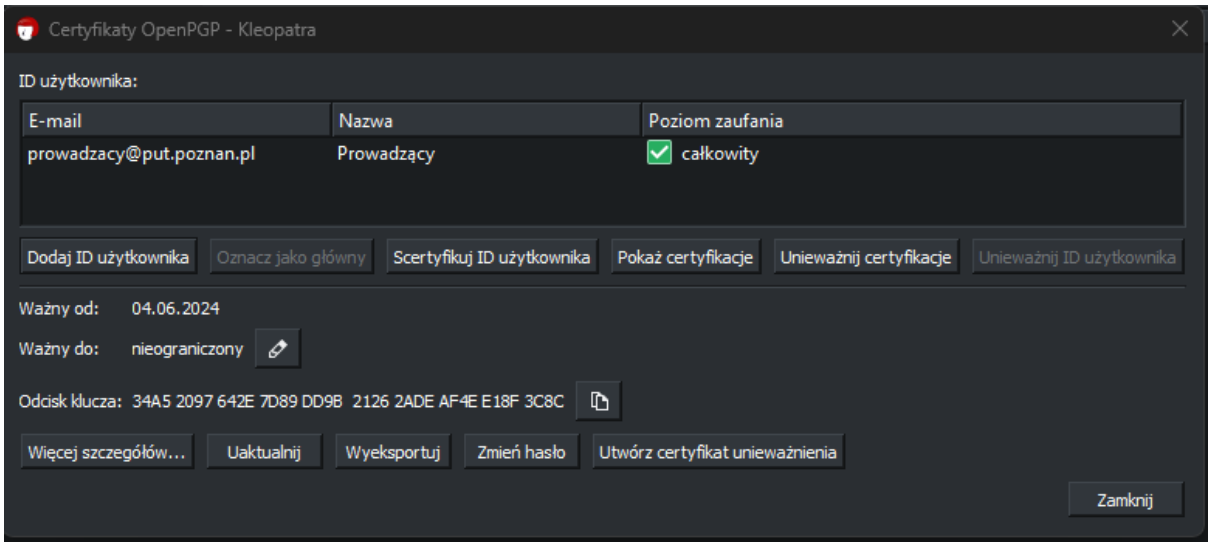
Kleopatra to graficzny interfejs użytkownika do zarządzania kluczami kryptograficznymi oraz szyfrowania i podpisywania danych, będący częścią pakietu oprogramowania Gpg4win opierającego się na standardzie OpenPGP. Umożliwia generowanie par kluczy publicznych i prywatnych, które są niezbędne do szyfrowania i deszyfrowania danych, a także zarządzanie nimi poprzez importowanie, eksportowanie, przechowywanie i tworzenie kopii zapasowych.



Rys.3 Interfejs graficzny Kleopatra

Kleopatra pozwala na szyfrowanie wiadomości i plików przy użyciu kluczy publicznych odbiorców oraz deszyfrowanie otrzymanych zaszyfrowanych danych przy użyciu klucza prywatnego. Oferuje również funkcje podpisywania cyfrowego, aby zapewnić integralność i autentyczność danych, oraz weryfikacji podpisów cyfrowych, co pozwala upewnić się, że dane nie zostały zmodyfikowane. Narzędzie to może być używane zarówno samodzielnie, jak i w połączeniu z innymi aplikacjami, takimi jak klienci poczty elektronicznej. Kleopatra znajduje zastosowanie w bezpiecznej

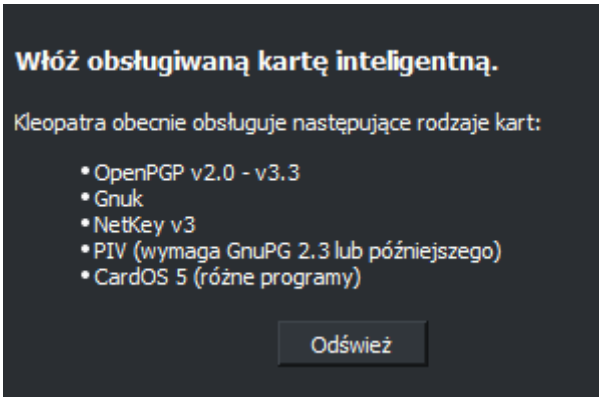
komunikacji poprzez szyfrowanie e-maili, ochronie plików i folderów na dysku twardym oraz zapewnianiu integralności danych poprzez podpisy cyfrowe, co czyni je przyjaznym dla użytkowników, szczególnie tych rozpoczynających przygodę z kryptografią PGP.



Rys.4 Funkcja zarządzania certyfikatami

6. Użycie inteligentnych kart w Open PGP

Program kleopatra nie jest wykorzystywany jedynie do samodzielnego tworzenia kluczy i przechowywaniu ich centralnie na dysku maszyny. Możliwe jest dodatkowe użycie różnych rodzajów kart kryptograficznych zgodnych z OpenPGP, takich jak OpenPGP v2.0 - v3.3, Gnuk, NetKey v3, PIV oraz CardOS 5. Każda z tych kart oferuje wsparcie dla standardów kryptograficznych, które umożliwiają bezpieczne przechowywanie kluczy oraz wykonywanie operacji kryptograficznych. Karty OpenPGP v2.0 - v3.3 są najczęściej używane do implementacji standardu OpenPGP. Gnuk jest wolną implementacją specyfikacji USB dla kart OpenPGP, opartą na otwartym oprogramowaniu. NetKey v3 zapewnia zaawansowane funkcje bezpieczeństwa dla profesjonalnych zastosowań. PIV (Personal Identity Verification) jest używany głównie w systemach federalnych USA, oferując wysokie bezpieczeństwo i interoperacyjność. CardOS 5 jest kartą inteligentną z zaawansowanymi funkcjami bezpieczeństwa, wykorzystywaną w różnych branżach do ochrony danych i zarządzania tożsamością. Stosowanie kart zapewnia nam dodatkowe bezpieczeństwo, gdyż klucze nie są dostępne wewnątrz pamięci komputera, przez co zagrożenie ich przechwycenia przez potencjalnych atakujących jest znacznie ograniczona.



Rys.5 Możliwość zastosowania inteligentnych kart

7. Basic Card / JavaCard z OpenPGP

W przestrzeni internetowej znajdują się dedykowane repozytoria dla kart Basic i typu JavaCard, które za pomocą ogólnodostępnych licencji dostępne są dla każdego użytkownika. Umożliwiają one implementację cech PGP dla obu typów kart.

Repozytorium OpenPGP Applet for JavaCard implementuje funkcjonalność karty OpenPGP na kartach A40CR sprzedawanych przez JavaCardOS. Umożliwia wykonywanie operacji podpisywania i szyfrowania za pomocą kluczy RSA lub ECC, zgodnie ze standardem OpenPGP v2.0.1. Projekt można budować za pomocą narzędzi JCIDE lub Eclipse z dodatkiem eclipse-jcde, a następnie instalować na kartach JavaCard przy użyciu narzędzia pyApduTool do przesyłania pliku CAP i instalacji apletu. Jest to elastyczne rozwiązanie dla programistów, którzy chcą korzystać z kart JavaCard do obsługi operacji kryptograficznych zgodnie ze standardem OpenPGP.

https://github.com/JavaCardOS/OpenPGPApplet

Repozytorium OpenPGP for BasicCard oferuje implementację karty OpenPGP na BasicCard 7.5 od Zeitcontrol. Kod można kompilować i ładować na profesjonalne karty BasicCard z wersją 7.5 lub wyższą, używając darmowego zestawu deweloperskiego dostępnego na stronie Zeitcontrol. Wymaga pliku Tlv12.def, który musi być umieszczony w folderze Lib zestawu deweloperskiego, ponieważ nie jest dostarczany z najnowszym zestawem. To rozwiązanie jest przydatne dla użytkowników BasicCard, którzy potrzebują implementacji OpenPGP do bezpiecznego podpisywania i szyfrowania danych.

https://github.com/Nitrokey/openpgp-card/tree/master

8. Dodatkowe zastosowanie bibliotek OpenPGP

Technologia OpenPGP, wykorzystywana do szyfrowania i podpisywania danych, jest wspierana przez wiele bibliotek w różnych językach programowania. Dla Javy i C# dostępne są Bouncy Castle oraz PGPainless dla Javy, które oferują niskopoziomowe wsparcie kryptograficzne. W C++ używane są biblioteki takie jak calccrypto/OpenPGP oraz NeoPG. Dla języka C dostępne jest GnuPG Made Easy (GPGME) z powiązaniami do Pythona i Lispa oraz NetPGP z powiązaniami do Pythona, Perla i Lua. Golang ma swoją natywną bibliotekę Golang OpenPGP. Haskell oferuje Haskell OpenPGP i hOpenPGP. W ekosystemie .NET, Java, C++, Python, Delphi, PHP, Node.js, Android i iOS można używać IPWorks OpenPGP. JavaScript ma kbpgp i OpenPGP.js, podczas gdy PHP korzysta z OpenPGP-PHP. Dla Objective C dostępna jest ObjectivePGP, dla OCaml OCaml PGP, a dla Pythona PGPy. Również C++ ma wsparcie w postaci RNP, Rust korzysta z Sequoia PGP, a Swift z Swift-PGP. Wszystkie te biblioteki implementują standard OpenPGP, umożliwiając programistom zabezpieczanie danych w różnych środowiskach programistycznych.

Rys.6 Lista dostępnych bibliotek na bazie PGP

9. Podsumowanie

Przytoczone w tekście PGP to łatwa do wdrożenia, darmowa technologia kryptograficzna, która oferuje szerokie zastosowania w dziedzinie bezpieczeństwa danych. Dzięki otwartemu standardowi i dostępności wielu narzędzi, PGP umożliwia bezpieczne podpisywanie i szyfrowanie wiadomości oraz plików, co jest kluczowe dla ochrony poufności i integralności informacji. Technologia ta jest szczególnie przydatna w firmach, które chcą zapewnić bezpieczeństwo komunikacji i danych, a także oferuje duże możliwości rozwoju oprogramowania i integracji z istniejącymi systemami. PGP jest elastyczne i może być dostosowane do różnych potrzeb, co czyni je cennym narzędziem w dzisiejszym cyfrowym świecie.