Oprogramowanie Open PGP Applet dla Basic / JavaCard

Paweł Kanclerzewski, Kamil Ambroży

Czy nasze dane są bezpieczne?

Yahoo Data Breach:

W latach 2013 i 2014 Yahoo padło ofiarą dwóch oddzielnych ataków hakerskich, które skutkowały wyciekiem danych miliardów użytkowników. Początkowo Yahoo ujawniło, że w wyniku ataków naruszono bezpieczeństwo 500 milionów kont użytkowników, jednak później ta liczba wzrosła do około 3 miliardów kont, co oznaczało, że praktycznie wszystkie konta Yahoo zostały dotknięte.

Wpływ na firmę:

Wartość Yahoo: Naruszenia miały poważny wpływ na wartość rynkową Yahoo. Podczas negocjacji zakupu Yahoo sytuacja ta skutkowała obniżeniem ceny zakupu o około 350 milionów dolarów.

PGP - Pretty Good Privacy

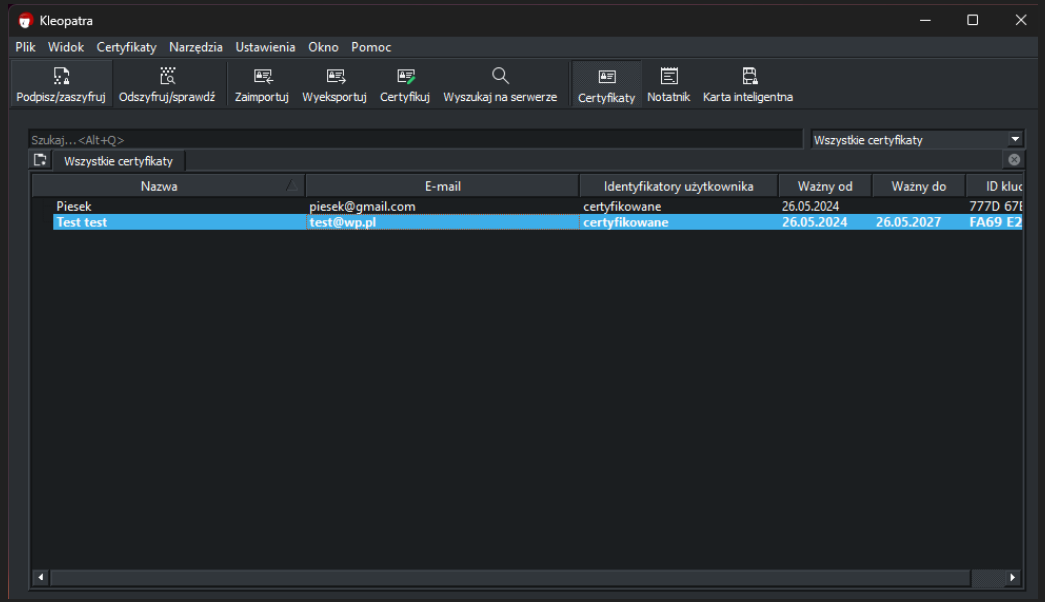
PGP to kryptograficzny program komputerowy zapewniający prywatność i uwierzytelnianie danych.

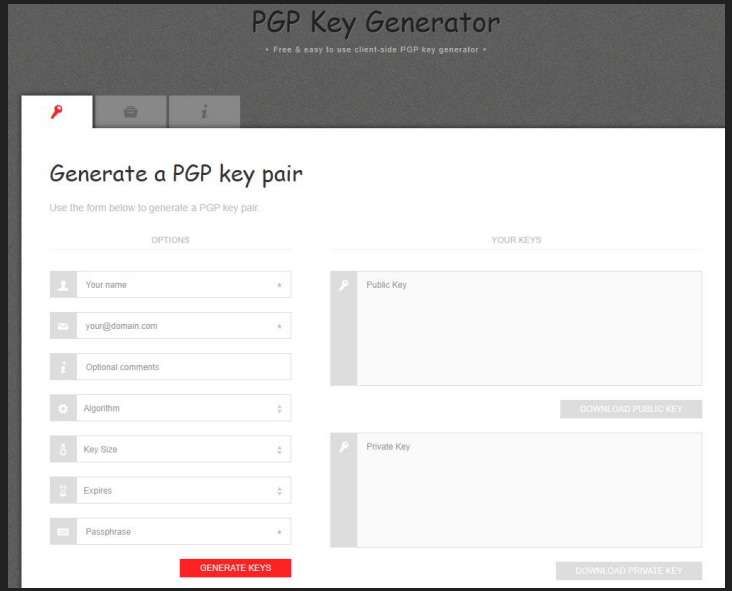
1. Kryptografia Hybrydowa: PGP wykorzystuje kombinację szyfrowania symetrycznego i asymetrycznego. Szyfrowanie symetryczne jest używane do szyfrowania samej wiadomości, podczas gdy asymetryczne szyfrowanie jest używane do szyfrowania klucza sesji symetrycznego szyfrowania.

2. Stosowane dla podpisów cyfrowych: PGP pozwala na tworzenie podpisów cyfrowych, które zapewniają integralność i autentyczność wiadomości. Odbiorca może zweryfikować, czy wiadomość nie została zmieniona i pochodzi od określonego nadawcy.

Jak wygenerować klucze?

Kleopatra lub serwisy generujące klucze - **BARDZO ŁATWY PROCES!!!**



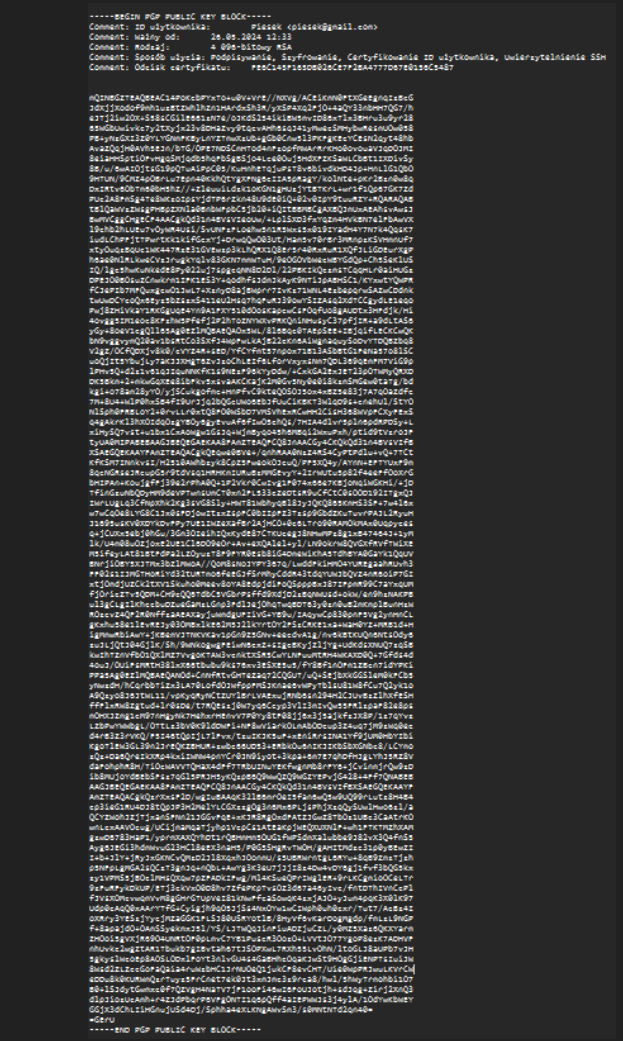


Struktura klucza PGP

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Comment: ID użytkownika:        Piesek <piesek@gmail.com>
Comment: Ważny od:      26.05.2024 12:33
Comment: Rodzaj:        4 096-bitowy RSA
Comment: Sposób użycia: Podpisywanie, Szyfrowanie, Certyfikowanie ID użytkownika, Uwierzytelnienie SSH
Comment: Odcisk certyfikatu:    FE6C145F165DB026CE7F2BA4777D67E0156C5487

mQINBGZTEAQBEAC14PoKcbPYxTo+u0V+VrE//NXVg/ACEiKmN0FtXGeEgnqIzBcG
JdXiiXodof9mh1uzBtZWhlhZn1HArdxSh3R/vXSP4Xq2FiO+4aOY33nbHH7OG7/h
```

```
8Wsd2ZLZccGoFaQaia4ruWzbHC1JrNUOeQ1jukCF8evCHT/Uie0WpPRJwuLKVrCW
eDDu8k0KURWmQzrTuyz5FrCnet7ek0Jt3xmJmc3z9rca8/hwl/5hWyTrmohbi1O7
B0+lSJdytGwmxc0f7QZVgH4NaTV7jF1ooFi46wI6FoUJotjh+sdJqg+Zirj2XnQ3
dlpJiozUcAmh+r4ZJdPbqrP6VFgONTI1q6pQff4aIEPWWJs3j4ylA/1OdYwKbWEY
GGjX3dChLIiHGnujUSd4Dj/Sphha4eXLKNgAWvSm3/s0MNtNTd2qn40=
=GErU
-----END PGP PUBLIC KEY BLOCK-----
```



Przykładowa zaszyfrowana wiadomość

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

hF4D/qIT1G8stUYSAQdARzsrkxvZFDuSHStyiHtog9vuCkqSGwrthUf4EBvwp1cw
nJjRfm4TkxTH04wp7ESFqpaoB8MljRs1FcSMRwrjiryMPtMmGq6K7tIem93cJN90
1FwBCQIQg/sEUVGs/GyZDoFEfMRj3UxBptyN8wSlNGiKnRdDh8p5jmPERZG/K/oP
kgRCPCLQmahR+cBS6KYS4DA6CYCa8tL93P6tM34iDDrzlSD/krsiRW+E+vtssA==
=PcIm
-----END PGP MESSAGE-----
```

Zastosowanie PGP

- Szyfrowanie poczty elektronicznej: Możliwość szyfrowania i deszyfrowania e-maili przy użyciu OpenPGP.

- Podpisy cyfrowe: Wykorzystywanie karty do podpisywania dokumentów cyfrowych, co zapewnia ich autentyczność i integralność.

- Uwierzytelnianie: Bezpieczne logowanie do systemów i usług, używając karty do uwierzytelniania użytkownika.

Basic Card / JavaCard z OpenPGP

PGP dla BasicCard:

https://github.com/Nitrokey/openpgp-card/tree/master (Wymagana wersja karty: 7.5 lub wyższa)

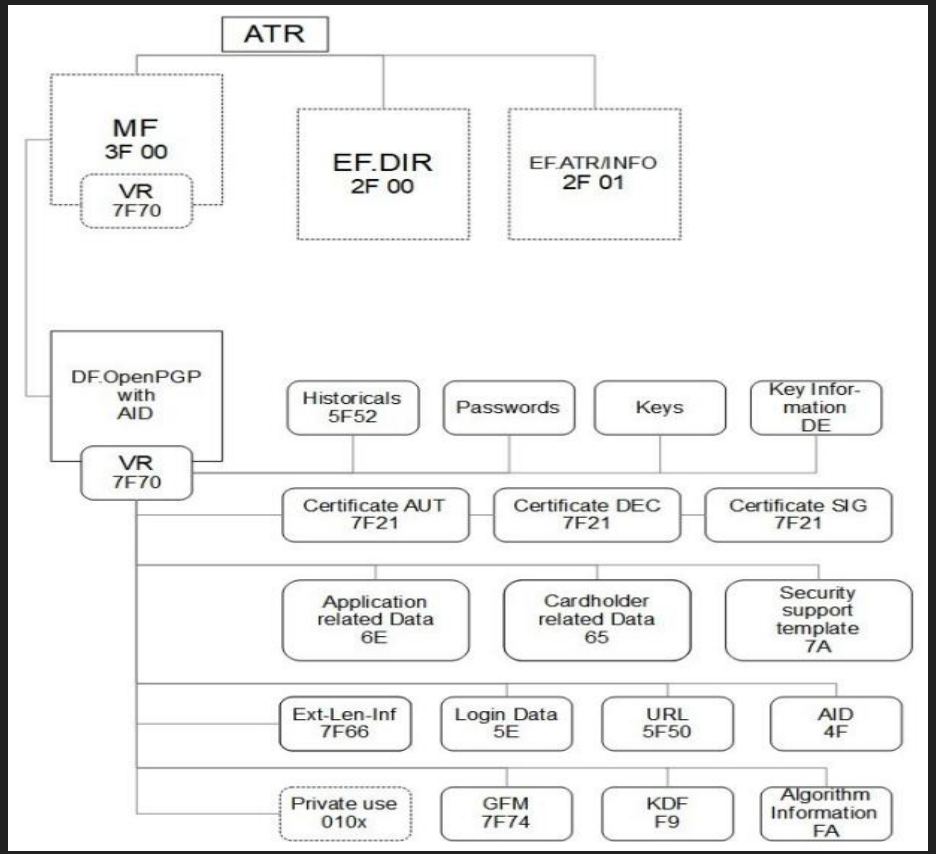
PGP dla JavaCard

https://github.com/JavaCardOS/OpenPGPApplet

OpenPGP Smart Card

- 3 independent keys for signature, encryption and authentication
- RSA keys from 2048 up to 4096 bits length
- key generation on card or import of existing keys
- signature counter
- safe hardware random number generator (complies AIS 31)
- PIN length between 6(8) and 64 characters, not limited to numbers
- separate PIN and admin PIN
- KDF-Encryption for passwords
- T=1 protocol, compatible with most chipcard terminals

Struktura ATR



Jak inaczej skorzystać z możliwości PGP?

OpenPGP Libraries

- Bouncy Castle (Low-level Java/C#)
- calccrypto/OpenPGP (C++)
- GnuPG Made Easy (GPGME) (C, with Python and Lisp bindings)
- Golang OpenPGP (Go)
- Haskell OpenPGP (Haskell)
- hOpenPGP (Haskell)
- IPWorks OpenPGP (.NET, Java, C++, Python, Delphi, PHP, Node.js, Android, iOS)
- kbpgp (JavaScript)
- NeoPG (C++, GnuPG fork as a library)
- NetPGP (C, with Python, Perl and Lua bindings)
- ObjectivePGP (Objective C)
- OCaml PGP (OCaml)
- OpenKeychain API (Java)
- OpenPGP-PHP (PHP)
- OpenPGP.js (Javascript)
- PGPainless (Java)
- PGPy (Python)
- RNP (C++)
- Sequoia PGP (Rust)
- Swift-PGP (Swift)

Dziękuję za uwagę