Instrukcja obsługi programu do podpisywania plików SmartSigning

Przemysław Świder, Tomasz Kozłecki

Cyberbezpieczeństwo 2022

Wstęp

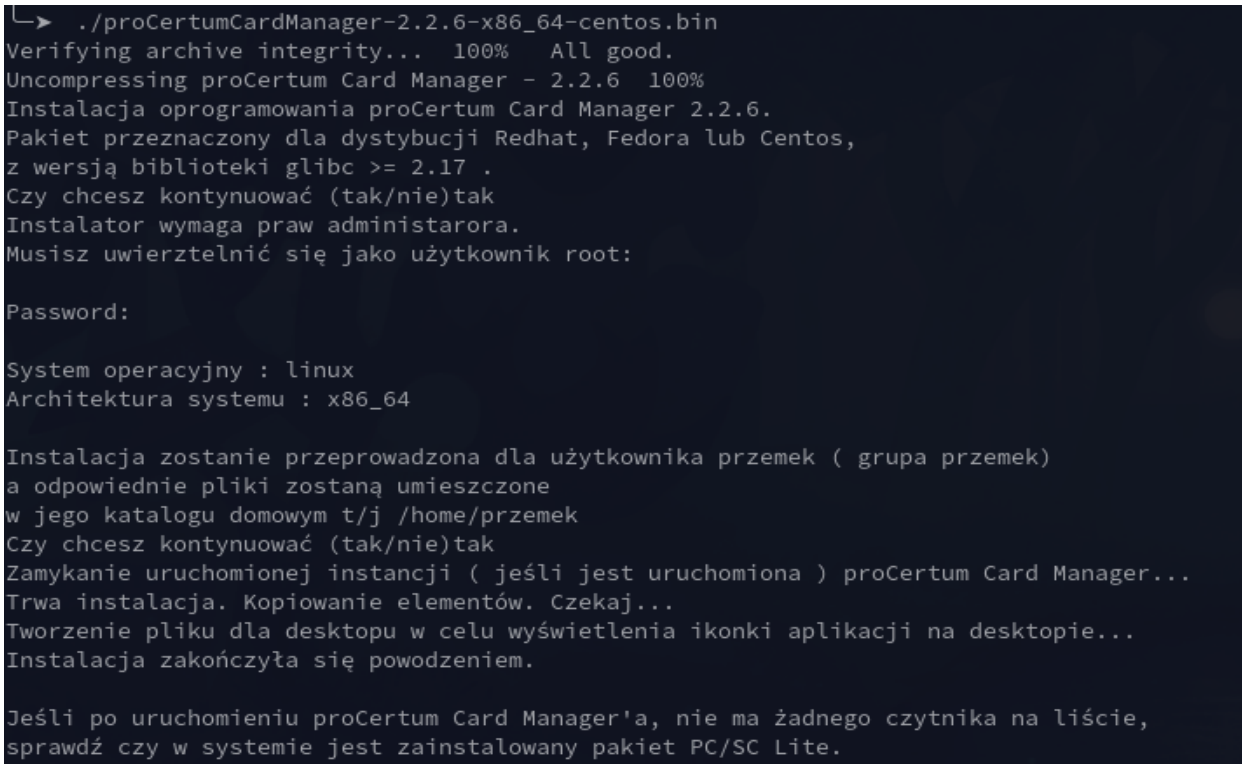
Program SmartSigning powstał w celach edukacyjnych w ramach projektu na Sprzętowe Aspekty Cyberbezpieczeństwa. Służy on do podpisywania plików wykorzystując funkcję profil standardowy na karcie kryptograficznej Certum.

Instrukcja instalacji

Wymagania systemowe: procesor: Pentium 800 MHz, system Linux - na Windows nie działa profil zwykły.
Wymaga zainstalowania oprogramowania producenta umożliwiającego komunikację z kartą, Python3, oraz oprogramowania sterującego pracą czytników, na przykład opensc.

Github: https://github.com/fusikk/SmartSigning

Należy pobrać i zainstalować na komputerze program producenta karty proCertum CardManager
https://pomoc.certum.pl/pl/oprogramowanie/procertum-cardmanager/
Instalacja na system Linux sprowadza się do uruchomienia pobranego pliku bin.



Jeśli karta nie jest widoczna w systemie należy zainstalować narzędzie opensc:
```
sudo apt-get install -y opensc
```

Przed uruchomieniem programu należy zainstalować niezbędne biblioteki Python. W tym celu uruchamiamy terminal w folderze głównym aplikacji SmartSigning i wpisujemy komendę
```
pip install -r requirements.txt
```

Uwaga: Podczas pierwszego uruchomienia aplikacji może być konieczne ręczne wprowadzenie lokalizacji do pliku .so z narzędzia proCertum CardManager, jeśli domyślnie wgrana do programu lokalizacja nie jest poprawna. Do tego celu należy użyć przełącznika –pkcs-path <ścieżka do pliku>. Program zapamięta ścieżkę dzięki czemu nie będzie konieczne ponowne podawanie jej.

Przykładowe scenariusze użycia aplikacji

- Eksport klucza publicznego do pliku public.pem, pin do karty 1234:
  ```
  python3 main.py -e 1234 public.pem
  ```

- Podpis pliku file.txt używając PIN-u 1234
  ```
  python3 main.py -s 1234 -in file.txt
  ```

- Weryfikacja podpisu znajdującego się w pliku file.sacproj do pliku file.txt, pin 1234, klucz publiczny w pliku public.pem
  ```
  python3 main.py -v public.pem file.sacproj -in file.txt -s 1234
  ```

- Wyświetlanie instrukcji obsługi programu
  ```
  python3 main.py -h
  ```

Przygotowanie karty

Aby podpisywanie plików było możliwe, należy posiadać certyfikat zainstalowany na karcie Certum. W tym celu można wykorzystać narzędzie openssl. Poniżej przykładowa instrukcja generowania certyfikatu testowana na systemie Linux Mint:

- Instalacja openssl
  ```
  sudo apt install openssl
  ```

- Generowanie certyfikatu i klucza prywatnego
  ```
  openssl req -newkey rsa:4096 -x509 -sha256 -days 3650 -nodes -out cert.crt -keyout private.key
  ```

  Po wywołaniu powyższej instrukcji konieczne będzie podanie danych certyfikatu o które poprosi program openssl

- Konwersja do pliku pfx
  ```
  openssl pkcs12 -export -out cert.pfx -inkey private.key -in cert.crt
  ```

W wyniku wykonania powyższych instrukcji powstanie plik cert.pfx który należy zaimportować do karty przy użyciu programu proCertum CardManager. Wspomniany program powinien również poprosić o ustawienie kodów PIN oraz PUK niezbędnych do poprawnego działania karty kryptograficznej.