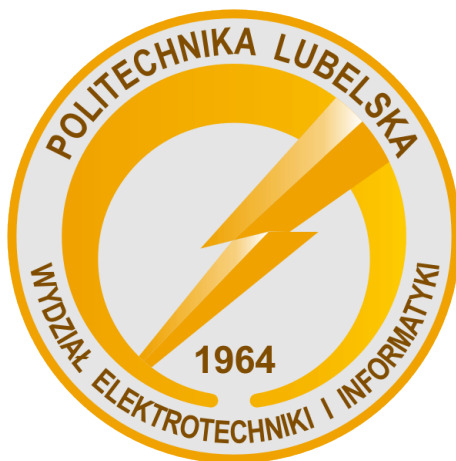


POLITECHNIKA LUBELSKA
Wydział Elektrotechniki i Informatyki
Kierunek Informatyka



PRAKTYKI STUDENCKIE

Aplikacja odczytująca dane paszportu COVID z kodu QR

1. Opis projektu

Aktualna sytuacja pandemiczna wprowadziła wiele zmian. Spora część osób musiała zamknąć się w domach i swoje pokoje zamienić w biura służące zarówno do pracy, jak i – w naszym przypadku – do nauki. Pandemia COVID-19 zmieniła również podejście do szczepień oraz ich identyfikacji. Ta ma być nie tylko jaśniejsza dla służb i samych obywateli, ale również prostsza w interpretacji.

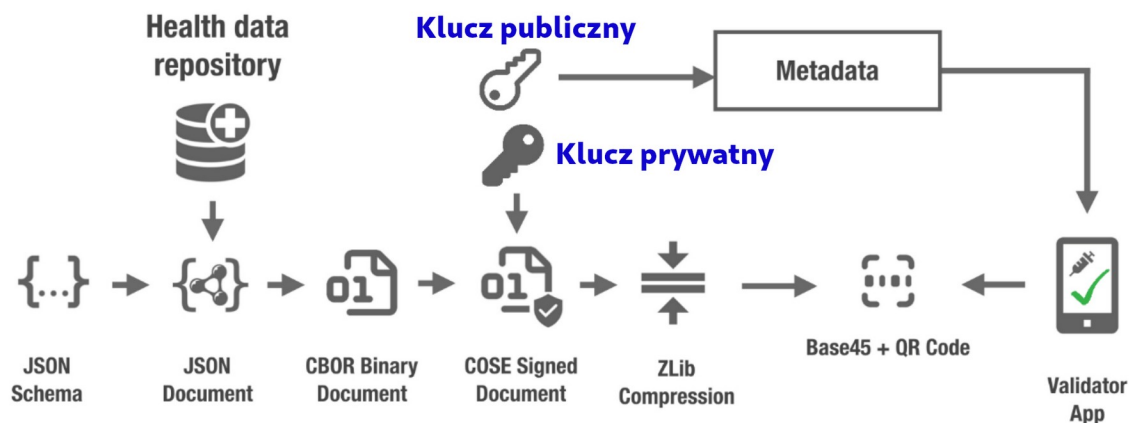
To też sprawiło, że na terenie Unii Europejskiej (ale również w krajach partnerskich) powstał specjalny paszport covidowy, który jest swego rodzaju potwierdzeniem i certyfikatem szczepienia przeciwko COVID-19. Przedstawiane one są w postaci kodu QR, który przenosi zaszyfrowane informacje.

Informacje te można odszyfrować za pomocą rządowych aplikacji. Niestety, mają one pewne wady. Pierwsza to fakt, że obywatel chcący przenosić swój certyfikat w aplikacji mobilnej musi mieć założony *Profil Zaufany*. Ponadto wiele obywateli nie ma zaufania do aplikacji rządowych – tym bardziej, że te nie opierają się o otwarty kod – Open Source.

Z tego też powodu wyszliśmy z pomysłem stworzenia własnej aplikacji, która pozwalałaby na odszyfrowanie i odczytanie informacji, które przenosi paszport covidowy. Program został opublikowany na zasadach Open Source oraz można go uruchamiać na przeróżnych platformach, w tym w systemach Windows, Android oraz Linux, a także na przeróżnych architekturach, w tym x86 i ARM.

2. Paszport covidowy – schemat działania

Paszport covidowy (EU Digital COVID Certificate) został oparty o pewne europejskie standardy, czego wynikiem jest długi ciąg znaków pokazywany w formie gotowego do zeskanowania kodu QR.



Fot. 1: Schemat szyfrowania paszportu covidowego (źródło: Guidelines on Technical Specifications for Digital Green Certificates)

Zgodnie ze schematem, szablon obiektu JSON jest wypełniany danymi osoby zaszczepionej z zewnętrznego repozytorium, który to jest przekształcany w postać binarną CBOR. Następnie certyfikat jest podpisywany kluczem prywatnym, czego wynikiem jest paczka COSE, która jest dekompresowana algorytmem Zlib Deflate. Otrzymane dane są kodowane protokołem BASE45 i w takiej postaci są przedstawiane jako kod QR.

Odczytanie otrzymanego kodu QR daje nam ciąg znaków podobny do poniższego:

```
HC1:6BFOXN%TS3DH1QG9WA6H98BRPRHO DJS4/ R-
%2%T4E+NAVDQ81LO2-36/X0X6BMF6.UCOMIN6R%E5UX4U96:/6N9R
%EPXCROGO3HOWGOKEQBKL/645YPL$R-
ROM47L*K1UPB65%PD*ZL*9DJZI202K-JKYJGCC:H3J1D1I3-*TW C57DNGSE
%CM6EJ.CN8TF*SD8CL0D3VCL0DK0D4.S%JCJBCTYDWBDWVDUMCS1J+PB/V
SQOL9DLSWCZ3EBKDVIJGDBDIT1NJGIA+OJ:CI-L3ZJA/
3CZIJFVA.QO5VA81K0ECM8CXVDC8C 1J17JSTNCA7G6M
%28ODSINQIVQUIRYQ4P7M9SB95S6M/355X7C25E8DLFEA3LS6FPOSXD79
NT+X4VIOS0I63K*+7SLS9NTRFB0X4YGFD.O8RJ5XPUVPQRHIY1VS1NQ1PRA
AUICO12Y99UE$V1*65CHK62HJEEK*M:C9GXN.SMPT1+2O::BOJHLTIPFEL-
D+HD.35IIM:/M0S4*PA6447S6+1TIARN/NV
1S86P.N2SBDNRW2GTET6/VTIKIX200TTJ2
```

Warto dodać, że na samym początku kodu dodawane są cztery znaki „HC1:”, co dokładnie oznacza *Healthcare Certificate Wersja 1*. W procesie dekodowania muszą one zostać usunięte.

3. Przygotowanie aplikacji

Aplikacja deszyfrująca paszport covidowy jest w rzeczywistości algorytmem, który odwraca proces szyfrowania. Wynikiem wyświetlanym przez algorytm powinien być obiekt JSON wypełniony danymi osoby zaszczepionej.

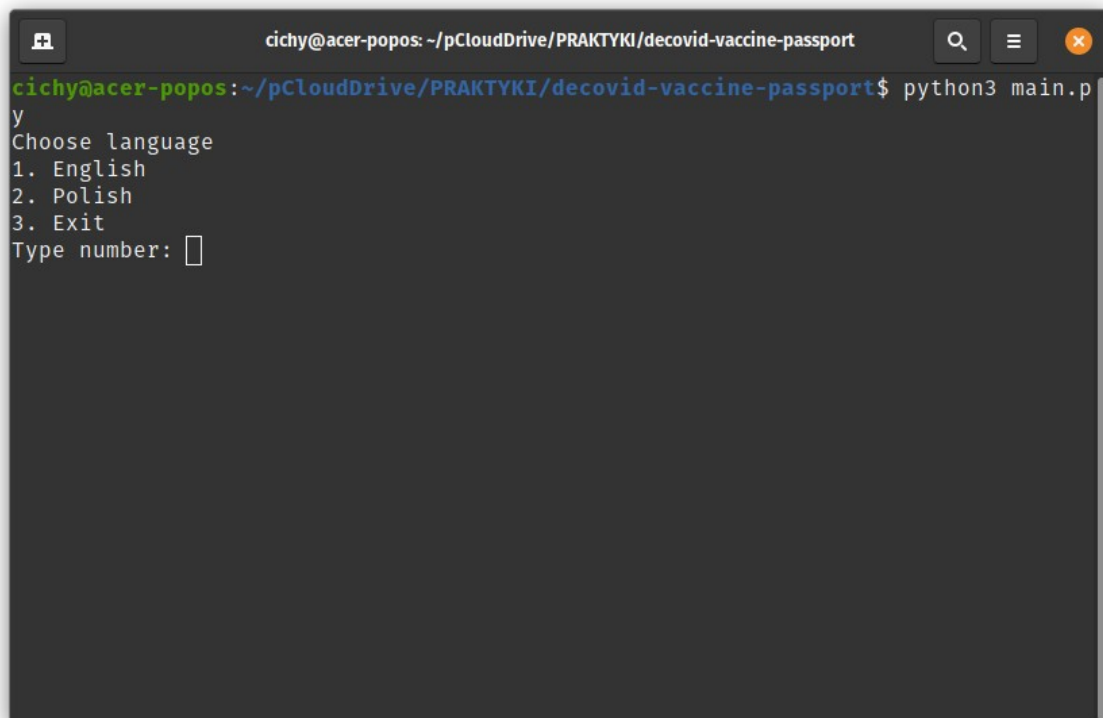
Program napisaliśmy w języku Python. Wybraliśmy go z kilku względów. Przede wszystkim Python oferuje prostą manipulację łańcuchami znakowymi oraz daje dostęp do wielu ważnych bibliotek niezbędnych do rozszyfrowania paszportu covidowego. Ponadto Python to język wieloplatformowy, a więc napisany kod w systemie GNU/Linux (gdzie właśnie aplikacja została stworzona) będzie tak samo działał zarówno na Windowsie, jak i Androidzie.

Aplikacja tekstowa (CLI)

Aplikacja tekstowa została napisana jako ta podstawowa. Składa się ona z 4 plików o rozszerzeniu `.py`. Dodatkowym plikiem jest `README.md` zawierający instrukcję uruchomienia w języku angielskim. Po wykonaniu kodu, tworzy się plik `cert.json`, zawierający obiekt JSON z wynikiem odszyfrowania.

Aplikacja została udostępniona publicznie w repozytorium GitHub i znajduje się »[pod tym linkiem](#)«.

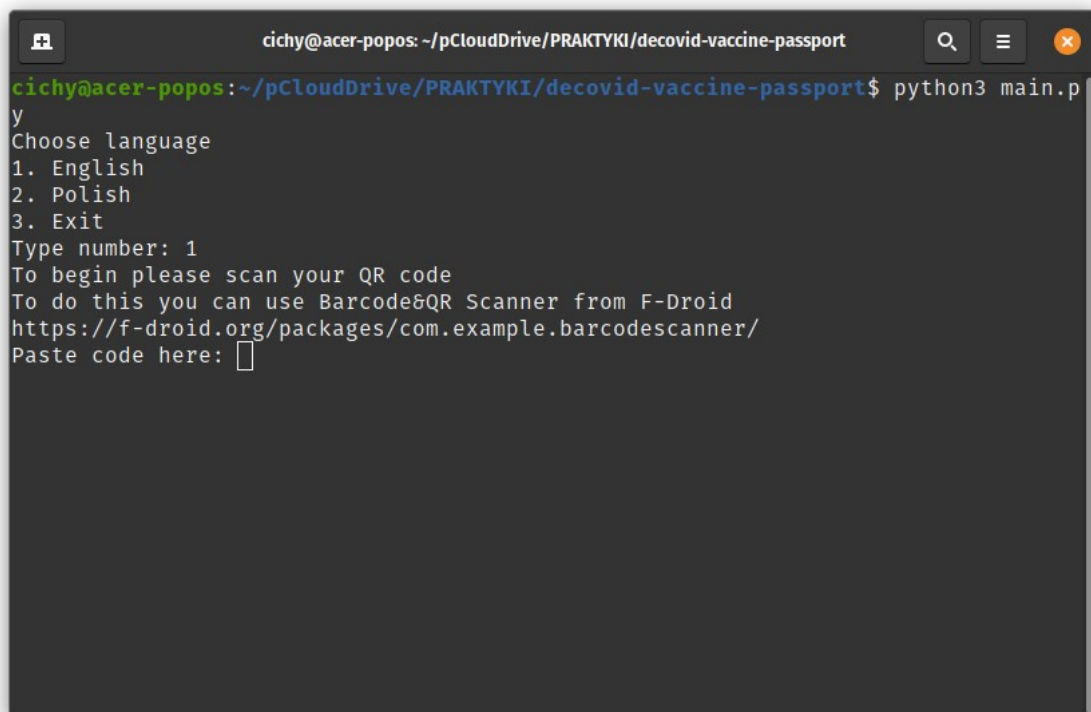
Po uruchomieniu aplikacji (wykonanie kodu znajdującego się w pliku głównym `main.py`) pojawia się zapytanie o język przewodni.

A terminal window with a dark background. The title bar shows the user 'cichy@acer-popos' and the current directory '~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport'. The command 'python3 main.py' has been executed. The program prompts the user to 'Choose language' and lists three options: '1. English', '2. Polish', and '3. Exit'. Below this, it asks 'Type number:' followed by a cursor.

```
cichy@acer-popos: ~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport
cichy@acer-popos:~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport$ python3 main.py
Choose language
1. English
2. Polish
3. Exit
Type number: 
```

Fot. 2: Uruchomienie aplikacji

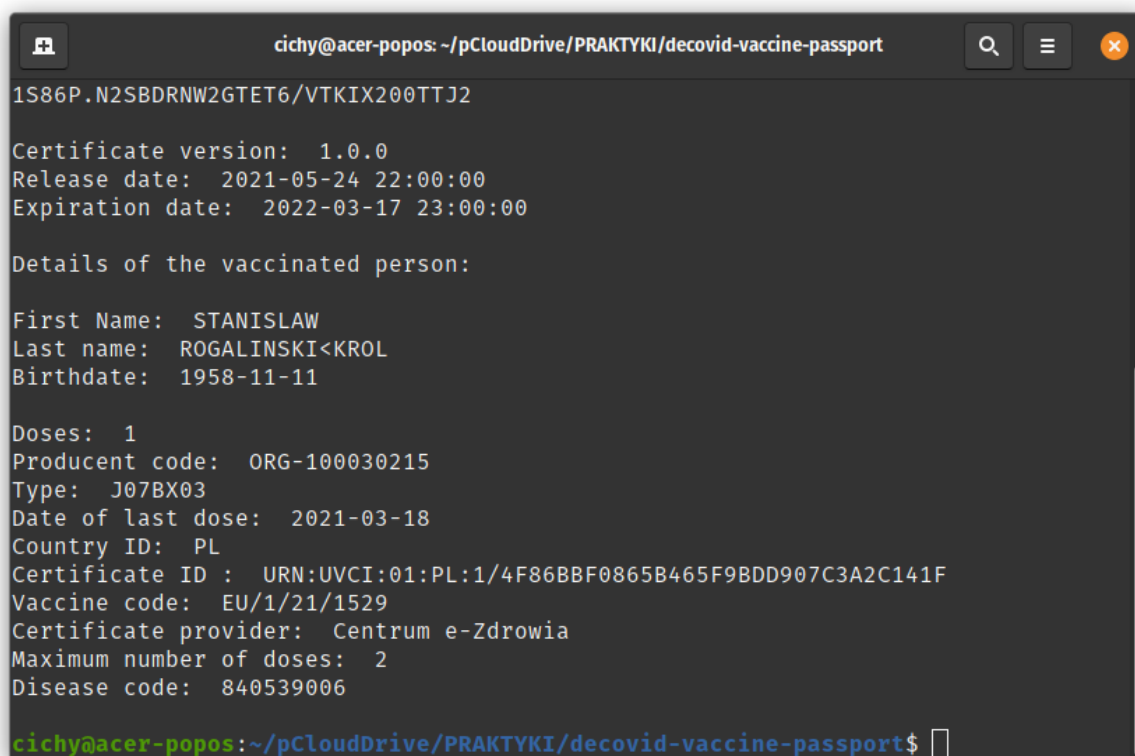
Po wybraniu języka, aplikacja poprosi o podanie kodu ukrytego w formie grafiki 2D QR.

The terminal window continues from the previous state. The user has entered '1' for English. The program now instructs the user to scan a QR code, provides a link to the F-Droid app page, and prompts for the QR code to be pasted.

```
cichy@acer-popos: ~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport
cichy@acer-popos:~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport$ python3 main.py
Choose language
1. English
2. Polish
3. Exit
Type number: 1
To begin please scan your QR code
To do this you can use Barcode&QR Scanner from F-Droid
https://f-droid.org/packages/com.example.barcodescanner/
Paste code here: 
```

Fot. 3: Prośba aplikacji o podanie kodu z grafiki QR

Po wklejeniu kodu rozpoczynającego się od znaków *HC1*, pojawiają się wszystkie zaszyfrowane informacje. Automatycznie stworzył się również plik *cert.json* zawierający te same dane w postaci obiektu JSON.



```
cichy@acer-popos: ~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport
1S86P.N2SBDNRW2GTET6/VTKIX200TTJ2

Certificate version: 1.0.0
Release date: 2021-05-24 22:00:00
Expiration date: 2022-03-17 23:00:00

Details of the vaccinated person:

First Name: STANISLAW
Last name: ROGALINSKI<KROL
Birthdate: 1958-11-11

Doses: 1
Producent code: ORG-100030215
Type: J07BX03
Date of last dose: 2021-03-18
Country ID: PL
Certificate ID : URN:UVC1:01:PL:1/4F86BBF0865B465F9BDD907C3A2C141F
Vaccine code: EU/1/21/1529
Certificate provider: Centrum e-Zdrowia
Maximum number of doses: 2
Disease code: 840539006

cichy@acer-popos:~/pCloudDrive/PRAKTYKI/decovid-vaccine-passport$
```

Fot. 4: Wynik aplikacji