How (not) to implement secure digital identity

Case study of Poland's Digital ID system

securing

Agenda 📜

Practical part 🤓

- Political background
- Historical background
- **Abusing the system in practice**
- Digital ID during red teaming

Technical part 🕵️

- Deep-diving into ID verification process
- **Vulnerabilites in the Poland's digital ID system**
- Government's reaction
- Lessons to learn

whoami

Szymon Chadam

IT Security Consultant at securing

Certificates:

Certified iOS Application Security Engineer (iASE)

eLearnSecurity Web Application Penetration Tester eXtreme (eWPTXv2)

Burp Suite Certified Practicioner (BSCP)

Publications:

Voice Biometrics – how easy is it to hack them with AI Deepfake?

Proof-Of-Work CAPTCHA with password cracking functionalities

OWASP WGI confidence

Disclaimer

- Completed the disclosure process
- Govt has already introduced fixes
- Pro bono, non-commercial research

🙋 Raise your hand if

Your country already has some sort of Digital ID

If you did 

- What are the similarities and differences?
- Let’s connect after this talk to compare.

If you didn’t 

- Only a matter of time before you’ll 
- Learn on other’s mistakes before its implemented in your country.

Political background in the EU

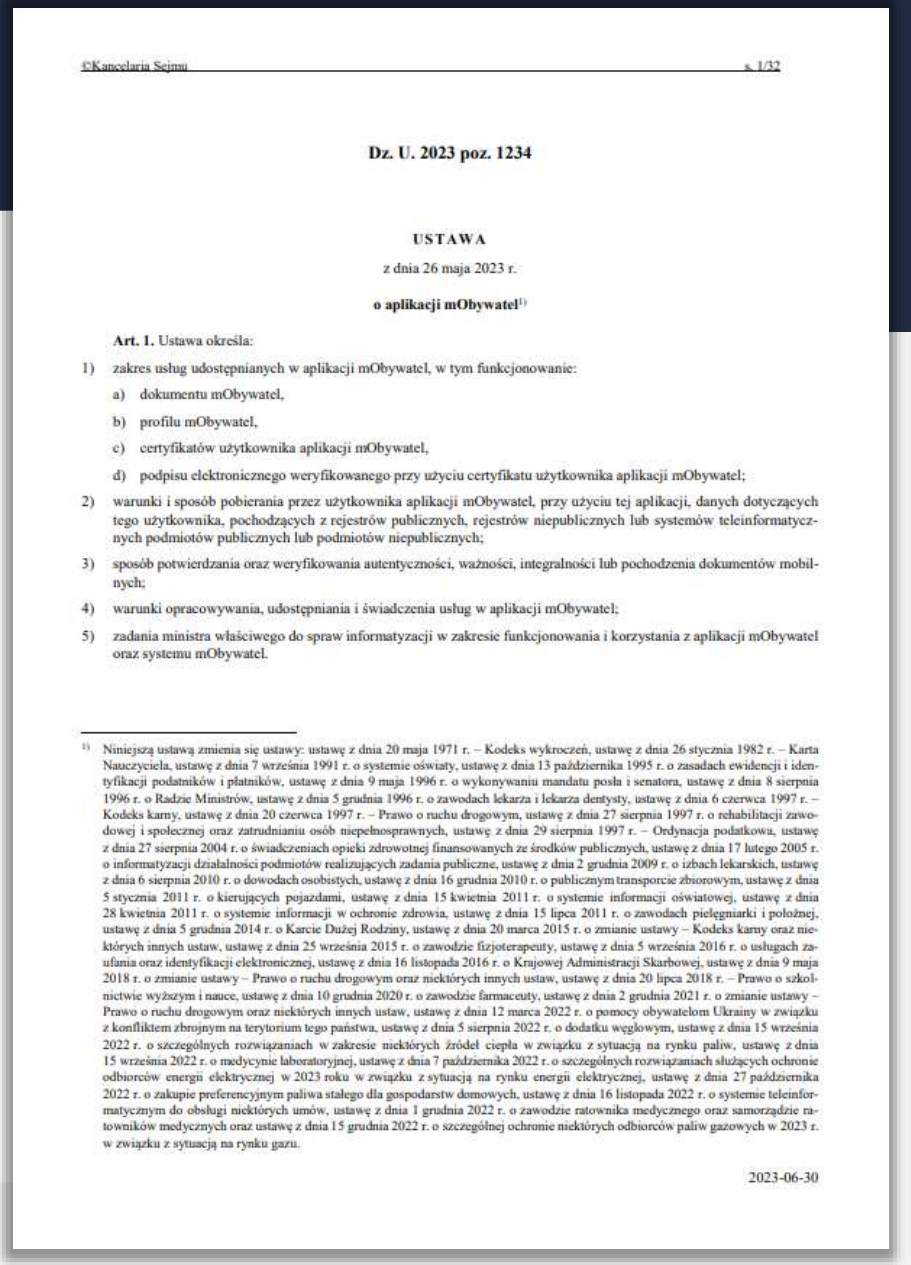
electronic **ID**entification, **A**uthentication and trust **S**ervices

- EU regulation regarding Digital ID
- Goals:
  - System unification across the EU states
  - Interoperability across the continent

Political background in Poland

The mCitizen application act

- The same legal framework as for the traditional Identity Card
- More than just ID card
- Introduction of legal sanctions



Dz. U. 2023 poz. 1234

USTAWA

z dnia 26 maja 2023 r.

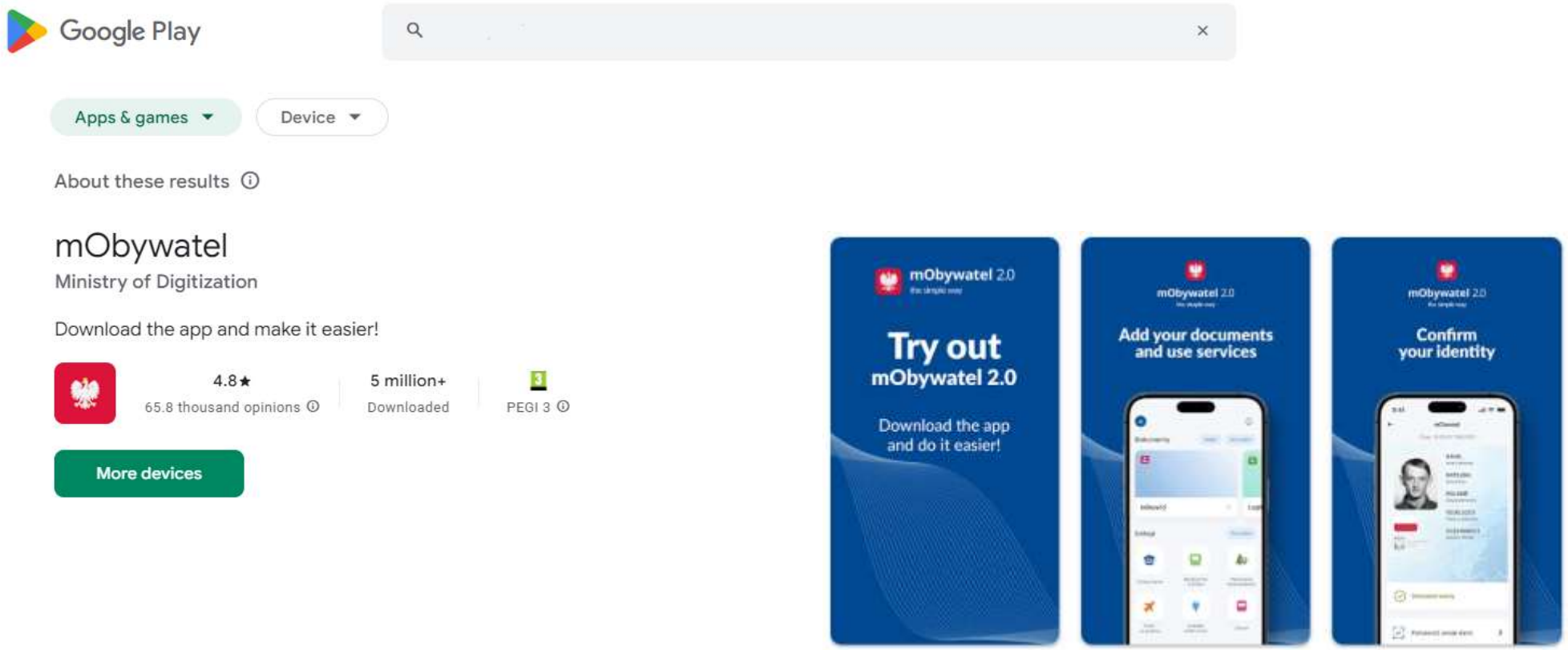
o aplikacji mObywatel[1)]

Art. 1. Ustawa określa:

1) zakres usług udostępnianych w aplikacji mObywatel, w tym funkcjonowanie:
   a) dokumentu mObywatel,
   b) profilu mObywatel,
   c) certyfikatów użytkownika aplikacji mObywatel,
   d) podpisu elektronicznego weryfikowanego przy użyciu certyfikatu użytkownika aplikacji mObywatel;
2) warunki i sposób pobierania przez użytkownika aplikacji mObywatel, przy użyciu tej aplikacji, danych dotyczących tego użytkownika, pochodzących z rejestrów publicznych, rejestrów niepublicznych lub systemów teleinformatycznych podmiotów publicznych lub podmiotów niepublicznych;
3) sposób potwierdzania oraz weryfikowania autentyczności, ważności, integralności lub pochodzenia dokumentów mobilnych;
4) warunki opracowywania, udostępniania i świadczenia usług w aplikacji mObywatel;
5) zadania ministra właściwego do spraw informatyzacji w zakresie funkcjonowania i korzystania z aplikacji mObywatel oraz systemu mObywatel.

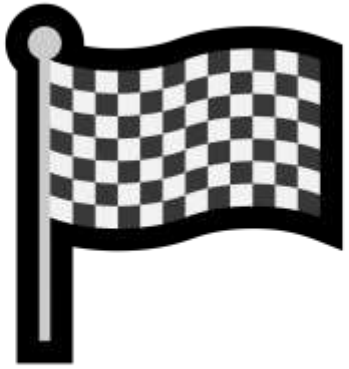
1) Niniejszą ustawą zmienia się ustawy: ustawę z dnia 20 maja 1971 r. – Kodeks wykroczeń, ustawę z dnia 26 stycznia 1982 r. – Karta Nauczyciela, ustawę z dnia 7 września 1991 r. o systemie oświaty, ustawę z dnia 13 października 1995 r. o zasadach ewidencji i identyfikacji podatników i płatników, ustawę z dnia 9 maja 1996 r. o wykonywaniu mandatu posła i senatora, ustawę z dnia 8 sierpnia 1996 r. o Radzie Ministrów, ustawę z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, ustawę z dnia 6 czerwca 1997 r. – Kodeks karny, ustawę z dnia 20 czerwca 1997 r. – Prawo o ruchu drogowym, ustawę z dnia 27 sierpnia 1997 r. o rehabilitacji zawodowej i społecznej oraz zatrudnianiu osób niepełnosprawnych, ustawę z dnia 29 sierpnia 1997 r. – Ordynacja podatkowa, ustawę z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych, ustawę z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne, ustawę z dnia 2 grudnia 2009 r. o izbach lekarskich, ustawę z dnia 6 sierpnia 2010 r. o dowodach osobistych, ustawę z dnia 16 grudnia 2010 r. o publicznym transporcie zbiorowym, ustawę z dnia 5 stycznia 2011 r. o kierujących pojazdami, ustawę z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej, ustawę z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, ustawę z dnia 15 lipca 2011 r. o zawodach pielęgniarki i położnej, ustawę z dnia 5 grudnia 2014 r. o Karcie Dużej Rodziny, ustawę z dnia 20 marca 2015 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, ustawę z dnia 25 września 2015 r. o zawodzie fizjoterapeuty, ustawę z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, ustawę z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej, ustawę z dnia 9 maja 2018 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw, ustawę z dnia 20 lipca 2018 r. – Prawo o szkolnictwie wyższym i nauce, ustawę z dnia 10 grudnia 2020 r. o zawodzie farmaceuty, ustawę z dnia 2 grudnia 2021 r. o zmianie ustawy – Prawo o ruchu drogowym oraz niektórych innych ustaw, ustawę z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa, ustawę z dnia 5 sierpnia 2022 r. o dodatku węglowym, ustawę z dnia 15 września 2022 r. o szczególnych rozwiązaniach w zakresie niektórych źródeł ciepła w związku z sytuacją na rynku paliw, ustawę z dnia 15 września 2022 r. o medycynie laboratoryjnej, ustawę z dnia 7 października 2022 r. o szczególnych rozwiązaniach służących ochronie odbiorców energii elektrycznej w 2023 roku w związku z sytuacją na rynku energii elektrycznej, ustawę z dnia 27 października 2022 r. o zakupie preferencyjnym paliwa stałego dla gospodarstw domowych, ustawę z dnia 16 listopada 2022 r. o systemie teleinformatycznym do obsługi niektórych umów, ustawę z dnia 1 grudnia 2022 r. o zawodzie ratownika medycznego oraz samorządzie ratowników medycznych oraz ustawę z dnia 15 grudnia 2022 r. o szczególnej ochronie niektórych odbiorców paliw gazowych w 2023 r. w związku z sytuacją na rynku gazu.

Research scope



Practical part 

2 main processes



Onboarding process

Verification process

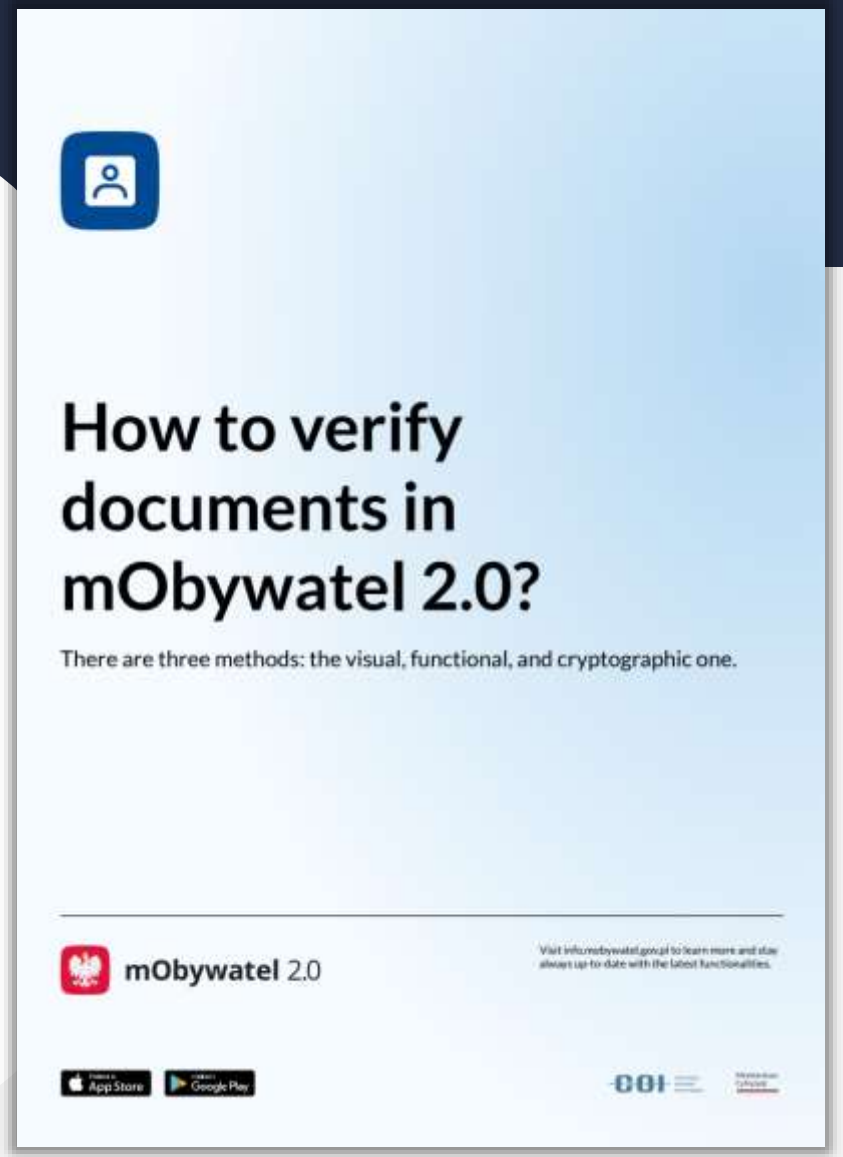
2 main processes

Verification process

Digital ID verification

Three verification methods

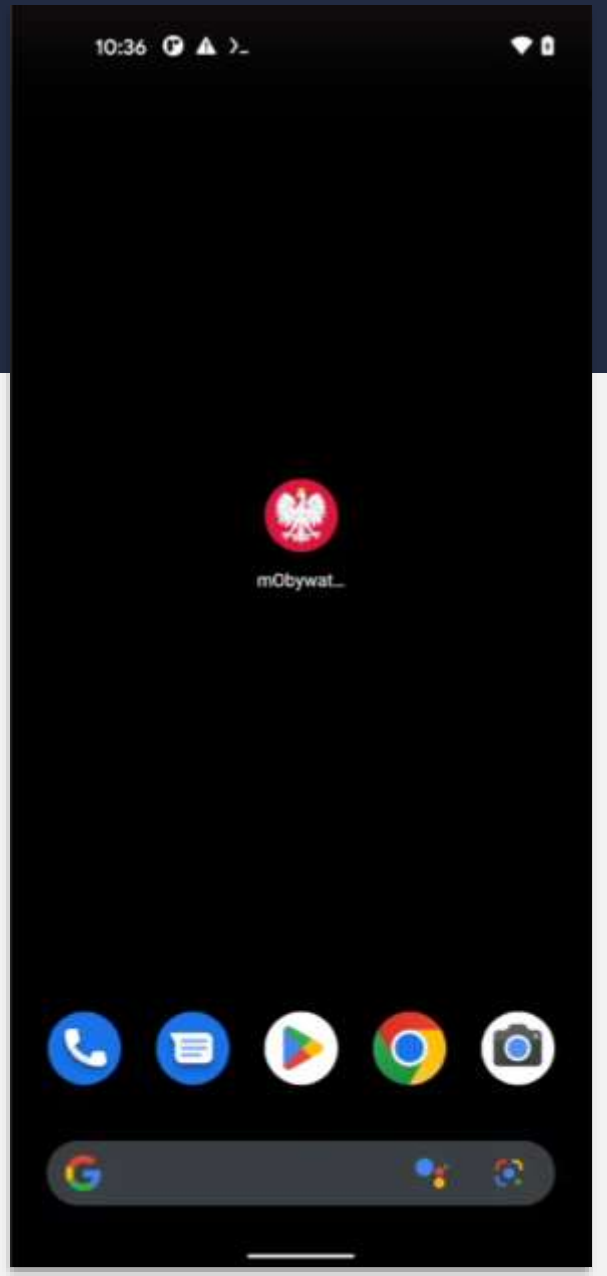
1. Visual verification
2. Functional verification
3. Cryptographical verification



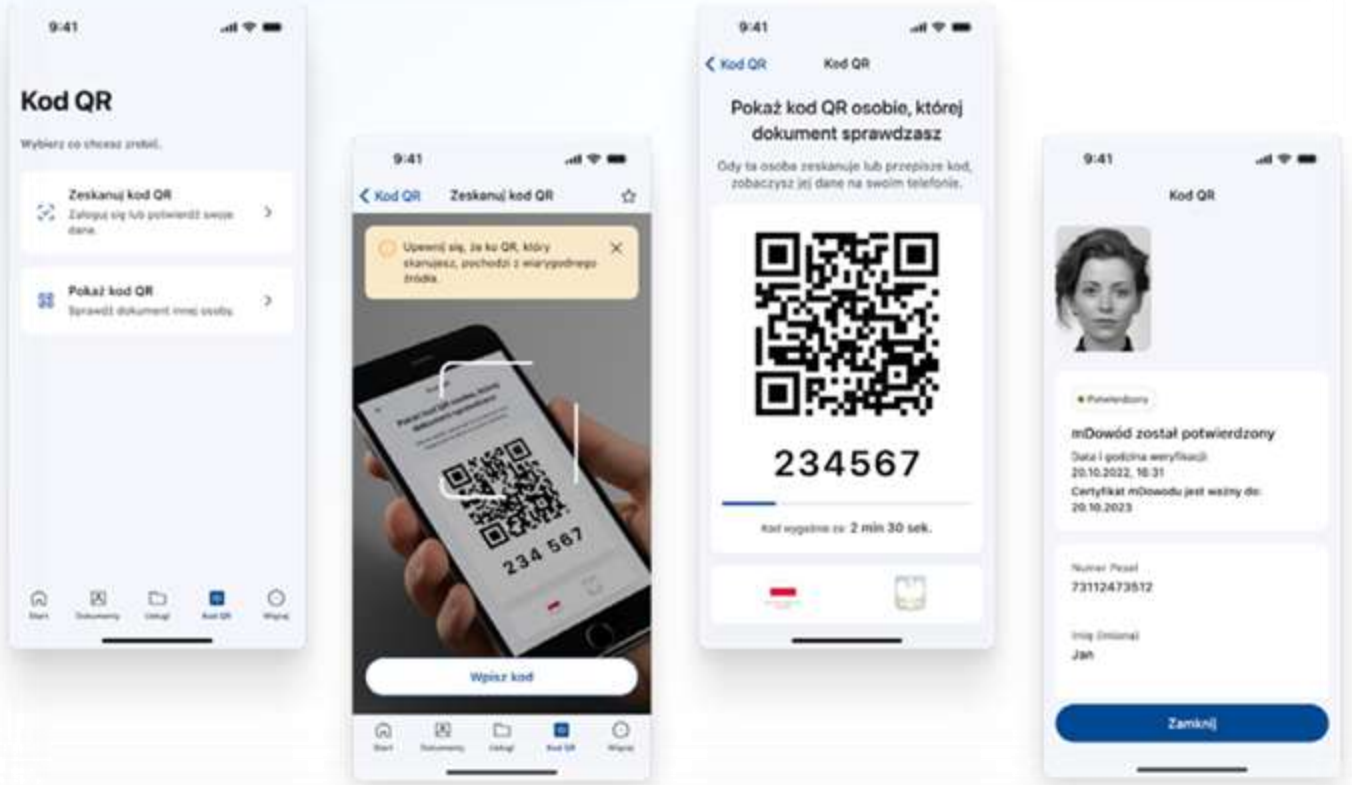
Visual verification

Functional verification

- Logging out and logging in back
- Performing an unrelated action within the app



Cryptographic verification



In reality...

Almost nobody uses the cryptographical verification

1. Visual verification
2. Functional verification
3. Cryptographical verification

To visualize the problem...

Let's imagine 4 different organizations:

 Clinic

 Airline

 Telecom company

 Bank

What are the risks associated with lack of proper ID verification?

Clinic

😈 Stealing medical records

Airline

😈 Fugitive fleeing the country

Telecom

😈 SIM-swapping attack

Bank

😈 Money theft

 Clinic

 Airline

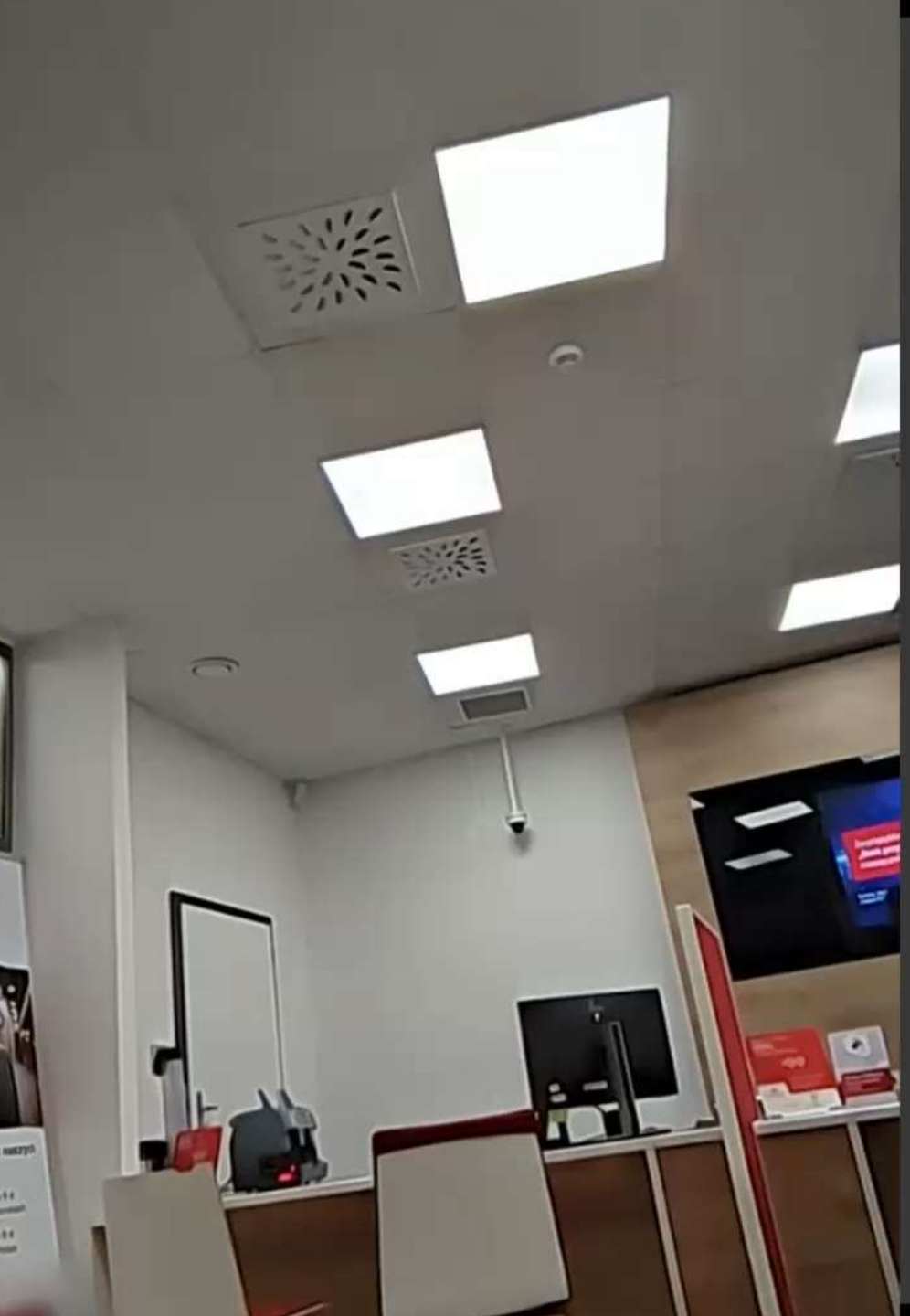
Which of these use the strongest verification method?

 Telecom

 Bank


rejestracja główna A
witamy


Światłowód



✗ Clinic

✗ Airline

Which of these use the strongest verification method?

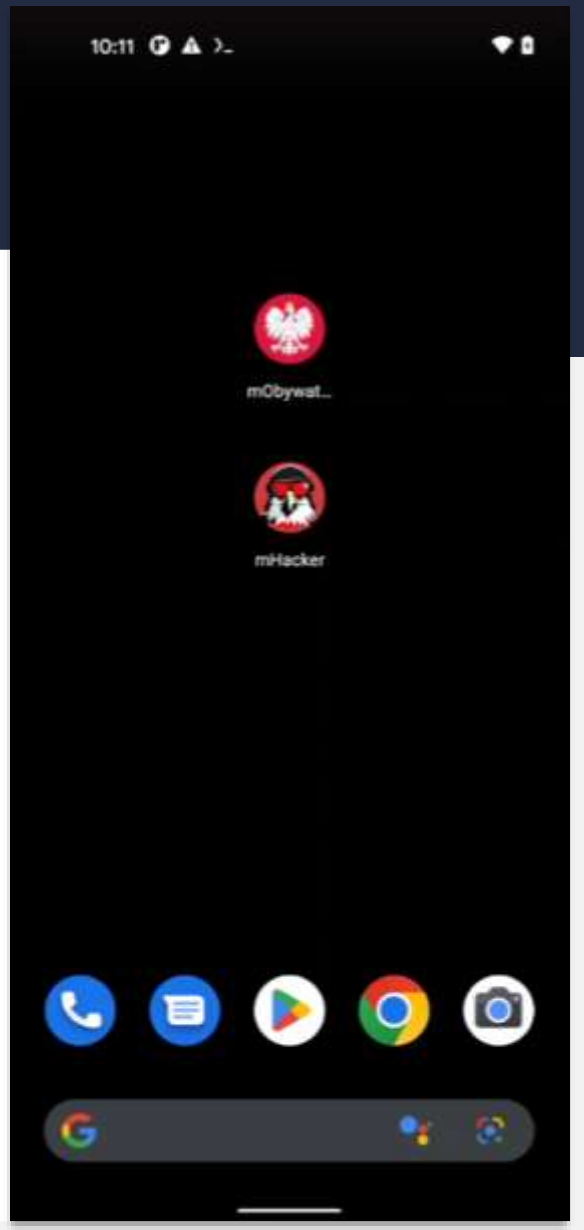
✗ Telecom

✓ Bank

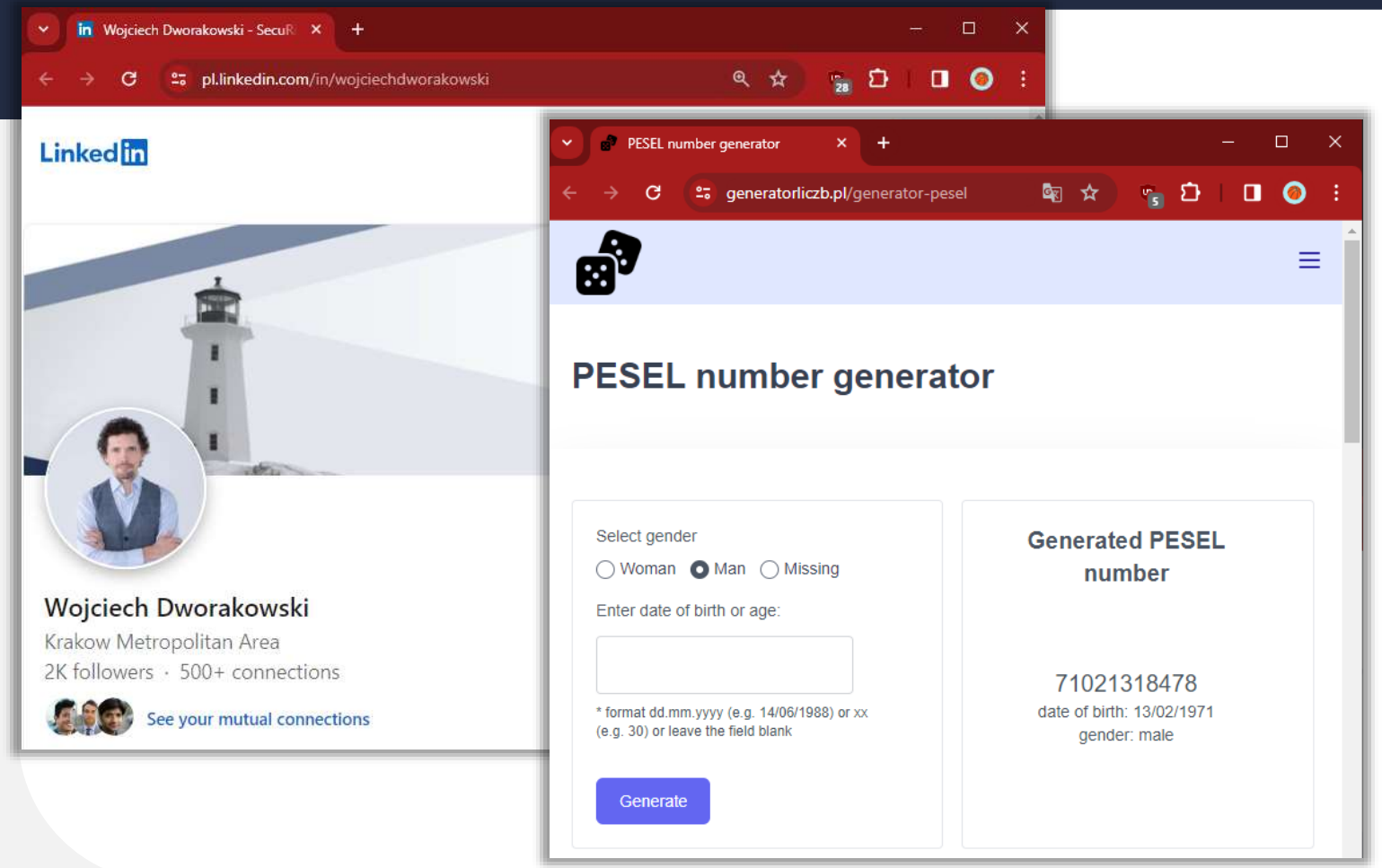
mHacker

Tool for injecting your own data into the mCitizen app

- Name
- Surname
- Social Security Number
- Birthdate
- Photo



This could be you!



RedTeam Op + mHacker + Linkedin = 💔

LinkedIn

+

100%

SUCCESS RATE

Almost the same thing as Fake ID...

Similarities:

- Both are illegal 👮

Differences:

- Arbitraty data change
- Faked in a matter of seconds
- Infinitely scalable
- Free to use

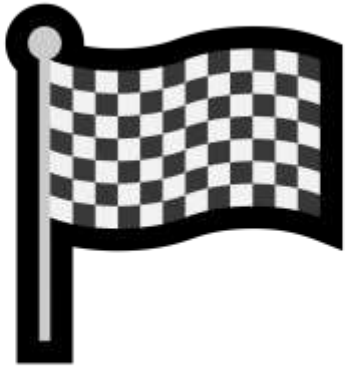
mHacker vs mCitizen

Three verification methods

1. Visual verification ✅
2. Functional verification ✅
3. Cryptographical verification ❌

Technical part 

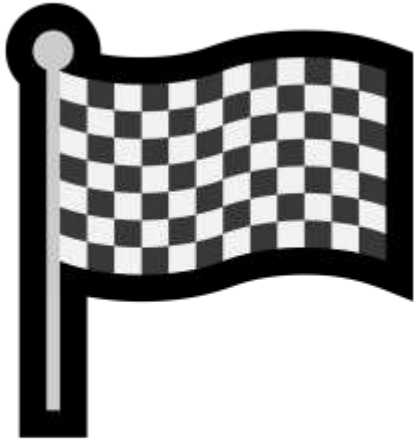
2 main processes



Onboarding process

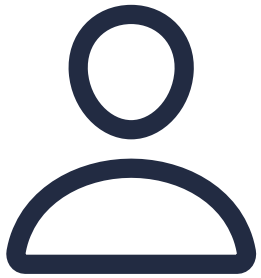
Verification process

2 main processes



Onboarding process

Onboarding

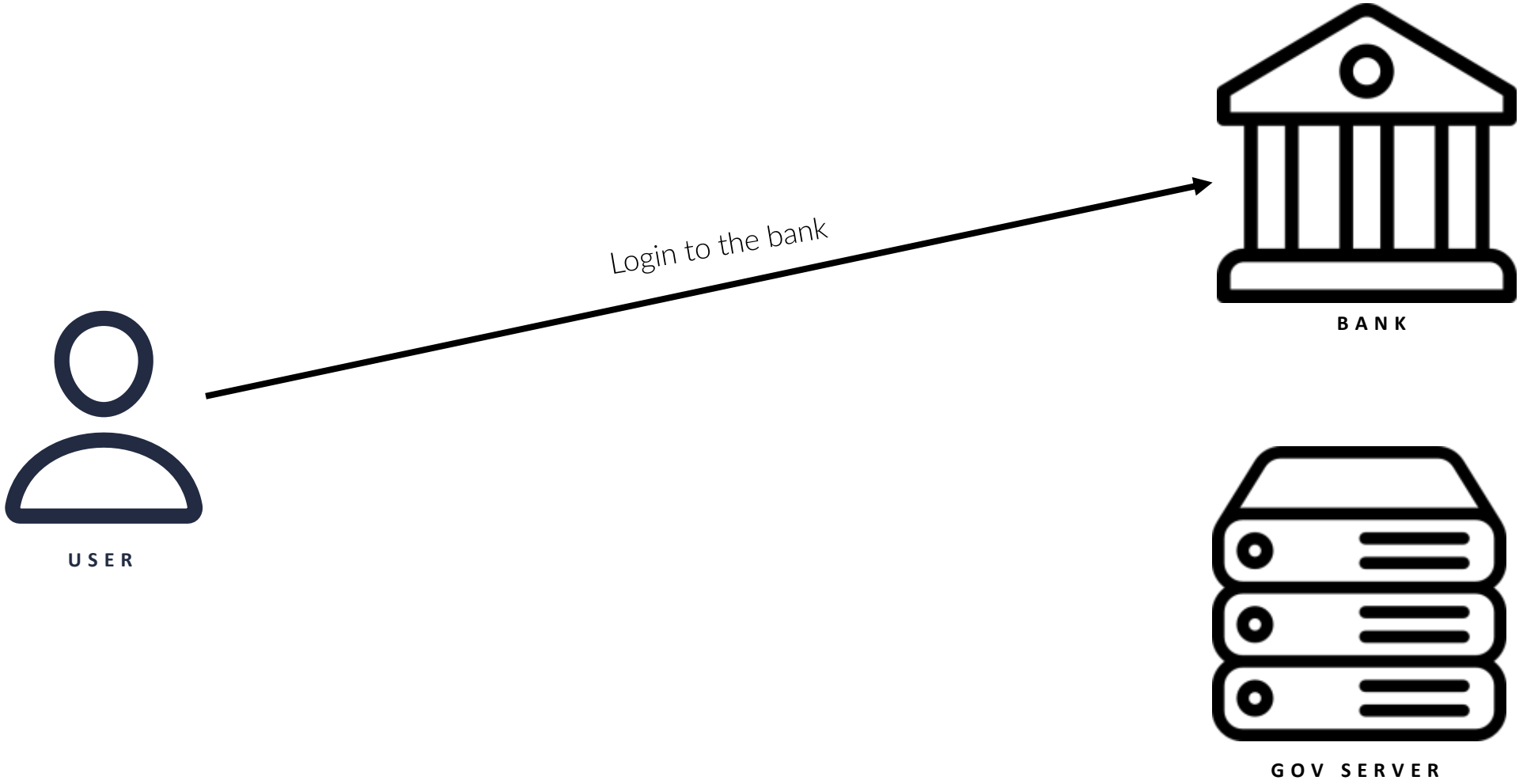


USER

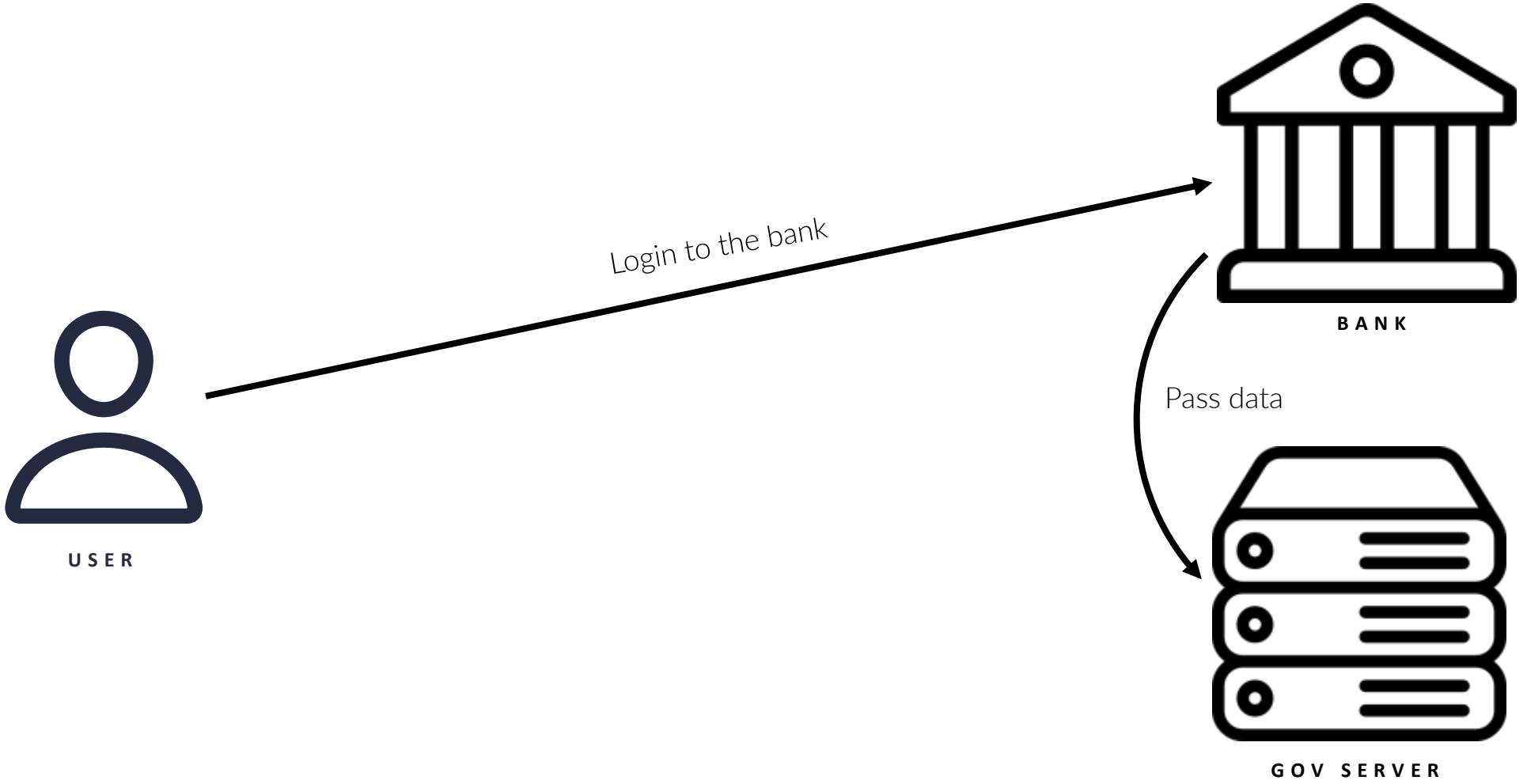
BANK

GOV SERVER

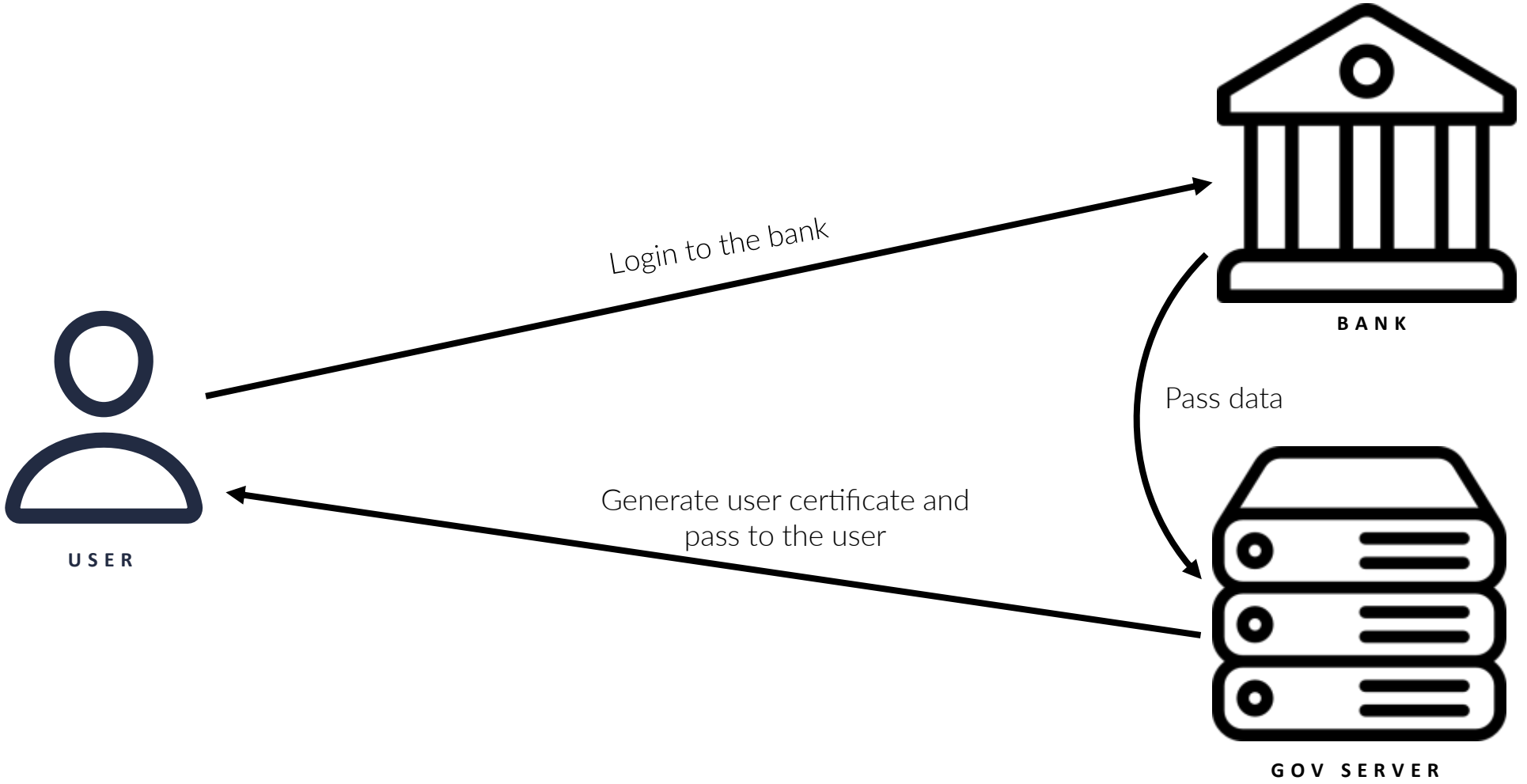
Onboarding



Onboarding

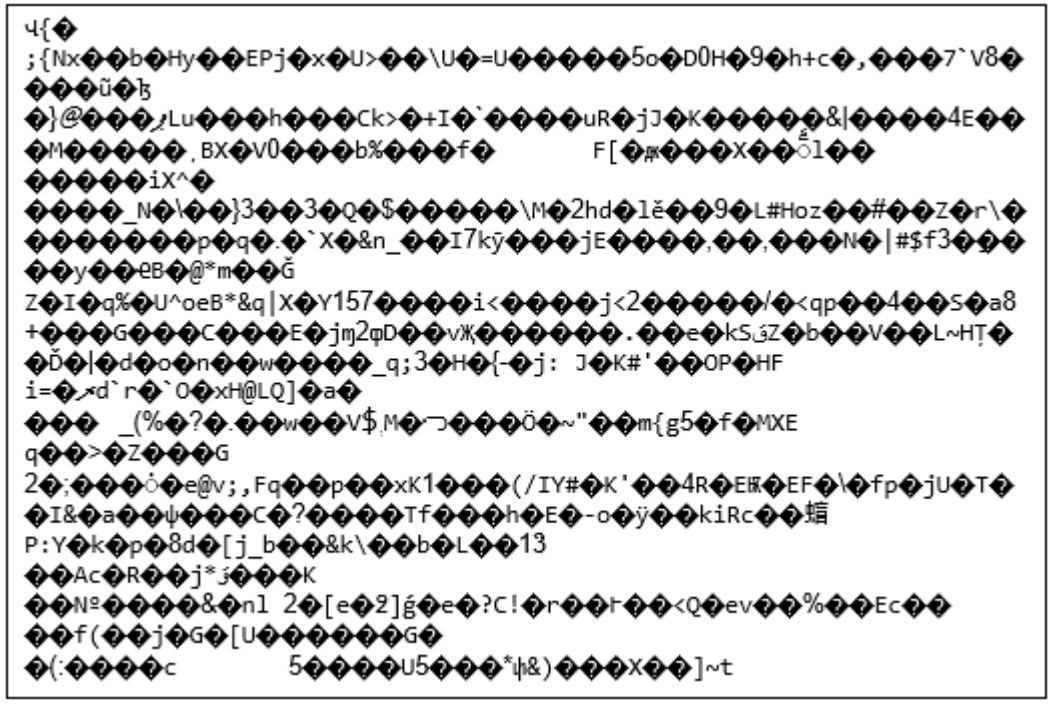


Onboarding

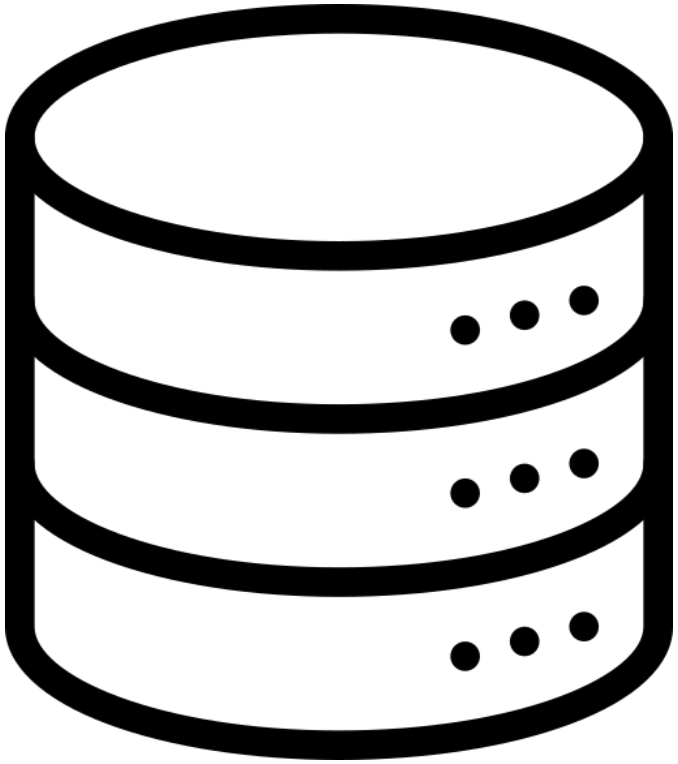

Login to the bank
BANK
Pass data
Generate user certificate and
pass to the user
USER
GOV SERVER

Onboarding

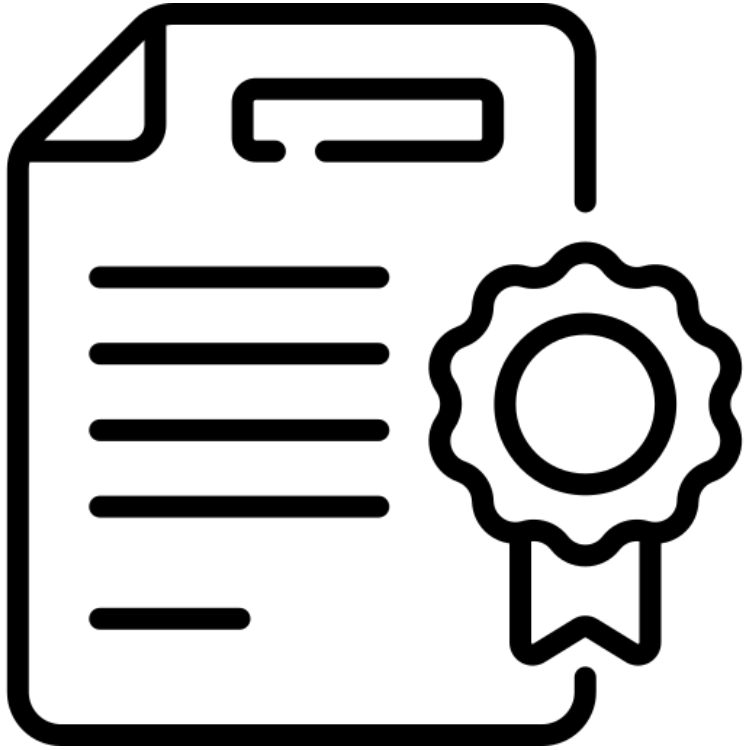
After onboarding, your encrypted digital ID is saved in your phone's internal storage.



What’s mCitizen under the hood?



Govt signed „container”



Personal certificate

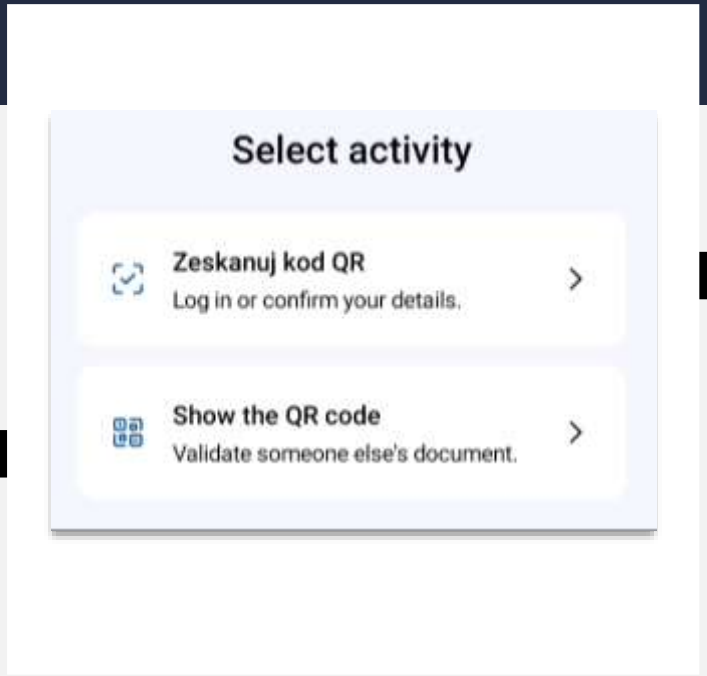

```
{
    "header": {
        "pesel": "90102631622", "internalDocumentId": "097...0f1", "version": "1",
        "documentType": "MOBILE_ID_CARD", "documentSubtype": null, "documentVersion": 1,
        "certificateSubjectDn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
        "certificateSerialNumber": "286...6b5", "certificateIssuerDn": "CN=MTMid 3,O=Kancelaria Prezesa Rady MinistrÃ³w,C=PL",
        "creationTimestamp": "2023-08-24T06:07:38.261890Z", "documentIssuer": "Kancelaria Prezesa Rady MinistrÃ³w"
    },
    "dh": {
        "tp": 8, "stp": 1, "ver": 1,
        "dn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
        "sn": "286...6b5", "isr": "CN=MTMid 3,O=Kancelaria Prezesa Rady MinistrÃ³w,C=PL",
        "ts": "20230824080738261", "rId": "d22952e6b5ba45bc8c3881fb326eb298",
        "iid": "097...0f1", "pe": "90102631622", "in": null,
        "id": "Kancelaria Prezesa Rady MinistrÃ³w"
    },
    "data": {
        "mobileIdCard": {
            "number": "DACK78741",
            "validFrom": "2023-07-15 T12:10:52.369188Z",
            "validTo": "2028-07-15T12:10:52.369188Z"
        },
        "personalData": {
            "name": "ADAM",
            "secondName": null,
            "surname": "NOWAK",
            "fatherName": "JAN",
            "motherName": "WERONIKA",
            "pesel": "90102631622",
            "birthDate": "1998-02-25",
            "citizenship": "POLSKIE",
            "picture": "/9j/4AAQSkZJRgABAQAAAQABAAD/2AQEBAQ[...]CgAoAKACgKAP/9k="
        }
    },
    "picture": null
}
```

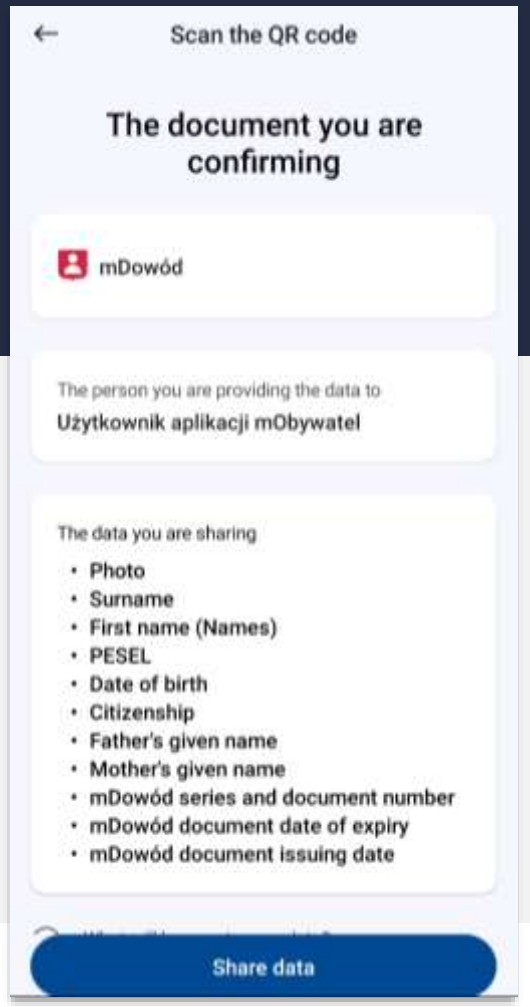
Observations

- Personal container is signed by GOV.
- Process requires access to trusted 3rd party.
- 3rd party communicating directly with GOV's servers.

2 main processes

Verification process

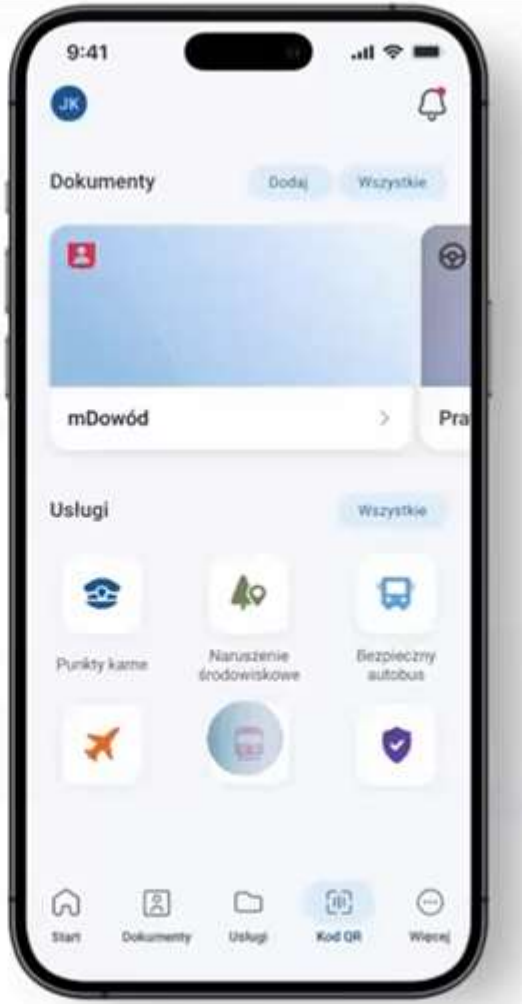




Person Verifying

Person being verified

Verifier's phone



Your phone

What information does the QR code store?

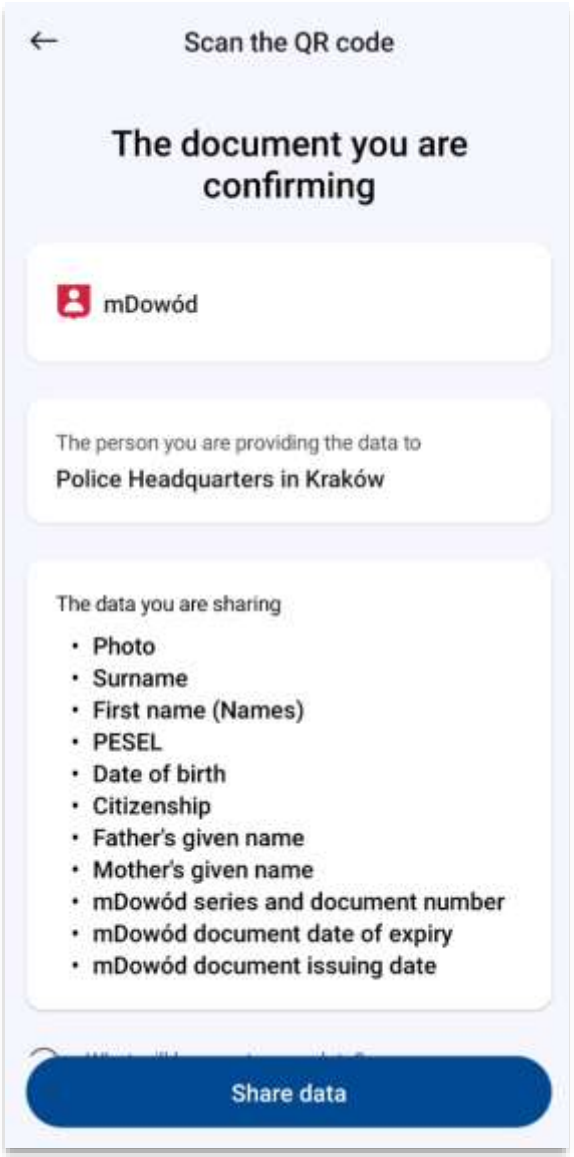
Document type	25
QR code type	D
ID	C086[...]2a2d
Creation date	16.09.2023 13:37:00
Expiry date	16.09.2023 13:40:00
Creator name	SZYMON CHADAM

What information does the QR code store?

Document type	25
QR code type	D
ID	C086[...]2a2d
Creation date	16.09.2023 13:37:00
Expiry date	16.09.2023 13:40:00
Creator name	**SZYMON CHADAM**

Can you change that data?

Creator Name
Police Headquarters in Krakow


Scan the QR code
The document you are confirming
mDowód
The person you are providing the data to
Police Headquarters in Kraków
The data you are sharing
Photo
Surname
First name (Names)
PESEL
Date of birth
Citizenship
Father's given name
Mother's given name
mDowód series and document number
mDowód document date of expiry
mDowód document issuing date
Share data

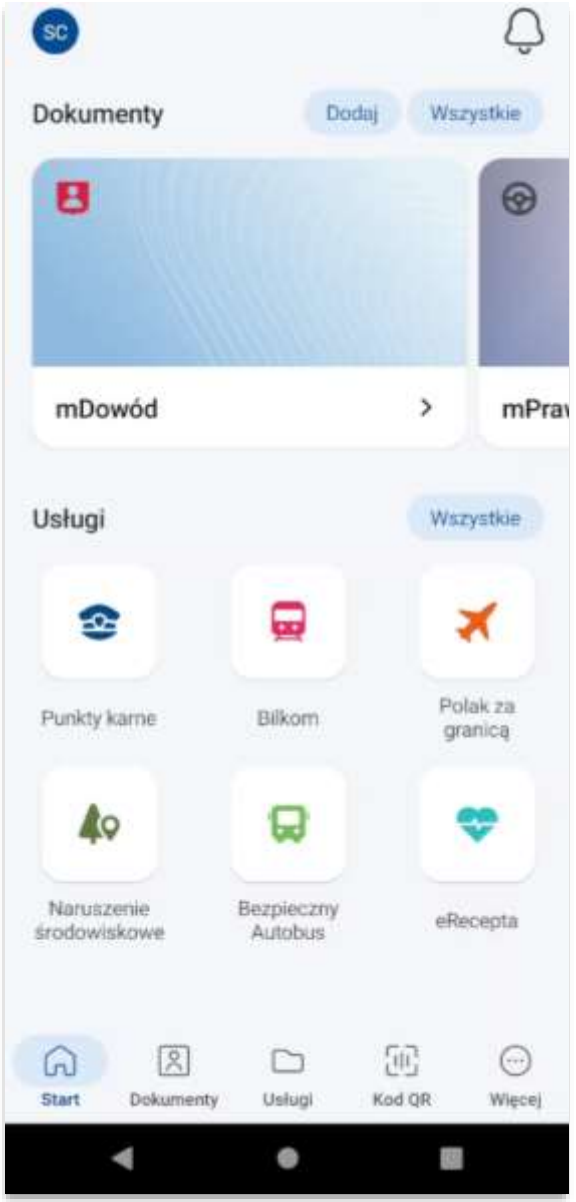
Creator Name

Orlen Investments S.A

The data you are sharing:

- Name and Surname
- Bank account number

After successful verification, your bank account will be credited with PLN 100,000
\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n\n


SC
Dokumenty
Dodaj
Wszystkie
mDowód
mPrav
Usługi
Wszystkie
Punkty karne
Bilkom
Polak za granicą
Naruszenie środowiskowe
Bezpieczny Autobus
eRecepta
Start
Dokumenty
Usługi
Kod QR
Więcej

We want more 🍽️

- Good phishing vector, but that's not enough
- Still blocked by cryptography
- Next goal:
  - Verifying identity using someone's data
  - Defeating cryptographic verification 🥊

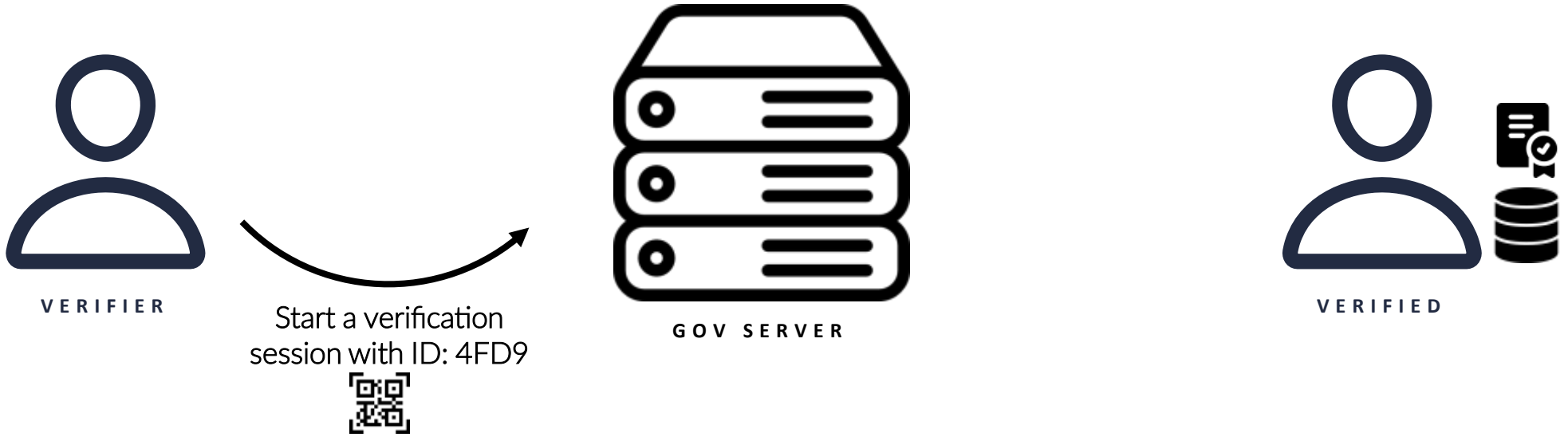
User verification process

VERIFIER

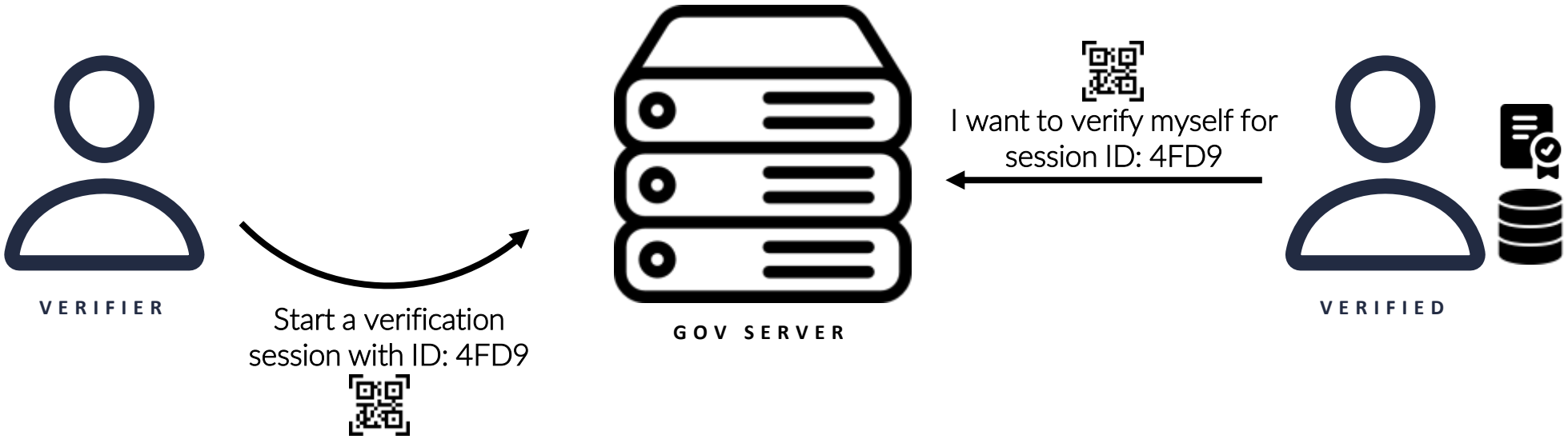
GOV SERVER

VERIFIED

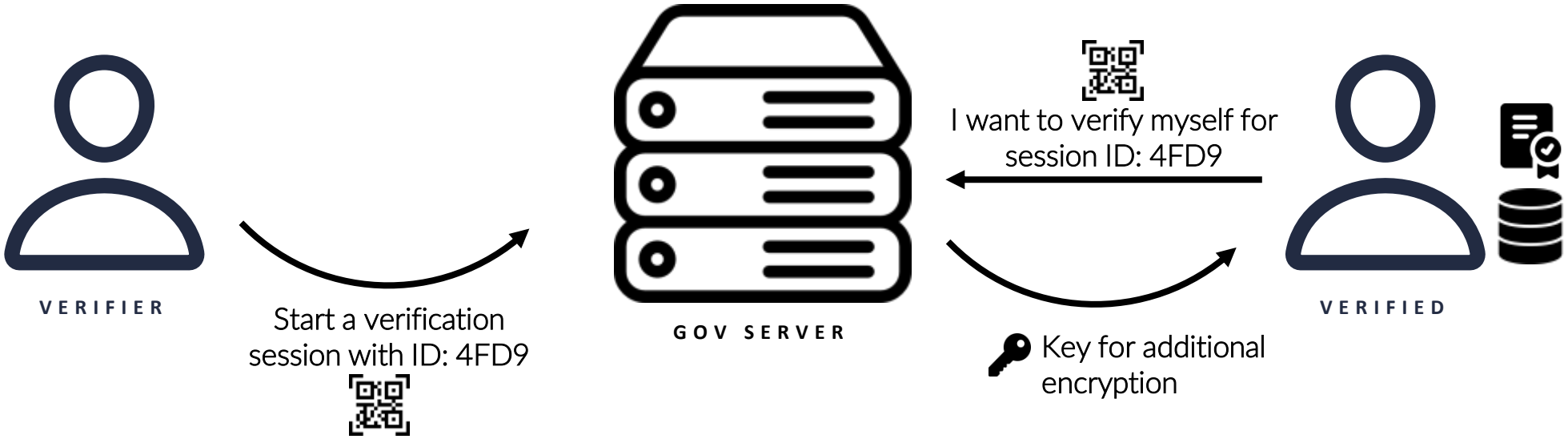
User verification process



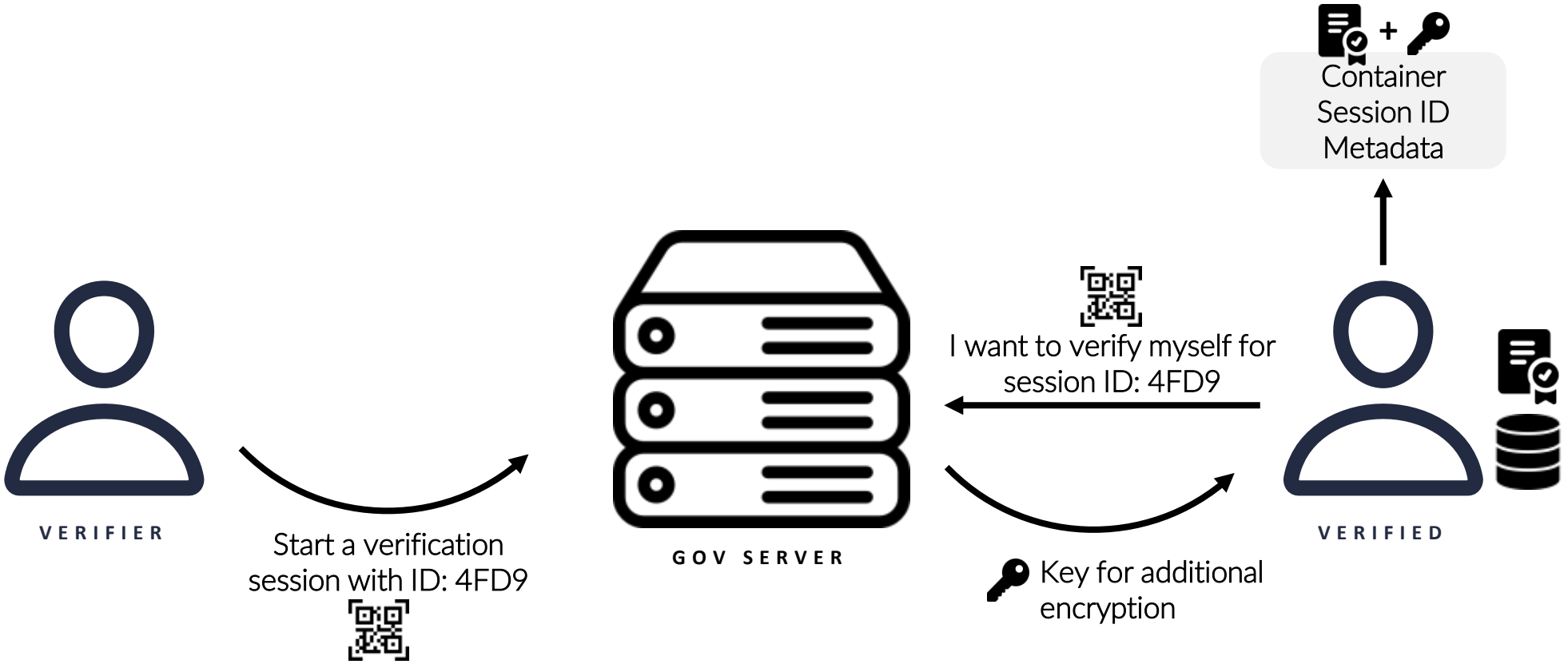
User verification process



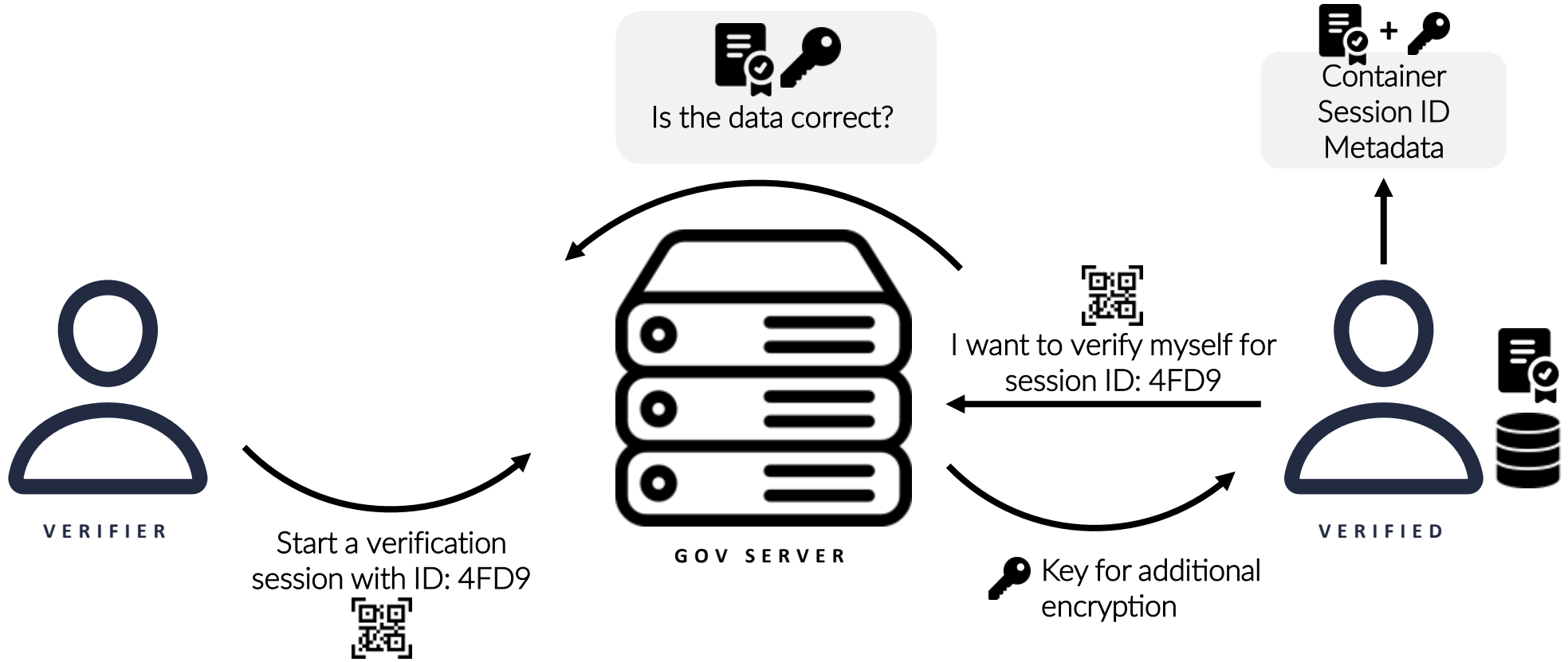
User verification process



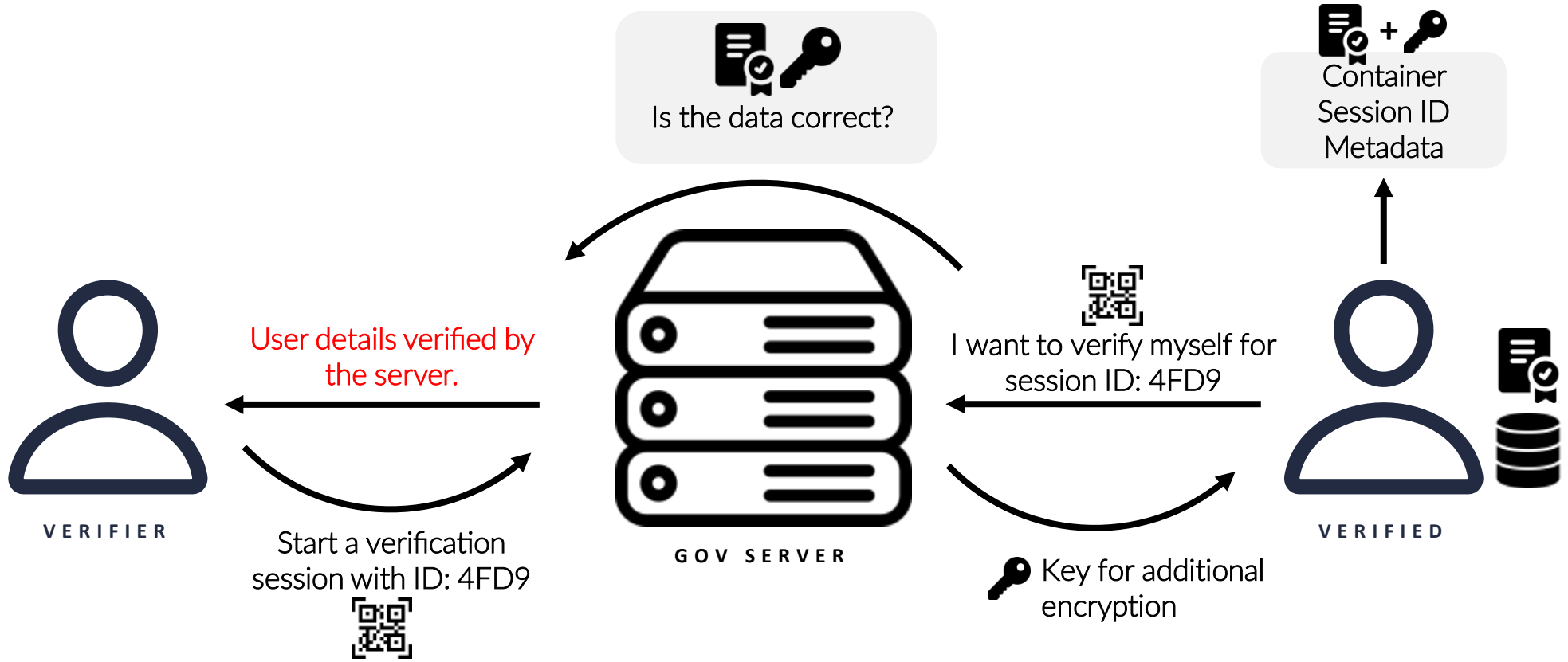
User verification process



User verification process



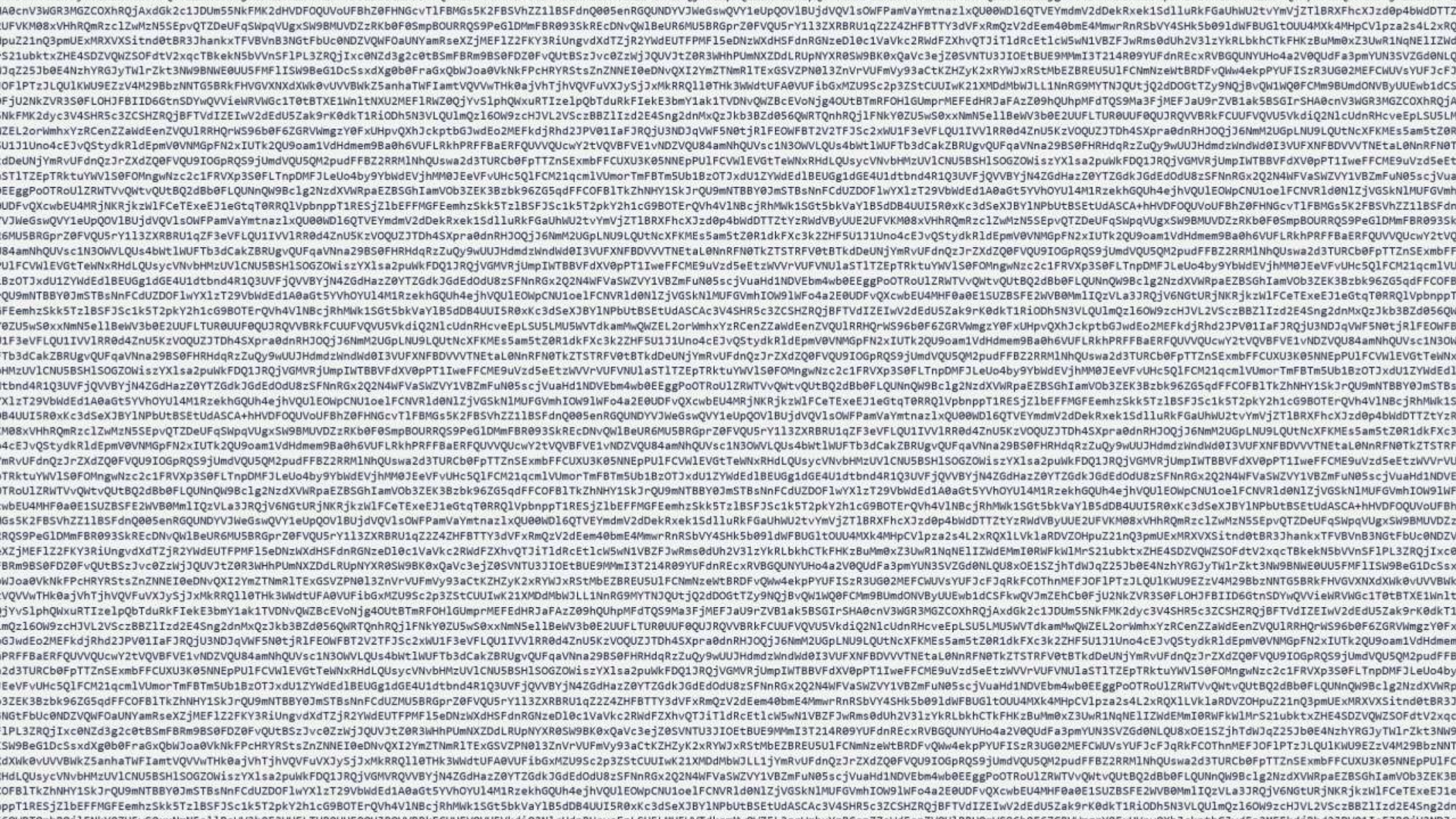
User verification process



What’s the result of verification?

- Verifier gets a confirmation on his device.
- What data is received „**under the hood**”?
  - What information does the verifier receive?

Verifier



```
{
    "header": {
        "pesel": "00789167876",
        "internalDocumentId": "534f[...]f2be",
        "version": "1",
        "documentType": "MOBILE_ID_CARD",
        "documentSubtype": null,
        "documentVersion": 1,
        "certificateSubjectDn": "GIVENNAME=ADAM JAN,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-0
        "certificateSerialNumber": "c52a4[...]1d13",
        "certificateIssuerDn": "CN=MTMid 3,O=Kancelaria Prezesa Rady Ministrow,C=PL",
        "creationTimestamp": "2023-08-23T14:10:06.960132Z",
        "documentIssuer": "Kancelaria Prezesa Rady Ministrów"
    },
    "dh": {
        "tp": 8,
        "stp": 1,
        "ver": 1,
        "dn": "GIVENNAME=ADAM JAN,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-00789167876,CN=A
        "sn": "c52a4[...]1d13",
        "isr": "CN=MTMid 3,O=Kancelaria Prezesa Rady Ministrow,C=PL",
        "ts": "202[...]0",
        "rId": "551a[...]502",
        "iid": "534f[...]1be",
        "pe": "00789167876",
        "in": null,
        "id": "Kancelaria Prezesa Rady Ministrów"
    },
    "data": {
        "mobileIdCard": {
            "number": "FARP62793",
            "validFrom": "2023-08-23",
            "validTo": "2028-08-23"
        },
        "personalData": {
            "name": "ADAM",
            "secondName": "JAN",
            "surname": "NOWAK",
            "fatherName": "PIOTR",
            "motherName": "ANNA",
            "pesel": "00789167876",
            "birthDate": "2000-09-12",
            "citizenship": "POLSKIE",
```


Looking similar?

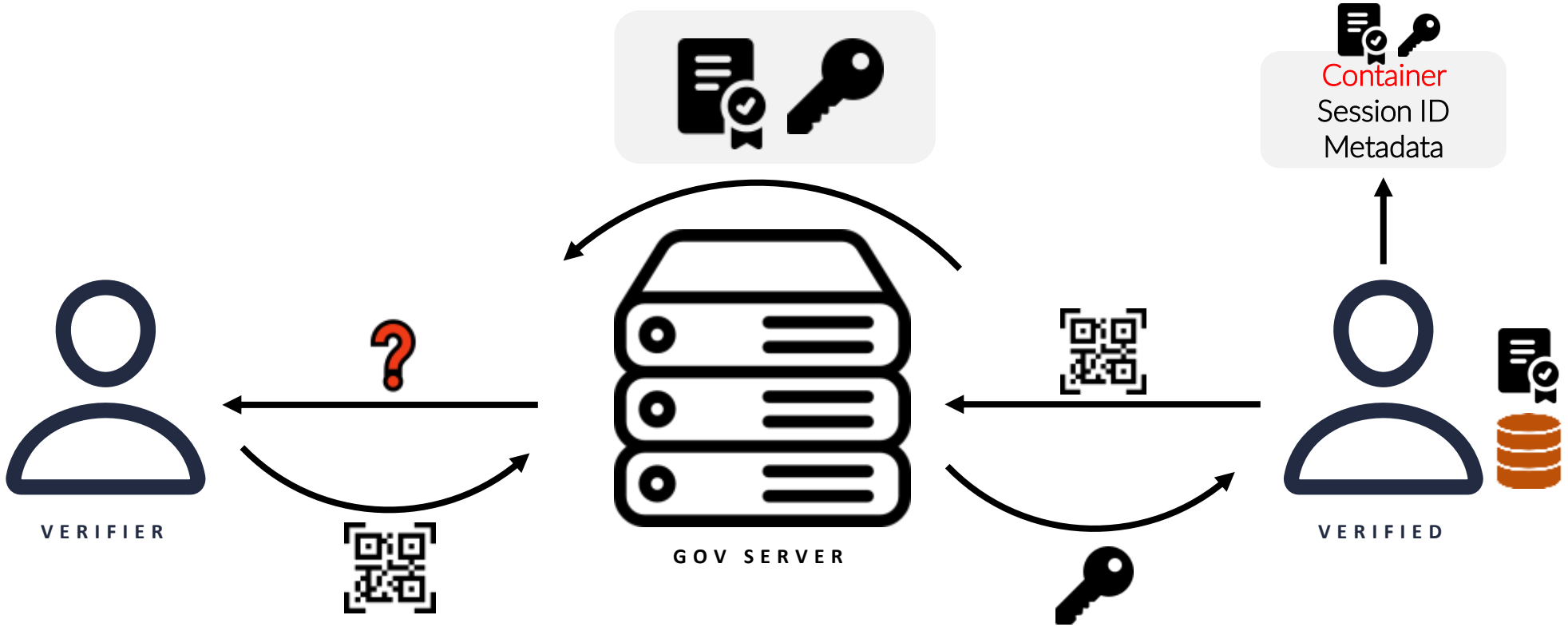

```
{
    "header": {
        "pesel": "90102631622", "internalDocumentId": "097...0f1", "version": "1",
        "documentType": "MOBILE_ID_CARD", "documentSubtype": null, "documentVersion": 1,
        "certificateSubjectDn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
        "certificateSerialNumber": "286...6b5", "certificateIssuerDn": "CN=MTMid 3,O=Kancelaria Prezesa Rady MinistrÃ³w,C=PL",
        "creationTimestamp": "2023-08-24T06:07:38.261890Z", "documentIssuer": "Kancelaria Prezesa Rady MinistrÃ³w"
    },
    "dh": {
        "tp": 8, "stp": 1, "ver": 1,
        "dn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
        "sn": "286...6b5", "isr": "CN=MTMid 3,O=Kancelaria Prezesa Rady MinistrÃ³w,C=PL",
        "ts": "20230824080738261", "rId": "d22952e6b5ba45bc8c3881fb326eb298",
        "iid": "097...0f1", "pe": "90102631622", "in": null,
        "id": "Kancelaria Prezesa Rady MinistrÃ³w"
    },
    "data": {
        "mobileIdCard": {
            "number": "DACK78741",
            "validFrom": "2023-07-15 T12:10:52.369188Z",
            "validTo": "2028-07-15T12:10:52.369188Z"
        },
        "personalData": {
            "name": "ADAM",
            "secondName": null,
            "surname": "NOWAK",
            "fatherName": "JAN",
            "motherName": "WERONIKA",
            "pesel": "90102631622",
            "birthDate": "1998-02-25",
            "citizenship": "POLSKIE",
            "picture": "/9j/4AAQSkZJRgABAQAAAQABAAD/2AQEBAQ[...]CgAoAKACgKAP/9k="
        }
    },
    "picture": null
}
```

```
{
    "header": {
        "pesel": "00789167876",
        "internalDocumentId": "534f[...]f2be",
        "version": "1",
        "documentType": "MOBILE_ID_CARD",
        "documentSubtype": null,
        "documentVersion": 1,
        "certificateSubjectDn": "GIVENNAME=ADAM JAN,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-0
        "certificateSerialNumber": "c52a4[...]1d13",
        "certificateIssuerDn": "CN=MTMid 3,O=Kancelaria Prezesa Rady Ministrow,C=PL",
        "creationTimestamp": "2023-08-23T14:10:06.960132Z",
        "documentIssuer": "Kancelaria Prezesa Rady Ministrów"
    },
    "dh": {
        "tp": 8,
        "stp": 1,
        "ver": 1,
        "dn": "GIVENNAME=ADAM JAN,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-00789167876,CN=A
        "sn": "c52a4[...]1d13",
        "isr": "CN=MTMid 3,O=Kancelaria Prezesa Rady Ministrow,C=PL",
        "ts": "202[...]0",
        "rId": "551a[...]502",
        "iid": "534f[...]1be",
        "pe": "00789167876",
        "in": null,
        "id": "Kancelaria Prezesa Rady Ministrów"
    },
    "data": {
        "mobileIdCard": {
            "number": "FARP62793",
            "validFrom": "2023-08-23",
            "validTo": "2028-08-23"
        },
        "personalData": {
            "name": "ADAM",
            "secondName": "JAN",
            "surname": "NOWAK",
            "fatherName": "PIOTR",
            "motherName": "ANNA",
            "pesel": "00789167876",
            "birthDate": "2000-09-12",
            "citizenship": "POLSKIE",
```


The verifier receives a full mCitizen ID container copy of the person being verified

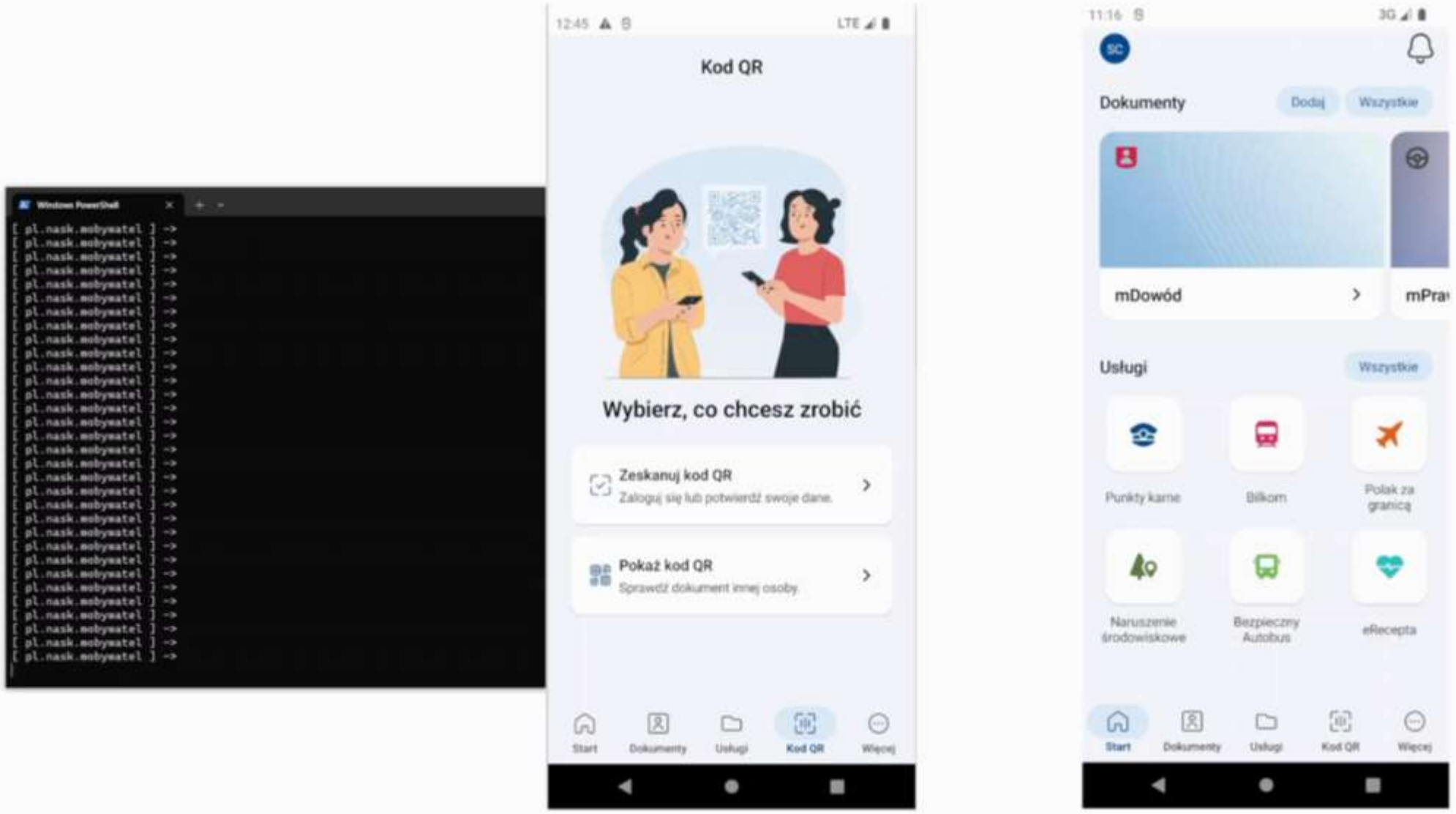
GOV signature included

Is it that simple?



Complete attack scenario

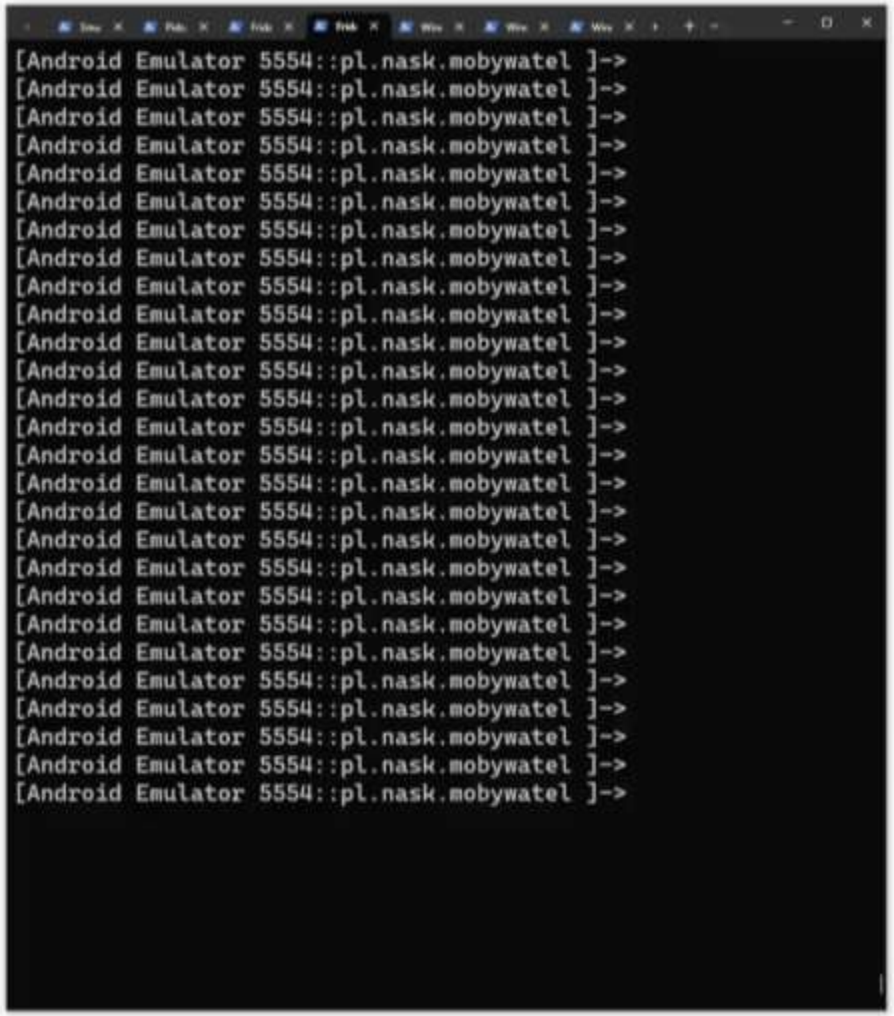
1. Generate phishing QR code
2. Lure victim into veryfing his data
3. Inject his/her data into your application process
4. Successfuly verify (not) your data 🙃



Attacker

Victim

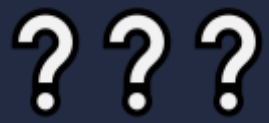
3rd party verifier



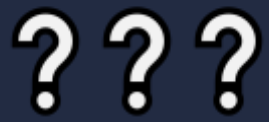
Attacker

It works!🏆🏆🏆

- Server-side logic vulnerability during verification
  - Works both on Android and iOS
- Excessive information exposure
- Container of *person A* signed with certificate of *person B*
- Attack invisble to the victim
- Collect now, scam later 🙃

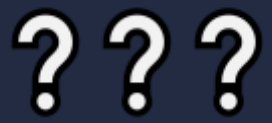


How long is the captured mCitizen ID valid for?

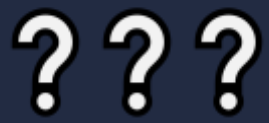


How long is the captured mCitizen ID valid for?

5 years

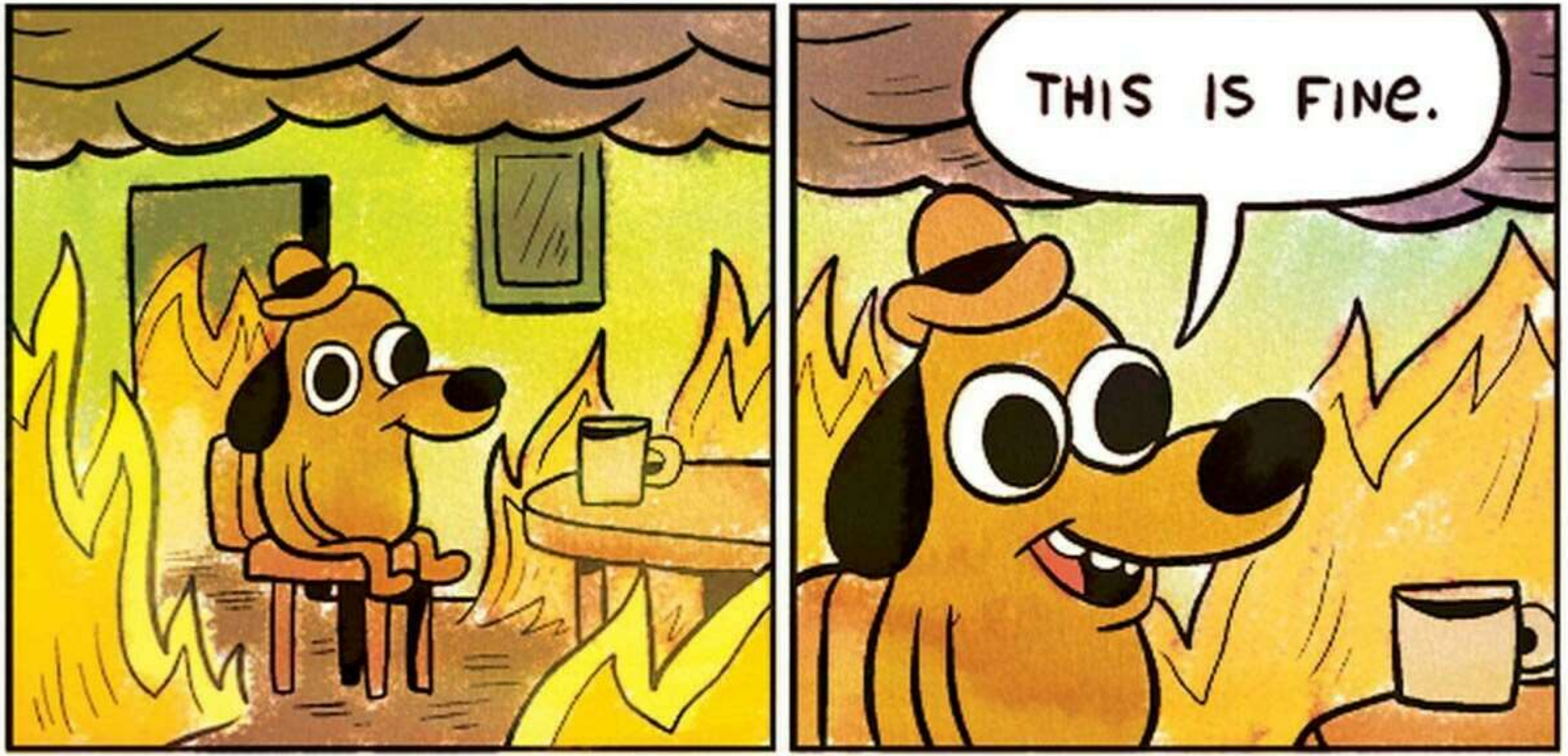


“I've shared my mCitizen ID with someone. What can I do to protect myself?”



“I've shared my mCitizen ID with someone.
What can I do to protect myself?”

Nothing


THIS IS FINE.

Timeline 

21st August 2023 – started testing

23rd August 2023 – vulnerability discovery

24th August 2023 – notified CERT NASK

25th August 2023 – notified CSIRT MON

28th August 2023 – direct contact with GOV's security department

Timeline 

21st August 2023 – started testing

23rd August 2023 – vulnerability discovery

24th August 2023 – notified CERT NASK

25th August 2023 – notified CSIRT MON

28th August 2023 – direct contact with GOV's security department

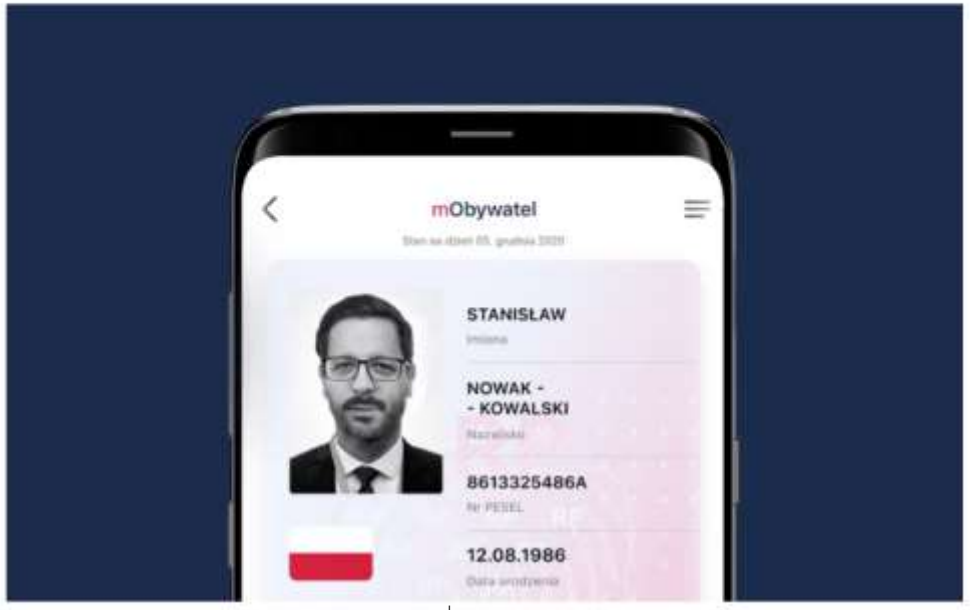
1st September 2023 – mCitizen in banks 

D-Day ⏰

/ Law / Law for you / IN COURT AND IN THE OFFICE

mCitizen 2.0. From Friday you can go to the bank without a plastic ID card

On Friday, September 1, the obligation for banks to respect mID in the mObywatel application was introduced.



rp.pl

Timeline 

21st August 2023 – started testing

23rd August 2023 – vulnerability discovery

24th August 2023 – notified CERT NASK

25th August 2023 – notified CSIRT MON

28th August 2023 – direct contact with GOV's security department

1st September 2023 – mCitizen in banks 

5th October 2023 – information from CERT about implemented fixes

GOV’s reaction 👨‍💻

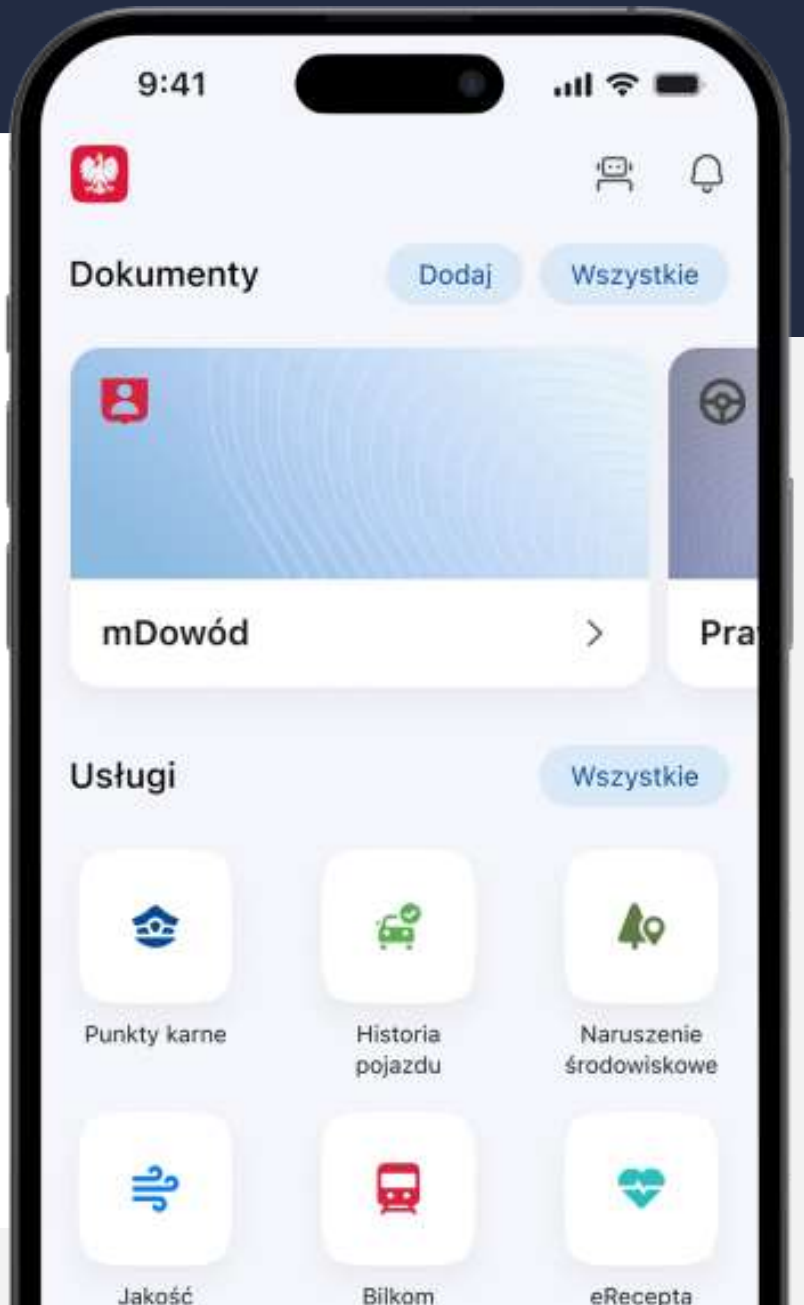
- Almost instantaneous reaction
- Direct meeting with the team
- Initial fix much sooner than the CERT’s information
- Listed a job offer for a pentester 😉

centralny ośrodek informatyki

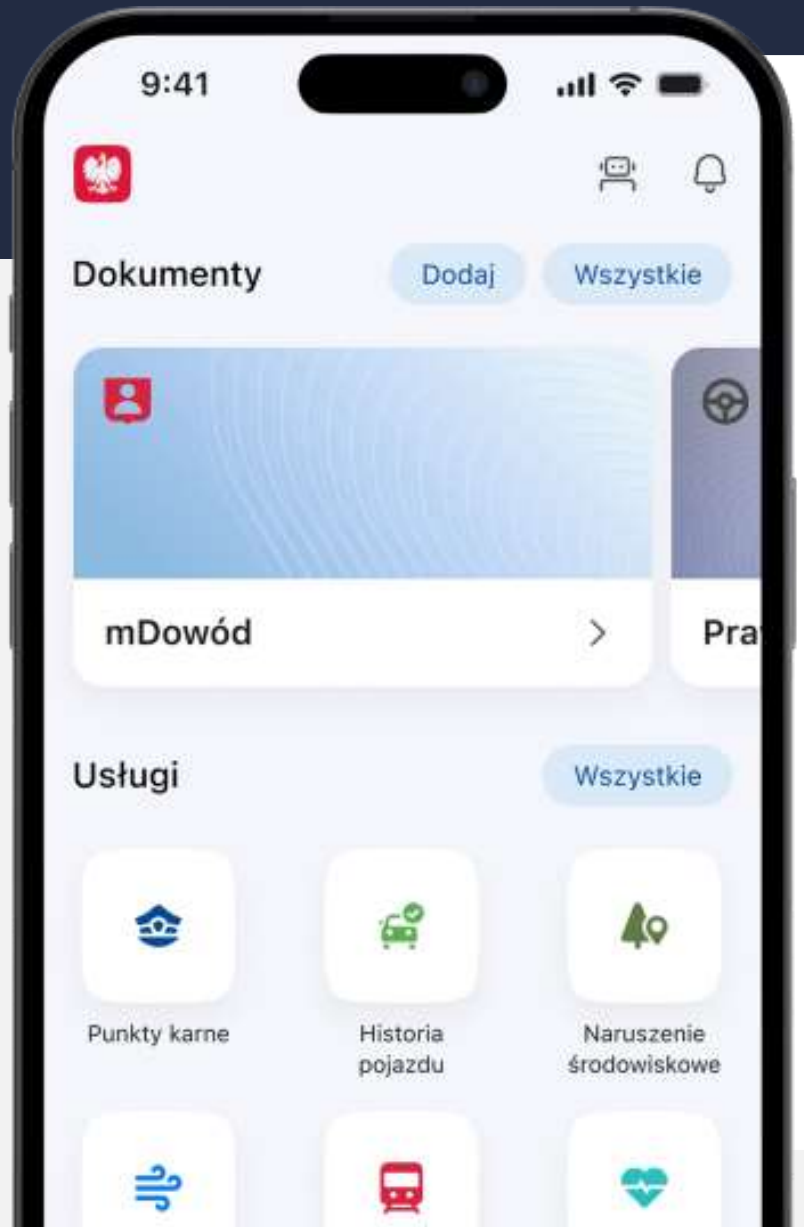
Lessons to learn 🧠

Using Digital ID?

- ✅ Always use the strongest verification method
- ✅ Spread security best practices
- ✅ NEVER VERIFY VISUALY!



Lessons to learn 🧠



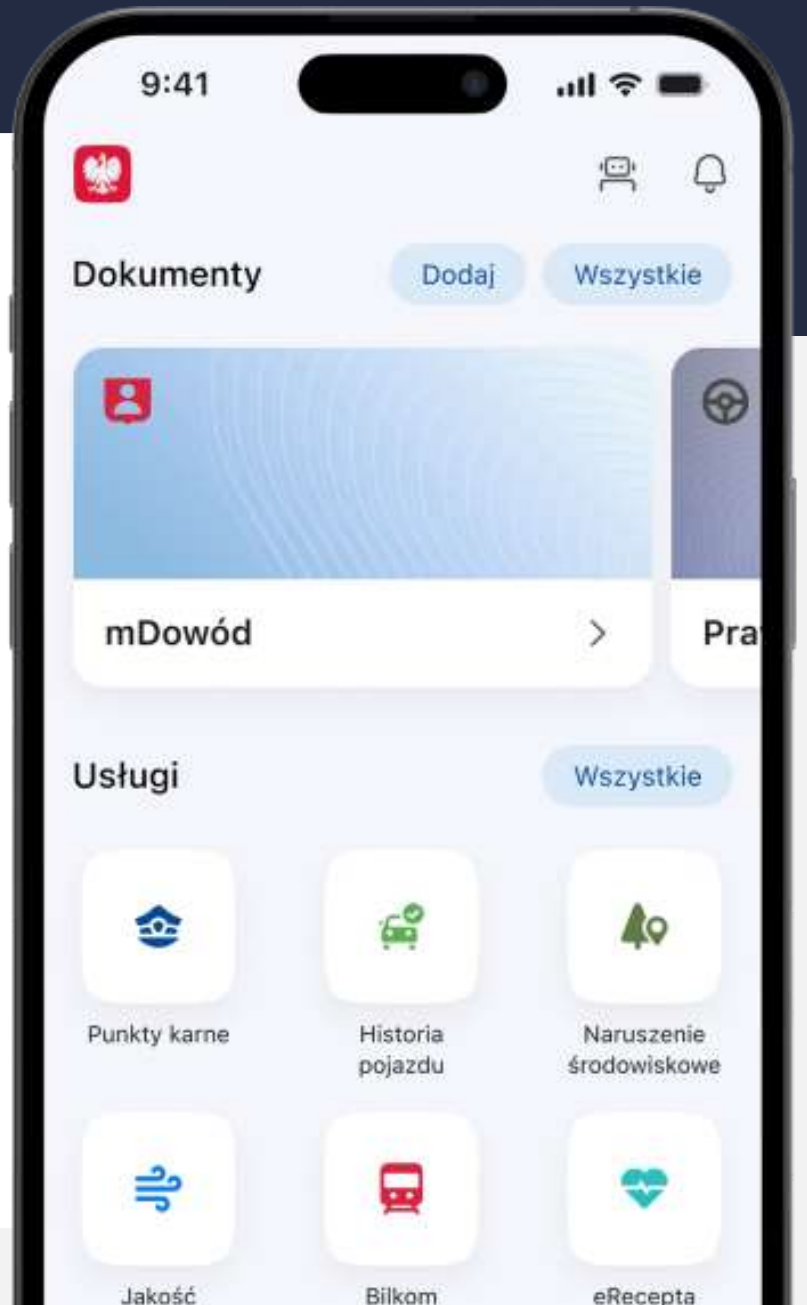
Creating Digial ID?

- ✅ Prioritize security
  - ⚠️ Security principles of traditional ID still apply!
- ✅ Test your solution
- ✅ Discourage visual verification
- ✅ Train others how to properly verify data

Lessons to learn 🧠

Integrating into Digital ID?

- ✅ Use only the strongest verification method
- ✅ Test the integration
- ✅ Assess the risk and consequences
  - 📐 Use threat modeling to cover all bases
  - ❓ *How will vulnerability in Digital ID affect your business?*



Thank you! Questions?

Szymon Chadam

IT Security Consultant at Securing

securing

szymon-chadam