How (not) to implement secure digital identity

Case study of Poland's Digital ID system





Practical part 🐲

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



- 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





Disclaimer

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





Your country already has some sort of Digital ID



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



- 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

ancelaria Sejma	s. 1/3
Dz. U. 2023 poz. 1234	
USTAWA	
z dnia 26 maja 2023 r.	
o aplikacji mObywatel ¹⁾	
Art. 1. Ustawa określa:	
zakres usług udostępnianych w aplikacji mObywatel, w tym funkcjonowanie:	
a) dokumentu mObywatel,	

b) profilu mObywatel,

108

D

- c) certyfikatów użytkownika aplikacji mObywatel,
- d) podpisu elektronicznego weryfikowanego przy użyciu certyfikatu użytkownika aplikacji mObywatel;
- 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;
- sposób potwierdzania oraz weryfikowania autentyczności, ważności, integralności lub pochodzenia dokumentów mobilnych;
- 4) warunki opracowywania, udostępniania i świadczenia usług w aplikacji mObywatel;
- zadania ministra właściwego do spraw informatyzacji w zakresie funkcjonowania i korzystania z aplikacji mObywatel oraz systemu mObywatel.

1) Niniejsza ustawą zmienia się ustawy: ustawę z dnia 20 maja 1971 r. - Kodeks wykroczeń, ustawe 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, ustawe z dnia 5 grudnia 1996 r. o zawodach lekarza i lekarza dentysty, ustawe 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, ustawe z dnia 15 lipca 2011 r. o zawodach pielegniarki 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, ustawe z dnia 10 grudnia 2020 r. o zawodzie farmaceuty, ustawe 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, ustawe z dnia 1 grudnia 2022 r. o zawodzie ratownika medycznego oraz samorzadzie 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





2 main processes



Onboarding process





2 main processes



Verification process

Digital ID verification

Three verification methods

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

How to verify documents in mObywatel 2.0?

There are three methods: the visual, functional, and cryptographic one.



Apg Store

°

Visit informatiyevatal googli to learn more and star alware up to date with the latest functionalities.

-001 =

Salation .

Visual verification



10:36 G A >_

G

•

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:









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







Which of these use the strongest verification method?

















Which of these use the strongest verification method?





mHacker 🕵

Tool for injecting your own data into the mCitizen app

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



9:03 O A)_ E This could be you! mDowód in Wojciech Dworakowski - SecuR × + ÷ SZYMON Imię (imiona) 옥 ☆ 🐂 🎦 । 🗖 🎯 🗄 C 25 pl.linkedin.com/in/wojciechdworakowski CHADAM Sumame PESEL number generator × + Linked in POLSKIE 🖹 🐾 🖸 I 🖬 🎯 🗄 generatorliczb.pl/generator-pesel 🖣 🕁 Citizenship 18.09.1995 **B** ≡ Date of birth 90898916787 PESEL Rzeczpospolita Polska **PESEL** number generator 4000 (\mathcal{A}) Valid Select gender Generated PESEL ○ Woman ○ Man ○ Missing number Wojciech Dworakowski Enter date of birth or age: Krakow Metropolitan Area Confirm your data 2K followers · 500+ connections 71021318478 See your mutual connections * format dd.mm.yyyy (e.g. 14/06/1988) or xx date of birth: 13/02/1971 (e.g. 30) or leave the field blank gender: male Re Document details Generate

♥ 0

2

>

>

Your other details

RedTeam Op + mHacker + Linkedin = 💙

Linked in 100% + **SUCCESS RATE**

Almost the same thing as Fake ID...

Similarities:



Differences:

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



mHacker vs mCitizen

Three verification methods

Visual verification
Functional verification
Cryptographical verification



2 main processes



Onboarding process





2 main processes



Onboarding process

Onboarding



USER

GOV SERVER

Onboarding



Onboarding


Onboarding



Onboarding

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

વા♥		
;{Nx��b�Hy�)EPj @x@U>@@ \U @=U@4	DOOO 50 O D0H O 9 O h+c O,OOO 7`V8 O
000ũ03		
&}@\$\$\$\$ _Lu \$	00h000Ck>0+I0`004	00uR@jJ@K@@@@@& @@@@4E@@
040000 BX	0v00000b%000f0	FIOMOOOXOO
00000ix^0	•••••••••	
0000 NO\00	3003000\$0000\N	\ @ 2hd @ 1ĕ @@ 9@L#Hoz @@#@@ Z@r\@
0000000000	að ð X0&n ÓÐI7kvð4	01E0000.00.000N0 #\$13000
ÔÔ v ÔÔ eB Ô @*m	ÔÔĞ	
7 0 T 0 0% 0 U^oeB*	8alx o y157 0000 i< 06	
+000000000	00F0 im2mD000//#000	000.00e0k5.70h00V001~HT0
ÔĎÔlÔdÔcÔnÔ	000000 a:30H0[-0-	i:]\$K#'\$\$0P\$HE
i=ð d`rð`00xl	₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩₩	
000 (%0?0	0000000 MA - 0000	∂∼"�� m{g5 � f � MXE
0 00>07000 6	••••••••••••••••••••••••••••••••••••••	\$ \$\$(8.\$.\$
າ ູູຸ 2 ລະລລລໍລ ⊨⊚ທ	Endondovk1000(/)	TV#&K'&&AR&FR&FF&\&fn&ill&T&
AT&A=AA AA	ACA7AAAAATFAAAAhA	
	- haally aahai aa19	
AAA-ADAA-1*:		,
	vvv ∿1 2¢[₀¢91ć¢₀¢2¢[¢	
		\ A A A Y A A] . +
4(.4444 c	SAAAAOSAAA IIW) ~~~

. ir 🕰

What's mCitizen under the hood?



NULNULNULNULNULNULNULNUL •0•AckN0•Eot6 ETXSTXSOHSTXSTXBELSIZ•WSKOØACK *•H•÷SOHSOHENQNULØh1vtØ ACKETXUEOTACKDC3STXPL1usØGSACKETXUEOT FF SYNENIGMA SOI Sp. z o. o.1806AcKETXUEOTETX FF/CenCert Centrum CertyfikatÃ³w Powszechnych 20170RsETB210805140107ZETB260805235959Z@

```
STXPL1+0)ACKETXUEOT
FF "Kancelaria Prez
                                "header":
STX • STXSOHNUL® DUÜÂ< CK EI
                                                                                                                                                       T••Pn•õZ¦×k¤`Æ+¶•}
                                    "pesel": "90102631622", "internalDocumentId": "097...0f1", "version": "1",
                                    "documentType": "MOBILE ID CARD", "documentSubtype": null, "documentVersion": 1,
; vÑscxÒ+sug¤±³0dc4/½
                                                                                                                                                       Ĺëv⊤+3fÎÖ`Àk вs •!₀c2<@
                                    "certificateSubjectDn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
                                    "certificateSerialNumber": "286...6b5", "certificateIssuerDn": "CN=MTMid 3,0=Kancelaria Prezesa Rady Ministrów,C=PL",
£ FF • ° • ' ` âØ2 so ?Û[Ñ•
                                                                                                                                                      Ë5vÅäus canÓ±ëË∙nak¾iÈ
                                    "creationTimestamp": "2023-08-24T06:07:38.261890Z", "documentIssuer": "Kancelaria Prezesa Rady Ministrów"
v1&Ù••£•þÖ•u•pc1°ýý
                                },
                                "dh": {
>£¢usÂ4 ,Vocze•p•¬!

 sohdc20 us acketxU gs #eotcai

                                    "tp": 8, "stp": 1, "ver": 1,
                                    "dn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
US TH FF ETBDFÅ?0 EM ACKET
                                                                                                                                                       GS ACKETXU GS SO EOTSYNEOTDC4P
                                    "sn": "286...6b5", "isr": "CN=MTMid 3,0=Kancelaria Prezesa Rady Ministrów,C=PL",
10 ?ê•0≻ACKETXUGS US
                                    "ts": "20230824080738261", "rId": "d22952e6b5ba45bc8c3881fb326eb298",
                                                                                                                                                       IK BS +ACKSOHENDENOBELØSTX •
                                    "iid": "097...0f1", "pe": "90102631622", "in": null,
                                                                                                                                                       NAK"CAN<●¦ÔGS+Ù¬ENQ¦j
;https://cencert.p
                                    "id": "Kancelaria Prezesa Rady MinistrÃ<sup>3</sup>w"
<sup>−</sup>H<sub>DC4</sub>*㕦+敦• GS •%)
                                                                                                                                                      Yüû§∙èÍð°¼!»ýl••rG
                                "data": {
eÐ×(Ãmè"ºÜ(Í7ÕµFó
                                                                                                                                                       NAK5•EMÎÁ´(Élson•Kwqsu
                                    "mobileIdCard": {
                                       "number": "DACK78741",
                                                                                                                                                       ¦ï••Èô½P¹•è•¥:Đ&!Ü"
●●●J●EscCñsiª3sLY●a
                                       "validFrom": "2023-07-15 T12:10:52.369188Z",
                                        "validTo": "2028-07-15T12:10:52.369188Z"
íi•¬ Rs 5•úhstxH · üp so
                                    "personalData": {
gvt •ÛJ¥d Rs Ôìw@DK•
                                        "name": "ADAM",
FF SYNENIGMA SOI Sp.
                                                                                                                                                          • HSOH CETXEOTSTX SOHENQNUL
                                       "secondName": null,
                                        "surname": "NOWAK",
      ETX1VTACK *•H•÷s
                                                                                                                                                         *•H•÷sohsohvtenonul@/a
                                       "fatherName": "JAN",
                                        "motherName": "WERONIKA",
nocz, â•Ô J6`h Fs sueYes
                                        "pesel": "90102631622",
                                                                                                                                                       ••0õH8L{;•Ì3´•´ŗŗõ
æple`%E•• us R÷UM•Q"ï
                                        "birthDate": "1998-02-25",
                                       "citizenship": "POLSKIE",
ÛŶiòÂSÉ,•Êa°#₌orÇ•
                                                                                                                                                       • âñeel?ýA•÷®%ùC¬¦6etx
                                       "picture": "/9j/4AAQSkZJRgABAQAAAQABAAD/2AQEBAQ[...]CgAoAKACgKAP/9k="
•(AjNUL•dpÛÑ• ±úVoci
                                                                                                                                                      ¾;ÈFF <sup>™</sup>, ESCP
z •~ cs üË₀c1 vτ Onvöðst
                                "picture": null
8usÎENQÅ ìÊáT∙uoÀÛi
$c°õú°4• ₂s • r¤¥É~Vh•, •N•ÈLO•ÿ~
```

Sùy gs ûR\nulnulnulnulnul

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





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





4 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





We want more 阿

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





VERIFIER



GOV SERVER



VERIFIED













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?

	Sprawdzanie dokumentu	>
F	(C) (A)	
Do	Potwierdzony okument mDowód został otwierdzony	
Da	ta i godzina weryfikacji: 24.08.2023 12:46 kument ważny do 23.08.2028	
NOW Nazw	AK isko	
ADAI Imię (V Imiona)	
0000	000000	

A0cnV3WGR3MGZCOXhRQjAxdGk2c1JDUm55NkFMK2dHVDF0QUVoUFBhZ0FHNGcvT1FBMGs5K2FBSVhZZ11BSFdnQ005enRGQUNDYVJWeGswQVY1eUpQ0V1BUjdVQV1sOWFPamVaYmtnaz1xQU00WD16QTVEYmdmV2dDekRxek1Sd11uRkFGaUhWU2tvYmVjZT1BRXFhcXJzd0p4bWdDTT2 UFVKM08xVHhRQmRzclZwMzN55EpvQTZDeUFqSWpqVUgxSW9BMUVDZzRKb0F0SmpBOURRQS9PeG1DMmFBR093SkREcDNvQW1BeUR6MU5BRGprZ0FVQU5rY113ZXRBRU1qZ2Z4ZHFBTTY3dVFxRmQzV2dEem40bmE4MmwrRnRSbVY4SHk5b091dWFBUG1tOUU4MXk4MHpcV1pza2s4L2xRC puZ21nQ3pmUExMRXVXSitnd@tBR3JhankxTFVBVnB3NGtFbUc@NDZVQWFOaUNYamRseXZjMEF1Z2FKY3RiUngvdXdTZjR2YWdEUTFPMF15eDNzWXdHSFdnRGNzeD1@c1VaVkc2RWdFZXhvQTJiT1dRcEt1cW5wN1VBZFJwRms@dUh2V31zYkRLbkhCTkFHKzBuN S21ubktxZHE4SDZVQWZSOFdtV2xqcTBkekN5bVVnSF1PL3ZRQj1xc0NZd3g2c0tBSmFBRm9BS0FDZ0FvQUtBSzJvc0ZzWjJQUVJtZ0R3WHhPUmNXZDdLRUpNYXR0SW9BK0xQaVc3ejZ0SVNTU3JIOEtBUE9MMmI3T214R09YUFdnREcxRVBGQUNYUHo4a2V0QUdFa3pmYUN3SVZGd0NLC JqZ25Jb0E4NzhYRGJyTW1rZkt3NW9BNWE0UU5FMF1ISW9BeG1DcSsxdXg0b0FraGxQbWJoa0VkNkFPcHRYRStsZnZNNEI0eDNvQXI2YmZTNmR1TExGSVZPN013ZnVrVUFmVy93aCtKZHZyK2xRYWJxRStMbEZBREU5U1FCNmNzeWtBRDFvQWw4ekpPYUFISzR3UG02MEFCWUVsYUFJcF OF1PTzJLOU1KWU9EZzV4M29BbzNNTG5BRkFHVGVXNXdXWk0vUVVBWkZ5anhaTWFIamtVOVVwTHk0aiVhTjhV0VFuVXJySjJxMkRR0110THk3WWdtUFA0VUFibGxMZU9Sc2p3ZStCUU1wK21XMDdMbWJLL1NnRG9MYTNJOUtj02dDOGtTzy9N0jBvOW1W00FCMm9BUmdONVBvUUEwb1dC5 FjU2NkZVR3SØFLOHJFBIID6GtnSDYwQVVieWRVWGc1TØtBTXE1WnltNXU2MEF1RWZ0QjYvSlphQWxuRTIze1pQbTduRkFIekE3bmY1ak1TVDNvQWZBcEVoNjg4OUtBTmRFOH1GUmprMEFEdHRJaFAzZ09hQUhpMFdTQS9Ma3FjMEFJaU9rZVB1ak5BSGIrSHA0cnV NkFMK2dyc3V4SHR5c3ZCSHZRQjBFTVdIZEIwV2dEdU5Zak9rK0dkT1RiODh5N3VLQU1mQz16OW9zcHJVL2VSczBBZ1Izd2E4Sng2dnMxQzJkb3BZd056QWRTQnhRQj1FNkY0ZU5wS0xxNmN5e11BeWV3b0E2UUFLTUR0UUF0QUJRQVVBRkFCUUFVQVU5VkdiQ2N1cUdnRHcveEpLSU5LK ZEL2orWmhxYzRCenZZaWdEenZVQUIRRHQrWS96b0F6ZGRVWmgzY0FxUHpvQXhJckptbGJwdEo2MEFkdjRhd2JPV01IaFJRQjU3NDJqVWF5N0tjR1FE0WFBT2V2TFJSc2xWU1F3eVFLQU1IVVIRR0d4ZnU5KzVOQUZJTDh4SXpra0dnRHJOQjJ6NmM2UGpLNU9LQUtNcXFKMEs5am5tZ0F U1J1Uno4cEJvQStydkR1dEpmV0VNMGpFN2xIUTk2QU9oam1VdHdmem9Ba0h6VUFLRkhPRFFBaERFQUVVQUcwY2tVQVBFVE1vNDZVQU84amNhQUVsc1N3OWVLQUs4bWt1WUFTb3dCakZBRUgvQUFqaVNna29BS0FHRHdqRzZuQy9wUUJHdmdzWndWd0I3VUFXNFBDVVV1 dDeUNjYmRvUFdnQzjrZXdZQ0FVQU9IOGpRQS9jUmdVQU5QM2pudFFBZ2RRM1NhQUswa2d3TURCb0FpTTZnSExmbFFCUXU3K05NNEpPU1FCVW1EVGtTeWNxRHdLQUsycVNvbHMzUV1CNU5BSH1SOGZOWiszYX1sa2puWkFDQ13RQjVGMVRjUmpIWTBBVFdXV0pPT1IweFFCME9uVzd5eEt ST1TZEpTRktuYWV1S0FOMngwNzc2c1FRVXp3S0FLTnpDMFJLeUo4by9YbWdEVjhMM0JEeVFvUHc5QlFCM21qcm1VUmorTmFBTm5Ub1BzOTJxdU1ZYWdEd1BEUGg1dGE4U1dtbnd4R1Q3UVFjQVVBYjN4ZGdHazZ0YTZGdkJGdEdOdU8zSFNnRGx2Q2N4WFVaSWZVY1VBZmFuN05scjVua EEggPoDTRoU1ZRWTVvQWtvQUtBQ2dBb0FLQUNnQW9Bc1g2NzdXVWRpaEZBSGhIamVOb3ZEK3Bzbk96ZG5qdFFCOFB1TkZhNHY1SkJrQU9mNTBBY0JmSTBsNnFCdUZDOF1wYX1zT29VbWdEd1A0aGt5YVhOYU14M1RzekhGQUh4ejhVQU1eOWpCNU1oe1FCNVR1d0N1ZjVGSkN1MUFGVmH UDFvOXcwbEU4MRjNKRjkzWlFCeTExeEJ1eGtqT0RR01vpbnppT1RESjZ1bEFFMGFEemhzSkk5Tz1BSFJSc1k5T2pkY2h1cG9BOTErOVh4V1NBcjRhMwk1SGt5bkVaY1B5dDB4UUI5R0xKc3dSeXJBY1NPbUtBSEtUdASCA+hHvDFOQUVoUFBhZ0FHNGcvT1FBMGs5K2FB5VhZZ11BSFdr VJWeGswQVY1eUpQ0V1BUjdVQV1sOWFPamVaYmtnaz1xQU00WD16QTVEYmdmV2dDekRxek1Sd11uRkFGaUhWU2tvYmVjZT1BRXFhcXJzd0p4bWdDTT2tYzRWdVByUUE2UFVKM08xVHhRQmRzc1ZwMzNSSEpvQTZDeUFqSWpqVUgxSW9BMUVDZzRKb0F0SmpBOURRQS9PeG1DMmFBR0935 6MU5BRGprZ0FVQU5rY113ZXRBRU1qZF3eVFLQU1IVV1RR0d4ZnU5KzVOQUZJTDh4SXpra0dnRHJOQjJ6NmM2UGpLNU9LQUtNcXFKMEs5am5tZ0R1dkFXc3k2ZHF5U1J1Uno4cEJvQStydkR1dEpmV0VNMGpFN2xIUTk2QU9oam1VdHdmem9Ba0h6VUFLRkhPRFFBaERFQUVVQUcwY2tV 84amNhQUVsc1N3OWVLQUs4bWt1WUFTb3dCakZBRUgvQUFqaVNna29BS0FHRHdqRzZuQy9WUUJHdmdzWndWd0I3VUFXNFBDVVVTNEtaL0NnRFN0TkZTSTRFV0tBTkdDeUNjYmRvUFdnQzJrZXdZQ0FVQU9IOGpRQS9jUmdVQU5QM2pudFFBZ2RRM1NhQUswa2d3TURCb0FpTTZnSExmbFf U1FCVW1EVGtTeWNxRHdLQUsycVNvbHMzUV1CNU5BSH1SOGZOWiszYX1sa2puWkFDQ1JRQ1VGMVRjUmpIWTBBVFdXV0pPT1IweFFCME9uVzd5eEtzWVVrVUFVNU1aST1TZEpTRktuYWV1S0FOMngwNzc2c1FRVXp3S0FLTnpDMFJLeUo4by9YbWdEVjhMM0JEeVFvUHc5Q1FCM21qcm1VL BzOTJxdU1ZYWdEd1BEUGg1dGE4U1dtbnd4R1Q3UVFjQVVBYjN4ZGdHazZ0YTZGdk3GdEdOdU8zSFNnRGx2Q2N4WFVaSWZVY1VBZmFuN05scjVuaHd1NDVEbm4wb0EEggPoOTRoU1ZRWTVvQWtvQUtBQ2dBb0FLQUNnQW9Bc1g2NzdXVWRpaEZBSGhIamVOb3ZEK3Bzbk96ZG5qdFFCOFE QU9mNTBBY0JmSTBsNnFCdUZDOF1wYX1zT29VbWdEd1A0aGt5YVhOYU14M1RzekhGQUh4ejhVQU1EOWpCNU1oe1FCNVR1d0N1ZjVGSkN1MUFGVmhIOW91WFo4a2E0UDFvQXcwbEU4MHF0a0E1SUZBSFE2WVB0Mm1IQzVLa3JRQjV6NGtURjNKRjkzW1FCeTExeEJ1eGtqT0RRQ1Vpbnpp FEemhzSkk5Tz1BSFJSc1k5T2pkY2h1cG9B0TErQVh4V1NBcjRhMwk1SGt5bkVaY1B5dDB4UUI5R0xKc3dSeXJBY1NPbUtBSEtUdASCAc3V4SHR5c3ZCSHZRQjBFTVdIZEIwV2dEdUSZak9rK0dkT1RiODh5N3VLQU1mQz16OW9zcHJVL2VSczBBZ1Izd2E4Sng2dnMxQzJkb3BZd0560W 0ZU5wS0xxNmN5e11BeWV3b0E2UUFLTUR0UUF0QUJRQVVBRkFCUUFVQVU5VkdiQ2N1cUdnRHcveEpLSU5LMU5WVTdkamMwQWZEL2orWmhxYzRCenZZaWdEenZVQU1RRHQrWS96b0F6ZGRVWmgzY0FxUHpvQXhJckptbGJwdEo2MEFkdjRhd2JPV01IaFJRQjU3NDJqVWF5N0tjR1FEOWF6 1F3eVFLQU11VV1RR0d4ZnU5KzVOQUZJTDh4SXpra0dnRHJOQjJ6NmM2UGpLNU9LQUtNcXFKMEs5am5tZ0R1dkFXc3k2ZHF5U1J1Uno4cEJvQStydkR1dEpmV0VNMGpFN2xIUTk2QU9oam1VdHdmem9Ba0h6VUFLRkhPRFFBaERFQUVVQUcwY2tVQVBFVE1vNDZVQU84amNhQUVsc1N30V Tb3dCakZBRUgvQUFqaVNna29BS0FHRHdqRzZuQy9wUUJHdmdzWndWd0I3VUFXNFBDVVVTNEtaL0NnRFN0TkZTSTRFV0tBTkdDeUNjYmRvUFdnQzJrZXdZQ0FVQU9IOGpRQS9jUmdVQU5QM2pudFFBZ2RRM1NhQUswa2d3TURCb0FpTTZnSExmbFFCUXU3K05NNEpPU1FCVW1EVGtTeWN HMzUV1CNU5BSH1SOGZOWiszYX1sa2puWkFDQ1JRQjVGMVRjUmpIWTBBVFdXV0pPT1IweFFCME9uVzd5eEtzWVVrVUFVNU1aST1TZEpTRktuYWV1S0FOMngwNzc2c1FRVXp3S0FLTnpDMFJLeUo4by9YbWdEVjhMM0JEeVFvUHc5Q1FCM21qcm1VUmorTmFBTm5Ub1Bz0TJx tbnd4R103UVFj0VVBYjN4ZGdHazZ0YTZGdkJGdEdOdU8zSFNnRGx202N4WFVaSWZVY1VBZmFuN05scjVuaHd1NDVEbm4wb0EEggPoOTRoU1ZRWTVvOWtvOUtB02dBb0FL0UNnOW9Bc1g2NzdXVWRpaEZBSGhIamVOb3ZEK3Bzbk96ZG5qdFFC0FB1TkZhNHY1SkJr0U9mNTBBY0JmSTBs X1zT29VbWdEd1A0agt5YVhOYU14M1RzekhGQUh4ejhVQU1EOWpCNU1oe1FCNVR1d0N1ZjVG5kN1MUFGVmhIOW91WFo4a2E0UDFvQXcwbEU4MRjNKRjkzW1FCeTExeEJ1eGtqT0RRQ1VpbnppT1RESjZ1bEFFMGFEemhzSkk5Tz1BSFJSc1k5T2pkY2h1cG9BOTErQVh4V1NBcjRhMWk1 B4UUISR0xKc3dSeXJBy1NPbUtBSEtUdASCA+hHVDF0QUVoUFBhZ0FHNGcvT1FBMGs5K2FBSVhZZ11BSFdnQ005enRGQUNDYVJWeGswQVY1eUpQ0V1BUjdVQV1sOWFPamVaYmtnaz1xQU00WD16QTVEYmdmV2dDekRxek1Sd11uRkFGaUhWU2tvYmVjZT1BRXFhcXJzd0p4bWdDTTZtYzF M08xVHhRQmRzclZwMzN5SEpvQTZDeUFqSWpqVUgxSW9BMUVDZzRKb0F0SmpBOURRQS9PeG1DMmFBR093SkREcDNvQW1BeUR6MU5BRGprZ0FVQU5rY113ZXRBRU1qZF3eVFLQU1IVV1RR0d4ZnU5KzVOQUZJTDh4SXpra0dnRHJOQjJ6NmM2UGpLNU9LQUtNcXFKMEs5am5tZ0R1dkFXc 4cEJvQStydkR1dEpmV0VNMGpFN2xIUTk2QU9oam1VdHdmem9Ba0h6VUFLRkhPRFFBaERFQUVVQUcwY2tVQVBFVE1vNDZVQU84amNhQUVsc1N3OWVLQUs4bWt1WUFTb3dCakZBRUgvQUFqaVNna29BS0FHRHdqRzZuQy9wUUJHdmdzWndWd0I3VUFXNFBDVVVT mRvUFdnQzJrZXdZQ0FVQU9IOGpRQS9jUmdVQU5QM2pudFFBZ2RRM1NhQUswa2d3TURCb0FpTTZnSExmbFFCUXU3K05NNEpPU1FCVW1EVGtTeWNxRHdLQUsycVNvbHMzUV1CNU5BSH1SOGZOWiszYX1sa2puWkFDQ1JRQjVGMVRjUmpIWTBBVFdXV0pPT1IweFFC TRktuYWV1S0F0MngwNzc2c1FRVXp3S0FLTnpDMFJLeUo4by9YbWdEVjhMM0JEeVFvUHc5Q1FCM21qcm1VUmorTmFBTm5Ub1BzOTJxdU1ZYWdEd1BEUGg1dGE4U1dtbnd4R1Q3UVFjQVVBYjN4ZGdHazZ0YTZGdkJGdEdOdU8zSFNnRGx2Q2N4WFVaSWZVY1VBZmFuN05scjVuaHd1NDVE TRoU1ZRWTVvQWtvQUtBQ2dBb0FLQUNnQW9Bc1g2NzdXVWRpaEZBSGhIamVOb3ZEK3Bzbk96ZG5qdFFCOFB1TkZhNHY1SkJrQU9mNTBBY0JmSTBsNnFCdUZDOF1wYX1zT29VbWdEd1A0aGt5YVhOYU14M1RzekhGQUh4ejhVQU1EOWpCNU1oe1FCNVR1d0N1ZjVGSkN1MUFGVmhIOW91WA wbEU4MHF0a0E1SUZBSFE2WVB0MmlIQzVLa3JRQjV6NGtURjNKRjkzWlFCeTExeEJ1eGtqT0RRQlVpbnppT1RESjZlbEFFMGFEemhzSkk5Tz1BSFJSc1k5T2pkY2h1cG9BOTErQVh4VlNBcjRhMwk1SGt5bkVaYlB5dDB4UUI5R0xKc3dSeXJBY1NPbUtBSEtUdASCA+hHVDF0QUVoUFB GsSK2FBSVhZZ11BSFdnQ005enRGQUNDYV3WeGswQVY1eUpQ0V1BUjdVQV1sOWFPamVaYmtnaz1xQU00WD16QTVEYmdmV2dDekRxek1Sd11uRkFGaUhWU2tvYmVjZT1BRXFhcX3zd0p4bWdDTTZtYzRWdVByUUE2UFVKM08xVHhRQmRzc1ZwMzN5SEpvQTZDeUFqSWpqVUgxSW9 RQS9PeG1DMmFBR093SkREcDNvQW1BeUR6MU5BRGprZ0FVQU5rY113ZXRBRU1qZ2Z4ZHFBTTY3dVFxRmQzV2dEem40bmE4MmwrRnRSbVY4SHk5b091dWFBUG1tOUU4MXk4MHpCV1pza2s4L2xRQX1LVk1aRDVZOHpuZ21nQ3pmUExMRXVXSitnd0tBR3JhankxTFVBV XZjMEF1Z2FKY3RiUngvdXdTZjR2YWdEUTFPMF15eDNzWXdHSFdnRGNzeD10c1VaVkc2RWdFZXhvQTJiT1dRcEt1cW5wN1VBZFJwRms0dUh2V31zYkRLbkhCTkFHKzBuMm0xZ3UwR1NqNE1IZWdEMmI0RWFkW1MrS21ubktxZHE4SDZVQWZSOFdtV2xqcTBkekN5bVVnSF1PL3ZRQj1xc0 BRm9BS0FDZ0FvQUtBSzJvc0ZzwjJQUVJtZ0R3WHPUmNXZDdLRUpNYXR0SW9BK0xQaVc3ejZ0SVNTU3JIOEtBUE9MMmI3T214R09YUFdnREcxRVBGQUNYUHo4a2V0QUdFa3pmYUN3SVZGd0NLQU8xOE1SZjhTdwJqZ25Jb0E4NzhYRGJyTW1rZkt3NW9BNWE0UU5FMF WJoa@VkNkFPcHRYRStsZnZNNEI@eDNvQXI2YmZTNmR1TExGSVZPN013ZnVrVUFmVy93aCtKZHZyK2xRYWJxRStMbEZBREU5U1FCNmNzeWtBRDFvQWw4ekpPYUFISzR3UG02MEFCWUVsYUFJcFJqRkFCOThnMEFJOF1PTzJLQU1KWU9EZzV4M29BbzNNTG5BRkFH VQVVwTHk0ajVhTjhVQVFuVXJySjJxMkRRQ110THk3WWdtUFA0VUFibGxMZU9Sc2p3Z5tCUUIwK21XMDdMbWJLL1NnRG9MYTNJQUtjQ2dDOGtTZy9NQjBvQW1WQ0FCMm9BUmdONVByUUEwb1dCSFkwQVJmZEhCb0FjU2NkZVR3S0FLOHJFBIID6GtnSDYwQVVieWRVWGc1T0tBTXE1Wn1t jYvSlphQWxuRTIzelpQbTduRkFIekE3bmY1ak1TVDNvQWZBcEVoNjg40UtBTmRFOHlGUmprMEFEdHRJaFAzZ09hQUhpMFdTQS9Ma3FjMEFJaU9rZVB1ak5BSGIrSHA0cnV3WGR3MGZCOXhRQjAxdGk2c1JDUm55NkFMK2dyc3V4SHR5c3ZCSHZRQjBFTVdIZEIwV2dEdU5Za mQz160W9zcHJVL2VScz8BZ1Izd2E4Sng2dnMxQz3kb3BZd056QWRTQnhRQj1FNkY0ZU5wS0xxNmN5e11BeWV3b0E2UUFLTUR0UUF0QUJRQVVBRkFCUUFVQVU5VkdiQ2N1cUdnRHcveEpLSU5LMU5WVTdkamMwQWZEL2orWmhxYzRCenZZaWdEenZVQU1RRHQrWS96b0F6ZGRVWmgzY0F GJwdEo2MEFkdjRhd2JPV01IaFJRQjU3NDJqVWF5N0tjR1FEOWFBT2V2TFJSc2xWU1F3eVFLQU1IVV1RR0d4ZnU5KzVOQUZJTDh4SXpra0dnRHJOQjJ6NmM2UGpLNU9LQUtNcXFKMEs5am5tZ0R1dkFXc3k2ZHF5U1J1Uno4cEJvQStydkR1dEpmV0VNMGpFN2xIUTk2QU9oam1VdHdmen PRFFBaERFQUVVQUcwY2tVQVBFVE1vNDZVQU84amNhQUVsc1N30WVLQUs4bWt1WUFTb3dCakZBRUgvQUFqaVNna29BS0FHRHdqRzZuQy9wUUJHdmdzWndWd0I3VUFXNFBDVVVTNEtaL0NnRFN0TkZTSTRFV0tBTkdDeUNjYmRvUFdnQz3rZXdZQ0FVQU9IOGpRQS9jUmdVQU5QM2pudFFE 2d3TURCb0FpTTZnSExmbFFCUXU3K05NNEpPU1FCVW1EVGtTeWNxRHdLQUsycVNvbHMzUV1CNU5BSH1SOGZOWiszYX1sa2puWkFDQ13RQjVGMVRjUmpIWTBBVFdXV0pPT1IweFFCME9uVzd5eEtzWVVrVUFVNU1aST1TZEpTRktuYWV1S0FOMngwNzc2c1FRVXp3S0FLTnpDMF3LeUo4by EeVFvUHc5QlFCM21qcmlVUmorTmFBTm5Ub1BzOTJxdU1ZYWdEd1BEUGg1dGE4U1dtbnd4R103UVFjQVVBYjN4ZGdHazZ0YTZGdkJGdEdOdU8zSFNnRGx2Q2N4WFVaSWZVY1VBZmFuN05scjVuaHd1NDVEbm4wb0EEggPoOTRoU1ZRWTVvQWtvQUtBQ2dBb0FLQUNnQW9Bc1g2NzdXVWRg 3ZEK38zbk96ZG5qdFFCOFB1TkZhNHY1SkJrQU9mNTBBY0JmSTBsNnFCdUZMU5BRGprZ0FVQU5rY113ZXRBRU1qZ2Z4ZHFBTTY3dVFxRmQzV2dEem40bmE4MmwrRnRSbVY4SHk5b091dWFBUG1tOUU4MXk4MHpcV1pza2s4L2xRQX1LVk1aRDVZOHpuZ21nQ3pmUExMRXVXSitnd0tBR3 NGtFbUc0NDZVQWFOaUNYamRseXZjMEF1Z2FKY3RiUngvdXdTZjR2YWdEUTFPMF15eDNzWXdHSFdnRGNzeD10c1VaVkc2RWdFZXhvQTJiT1dRcEt1cW5wN1VBZFJwRms0dUh2V31zYkRLbkhCTkFHKzBuMm0xZ3UwR1NqNE1IZWdEMmI0RWFkW1MrS21ubktxZHE4SDZVQWZSOFdtV2xqc 1PL3ZRQjIxc0NZd3g2c0tBSmFBRm9BS0FDZ0FvQUtBSzJvc0ZzWjJQUVJtZ0R3WHPUmNXZDdLRUpNYXR0SW9BK0xQaVc3ejZ0SVNTU3JIOEtBUE9MMmI3T214R09YUFdnREcxRVBGQUNYUHo4a2V0QUdFa3pmYUN3SVZGd0NLQU8xOE1SZjhTdwJqZ25Jb0E4NzhYRGJyTW1rZkt3NW SW9BeG1Dc5sxdXg0b0FraGxQbWJoa0VkNkFPcHRYRStsZnZNNEI0eDNvQXI2YmZTNmR1TExGSVZPN013ZnVrVUFmVy93aCtKZHZyK2xRYWJxRStMbEZBREU5U1FCNmNzeWtBRDFvQWw4ekpPYUFISzR3UG02MEFCWUVsYUFJcFJqRkFCOThnMEFJOF1PTzJLQU1KWU9EZzV4M29BbzNN dXWk@vUVVBWkZ5anhaTWFIamtVQVVwTHk@ajVhTjhVQVFuVXJySjJxMkRRQ110THk3WWdtUFA@VUFibGxMZU9Sc2p3ZStCUUIwK21XMDdMbWJLL1jYmRvUFdnQzJrZXdZQ@FVQU9I0GpRQS9jUmdVQU5QM2pudFFBZ2RRM1NhQUswa2d3TURCb@FpTTZnSExmbFFCUXU3K@5NNEpPU1F0 HdLQUsycVNvbHMzUV1CNU5BSH1SOGZOWiszYX1sa2puWkFDQ1JRQjVGMVRQvVBYjN4ZGdHazZ0YTZGdkJGdEdOdU8zSFNnRGx2Q2N4WFVaSWZVY1VBZmFuN05scjVuaHd1NDVEbm4wb0EEggPoOTRoU1ZRWTVvQWtvQUtBQ2dBb0FLQUNnQW9Bc1g2NzdXVWRpaEZBSGhIamVOb3ZEK38 OFB1TkZhNHY1SkJrQU9mNTBBY0JmSTBsNnFCdUZDOF1wYX1zT29VbWdEd1A0aGt5YVhOYU14M1RzekhGQUh4ejhVQU1EOWpCNU1oe1FCNVR1d0N1ZjVGSkN1MUFGVmhIOW91WFo4a2E0UDFvQXcwbEU4MHF0a0E1SUZBSFE2WVB0Mm1IQzVLa3JRQjV6NGtURjNKRjkzW1FCeTExeEJ1e ppT1RESjZ1bEFFMGFEemhzSkk5Tz1BSFJSc1k5T2pkY2h1cG9B0TErQVh4V1NBcjRhMwk1SGt5bkVaY1B5dDB4UUI5R0xKc3dSeX3BY1NPbutBSEtUdASCAc3V4SHR5c3ZCSHZRQjBFTVdIZEIwV2dEdU5Zak9rK0dkT1RiODh5N3VLQU1mQz160W9zcHJVL2VSczBBZ1Izd2E4Sng2dr

```
"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 3,0=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=
    "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?

NULNULNULNULNULNULNULNUL •0•AckN0•Eot6 ETXSTXSOHSTXSTXBELSIZ•WSKOØACK *•H•÷SOHSOHENQNULØh1vtØ ACKETXUEOTACKDC3STXPL1usØGSACKETXUEOT FF SYNENIGMA SOI Sp. z o. o.1806AcKETXUEOTETX FF/CenCert Centrum CertyfikatÃ³w Powszechnych 20170RsETB210805140107ZETB260805235959Z@

```
STXPL1+0)ACKETXUEOT
FF "Kancelaria Prez
                                "header":
STX • STXSOHNUL® DUÜÂ< CK EI
                                                                                                                                                       T••Pn•õZ¦×k¤`Æ+¶•}
                                    "pesel": "90102631622", "internalDocumentId": "097...0f1", "version": "1",
                                    "documentType": "MOBILE ID CARD", "documentSubtype": null, "documentVersion": 1,
; vÑscxÒ+sug¤±³0dc4/½
                                                                                                                                                       Ĺëv⊤+3fÎÖ`Àk вs •!₀c2<@
                                    "certificateSubjectDn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
                                    "certificateSerialNumber": "286...6b5", "certificateIssuerDn": "CN=MTMid 3,0=Kancelaria Prezesa Rady Ministrów,C=PL",
£ FF • ° • ' ` âØ2 so ?Û[Ñ•
                                                                                                                                                      Ë5vÅäus canÓ±ëË∙nak¾iÈ
                                    "creationTimestamp": "2023-08-24T06:07:38.261890Z", "documentIssuer": "Kancelaria Prezesa Rady Ministrów"
v1&Ù••£•þÖ•u•pc1°ýý
                                },
                                "dh": {
>£¢usÂ4 ,Vocze•p•¬!

 sohdc20 us acketxU gs #eotcai

                                    "tp": 8, "stp": 1, "ver": 1,
                                    "dn": "GIVENNAME=ADAM,SURNAME=NOWAK,C=PL,SERIALNUMBER=PNOPL-90102631622,CN=ADAM NOWAK",
US TH FF ETBDFÅ?0 EM ACKET
                                                                                                                                                       GS ACKETXU GS SO EOTSYNEOTDC4P
                                    "sn": "286...6b5", "isr": "CN=MTMid 3,0=Kancelaria Prezesa Rady Ministrów,C=PL",
10 ?ê•0≻ACKETXUGS US
                                    "ts": "20230824080738261", "rId": "d22952e6b5ba45bc8c3881fb326eb298",
                                                                                                                                                       IK BS +ACKSOHENDENOBELØSTX •
                                    "iid": "097...0f1", "pe": "90102631622", "in": null,
                                                                                                                                                       NAK"CAN<●¦ÔGS+Ù¬ENQ¦j
;https://cencert.p
                                    "id": "Kancelaria Prezesa Rady MinistrÃ<sup>3</sup>w"
<sup>−</sup>H<sub>DC4</sub>*㕦+敦• GS •%)
                                                                                                                                                      Yüû§∙èÍð°¼!»ýl••rG
                                "data": {
eÐ×(Ãmè"ºÜ(Í7ÕµFó
                                                                                                                                                       NAK5•EMÎÁ´(Élson•Kwqsu
                                    "mobileIdCard": {
                                       "number": "DACK78741",
                                                                                                                                                       ¦ï••Èô½P¹•è•¥:Đ&!Ü"
●●●J●EscCñsiª3sLY●a
                                       "validFrom": "2023-07-15 T12:10:52.369188Z",
                                        "validTo": "2028-07-15T12:10:52.369188Z"
íi•¬ Rs 5•úhstxH · üp so
                                    "personalData": {
gvt •ÛJ¥d Rs Ôìw@DK•
                                        "name": "ADAM",
FF SYNENIGMA SOI Sp.
                                                                                                                                                          • HSOH CETXEOTSTX SOHENQNUL
                                       "secondName": null,
                                        "surname": "NOWAK",
      ETX1VTACK *•H•÷s
                                                                                                                                                         *•H•÷sohsohvtenonul@/a
                                       "fatherName": "JAN",
                                        "motherName": "WERONIKA",
nocz, â•Ô J6`h Fs sueYes
                                        "pesel": "90102631622",
                                                                                                                                                       ••0õH8L{;•Ì3´•´ŗŗõ
æple`%E•• us R÷UM•Q"ï
                                        "birthDate": "1998-02-25",
                                       "citizenship": "POLSKIE",
ÛŶiòÂSÉ,•Êa°#₌orÇ•
                                                                                                                                                       • âñeel?ýA•÷®%ùC¬¦6etx
                                       "picture": "/9j/4AAQSkZJRgABAQAAAQABAAD/2AQEBAQ[...]CgAoAKACgKAP/9k="
•(AjNUL•dpÛÑ• ±úVoci
                                                                                                                                                      ¾;ÈFF <sup>™</sup>, ESCP
z •~ cs üË₀c1 vτ Onvöðst
                                "picture": null
8usÎENQÅ ìÊáT∙uoÀÛi
$c°õú°4• ₂s • r¤¥É~Vh•, •N•ÈLO•ÿ~
```

Sùy gs ûR\nulnulnulnulnul

```
"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 3,0=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=
    "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

Generate phishing QR code
 Lure victim into veryfing his data
 Inject his/her data into your application process
 Successfuly verify (not) your data

Wintow PowerShall	× + -
[pl.nask.mobywatel]	
[pl.nask.mohymatel]	
[pl.nask.mohymatel]	+3
[pl.nask.mobywatel]	
[pl.nask.mobymatel]	-3
[pl.nask.mobywatel]	
[pl.nask.mobymatel]	
[pl.nask.mobymatel]	
[pl.nask.mobymatel]	
[pl.nask.mobywatel]	
[pl.nask.mobywatel]	
[pl.nask.mobymatel]	
[pl.nask.mobywatel]	
[pl.nask.mobymatel]	+2
[pl.nask.mubymatel]	+9
[pl.nask.mobymatel]	-
[pl.nask.mobywatel]	
[pl.nask.mobywatel]	
[pl.nask.mobymatel]	
[pl.nask.mobymatel]	
[pl.nask.mobymatel]	
[pl.mask.mobymatel]	*
[pl.mask.mobywatel]	
[pl.nask.mobymatel]	
[pl.nask.mobywatel]	1 B
[pl.nask.mobywatel]	
[pl.nask.mobywatel]	**
[pl.nask.mobywatel]	
[pl.mask.mobywatel]	
[pl.nask.mobymatel]	
[pl.nask.mobywatel]	
[pl.nask.mobymatel]	**







3rd party verifier



Attacker

1	-	No. 11	Ww x + +
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->
[Android	Emulator	5554::pl.nask.mobywatel]->



- 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?



???

"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?"




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 ⁽¹⁾



Y 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.

Published (7)/04/2023 14/08



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 1_{st} 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



Using Digital ID?

Always use the strongest verification method

- Spread security best practices
- NEVER VERIFY VISUALY!



Lessons to learn 🧼

9:41		ul 🗟 🔳	
*			Ô
Dokumenty	Dodaj	Wszystkie	
8			•
mDowód		>	Pra
Usługi		Wszystkie	
•	ŝ	40	
Punkty karne	Historia pojazdu	Naruszenie środowiskow	e we
î		-	

Creating Digial ID?

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



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

Osecuring

in szymon-chadam