Informacje o
publicznej aplikacji mobilnej mObywatel

Spis treści

Słownik pojęć

Minister – minister właściwy do spraw informatyzacji – Minister Cyfryzacji, Kancelaria Prezesa Rady Ministrów, Al. Ujazdowskie 1/3, 00-583 Warszawa. Minister jest także administratorem danych osobowych.

Aplikacja mObywatel lub Aplikacja – udostępniona Ci aplikacja mObywatel stanowi wersję publicznej aplikacji mobilnej, o której mowa w art. 19e ustawy o informatyzacji, przeznaczoną dla obywateli Ukrainy, którzy w okresie od dnia 24 lutego 2022 r. przybyli na terytorium Rzeczypospolitej Polskiej w związku z trwającymi działaniami wojennymi na terenie Ukrainy i których pobyt na terytorium Rzeczypospolitej Polskiej został uznany za legalny. Warunki funkcjonowania publicznej aplikacji mobilnej i jej udostępniania przez ministra właściwego do spraw informatyzacji określają art. 19e -19i ww. ustawy oraz art. 10 ust. 1 ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa.

Użytkownik – osoba, która korzysta na urządzeniu mobilnym z Aplikacji.

Diia.pl lub **Usługa Diia.pl** (Android, iOS) – usługa Ministra, o której mowa w art. 19e ust. 2 pkt 2 ustawy o informatyzacji w zw. z art. 10 ust. 1 o pomocy obywatelom Ukrainy, dostępna na urządzeniu mobilnym Użytkownika w Aplikacji, która pozwala na pobranie danych osobowych Użytkownika, który jest obywatelem Ukrainy i przybył na terytorium Rzeczypospolitej Polskiej z terytorium Ukrainy w okresie od dnia 24 lutego 2022 r., z Rejestru, przechowywane ich w zaszyfrowanej formie na urządzeniu mobilnym Użytkownika, okazywanie danych Użytkownika innym osobom w celu potwierdzenia tożsamości Użytkowania.

Unijny Certyfikat Covid (UCC) (Android, iOS) – usługa Ministra Zdrowia zapewniająca na podstawie art. 7b ust. 1a ustawy z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia również w Aplikacji potwierdzenie, że dana osoba została zaszczepiona przeciw wirusowi SARS-Cov-2 i/lub uzyskała negatywny wynik testu na obecność wirusa SARS-Cov-2 i/lub przebyła chorobę COVID-19.

Krajowy Certyfikat Ozdrowienia (KCO) (Android, iOS) – usługa Ministra Zdrowia;
prezentowany w usłudze Unijny Certyfikat COVID. KCO jest elektronicznym dowodem na to, że dana osoba przebyła chorobę COVID-19. Uznawany wyłącznie na terenie Polski.

eRecepta lub Usługa eRecepta (Android, iOS) – usługa online Ministra Zdrowia pozwalająca na dostęp, za pośrednictwem Aplikacji, do Internetowego Konta Pacjenta w zakresie prezentacji niezrealizowanych recept elektronicznych – dokumentów elektronicznych o których mowa w art. 2 ust. 6 lit. a ustawy o systemie informacji w ochronie zdrowia (Dz. U. z 2019 r., poz. 408 z późn. zm.)

Profil Zaufany – środek identyfikacji elektronicznej zawierający zestaw danych identyfikujących i opisujących osobę fizyczną, który został wydany w sposób, o którym mowa w art. 20c ustawy o informatyzacji (pz.gov.pl) w publicznym systemie identyfikacji elektronicznej administrowanym przez Ministra.

Kod QR – alfanumeryczny, dwuwymiarowy, matrycowy, kwadratowy kod graficzny.

Centrum e-Zdrowia (CeZ) – państwowa jednostką budżetowa powołana przez Ministra Zdrowia, której głównym przedmiotem działalności jest realizacja zadań z zakresu budowy społeczeństwa informacyjnego, obejmujących organizację i ochronę zdrowia oraz wspomaganie decyzji zarządczych ministra właściwego do spraw zdrowia na podstawie prowadzonych analiz.

System Informacji Medycznej (SIM) – o którym mowa w ustawie z dnia 28 kwietnia 2011 r. o systemie informacji w ochronie zdrowia, w którym znajdują się informacje o zdarzeniach

medycznych wszystkich obywateli Polski – niezależnie od płatnika – oraz obywateli Unii Europejskiej i innych krajów, którzy skorzystają ze świadczeń zdrowotnych w Polsce.

Internetowe Konto Pacjenta (IKP) – moduł systemu, o którym mowa w art. 7 ust. 1 ustawy o systemie informacji w ochronie zdrowia z dnia 28 kwietnia 2011 r. (Dz. U. z 2021 r. poz. 666 z późn. zm.), w którym są przetwarzane dane dotyczące usługobiorcy zawarte w Systemie Informacji Medycznej oraz Systemie Rejestru Usług Medycznych Narodowego Funduszu Zdrowia.**mWeryfikator** (Android, iOS) – oprogramowanie pod nazwą „mWeryfikator", stanowiące element publicznej aplikacji mobilnej, o której mowa w art 19e ustawy o informatyzacji, przeznaczone do zainstalowania na urządzeniu mobilnym, współpracujące z Usługą i umożliwiające potwierdzenie danych osobowych Użytkownika Usług. Korzystanie z mWeryfikator odbywa się na odrębnie określonych zasadach.

Certyfikat – certyfikat kryptograficzny potwierdzający autentyczność pobranych danych. Certyfikat przypisany jest do Użytkownika i urządzenia mobilnego, którym posługuje się Użytkownik.

Urządzenie mobilne (smartfon) – przenośne urządzenie elektroniczne, którym posługuje się Użytkownik, pozwalające na przetwarzanie, odtwarzanie, odbieranie i wysyłanie danych bez konieczności utrzymywania przewodowego połączenia z siecią.

Węzeł krajowy – usługa umożliwiająca uwierzytelnianie użytkownika systemu teleinformatycznego, korzystającego z usługi online, z wykorzystaniem środka identyfikacji elektronicznej wydanego w systemie identyfikacji elektronicznej przyłączonym do tego węzła bezpośrednio albo za pośrednictwem węzła transgranicznego.

Ustawa o informatyzacji – ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2021 r. poz. 2070 z późn. zm.).

Ustawa o pomocy obywatelom Ukrainy – ustawa z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa (Dz. U. z 2022 r. poz. 583).

Rejestr – rejestr obywateli Ukrainy, którym nadano numer PESEL, o którym mowa w art. 6 ust. 1 ustawy o pomocy obywatelom Ukrainy.

1 Wymagania techniczne dotyczące korzystania z Aplikacji

1.1 Wymagania techniczne

Wymagania techniczne dla urządzeń mobilnych:

- system operacyjny Android w wersji 6.0 lub wyższej (z domyślnie dostępnymi usługami mobilnymi Google – Google Mobile Services), lub
- system operacyjny iOS w wersji 13 lub wyższej
- dostęp do sklepu Google Play lub App Store
- przynajmniej 100 MB wolnej przestrzeni pamięci dla Aplikacji
- system operacyjny bez modyfikacji, w szczególności polegających na przełamaniu zabezpieczeń producenta urządzenia mobilnego lub producenta systemu operacyjnego (tzw. jailbreaking czy rooting)
- moduł łączności Bluetooth i/lub WiFi na potrzeby nawiązania łączności w procesie przekazywania danych po zeskanowaniu kodu QR do mWeryfikatora
- połączenie z Internetem
- udostępnienia lokalizacji (jednorazowo, tylko dla Android 8.1 i wyższej) - na potrzeby ustalenia identyfikatora interfejsu sieciowego
- aparat fotograficzny.

Minister dokłada starań, aby zapewnić jak największą kompatybilność Aplikacji z urządzeniami mobilnymi różnych producentów. Jednak nie gwarantuje, że Aplikacja będzie działać poprawnie na urządzeniach, na których nie została przetestowana (lista przetestowanych urządzeń).

Wymagania dostępu aplikacji do zasobów urządzenia mobilnego, w szczególności do:

- Internetu
- usługi telefon – na potrzeby ustalenia identyfikatora urządzenia (numer IMEI urządzenia).

Połączenia z Internetem wymagają następujące czynności:

- pobranie i aktywacja Aplikacji
- weryfikacja aktualności Certyfikatu innego Użytkownika
- pobranie Certyfikatu danej Usługi w Aplikacji i powiązanych z nim danych
- Aktualizacja Certyfikatu danej Usługi w Aplikacji i powiązanych z nim danych (funkcja **Aktualizuj dane**).

1.2 Wymagania dotyczące instalacji aktualizacji

Do prawidłowego działania Aplikacji i właściwego zabezpieczenia zawartych w niej danych konieczna może być **instalacja aktualizacji**, którą cyklicznie dostarcza Minister. Minister nie gwarantuje poprawnego działania Aplikacji w przypadku braku zainstalowanych aktualizacji niezwłocznie po ich udostępnieniu w sklepie Google Play lub App Store.

Użytkownik powinien instalować uaktualnienia systemu operacyjnego zgodnie z zaleceniami producenta swojego urządzenia mobilnego oraz producenta systemu operacyjnego. Brak aktualizacji systemu operacyjnego lub Aplikacji może prowadzić do obniżenia poziomu bezpieczeństwa korzystania z Aplikacji, a nawet do wycieku danych z Aplikacji.

1.3 Warunki użytkowania Aplikacji

W przypadku zgubienia, kradzieży lub utraty z innych przyczyn urządzenia mobilnego, Użytkownik powinien niezwłocznie zgłosić ten fakt Ministrowi. Zgłoszenia można dokonać telefonicznie, dzwoniąc pod numer 22 182 22 51.

Minister zaleca, aby w przypadku zakończenia korzystania z danego urządzenia mobilnego przez Użytkownika – przed przekazaniem urządzenia osobie trzeciej – usunąć dane z Aplikacji.

Hasło dostępu do Aplikacji nie jest przechowywane poza urządzeniem mobilnym Użytkownika. Minister nie umożliwia odtworzenia hasła dostępu do Aplikacji.

W przypadku utraty tego hasła należy:

1. Usunąć Aplikację z urządzenia mobilnego wraz ze wszystkimi danymi.
2. Ponownie zainstalować i aktywować Aplikację oraz zastrzec stary Certyfikat.

Podanie hasła dostępu do Aplikacji jest wymagane za każdym razem po:

- przerwie w korzystaniu z Aplikacji trwającej minimum 5 (pięć) minut
- uruchomieniu Aplikacji po jej wyłączeniu
- wyłączeniu urządzenia mobilnego.

Trzykrotne wprowadzenie nieprawidłowego hasła będzie powodować czasową blokadę dostępu do Aplikacji.

W przypadku urządzeń mobilnych obsługujących funkcję biometrii, dostęp do Aplikacji możliwy jest przy wykorzystaniu tej funkcji. Skorzystanie z funkcji biometrii nie zwalnia Użytkownika z obowiązku ustawienia hasła dostępu do Aplikacji.

Minister dokłada największych starań, aby zapewnić wysoki poziom bezpieczeństwa teleinformatycznego Aplikacji i danych Użytkowników. Jednak – ze względu na specyfikę technologii informatycznych – w przyszłości może zostać ujawniona podatność Aplikacji na określone zagrożenia. Z tego względu Minister:

- zaleca aktualizację Aplikacji
- wskazuje, że może wydawać publicznie dostępne zalecenia dotyczące zasad bezpieczeństwa związanych z korzystaniem z Aplikacji.

W przypadku wszystkich usług dostępnych w Aplikacji, pobrane dane są przechowywane w zaszyfrowanej formie na urządzeniu mobilnym.

Aplikacja umożliwia wymianę danych z **mWeryfikatorem**. Warunkiem wymiany jest posługiwanie się dwoma urządzeniami mobilnymi o tym samym systemie operacyjnym, tj. Android w wersji 7.0 lub wyższej lub iOS w wersji 13 lub wyższej.

1.4 Dostępność

Aplikacje mObywatel i mWeryfikator można pobrać ze sklepu Google Play (Android) lub ze sklepu App Store (iOS).

1.4.1 Aplikacja mObywatel

Google Play (Android):
https://play.google.com/store/apps/details?id=pl.nask.mobywatel&hl=UK&gl=UK
App Store (iOS):
https://apps.apple.com/pl/app/mobywatel/id1339613469?l=uk

1.4.2 mWeryfikator

Google Play (Android):
https://play.google.com/store/apps/details?id=pl.nask.mweryfikator&hl=uk&gl=UK

App Store (iOS):
https://apps.apple.com/pl/app/mweryfikator/id1350403097?l=uk

2 Opis Aplikacji

2.1 Ogólny opis

Aplikacja to bezpłatna, instalowana dobrowolnie, rządowa, publiczna aplikacja mobilna, dzięki której można uzyskać szybki dostęp do swoich dokumentów. Usługi dostępne w ramach Aplikacji:

- Usługa Diia.pl (Android, iOS)
- Unijny Certyfikat COVID (Android, iOS)
- eRecepta (Android, iOS).

Za pomocą ww. usługmożna:

- okazać swoją tożsamość
- zaprezentować potwierdzenie przyjęcia szczepienia przeciwko wirusowi SARS-CoV-2 i/lub uzyskania negatywnego wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przebyciu choroby COVID-19
- pobrać, przeglądać i realizować recepty wystawione Użytkownikowi
- przekazać w bezpieczny sposób swoje dane zweryfikowanym podmiotom publicznym lub prywatnym w celu skorzystania z oferowanych przez nie usług

Szczegółowe procedury oraz usługi, w których dokument diia.pl może być wykorzystywany do stwierdzania tożsamości obywatela Ukrainy są określone w Rozporządzeniu z dnia 04 kwietnia 2022 roku (Dz.U. z 2022 r. poz 841).

2.2 Opis pozycji menu

Funkcje głównego menu (dla Android):

- **Wyloguj** – wylogowanie Użytkownika z Aplikacji
- **Strona główna** – powrót do głównej strony Aplikacji
- **Historia logowania** – podgląd historii logowania do Aplikacji Użytkownika
- **Pomoc techniczna** – dane kontaktowe do pomocy technicznej
- **Regulamin** – możliwość podglądu regulaminu zaakceptowanego w procesie aktywacji Aplikacji
- **Włącz Bluetooth po zalogowaniu** – aktywowanie funkcji spowoduje uruchamianie modułu komunikacji Bluetooth od razu zalogowaniu do Aplikacji. Włączenie Bluetooth po zalogowaniu przyspieszy proces wymiany danych z innymi Użytkownikami
- **Zmień hasło** – możliwość zmiany hasła do Aplikacji
- **Zmień PIN** – możliwość zmiany PIN, jeśli aktywowana była funkcja logowania biometrycznego
- **Włącz (lub wyłącz) logowanie biometryczne z PIN-em** – aktywowanie lub deaktywowanie logowania danymi biometrycznymi z kodem PIN
- **Dezaktywuj aplikację** – usuwanie danych z Aplikacji oraz unieważnienie Certyfikatów Usług. Jeśli nie ma połączenia z Internetem, usuwane są tylko dane z Aplikacji. Użytkownik jest o tym informowany i może anulować dezaktywację.

Funkcje głównego menu (dla iOS):

- **Wyloguj** – wylogowanie Użytkownika z Aplikacji
- **Strona główna** – powrót do głównej strony Aplikacji
- **Aktualizuj dane** – aktualizacja danych dotyczących tożsamości

- **Wydane certyfikaty** – informacja o wydanych Certyfikatach dla Użytkownika, wraz z informacją o ważności Certyfikatów oraz urządzeniach, na których są Certyfikaty
- **Historia aktywności** – podgląd historii aktywności Użytkownika Aplikacji
- **Pomoc techniczna** – dane kontaktowe do pomocy technicznej
- **Regulamin** – możliwość podglądu regulaminu zaakceptowanego w procesie aktywacji Aplikacji
- **Zmień hasło** – możliwość zmiany hasła do Aplikacji
- **Zmień PIN** – możliwość zmiany PIN, jeśli aktywowana była funkcja logowania TouchID/FaceID
- **Włącz (lub wyłącz) logowanie biometryczne z PIN-em** – aktywowanie lub deaktywowanie logowania z wykorzystaniem TouchID/FaceID z kodem PIN
- **Dezaktywuj aplikację** – usuwanie danych z Aplikacji oraz unieważnienie Certyfikatów Usług. Jeśli nie ma połączenia z Internetem, usuwane są tylko dane z Aplikacji. Użytkownik jest o tym informowany i może anulować dezaktywację.

2.3 Zabezpieczenie logowania z użyciem biometrii i PIN-u

Aplikacja obsługuje logowanie biometryczne. Ten sposób logowania dodatkowo zabezpieczony jest PIN-em. Aby możliwe było użycie tej funkcji wymagane jest aktywowanie co najmniej jednej usługi.

Aby aktywować logowanie biometryczne należy:

- wybrać odpowiednią opcję w głównym menu Aplikacji
- zapoznać się z opisem tej funkcjonalności oraz zaakceptować obniżenie poziomu bezpieczeństwa
- wprowadzić aktualne hasło do Aplikacji
- ustalić PIN
- przyłożyć palec do skanera linii papilarnych na urządzeniu mobilnym, użyć funkcji Face ID lub Face Unlock
- zalogować się do Aplikacji przy użyciu aktywowanej funkcji.

3 Opis mWeryfikator

3.1 Ogólny opis

mWeryfikator jest oprogramowaniem dodatkowym, dzięki któremu możliwe jest w sposób obiektywny i niezależny zweryfikowanie danych przekazywanych przez Aplikację mObywatel.

3.2 Opis pozycji menu

- **Pomoc techniczna** – dane kontaktowe do pomocy technicznej
- **Regulamin** – możliwość podglądu zaakceptowanego w procesie aktywacji mWeryfikatora regulaminu

Ustawienia:

- **Aktualizuj certyfikaty** – Aktualizuje certyfikaty systemowe
- **Włącz Bluetooth po uruchomieniu (tylko dla systemu Android)** – aktywowanie funkcji spowoduje uruchamianie modułu komunikacji Bluetooth od razu po zalogowaniu do mWeryfikatora. Przyspieszy to proces wymiany danych z innymi użytkownikami
- **Dezaktywuj aplikację** – funkcja usuwa dane z aplikacji.

4 Aktywacja Aplikacji

4.1 Aplikacja mObywatel (Android, iOS)

4.1.1 Aby aktywować Aplikacjęnależy:

- pobrać Aplikację ze sklepu Google Play lub App Store
- zapoznać się z regulaminem i zaakceptować go
- zapoznać się z polityką prywatności i zaakceptować ją
- wybrać **Dalej**
- zdefiniować nazwę urządzenia
- ustawić hasło (patrz → 4.1.2); możliwość aktywacji logowania biometrycznego z użyciem Personal Identification Number (PIN)
- wybrać Dodaj dokument
- wyrazić zgodę dla systemu Android lub iOS na używanie zasobów systemowych.

Po zakończeniu aktywacji Aplikacji użytkownik będzie mógł aktywować poszczególne Usługi.

4.1.2 Ustawienie hasła

Dane dostępne w Aplikacji są zabezpieczone hasłem ustawianym przez Użytkownika w procesie aktywacji. Hasło musi mieć minimum 8 znaków i co najmniej:

- jedną dużą
- jedną małą literę
- jedną cyfrę
- jeden znak specjalny.

4.2 mWeryfikator (Android, iOS)

4.2.1 Aktywacja

Aby aktywować oprogramowanie dodatkowe mWeryfikator, należy:

- pobrać mWeryfikator ze sklepu Google Play lub App Store
- zapoznać się z regulaminem i zaakceptować go
- zapoznać się z polityką prywatności i zaakceptować ją
- wybrać **Dalej**
- zdefiniować nazwę urządzenia
- wybrać **Dalej.**

Po wykonaniu powyższych czynności dodatkowo zostanie automatycznie wydany Certyfikat systemu mObywatel.

5 Aktywacja usług

5.1 Usługa Diia.pl (Android, iOS)

5.1.1 Aktywacja usługi

- Uruchomić Aplikację i zalogować się do niej (patrz → 4)
- zapoznać się z regulaminem Aplikacji
- zapoznać się z regulaminem Usługi Diia.pl
- zapoznać się z polityką prywatności
- wybrać **Dalej**
- wyrazić zgodę dla systemu Android lub iOS na używanie zasobów systemowych
- wybrać **Dalej**
- zdefiniować nazwę urządzenia
- wybrać **Dalej**
- ustawić hasło (patrz → 4.1.2); możliwość aktywacji logowania biometrycznego z użyciem Personal Identification Number (PIN)
- wybrać **Dalej**
- potwierdzić tożsamość przy pomocy Profilu zaufanego
- wybrać **Autoryzuj**
- zalogować się do Profilu zaufanego
- wprowadzić kod autoryzacyjny przesłany przez SMS.

5.1.2 Potwierdzenie tożsamości

Do aktywacji Usługi Diia.pl potrzebne jest potwierdzenie tożsamości. Do aktywacji usługi oraz potwierdzenia tożsamości niezbędne jest posiadanie profilu zaufanego.

Do potwierdzenia tożsamości Użytkownika przy użyciu Profilu zaufanego, pobrania Certyfikatu oraz pobrania danych z Rejestru niezbędne jest połączenie z Internetem.

5.1.3 Wydanie Certyfikatu

Po pobraniu danych z Rejestru automatycznie jest tworzony i pobierany Certyfikat kryptograficzny potwierdzający autentyczność pobranych danych. Certyfikat przypisany jest do Użytkownika i urządzenia mobilnego, którym posługuje się Użytkownik.

W celu utworzenia Certyfikatu i zarządzania Certyfikatami Minister przetwarza dane osobowe Użytkownika oraz nazwę urządzenia, dla którego Certyfikat został wydany. Ważność Certyfikatu jest ograniczona w czasie i wynosi jeden (1) rok od daty aktywacji Usługi.

Z Usługą Diia.pl automatycznie dodawana jest Usługa eRecepta.

5.2 Unijny Certyfikat COVID (Android, iOS)

Usługa Unijny Certyfikat COVID umożliwia prezentację potwierdzenia przyjęcia szczepienia przeciwko wirusowi SARS-CoV-2 i/lub uzyskania negatywnego wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przebyciu choroby COVID-19.

Unijny Certyfikat COVID prezentuje wszystkie kody QR otrzymane w ramach szczepienia podstawowego przeciwko COVID-19 oraz kody otrzymane w ramach dawki dodatkowej. Kody można pobrać pod warunkiem prawidłowego zarejestrowania szczepienia przez punkt szczepień.

5.2.1 Aktywacja usługi (dla Użytkowników, którzy posiadają Usługę mObywatel)

Aby aktywować Unijny Certyfikat COVID należy:

- uruchomić Aplikację mObywatel i zalogować się do niej
- wybrać opcję **Dodaj dokument**, z listy dostępnych dokumentów wybrać Unijny Certyfikat COVID
- zapoznać się z regulaminem Unijnego Certyfikatu COVID i zaakceptować go.

Jeżeli Użytkownik posiada zaświadczenie o szczepieniu przeciwko wirusowi SARS-CoV-2 i/lub uzyskał negatywny wynik testu na obecność wirusa SARS-Cov-2 i/lub informację o przebyciu choroby COVID-19 w systemie Internetowe Konto Pacjenta, odpowiednie zaświadczenie zostanie automatycznie wyświetlone na ekranie urządzenia Użytkownika.

5.2.2 Aktywacja usługi (dla Użytkowników, którzy nie posiadają Usługi mObywatel)

Aby aktywować Usługę Unijny Certyfikat COVID, należy:

- uruchomić Aplikację
- aktywować aplikację
- wybrać **Dodaj swój pierwszy dokument**, następnie wskazać Unijny Certyfikat COVID
- zapoznać się z regulaminem Usługi mObywatel i zaakceptować go
- zapoznać się z regulaminem Unijny Certyfikat COVID i zaakceptować go
- wybrać sposób potwierdzenia tożsamości środkiem identyfikacji elektronicznej wydanym w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl, np. Profil Zaufany, e-dowód, wybrany bank)
- potwierdzić tożsamość (patrz → **Błąd! Nie można odnaleźć źródła odwołania.**).

Po pozytywnym procesie uwierzytelnienia automatycznie zostanie dodana Usługa mObywatel oraz Unijny Certyfikat COVID (jeżeli Użytkownik posiada zaświadczenie o szczepieniu przeciwko wirusowi SARS-CoV-2 i/lub uzyskał negatywny wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przebyciu choroby COVID-19 w systemie IKP).

5.2.3 Weryfikacja poprawności kodu Usługi Unijny Certyfikat COVID

Poprawność kodu QR pobranego z systemu IKP do Usługi Unijny Certyfikat COVID można zweryfikować korzystając z aplikacji Skaner Certyfikatów COVID wydanej przez Centrum e-Zdrowia.

- Skaner Certyfikatów COVID (Android): https://play.google.com/store/apps/details?id=pl.gov.cez.sws

- Skaner Certyfikatów COVID (iOS): https://apps.apple.com/pl/app/ucc-unijny-certyfikat-covid/id1544064914

5.3 Usługa eRecepta (Android, iOS)

Usługa eRecepta aktywowana jest automatycznie przy aktywacji Usługi mObywatel (patrz → 5.1).

5.3.1 Warunki aktywacji usługi

Aby Użytkownik mógł korzystać z Usługi eRecepta, musi posiadać:

- ważną Usługę mObywatel
- konto w Internetowym Koncie Pacjenta (https://pacjent.gov.pl).

5.3.2 Aktywacja usługi

Aby aktywować usługę należy:

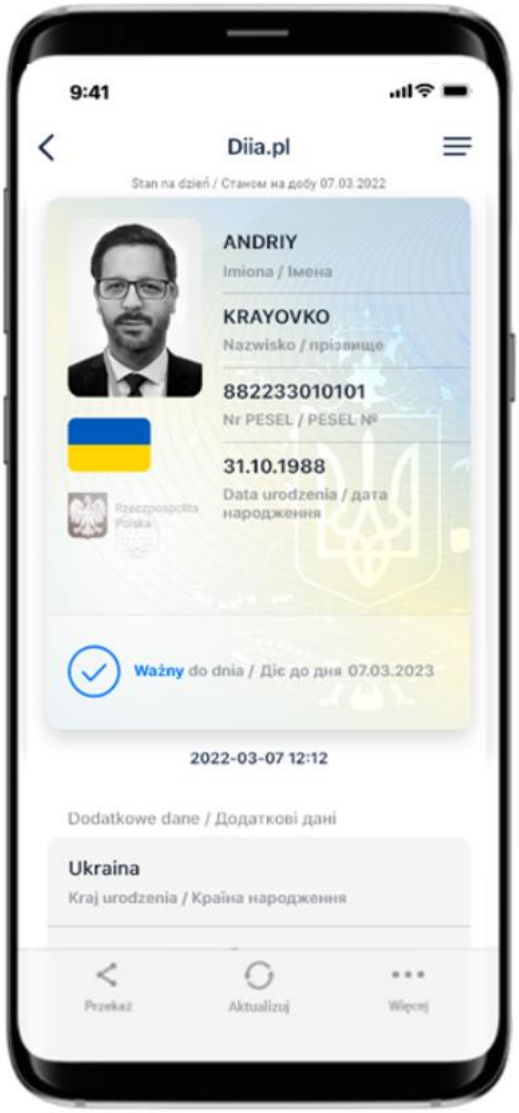
- aktywować Usługę mObywatel (patrz → 5.1)
- zaakceptować regulamin Internetowego Konta Pacjenta.

Poniżej przedstawiono ekran z komunikatem akceptacji Internetowego Konta Pacjenta.

6 Funkcje dostępne w ramach Usługi Diia.pl (Android, iOS)

6.1 Okazanie tożsamości w Aplikacji

Użytkownik może okazać drugiej osobie swoje dane osobowe na ekranie urządzenia mobilnego, którym się posługuje. Funkcja dostępna jest po wybraniu ikony Usługi Diia.pl z ekranu startowego Aplikacji. Poniżej przedstawiono ekran prezentacji danych Usługi Diia.pl:



Podstawowy zakres prezentowanych danych:

- imiona
- nazwisko
- zdjęcie
- nr PESEL
- data urodzenia
- data ważności

Rozszerzony zakres prezentowanych danych:

- kraj urodzenia
- miejsce urodzeniaobywatelstwo

6.2 Przekaż

6.2.1 Przekazanie danych osobie weryfikującej tożsamość

Aby przekazać dane osobie weryfikującej Twoją tożsamość w ramach Usługi Diia.pl, należy:

- uruchomić Usługę Diia.pl

- wybrać funkcję **Przekaż**, a następnie wybrać przekaż **Osobie weryfikującej Twoją tożsamość**. Wyświetli się okno informujące jakie dane osobowe przekazujesz, komu i w jakim celu
- zaakceptować przekazanie danych
- na ekranie urządzenia wyświetli się QR kod — należy go udostępnić osobie weryfikującej Twoją tożsamość do zeskanowania
- wyświetli się komunikat z prośbą o potwierdzenie celu pobrania danych.

Aplikacja przekaże dane do mWeryfikatora — imiona i nazwisko oraz zdjęcie w niskiej rozdzielczości. Wyświetli się również status Certyfikatu, który gwarantuje bezpieczeństwo i aktualność danych.

Wyświetlone dane można dodatkowo zweryfikować online.

Przy wymianie danych pomiędzy różnymi systemami operacyjnymi Aplikacja może poprosić również o zeskanowanie kodu wyświetlonego na urządzeniu z mWeryfikatorem, a następnie o zeskanowanie serii kodów QR.

Aplikacja zależnie od rodzaju systemu operacyjnego używanego na urządzeniu weryfikowanym i urządzeniu weryfikującym, dobierze odpowiednią metodę przekazania danych.

a) w przypadku przekazania danych pomiędzy urządzeniami z systemem Android: Bluetooth.
b) w przypadku przekazania danych pomiędzy urządzeniami z systemem iOS: Bluetooth i/lub WiFi.
c) w przypadku przekazania danych pomiędzy urządzeniami z systemami Android i iOS: seria kodów QR.

Aplikacja mObywatel przekaże dane do mWeryfikatora.

6.2.2 Przekazanie danych do instytucji lub firmy

Użytkownik może przekazać online swoje dane podmiotom publicznym lub prywatnym (instytucji) w celu skorzystania z oferowanych przez nie usług. Przekazanie danych odbywa się tylko do zweryfikowanych w systemie mObywatel instytucji.

Aby przekazać dane do instytucji należy:

- uruchomić Usługę mObywatel
- wybrać funkcję **Przekaż**, a następnie wybrać przekaż **Instytucji lub firmie**
- zeskanować kod QR lub skopiować do schowka (kod QR dostępny online lub offline). Wyświetli się informacją jakie dane, jakiej instytucji i w jakim celu zostaną przekazane
- potwierdzić przekazanie danych wskazanej instytucji.

Operacje wykonywane podczas przekazywania danych są szyfrowane kryptograficzne, co gwarantuje bezpieczeństwo procesu.

Przy wymianie danych pomiędzy różnymi systemami operacyjnymi Aplikacja może poprosić również o zeskanowanie kodu wyświetlonego na urządzeniu z mWeryfikatorem, a następnie o zeskanowanie serii kodów QR.

Aplikacja zależnie od rodzaju systemu operacyjnego używanego na urządzeniu weryfikowanym i urządzeniu weryfikującym, dobierze odpowiednią metodę przekazania danych.

a) w przypadku przekazania danych pomiędzy urządzeniami z systemem Android: Bluetooth.

b) w przypadku przekazania danych pomiędzy urządzeniami z systemem iOS: Bluetooth i/lub WiFi.
c) w przypadku przekazania danych pomiędzy urządzeniami z systemami Android i iOS: seria kodów QR.

6.3 Aktualizuj

Funkcja **Aktualizuj** umożliwia pobranie aktualnych danych Użytkownika.

Aktualizowanie odbywa się na podstawie pobrania danych (logowania się) z wykorzystaniem wydanego wcześniej Profilu zaufanego.

6.4 Menu Więcej

- **Aktualizuj certyfikaty** – umożliwia automatyczne aktualizowanie Certyfikatów
- **Wydane certyfikaty** – umożliwia podgląd wydanych użytkownikowi Certyfikatów wraz ze statusem ważności
- **Historia** – umożliwia zapoznanie się z historią weryfikacji danych osobowych za pomocą mWeryfikatora zawierającą: identyfikator użytkownika oraz datę i czas przekazania danych. Funkcja „Historia" przechowuje dane, o których mowa powyżej, przez jeden (1) rok od daty ich zapisania w zakresie danych wskazanych powyżej.
- **Historia aktywności** – umożliwia podgląd historii pobrań danych oraz wydanych Certyfikatów
- **Regulamin** - wyświetla regulamin zaakceptowany przez Użytkownika dla Usługi Diia.pl
- **Usuń Usługę Diia.pl** - unieważnia wydane Certyfikaty i usuwa dokument.

Aplikacja może być aktywowana maksymalnie na 3 urządzeniach.

7 Funkcje dostępne w ramach Unijny Certyfikat Covid (Android, iOS)

7.1 Przeglądanie certyfikatów

Po aktywowaniu Usługi Unijny Certyfikat Covid (patrz → **Błąd! Nie można odnaleźć źródła odwołania.**2) i wybraniu na ekranie głównym aplikacji mObywatel ikony podpisanej Unijny Certyfikat Covid, automatycznie pobierana jest lista certyfikatów przypisanych do danego Użytkownika Aplikacji.

Jeżeli Użytkownik nie posiada certyfikatów dotyczących COVID-19, na ekranie pojawi się komunikat o braku certyfikatów dotyczących COVID-19. (Jeżeli zostałeś/aś niedawno zaszczepiony/a i certyfikat się nie wyświetla, naciśnij **Aktualizuj dane** na dole ekranu.)

Jeżeli Użytkownik posiada tylko jeden certyfikat (jedno zaświadczenie o szczepieniu przeciwko wirusowi SARS-CoV-2 i/lub uzyskał negatywny wyniku testu na obecność wirusa SARS-Cov-2 i/lub informację o przejściu choroby COVID-19), po wybraniu z ekranu głównego Aplikacji kafelka Unijny Certyfikat Covid, zobaczy od razu ekran z kodem QR danego certyfikatu.

Jeżeli Użytkownik posiada wiele certyfikatów, najnowszy dostępny certyfikat zostanie wyświetlony na górze listy dostępnych certyfikatów.

Pierwszy ekran certyfikatu wyświetlony jest w dwóch językach: polskim i angielskim. Na kolejnym ekranie istnieje możliwość wyboru preferencyjnego języka, w którym wyświetlany będzie certyfikat.

7.2 Prezentacja kodu QR

Po wybraniu danego certyfikatu, na ekranie znajdują się następujące dane:

- nazwa dokumentu (usługi)
- zdjęcie pochodzące z Usługi mObywatel
- imię (imiona)
- nazwisko
- data urodzenia
- unikalny identyfikator certyfikatu
- kod QR zawierający zaszyfrowane dane przekazane z systemu SI CEZ/IKP
- informacja o ważności kodu QR.

Dane dodatkowe w rozwijanej liście:

Dane zawarte w certyfikacie potwierdzającym szczepienie ochronne przeciw COVID-19:

- rodzaj certyfikatu
- nazwa choroby lub czynnik chorobotwórczy: COVID-19 (co oznacza również SARS-CoV-2 lub jeden z jego wariantów)
- szczepionka / profilaktyka
- produkt leczniczy
- producent dopuszczający szczepionkę do obrotu
- liczba w serii szczepień / dawek
- data szczepienia, wskazująca datę ostatniej otrzymanej dawki
- państwo członkowskie
- wystawca certyfikatu.

Dane zawarte w certyfikacje zawierającym wynik testu na obecność wirusa SARS-Cov-2:

- rodzaj certyfikatu
- nazwa choroby lub czynnik chorobotwórczy: COVID-19 (co oznacza również SARS-CoV-2 lub jeden z jego wariantów)
- rodzaj testu
- nazwa testu (opcjonalnie w przypadku testu NAAT)
- producent testu (nieobowiązkowo w przypadku testu NAAT)
- data i godzina pobrania próbki do badań
- wynik testu
- ośrodek testowy lub placówka (nieobowiązkowe w przypadku szybkiego testu antygenowego)
- państwo członkowskie
- wystawca certyfikatu.

Dane zawarte w certyfikacje krajowym zawierającym wynik testu na obecność wirusa SARS-Cov-2:

- rodzaj certyfikatu

- nazwa choroby lub czynnik chorobotwórczy: COVID-19 (co oznacza również SARS-CoV-2 lub jeden z jego wariantów)
- data pierwszego pozytywnego testu
- data, od której jest ważny certyfikat
- państwo członkowskie
- wystawca certyfikatu.

Dane zawarte w potwierdzeniu przebycia choroby COVID-19:

- rodzaj certyfikatu
- nazwa choroby lub czynnik chorobotwórczy, z którego obywatel wyzdrowiał: COVID-19 (czyli również SARS-CoV-2 lub jeden z jego wariantów)
- data pierwszego pozytywnego testu
- certyfikat ważny od
- państwo członkowskie, w którym wykonano test
- wystawca certyfikatu.

7.3 Funkcje menu dolnego Unijnego Certyfikatu Covid

- **mObywatel** - kliknięcie na ikonkę „mObywatel” pozwala na wyświetlenie Usługi mObywatel w celu potwierdzenia swoich danych osobowych
- **Aktualizuj** - kliknięcie na ikonkę „Aktualizuj” powoduje ponowne pobranie danych (kodu QR) potwierdzających przyjęcie szczepienia wraz z datą jego ważności i/lub uzyskania negatywnego wyniku testu na obecność wirusa SARS-Cov-2 i/lub informacji o przebytej chorobie COVID-19
- **English** - kliknięcie na ikonkę „English” powoduje zmianę języka z języka polskiego na język angielski i odwrotnie
- **Więcej** – kliknięcie na ikonkę „Więcej” powoduje wyświetlenie dodatkowego menu (patrz 7.4).

7.4 Menu Więcej

- **Regulamin** Unijnego Certyfikatu COVID – wyświetla regulamin usługi zaakceptowany przez Użytkownika w trakcie jej aktywacji
- **Usuń** Unijny Certyfikat Covid – usuwa dokument.

8 Funkcje dostępne w ramach Usługi eRecepta (Android, iOS)

8.1 Przeglądanie niezrealizowanych eRecept

Po utworzeniu konta w Internetowym Koncie Pacjenta, Aplikacja automatycznie pobiera listę niezrealizowanych recept. Na początku wyświetlane są recepty właściciela Usługi mObywatel, a następnie recepty jego podopiecznych oraz osób, które udzieliły mu pełnomocnictwa. Udzielenie pełnomocnictwa możliwe jest z wykorzystaniem funkcjonalności m.in. udostępnianych z poziomu Internetowego Konta Pacjenta (https://pacjent.gov.pl).

8.2 Realizacja eRecept

Wybranie konkretnej recepty powoduje pobranie szczegółów danej recepty i jej wyświetlenie w Aplikacji. Po wyborze recepty, Aplikacja wyświetli jej dane szczegółowe, w tym informacje o lekach i statusie recepty.

Wyświetlenie szczegółów recepty daje możliwość jej realizacji online na dwa możliwe sposoby:

- podanie numeru PESEL osoby, na którą wystawiona została recepta wraz z kodem wyświetlonym pod kodem QR
- zeskanowanie przez pracownika apteki kodu QR.

W przypadku gdy apteka nie ma połączenia online z system P1 eZdrowie, możliwe jest zrealizowanie recepty w trybie off-line. W tym celu należy użyć przycisku **Pobierz PDF**, który umożliwia pobranie wydruku informacyjnego zawierającego kod, po zeskanowaniu którego pracownik apteki będzie posiadał wszystkie niezbędne informacje umożliwiające realizację recepty.

9 Funkcje dostępne w ramach mWeryfikatora

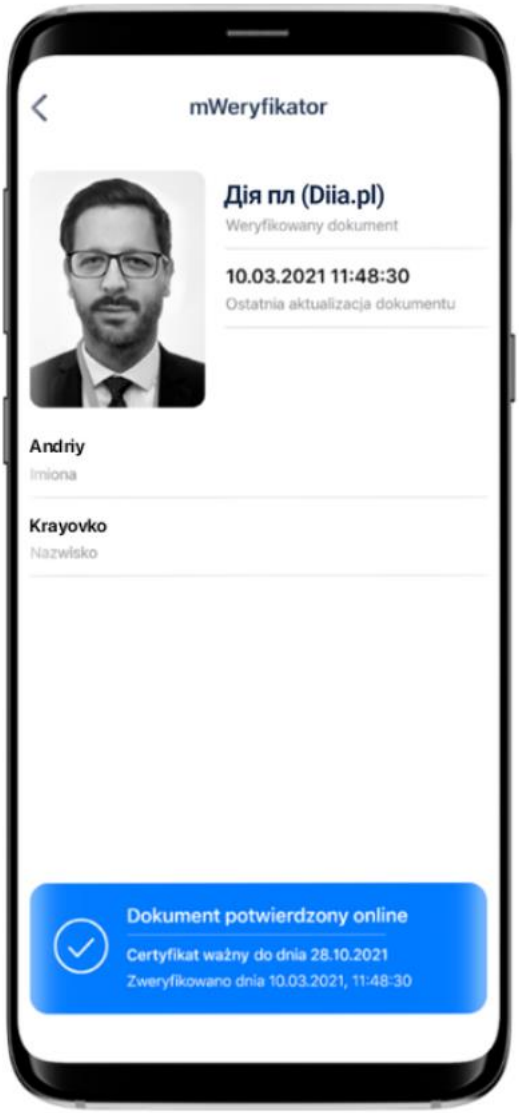
9.1 Sprawdzenie danych

Aby sprawdzić dane Użytkownika posługującego się Aplikacją należy:

- uruchomić mWeryfikatora i wybrać ikonę aparatu z ekranu startowego (patrz ilustracja poniżej)
- Użytkownik Aplikacji wybiera usługę Diia.pl, w ramach której decyduje się udostępnić dane do weryfikacji
- Użytkownik Aplikacji, wybiera funkcję **Osobie weryfikującej Twoją tożsamość**, a następnie okazuje wygenerowany kod QR
- użytkownik mWeryfikatora odczytuje udostępniony kod QR
- Użytkownik Aplikacji potwierdza chęć przekazania danych na swoim urządzeniu mobilnym
- nawiązywane jest połączenie pomiędzy urządzeniami i następuje przekazanie danych do mWeryfikatora. Dane Użytkownika Aplikacji wyświetlane są na urządzeniu użytkownika mWeryfikatora.

9.2 Weryfikacja danych z Usługi Diia.pl w Aplikacji mObywatel

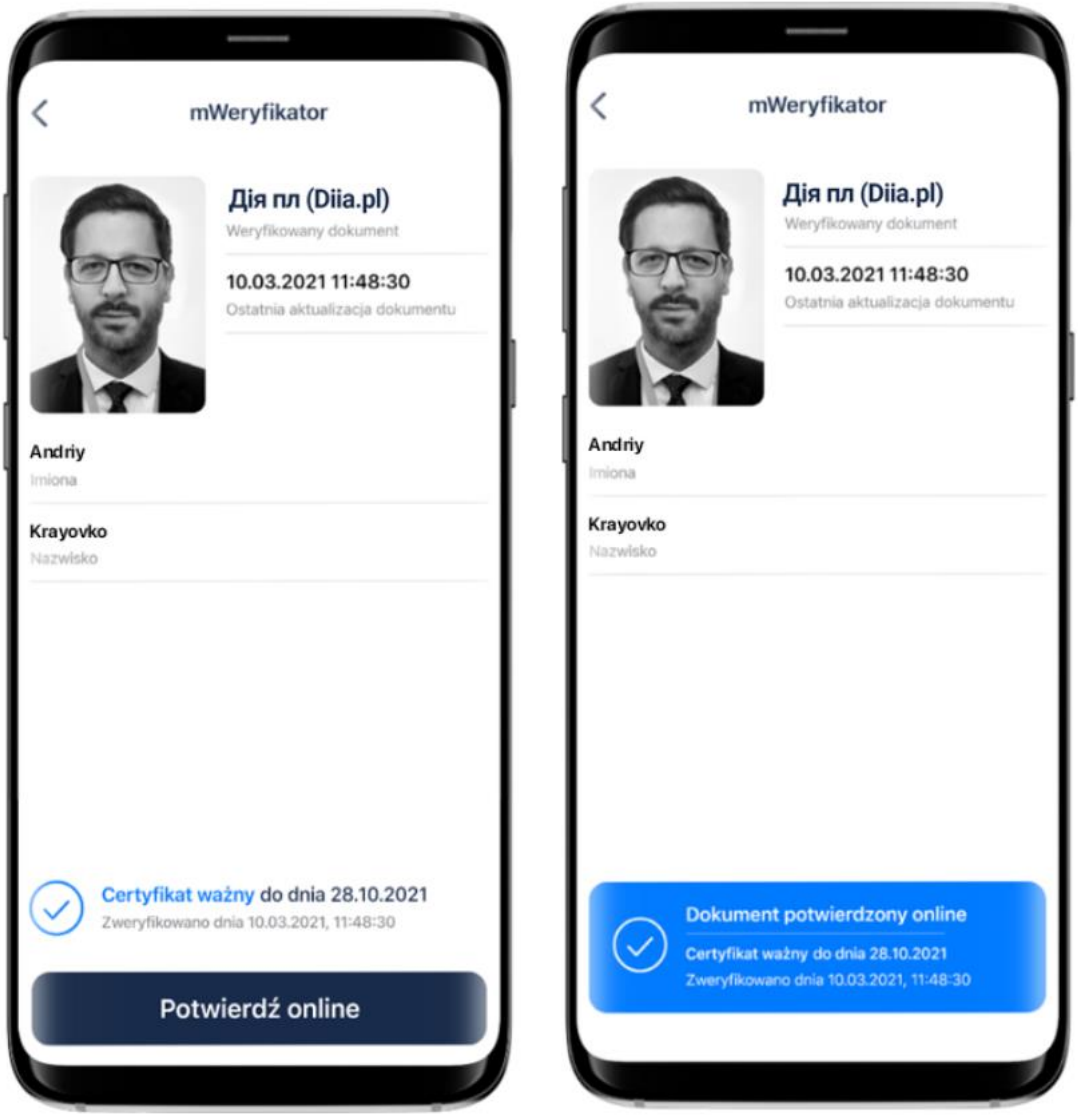
Po prawidłowym zakończeniu elektronicznej weryfikacji danych Użytkownika Aplikacji żadne jego dane nie są zapisywane na urządzeniu użytkownika mWeryfikatora. Zakres weryfikowanych danych Usługi mObywatel przedstawiono na ilustracji poniżej:



Po wyjściu z ekranu wyświetlania wyświetlone dane są usuwane z urządzenia użytkownika mWeryfikatora.

9.2.1 Weryfikacja aktualności Certyfikatu

Weryfikacja aktualności Certyfikatu Użytkownika Aplikacji w ramach Usługi Diia.pl wymaga aktywnego połączenia internetowego. Aby zweryfikować aktualność Certyfikatu takiej osoby, należy wybrać funkcję **Weryfikuj** (niebieska ikona).



Powyższy przykład pokazuje dokument przed weryfikacją (po lewej) i po weryfikacji (po prawej). Przedstawiono wynik weryfikacji pozytywny.

9.2.2 Zakres prezentowanych danych

Przy korzystaniu z funkcji elektronicznej weryfikacji danych osobowych wyświetlane są następujące dane Użytkownika Aplikacji w ramach Usługi Diia.pl:

- imiona
- nazwisko
- zdjęcie o zredukowanej jakości
- data wydania danych
- data i godzina wymiany danych
- status Certyfikatu.

10 Ochrona prywatności i bezpieczeństwo

10.1 Zabezpieczenie hasłem lub biometrią z PIN-em

Dostęp do danych przechowywanych w Aplikacji mObywatel jest zabezpieczony hasłem ustawianym w procesie jej aktywacji. Hasło musi spełniać określone wymagania zgodnie z punktem 4.1.2.

Dodatkowo, Aplikacja mObywatel obsługuje logowanie biometryczne. Ten sposób logowania dodatkowo zabezpieczony jest PIN-em. Sposób logowania biometrycznego z PIN-em opisany został w punkcie .

10.2 Ochrona danych w telefonie

Dane pobrane i przechowywane w urządzeniu mobilnym Użytkownika w procesie aktywacji usługi są szyfrowane, aby dostęp do nich nie był możliwy dla osób trzecich. Dostęp do danych jest możliwy wyłącznie po podaniu hasła dostępu, które jest ustalane w procesie aktywacji Aplikacji.

10.3 Liczba urządzeń

Użytkownik może aktywować Usługę Diia.pl i pobrać dane z Rejestru na nie więcej niż trzech urządzeniach mobilnych. Na jednym urządzeniu mobilnym można aktywować Usługę Diia.pl oraz pobrać dane z Rejestru tylko jednego Użytkownika.

Historia weryfikacji przez mWeryfikatora jest dostępna w Aplikacji przez 12 miesięcy. mWeryfikator nie umożliwia zapisania danych Użytkownika Aplikacji, którego dane zostały zweryfikowane.

10.4 Eksport/import danych, zrzuty ekranów

Poza funkcjami elektronicznego przekazania danych oraz elektronicznej weryfikacji danych osobowych Aplikacja nie oferuje funkcji eksportu ani importu danych.

Aplikacja mObywatel oraz mWeryfikator dla systemu Android blokują możliwość wykonywania zrzutów ekranów, tzw. screen shot'ów.

10.5 Zakres danych przekazywanych do weryfikacji

Przy wymianie danych z innym Użytkownikiem, przekazywane jest zdjęcie Użytkownika Aplikacji o zredukowanej jakości oraz dodawany jest znak wodny.

Przy weryfikacji danych przez innego Użytkownika, ograniczane są dane przekazywane do weryfikacji:

Dla Usługi Diia.pl:

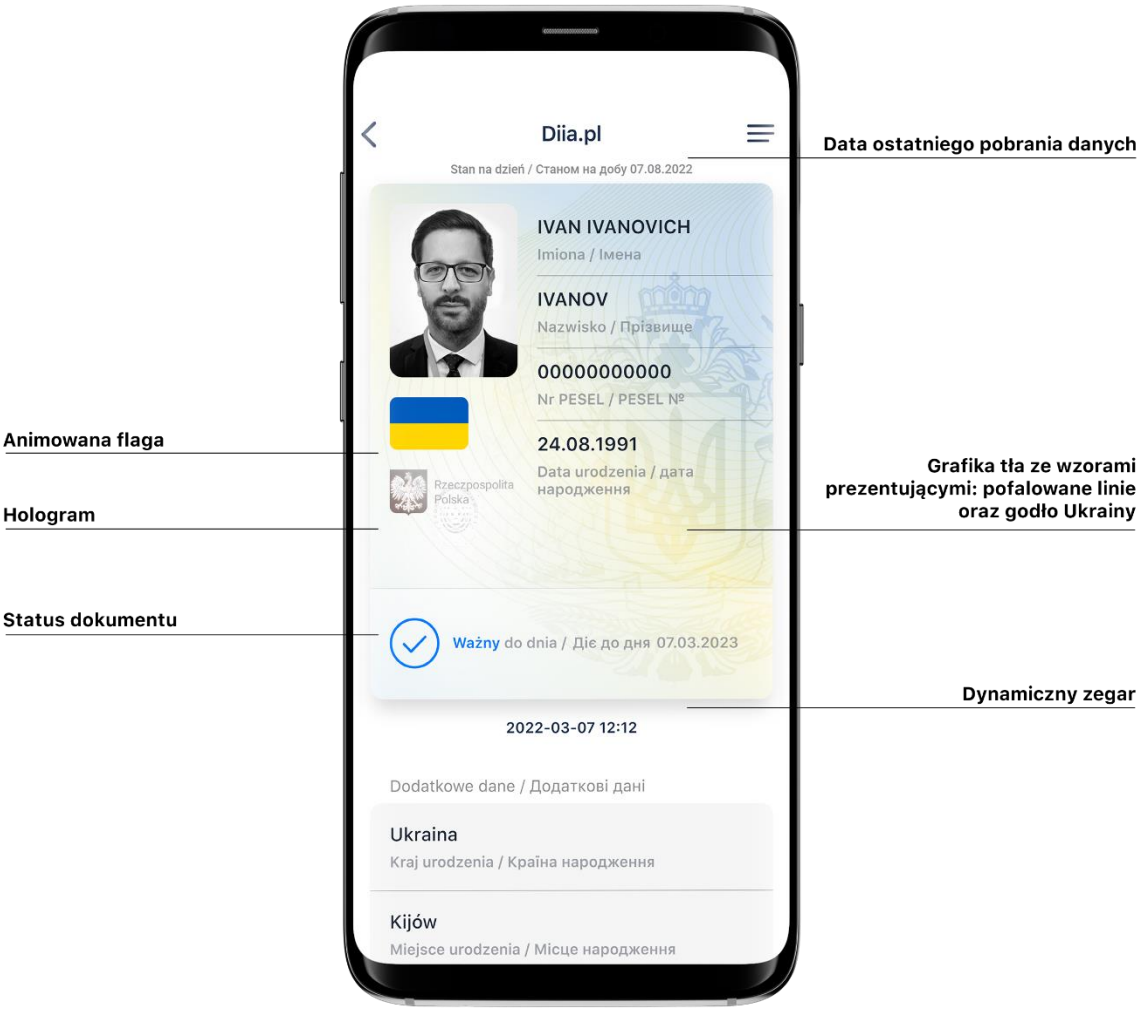
- imiona
- nazwisko
- zdjęcie o zredukowanej jakości.

10.6 Zabezpieczenia wizualne

10.6.1 Zabezpieczenia wizualne Usługi Diia.pl

Dane Usługi Diia.pl w Aplikacji są wyświetlane wraz z następującymi zabezpieczeniami wizualnymi:

- **Element dynamiczny** (animowana flaga) – ruchomy element graficzny, prezentujący niebiesko-żółtą flagę
- **Hologram** – element graficzny o zmiennej kolorystyce, uzależnionej od kąta pochylenia urządzenia mobilnego, w kształcie odpowiadającym godłu Rzeczypospolitej Polskiej
- **Status dokumentu** – data ważności dokumentu
- **Stan na dzień** - data ostatniego pobrania lub aktualizacji danych.)
- **Gilosz** – grafika tła ze wzorami prezentującymi: pofalowane linie, cyfry, napis RP, grafikę przypominającą geograficzny obrys Polski
- **Dynamiczny zegar** – zegar pokazujący aktualną datę i godzinę.



10.6.2 Zabezpieczenia wizualne Usługi Unijny Certyfikat Covid

Dane Unijnego Certyfikatu Covid w Aplikacji są wyświetlane wraz z następującymi zabezpieczeniami wizualnymi:

- **Element dynamiczny (animowana flaga)** - ruchomy element graficzny, prezentujący niebieską flagę z dwunastoma złotymi gwiazdami i skrótem „PL”
- **Dynamiczny zegar** – zegar pokazujący aktualną datę i czas w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z biegiem czasu. Potwierdza, że okazywany dokument prezentowany jest w Aplikacji
- **Termin ważności** kodu QR – data, do której kod będzie ważny, jeśli wcześniej niezostanie unieważniony.

10.7 Certyfikat

Certyfikat jest narzędziem kryptograficznym wykorzystywanym do potwierdzenia integralności i pochodzenia danych dokumentu elektronicznego.

Wygenerowany dokument jest zaszyfrowany i podpisany certyfikatem Ministra Cyfryzacji, który potwierdza autentyczność dokumentu.

W procesie pobierania danych Użytkownika, generowany jest dodatkowo jego indywidualny certyfikat, wykorzystywany do uwierzytelniania komunikacji pomiędzy urządzeniem mobilnym a centralnym rejestrem lub Aplikacją weryfikującą autentyczność dokumentu.

Dla każdej usługi wydawany jest osobny Certyfikat.

10.8 mWeryfikator

mWeryfikator jest oprogramowaniem dodatkowym, dzięki któremu możliwe jest, w sposób obiektywny i niezależny, zweryfikowanie danych przekazywanych przez Aplikację.

mWeryfikator nie pozwala na weryfikację poprawności kodu na karcie głównej Usługi Karta Dużej Rodziny.

11 Metody weryfikacji usługi w Aplikacji

11.1 Metody weryfikacji – ogólne

Sprawdzenie autentyczności Aplikacji i dostępnych dokumentów może być dokonane z wykorzystaniem następujących metod weryfikacji:

11.1.1 Weryfikacja wizualna

Weryfikacja wizualna ma na celu sprawdzenie dokumentu elektronicznego w analogiczny sposób jak przy weryfikacji wzrokowej tradycyjnego dokumentu.

Okazanie dokumentu elektronicznego osobie weryfikującej dokonywane jest na ekranie urządzeniu mobilnym.

Elementy graficzne dokumentu elektronicznego prezentowanego w Aplikacji podlegające weryfikacji:

- **Hologram** – element graficzny o kolorystyce zmieniającej się zależnie od kąta pochylenia urządzenia mobilnego, w kształcie odpowiadającym godłu Rzeczypospolitej Polskiej
- **Element dynamiczny** (animowana flaga) – ruchomy element graficzny, prezentujący niebiesko-żółtą flagę
- **Status dokumentu** – data ważności Certyfikatu
- **Stan na dzień**- data ostatniego pobrania lub aktualizacji danych
- **Gilosz** – grafika tła ze wzorami prezentującymi herb Ukrainy
- **Dynamiczny zegar** – zegar pokazujący aktualną datę i godzinę
- **Tło**– każdy dokument posiada unikalne tło w postaci znaku wodnego lub jednolitej grafiki przypisanej do konkretnego dokumentu.

11.1.2 Weryfikacja funkcjonalna

Weryfikacja funkcjonalna ma na celu weryfikację autentyczności Aplikacji lub dokumentów elektronicznych na podstawie prezentacji funkcjonalności Aplikacji. Jest to dodatkowa weryfikacja, której nie można wykonać przy sprawdzeniu tradycyjnego dokumentu. Weryfikacja polega na wykonaniu akcji lub na okazanym dokumencie elektronicznym, np.:

- wejście w funkcję **Przekaż** w dolnym menu, następnie wybranie i akceptacja przekazania danych osobie weryfikującej Twoją tożsamość. Pojawi się ekran z kodem QR oraz elementami graficznymi do weryfikacji: hologram i pulsująca flaga
- sprawdzenie poprawności Certyfikatu poprzez wejście w dolnym menu **Więcej → Wydane certyfikaty** a następnie wybranie ważnego certyfikatu z niebieską flagą. Pojawią się informacje dot. certyfikatu między innymi: Ważny od, Ważny do, Wystawca O=Ministerstwo Cyfryzacji, Status: Ważny/Nieważny
- Aktualizacja danych poprzez ponowne zalogowanie Profilem Zaufanym. W dolnym menu kliknięcie **Więcej → Aktualizuj Dane**.

11.1.3 Weryfikacja kryptograficzna

Dokument elektroniczny jest zaszyfrowany i podpisany Certyfikatem systemu mObywatel, który potwierdza autentyczność dokumentu. Certyfikat jest narzędziem kryptograficznym, wykorzystywanym do potwierdzenia integralności i pochodzenia danych dokumentu elektronicznego.

mWeryfikator służy do potwierdzenia integralności i pochodzenia danych dokumentu elektronicznego (weryfikacja bez połączenia internetowego) oraz do sprawdzenia ważności Certyfikatu (weryfikacja z połączeniem internetowym). Instalacja mWeryfikatora jest bezpłatna i nie wymaga posiadania Profilu Zaufanego. Dane osoby weryfikowanej nie są przechowywane w mWeryfikatorze.

- wybranie funkcji **Przekaż** w dolnym menu
- następnie wybranie funkcji Osobie weryfikującej Twoją tożsamość i **Przekaż**
- akceptacja celu przekazania
- pokazanie do zeskanowania kodu QR osobie weryfikującej
- akceptacja zakresu przekazywanych danych użytkownikowi mWeryfikatora
- użytkownik mWeryfikatora zobaczy na swoim urządzeniu dane Użytkownika — imiona i nazwisko oraz zdjęcie w niskiej rozdzielczości, a także datę weryfikacji

(weryfikacja integralności i pochodzenia danych). Może też sprawdzić ważność Certyfikatu online (z połączeniem internetowym).

11.2 Usługa Diia.pl

11.2.1 Weryfikacja wizualna

Elementy graficzne podlegające weryfikacji:

- **Element dynamiczny** (animowana flaga) – ruchomy element graficzny prezentujący niebiesko-żółtą flagę
- **Hologram** – element graficzny o zmiennej kolorystyce, uzależnionej od kąta pochylenia urządzenia mobilnego, w kształcie odpowiadającym godłu Rzeczpospolitej Polskiej
- **Status dokumentu** – data ważności dokumentu
- **Stan na dzień**- data ostatniego pobrania lub aktualizacji danych
- **Gilosz** – grafika tła ze wzorami prezentującymi: pofalowane linie, cyfry, napisy RP, grafikę przypominającą geograficzny obrys Polski
- **Dynamiczny zegar** – zegar pokazujący aktualną datę i godzinę.

Poniżej przedstawiono wizualizację dokumentu elektronicznego mObywatel.

11.2.2 Weryfikacja funkcjonalna

Wykonanie dowolnej akcji w Aplikacji lub na okazywanym dokumencie tj.:

- wejście w funkcję **Przekaż** w dolnym menu, następnie wybranie i akceptacja przekazania danych osobie weryfikującej Twoją tożsamość. Pojawi się ekran z kodem QR oraz elementami graficznymi do weryfikacji: hologram i pulsująca flaga
- sprawdzenie poprawności Certyfikatu poprzez wejście w dolnym menu **Więcej → Wydane certyfikaty** a następnie wybranie ważnego certyfikatu z niebieską flagą. Pojawią się informacje dot. certyfikatu między innymi: Ważny od, Ważny do, Wystawca O=Ministerstwo Cyfryzacji, Status: Ważny/Nieważny
- Aktualizacja danych poprzez ponowne zalogowanie Profilem Zaufanym. W dolnym menu kliknięcie **Więcej → Aktualizuj Dane**.

11.2.3 Weryfikacja kryptograficzna

Weryfikacja kryptograficzna polega na sprawdzeniu integralności i pochodzenia danych (offline) oraz ważności Certyfikatu (online), przez osobę weryfikującą, za pomocą mWeryfikatora (jego instalacja nie wymaga logowania środkiem identyfikacji elektronicznej wydanym w systemie identyfikacji elektronicznej przyłączonym do Węzła Krajowego (login.gov.pl)). Aby przekazać dane osobie weryfikującej należy wykonać następujące czynności:

- wybranie funkcji **Przekaż** w dolnym menu
- następnie wybranie funkcji Osobie weryfikującej Twoją tożsamość i Przekaż
- akceptacja celu przekazania
- pokazanie do zeskanowania kodu QR osobie weryfikującej

- akceptacja zakresu przekazywanych danych użytkownikowi mWeryfikatora
- użytkownik mWeryfikatora zobaczy na swoim urządzeniu dane Obywatela — imię/imiona i nazwisko oraz zdjęcie w niskiej rozdzielczości, a także datę weryfikacji (weryfikacja integralności i pochodzenia danych). Może też sprawdzić ważność Certyfikatu online (z połączeniem internetowym).

11.3 Dokument elektroniczny Unijny Certyfikat COVID

11.3.1 Weryfikacja wizualna

Elementy graficzne podlegające weryfikacji:

- **Element dynamiczny (animowana flaga)** - ruchomy element graficzny, prezentujący niebieską flagę z dwunastoma złotymi gwiazdami i skrótem „PL”
- **Dynamiczny zegar** – zegar pokazujący aktualną datę i czas w godzinach, minutach i sekundach, zmieniający się dynamicznie wraz z biegiem czasu. Potwierdza, że okazywany dokument prezentowany jest w Aplikacji
- **Termin ważności** kodu QR – data, do której kod będzie ważny, jeśli wcześniej nie zostanie unieważniony.

11.3.2 Weryfikacja funkcjonalna

Wykonanie dowolnej akcji w Aplikacji lub na okazywanym dokumencie tj.:

- Aktualizowanie kodu QR poprzez kliknięcie ikonki **Aktualizuj** w menu na dole ekranu
- przejście do Usługi mObywatel poprzez kliknięcie ikonki **mObywatel** w menu na dole ekranu.

11.3.3 Weryfikacja kryptograficzna

Weryfikacja kryptograficzna Usługi Unijny Certyfikat Covid polega na zeskanowaniu kodu QR przy pomocy dedykowanej aplikacji dostarczanej przez Centrum e-Zdrowia.

Krajowy Certyfikat Ozdrowienia można zweryfikować przy pomocy dedykowanej aplikacji dostarczanej przez Centrum e-Zdrowia, jest nią Skaner Certyfikatów Covid.

Krajowy Certyfikat Ozdrowienia jest ważny jedynie na terenie Polski.

12 Regulaminy

12.1 Regulamin Aplikacji mObywatelUA

Regulamin Aplikacji mObywatelUA iOS	https://www.mobywatel.gov.pl/mobywatel.ios.regulamin.UA.1.0.pdf
Regulamin Aplikacji mObywatelUA Android	https://www.mobywatel.gov.pl/mobywatel.android.regulamin.UA.1.0.pdf

12.2 Regulamin usługi Diia.pl

Regulamin usługi Diia.pl	https://www.mobywatel.gov.pl/mobywatel.diia.pl.regulamin.UA.2.0.0.pdf

12.1 Regulamin usługi Unijny Certyfikat COVID.pl

Regulamin usługi Unijny Certyfikat COVID	https://www.mobywatel.gov.pl/mobywatel.UCC.regulamin.UA.1.0.0.pdf

12.2 Regulamin Aplikacji mWeryfikator

Regulamin Aplikacji mWeryfikator	https://www.mobywatel.gov.pl/mweryfikator.regulamin.7.0.0.pdf

13 Kontakt i pomoc techniczna

13.1 Service Desk dla Aplikacji mObywatel i aplikacji mWeryfikator

(ogólne informacje o Aplikacji, wsparcie techniczne)

tel. +48 22 182 22 51 (w języku ukraińskim)

mobywatel-pomoc@nask.pl

od poniedziałku do piątku, z wyjątkiem świąt, w godzinach 7:00 do 18:00.

Minister zastrzega, że czas pracy Service Desk może ulec zmianie.