Koncepcja

e-Dowód – kontynuacja projektu pl.ID i realizacja projektów powiązanych

Załącznik 2 Opis planowanej funkcjonalności i architektury IT oraz otoczenie prawno-organizacyjne

1. FUNKCJONALNOŚĆ E-DOWODU

1.1. Zastosowania biznesowe e-Dowodu

Planuje się następujące możliwości zastosowania e-Dowodu:

1) **Identyfikacja i uwierzytelnienie** obywatela:
   - do systemów informatycznych on-line (wymagany będzie PIN), dzięki czemu uzyska się dostęp do wszystkich e-usług administracji publicznej na portalach wykorzystujących węzeł krajowy do identyfikacji elektronicznej (węzeł planowany do wdrożenia w 2017 roku)
   - bezpośrednio do systemu informatycznego administracji publicznej i komercyjnej poprzez interfejs z oprogramowaniem odpowiadającym za komunikację z e-Dowodem (o ile dany system zostanie do tego przygotowany; zadanie w gestii opiekunów systemów);
2) **Elektroniczne podpisanie dokumentu** przez obywatela w procesach on-line z administracją publiczną i służbą zdrowia (podpis serwerowy; wymagany będzie PIN do wcześniejszego uwierzytelnienia przed podpisem);
3) **Potwierdzenie obecności obywatela** w procesach z administracją publiczną, służbą zdrowia i innych (bez PIN); właściwie jest to potwierdzenie uczestniczenia e-dowodu w transakcji elektronicznej; możliwe zastosowanie to: uzyskanie dostępu na bramkach w zakładzie pracy, poświadczanie uzyskania przez pacjenta świadczenia medycznego;
4) **Możliwość odczytu danych zawartych warstwie wizualnej z warstwy elektronicznej** – w celu pobrania danych do procesu elektronicznego i w celu podwyższenia poziomu bezpieczeństwa dokumentu (praktycznie niemożliwe podrobienie danych w warstwie elektronicznej); dostęp do danych będzie zabezpieczony przed przypadkowym odczytem;

5) **Możliwość przechowania dodatkowych danych do odczytu** innych niż w warstwie wizualnej do indywidualnego wykorzystania przez obywatela (np. informacje **ICE** (ang. *In Case of Emergency*) – z kim kontaktować się w razie wypadku);

6) **Dokument podróży zgodny z ICAO**[1] (zawierający **cechę biometryczną** – zdjęcie twarzy) umożliwiający automatyczne przekraczanie e-bramek kontroli granicznej na lotniskach UE;

7) **Możliwość zainicjowania kwalifikowanego podpisu serwerowego** od dowolnego dostawcy wybranego przez obywatela (uzależnione od udostępnienia takiej opcji przez poszczególnych dostawców podpisów kwalifikowanych);

8) **Możliwość użycia w przyszłości w Urzędomatach** (ZUS/US/nowe), czyli terminalach samoobsługowych do identyfikacji i uwierzytelnienia w usługach udostępnionych w terminalach (uzależnione od szczegółowych planów rozwoju dotyczących Urzędomatów);

9) **Będzie parę możliwości użycia e-Dowodu**:

   - na komputerze z wewnętrznym albo zewnętrznym **czytnikiem kart bezstykowych** – wykorzystanie w Urzędzie, u świadczeniodawców lub w domu,
   - na **terminalu POS** – wykorzystanie w tych placówkach, które są już wyposażone w terminale (np. Poczta Polska – możliwość potwierdzania odbioru przesyłek poleconych, Urząd/Bank/inna placówka – możliwość potwierdzenia tożsamości); planowane jest też znaczące zwiększenie ilości terminali w wyniku działań Rządu dla promocji obrotu bezgotówkowego,
   - na **smartfonie (urządzeniu mobilnym) z funkcją NFC** (samodzielnie albo w połączeniu z komputerem) – wykorzystanie przez funkcjonariuszy służb i przez obywateli;

10) **Dotychczasowa funkcjonalność dowodu bez warstwy elektronicznej pozostaje bez zmian** – e-Dowód będzie mógł być wykorzystywany w kontaktach z administracją i służbami oraz w sektorze komercyjnym poprzez okazanie bez wykorzystania warstwy elektronicznej.

Przedmiotem analiz była także możliwość połączenia dowodu osobistego z Kartą Specjalisty Medycznego (KSM). Jednak łączenie funkcjonalności Karty Specjalisty Medycznego z elektronicznym dowodem osobistym prowadzi do istotnej komplikacji całego projektu, generując dodatkowe ryzyka dla jego realizacji. Ponadto nie ma obiektywnego uzasadnienia dla włączenia

[1] ICAO - Organizacja Międzynarodowego Lotnictwa Cywilnego wyznaczająca standardy dla dokumentów podróży.

do dowodów funkcjonalności KSM przy pominięciu potrzeb innych grup zawodowych. W przyszłości – po przystosowaniu i integracji rejestrów przechowujących informacje o kwalifikacjach zawodowych, e-Dowód będzie mógł być też kluczem do tych rejestrów i uwierzytelniać zwrócenie odpowiednich danych. Jednakże dopóki brak jest zintegrowanych centralnych rejestrów kwalifikacji, nie jest to możliwe.

Dlatego też postuluje się wydanie KSM w postaci odrębnego dokumentu z zastosowaniem wymaganych rozwiązań technicznych, zdefiniowanych przez Ministerstwo Zdrowia (zabezpieczenia fizyczne, dedykowane funkcjonalności elektroniczne) dla dokumentu tego typu. Wdrożenie KSM jest niezbędne dla upowszechnienia wymiany elektronicznej dokumentacji medycznej, istotnej dla podniesienia efektywności służby zdrowia. Opis KSM znajduje się w dalszej części dokumentu.

Wdrożenie e-Dowodu i KSM będzie realizowane jako osobne projekty.

Więcej szczegółów odnośnie technicznej implementacji opisanych wyżej zastosowań znajduje się w dalszej części załącznika.

1.2. Wykorzystanie e-Dowodu w e-usługach

Zakłada się, że e-Dowód umożliwi uwierzytelnienie na poziomie wysokim (ang. High) i możliwość złożenia podpisu elektronicznego zgodnego z rozporządzeniem eIDAS dla zaawansowanego podpisu elektronicznego. Nie zakłada się jednak, aby podpis ten był transgraniczną usługą zaufania – będzie on umocowany prawnie w przepisach krajowych do kontaktu z administracją publiczną. Poziom uwierzytelnienia „wysoki” pozwoli na wykonanie wszystkich e-usług administracji publicznej – tych istniejących i planowanych. Zakłada się, że domyślnie wszystkie istniejące e-usługi, które wymagają tylko uwierzytelnienia i nie wymagają podpisu będą na poziomie „średnim”, czyli będą wymagać uwierzytelnienia środkiem identyfikacji o poziomie zaufania minimum „średnim”. Obecnie oferowany przez administrację publiczną środek identyfikacji elektronicznej Profil Zaufany (PZ, eGO) jest obecnie planowany do notyfikacji na poziomie średnim. Jednakże, oczekuje się, że właściciele biznesowi e-usług będą dla wybranych e-usług oczekiwali podwyższonego poziomu zaufania (czyli wysokiego) – w takim przypadku nie będzie możliwe użycie PZ, ale właśnie e-Dowodu. Niemniej w celu popularyzacji wszystkich narzędzi dających dostęp do e-Administracji rozważa się zakładanie PZ przy okazji wydawania e-Dowodu wszystkim obywatelom, którzy będą zgłaszać się do Urzędu po nowy dowód i do tego czas nie będą mieli założonego PZ. PZ może być stosowany tylko w usługach cyfrowych i bazuje na autoryzacji hasłami jednorazowymi SMS, natomiast e-Dowód będzie mógł być stosowany zarówno w świecie cyfrowym jak i fizycznym, i bazuje na karcie kryptograficznej i autoryzacji PINem.

E-Dowód będzie miał też zastosowanie w placówkach zdrowia – do potwierdzania faktu odebrania świadczenia medycznego.

Wykorzystanie e-Dowodu w świecie komercyjnym będzie zależało od przygotowania systemów komercyjnych do akceptacji e-Dowodu. Udostępnienie SDK do integracji systemów trzecich z e-Dowodem pozwoli na dynamiczny rozwój zastosowań e-Dowodu, pamiętając jednak że e-Dowód (bez opcji z podpisem kwalifikowanym serwerowym) nie zastępuje podpisu kwalifikowanego i nie pozwala z mocy prawa na składanie oświadczeń woli poza administracją publiczną (chyba że strony komercyjne i obywatel wyrażą zgodę na takie zastosowanie).

1.2.1. Korzyści z wykorzystania e-Dowodu do częściowego pokrycia funkcjonalności Karty Ubezpieczenia Zdrowotnego wraz z wydaniem Karty Specjalisty Medycznego

Jednym z efektów wprowadzenia na e-Dowodzie funkcjonalności pierwotnie planowanej Karty Ubezpieczenia Zdrowotnego (KUZ), związanych z funkcją potwierdzania wykonania świadczenia opieki zdrowotnej, ma być wyeliminowanie sytuacji polegających na zgłaszaniu przez świadczeniodawców do zapłaty przez Narodowy Fundusz Zdrowia (NFZ):

1) udzielenia świadczeń na rzecz pacjentów, którzy w danym dniu ich nie uzyskali, a w związku z tym nie rejestrowali się u świadczeniodawcy,
2) udzielenia fikcyjnych świadczeń tym pacjentom, którzy w danym dniu uzyskali inne, najczęściej „tańsze” świadczenie u danego świadczeniodawcy.

Ministerstwo Zdrowia wraz z NFZ próbowało oszacować finansowy skutek uszczelnienia systemu opieki zdrowotnej. Jeśli przyjmie się średni budżet roczny NFZ (koszty świadczeń opieki zdrowotnej) w wysokości 71 mld zł (2016 rok), a poziom nieprawidłowości, których zatrzymanie będzie możliwe przy użyciu kart generujących odpowiednie poświadczenia/podpisy elektroniczne na co najmniej 1% tego budżetu, to oznacza to, że wartość tak oszacowanego strumienia nieprawidłowości może wynosić co najmniej 710 mln zł rocznie. To oznacza tym samym dodatkowe środki do wykorzystania w obszarze ochrony zdrowia (kiedy wszyscy pełnoletni obywatele będą już posiadali dowody z warstwą elektroniczną).

Takie prognozowane efekty można będzie jednak uzyskać dopiero po wprowadzeniu obowiązkowego posługiwania się e-dowodem, a więc w obecnie proponowanym wariancie dopiero w 2029 roku. Dlatego MZ i MC pracują nad przygotowaniem alternatywnego rozwiązania na okres przejściowy.

1.3. Zakres danych umieszczanych w warstwie elektronicznej i sposób jej personalizacji

Warstwa graficzna oraz elektroniczna będą zawierać następujące dane:

1) dane dotyczące osoby:

a) nazwisko,

b) imię pierwsze

c) pozostałe imiona,

d) nazwisko rodowe,

e) imiona rodziców,

f) datę i miejsce urodzenia,

g) płeć,

h) wizerunek twarzy (wymogi dla fotografii pozostaną zgodne z aktualnym stanem prawnym i będą identyczne, jak dla zdjęć paszportowych czyli będzie to **zdjęcie biometryczne**),

i) numer PESEL,

j) obywatelstwo;

2) dane dotyczące dowodu osobistego:

a) serię i numer dowodu osobistego,

b) datę wydania,

c) datę ważności,

d) oznaczenie organu wydającego dowód osobisty.

Dodatkowo warstwa elektroniczna będzie zawierać certyfikaty do uwierzytelnienia (wymagający PIN) i do potwierdzenia obecności (nie wymagający PIN). Wydawcą certyfikatów będzie Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA) i będą one miały ważność równą ważności dokumentu, tj. 10 lat. Certyfikat ten będzie także honorowany przez Ministerstwo Zdrowia (MZ) na potrzeby wykorzystania w służbie zdrowia. Blankiet dowodu będzie dostarczany przez Polską Wytwórnię Papierów Wartościowych S.A. (zwaną dalej PWPW). W warstwie elektronicznej pozostawione będzie dedykowane oddzielnie miejsce (kontener; oddzielony od pozostałych) do wykorzystania przez obywatela do przechowania dowolnych danych (ang. *Flash memory*) - wielkość kontenera do ustalenia na etapie projektu technicznego (będzie to przestrzeń pozostała do dyspozycji po instalacji na chip pozostałych kontenerów i systemu operacyjnego). Wszelkie czynności na kontenerze do użytku własnego nie będą zagrażały bezpieczeństwu danych zamieszczonych w kontenerach MSWiA. Szczegóły rozwiązania i warunki bezpieczeństwa w tym zakresie zostaną doprecyzowane na etapie projektu technicznego. Odpowiedzialność za przechowane dane będzie po stronie obywatela.

E-Dowód będzie posiadał tylko interfejs bezstykowy.

Wymieniony wyżej zakres danych osobowych jest tożsamy z dotychczasowym. Dane w warstwie elektronicznej będą zapisywane w dokumencie na etapie personalizacji i nie będą podlegały zmianie przez cały okres ważności dokumentu (z wyjątkiem inicjalnie pustego kontenera dla użytku własnego obywatela).

Nowy dowód osobisty będzie posiadał także w warstwie graficznej pasek odczytu maszynowego na rewersie dokumentu (tzw. MRZ), analogiczne do obecnego dowodu.

Zamiast umieszczania w warstwie elektronicznej dokumentu dodatkowych danych, które podlegałyby późniejszej aktualizacji (ang. *post-issuance*), e-Dowód będzie wykorzystany jako klucz do usług udostępnianych przez systemy, w których gromadzone są dane (np. tak dla adresu zameldowania będzie to rejestr PESEL). Dzięki temu uzyskujemy gwarancję aktualności danych na e-Dowodzie względem Systemu Rejestrów Państwowych. Obywatel po elektronicznym uwierzytelnieniu dowodem osobistym będzie miał możliwość odczytu oraz wprowadzania/zmiany danych osobowych w systemach e-administracji za pośrednictwem e-usług (zgodnie z logiką biznesowych tych e-usług i zgodnie z tym na co pozwoli obywatelowi proces autoryzacji w tych usługach).

1.4. Proces produkcji i wydawania e-Dowodu

Bez zmian pozostaną zasady personalizacji dowodów osobistych. Dostarczanie blankietów i pre-personalizacja dokumentu będzie odbywać się PWPW. Warstwę graficzną nadal będzie personalizowało Centrum Personalizacji Dokumentów MSWiA równocześnie z personalizacją nowej warstwy elektronicznej. Spersonalizowane e-Dowody dostarczane będą do gmin z aktywnymi certyfikatami bez zdefiniowanego PIN wraz z kopertami z tzw. PIN-em transportowym. Przed otrzymaniem e-Dowodu obywatel wprowadza PIN transportowy przy urzędniku i musi ustalić nowy PIN. Alternatywnie definicja PIN w Urzędzie byłaby opcjonalna – proces można by dokończyć w późniejszym okresie (w Urzędzie lub zdalnie w domu). Szczegółowy proces obsługi obywatela (w tym aktywacji certyfikatów i wydania dokumentu) zostanie opisany na etapie projektu technicznego.

Jeśli chodzi o dowody wydane w latach 2001 - 2015 na czas nieoznaczony, nie będą one podlegały obowiązkowej wymianie, choć będą mogły być wydane na wniosek obywatela (sposób obsługi tych obywateli w placówkach zdrowia po wprowadzeniu obowiązkowości elektronicznego potwierdzania odebrania świadczeń zostanie ustalony na etapie projektu technicznego). Zakładany jest jeden wzór dowodu dla wszystkich obywateli, w tym małoletnich, a więc osoby małoletnie także będą mogły otrzymywać e-Dowód. Do czasu osiągnięcia pełnoletności nie będą one mogły używać e-Dowodu do podpisu i uwierzytelnienia, ale będą mogły potwierdzać obecność w placówkach zdrowia oraz pozwalać na odczytanie danych z warstwy elektronicz-

nej. Sposób zablokowania możliwości podpisu i uwierzytelnienia zostanie przesądzony na etapie projektu technicznego. Rozważane jest np. brak wydania PIN transportowego (z koniecznością zgłoszenia się do Urzędu po osiągnięciu pełnoletności) lub ustawienie daty ważności certyfikatu dopiero od daty osiągnięcia pełnoletności. Do potwierdzenia jest też decyzja o okresie ważności dowodu dla osób małoletnich – w każdym przypadku okres ważności certyfikatu będzie dostosowany do okresu ważności dowodu.

Na potrzeby kalkulacji kosztów zakłada się, że zostaną wymienione wszystkie dowody, których termin ważności mija w latach 2017-2028 oraz wszystkie dowody wydawane z innych powodów (nowy, utrata, kradzież, zmiana nazwiska). Ta druga grupa jest szacowana na ok. 30% terminowej wymiany dowodów. Szczegółowa prognoza dla poszczególnych lat została przedstawiona w załączniku z Zestawieniem kosztów.

Zakłada się rozpoczęcie wydawania nowych dowodów z warstwą elektroniczną od początku 2019 roku.

Przewidywane jest zaoferowanie wsparcia obywatelom jak i odpowiedzialnym za wydanie e-Dowodu urzędnikom w formie Infolinii. Szczegółowy zakres serwisu zostanie ustalony na etapie projektu technicznego i umowy z dostawcą. **Koszty związane z przygotowaniem i świadczeniem wsparcia nie zostały uwzględnione w przedstawionych kalkulacjach. Koszty będą pokryte z budżetu MSWiA lub MC, zależnie przyjętego podejścia po uzgodnieniu kosztów z dostawcami. Zależnie od wysokości kosztów zostaną one pokryte z obecnie planowanego zwiększenia środków lub planowane koszty zostaną skorygowane.**

1.5. Uwarunkowania techniczne użycia e-Dowodu

Biorąc pod uwagę planowane rozwiązanie techniczne dla e-Dowodu, użycie e-Dowodu będzie możliwe przy spełnieniu następujących wymagań dla środowisk (zakres funkcjonalny, opisany w punkcie 1.1 jest tożsamy dla każdego środowiska – z wyjątkiem terminali POS, gdzie złożenie podpisu nie będzie możliwe, w pozostałych środowiskach do złożenia podpisu będzie wymagane połączenie z Internetem; uwierzytelnienie i potwierdzenia obecności będzie możliwe off-line):

1) Komputer PC (stacjonarny/laptop) połączony z czytnikiem kart bezstykowych (ang. *Contact-less*) i wgranym oprogramowaniem do obsługi czytnika (sterownik) i e-Dowodu,

2) Komputer PC (stacjonarny/laptop) połączony z terminalem POS (ang. *Point-of-sale*); aplikacja dostępowa na komputerze PC musi być zintegrowana z oprogramowaniem

terminala POS, a terminal POS musi mieć zainstalowaną dedykowaną aplikację do obsługi e-Dowodu; złożenie podpisu niepraktyczne, bo na terminalu POS nie można wyświetlić zawartości podpisywanego dokumentu – pozostaje funkcja uwierzytelnienia oraz potwierdzenia obecności,

3) Komputer PC (stacjonarny/laptop) połączony ze Smartfonem z zainstalowaną aplikacją NFC Relay jako czytnikiem kart bezstykowych,

4) Smartfon albo tablet z obsługą NFC i zainstalowaną aplikacją mobilną i aplikacją NFC Relay jako czytnikiem kart bezstykowych.

Opcje 2) do 4) z racji nowatorskiego charakteru (szczególnie opcja 2) będą wymagać przygotowania studium wykonalności, aby w pełni potwierdzić możliwość realizacji tych wariantów dla e-Dowodu oraz zweryfikować szczegółowy zakres niezbędnych zmian. Studium obejmie zarówno analizę techniczną jak i analizę bezpieczeństwa oraz prawną.

Opcje 2) do 4) nie są niezbędne do dokończenia projektu pl.ID (nie były one ujęte w pierwotnym zakresie projektu pl.ID). Opcje te mogą być realizowane jako osobne projekty.

1.6. Komponenty techniczne e-Dowodu i rozwiązań wspomagających

Zakłada się przygotowanie w ramach projektu następujących rozwiązań technicznych:

1) **Dowód z warstwą elektroniczną** (dostawca PWPW)

   - interfejs bezstykowy (większa trwałość i szybsza transmisja danych niż interfejsu stykowego; poza tym zaledwie w 12 krajach na 27 państw europejskich brak interfejsu bezstykowego),
   - aplikacja ICAO (dodatkowo chroniona protokołem PACE aby uniknąć skimmingu; hasło uwidocznione w warstwę graficznej),
   - 1 kontener (z certyfikatem niekwalifikowanym i kluczem prywatnym do uwierzytelnienia) z dedykowanym numerem PIN,
   - 1 kontener bez PIN (z certyfikatem niekwalifikowanym i kluczem prywatnym do potwierdzania obecności - cyfrowy podpis bez PIN); szczegółowa zawartość danych certyfikatu i jego sposób zabezpieczenia będzie ustalony na etapie projektu technicznego – wybór rozwiązania może mieć wpływ na rodzaj dopuszczalnych czytników),

- 1 kontener (do własnego użytku) z dedykowanym numerem PIN lub bez (do decyzji na etapie projektu technicznego).

2) **Oprogramowanie do dowodu z warstwą elektroniczną** (dostawca PWPW)
   - Uwierzytelnianie certyfikatem z eDowodu,
   - Potwierdzanie obecności (cyfrowy podpis bez PIN),
   - Integracja z PKI,
   - Komunikacja z Systemem Zarządzania Kartą,
   - Middleware dla systemów środowisk Windows, Linux i OS X, sterownik obsługujący PKCS#11,
   - Udostępniany publicznie darmowy Software Development Kit (Middleware z API / SDK) do integracji aplikacji biznesowych bezpośrednio z e-Dowodem; zakłada się, że udostępniona będzie w nim cała funkcjonalność związana z wykorzystaniem e-Dowodu.

3) **Modyfikacja Systemu Produkcji Dowodów** (SPD) do obsługi certyfikatów oraz do personalizacji warstwy graficznej i elektronicznej wraz z modyfikacją interfejsu wymiany danych pomiędzy SPD, a Rejestrem Dowodów Osobistych. Wykonawcą systemu jest PWPW, który dokona modyfikacji.

4) **Dostosowanie parku maszyn Centrum Personalizacji Dokumentów (CPD) MSWiA** do potrzeb personalizacji dowodów osobistych z warstwą elektroniczną. Centrum Personalizacji Dokumentów MSWiA dysponuje trzema urządzeniami do personalizacji dokumentów (kart) formatu ID-1 o łącznej wydajności 4180 szt./h obecnego dowodu osobistego. W przypadku wprowadzenia do personalizacji warstwy elektronicznej wydajność produkcyjna spadnie. Spadek będzie uzależniony od przyjętego sposobu personalizacji warstwy elektronicznej i będzie wynosił od ok. 5% do nawet 35%. W celu zapewnienia oczekiwanego poziomu wydajności niezbędne będzie przeprowadzenie modernizacji parku maszynowego CPD tj. kupno w miejsce najwolniejszego urządzenia, nowej wysokowydajnej maszyny grawerującej.

5) **System Zarządzania Kartami (SZK)** - System do Zarządzania pełnym cyklem życia Karty, zarządzanie certyfikatami po wydaniu dokumentu i przed jego unieważnieniem aż do utylizacji (aktywacja certyfikatów, blokowanie/odblokowywanie/unieważnianie certyfikatów). Wykonawcą SZK będzie PWPW. Będzie posiadał następujące funkcjonalności:
   - Umożliwia zarządzanie cyklem życia karty,

- Z aplikacji SPD otrzymuje dane dotyczące wydawanego dowodu osobistego takie jak: Nr karty, nr chip,
- Z aplikacji Źródło otrzymuje informację o unieważnieniu dowodu osobistego - na tej podstawie rozsyła żądania unieważnienia certyfikatu do identyfikacji i uwierzytelnienia,
- Z aplikacji Źródło otrzymuje informację o odebraniu dowodu osobistego przez obywatela - na tej podstawie wysyła żądanie uchylenia zawieszenia certyfikatu do identyfikacji i uwierzytelnienia,
- Wysyła żądanie unieważnienia certyfikatu do identyfikacji i uwierzytelnienia do systemu wydawania certyfikatów (PKI),
- Wspiera utylizację e-Dowodów: paczki z dokumentami do utylizacji z Urzędów, raporty ze zniszczenia, bieżąca kontrola stanu utylizacji.

6) **Infrastruktura PKI (System Zarządzania Certyfikatami)** - dla wydawania dowodów z warstwą elektroniczną niezbędna będzie infrastruktura do wydawania certyfikatów uwierzytelnienia w systemach. Do przygotowania przez PWPW; na etapie projektu technicznego zostanie też przeanalizowana możliwość wykorzystania infrastruktury PKI zbudowanej i odebranej w NFZ w ramach projektu RUM II.

7) **System Identyfikacji Elektronicznej dla e-Dowodu** - oprogramowanie zapewniające komunikację eDowodu z Węzłem Krajowym, co jest niezbędne w celu zapewnienia powszechnego użycia eDowodu w portalach e-usług połączonych z Węzłem Krajowym. Wykonawcą oprogramowania będzie PWPW albo COI.

8) **Modyfikacja RDO / aplikacji Źródło** – niezbędne będzie dokonanie modyfikacji Rejestru Dowodów Osobistych i aplikacji Źródło. Zadanie wykona Centralny Ośrodek Informatyki (COI) na zlecenie MC.

- Zmiana modelu danych, interfejsów, funkcjonalności na potrzeby obsługi wniosków o wydanie dowodu osobistego i pobrania informacji zawartych w części elektronicznej dowodu osobistego,
- Dostosowanie do powyższego aplikacji Źródło,
- Aktualizacja interfejsu na potrzeby Systemu Personalizacji Dokumentów i modyfikacja lub utworzenie nowych usług sieciowych (oba do potwierdzenia na etapie projektu technicznego),
- Integracja RDO z SZK (poprzez usługi) i wywołanie funkcji SZK w aplikacji Źródło, tak aby Urzędnik miał jedną aplikację do obsługi e-Dowodu.

9) **Aplikacja mobilna NFC Relay i Aplikacja stacjonarna (sterownik)** do obsługi czytnika NFC w telefonie jako czytnika kart dla PC. Zadanie wykona COI na zlecenie MC.
    - Aplikacja mobilna w dwóch wersjach (dla Android 4.4+ i iOS 9.x+) działająca jako NFC Relay,
    - Aplikacja stacjonarna w trzech wersjach (dla Windows, Linux, Mac OS) działająca jako sterownik; obsługuje standard PKCS#11.
10) **Aplikacja mobilna** na smartfony z czytnikami NFC działająca bez potrzeby korzystania z komputera PC (wersja dla Android i dla iOS). Zadanie wykona COI na zlecenie MC lub dostawca rozwiązania zostanie wyłoniony w przetargu publicznym.
11) **Aplikacja na terminal POS** dedykowana do obsłużenia funkcji identyfikacji, uwierzytelnienia i potwierdzania obecności. Aplikacja będzie przygotowana we współpracy z Agentami rozliczeniowymi i/lub producentami terminali, a dostawca wyłoniony zostanie w przetargu publicznym.
12) **Czytniki do obsługi kart w urzędach i przez służby** – zakup czytników do kart bezstykowych. Dostawca czytników zostanie wyłoniony w przetargu publicznym.

Projektowane rozwiązania umożliwią także pełną realizację zadań wynikających z art. 35 ust. 4 ustawy z dnia 24 maja 2002r.o Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu (Dz.U.z 2015r., poz. 1929, z późn. zmianami). Szczegóły zostaną ustalone na etapie projektu technicznego.

Elementami niezbędnymi do rozpoczęcia procesu wydawania nowych e-Dowodów są:

1) i 2) – Dowód z warstwą elektroniczną z dedykowanym oprogramowaniem

3) i 4) – Modyfikacja SPD i rozbudowa CPD

5), 6) i 8) – System Zarządzania Kartą (SZK), PKI i modyfikacje RDO

7) – System środka identyfikacji dla e-Dowodu; bez niego nie można wykorzystywać e-Dowodu w portalach e-usług

12) Czytniki do obsługi kart

Elementami opcjonalnymi na moment rozpoczęcia wydawana nowych e-Dowodów są:

9) i 10) Aplikacja mobilna NFC Relay i Aplikacja stacjonarna (sterownik) oraz Aplikacja mobilna (standalone); rekomendowane dostarczenie wersji produkcyjnej w pierwszym kwartale 2019, a najpóźniej do końca 2019 roku,

11) Aplikacja na Terminal POS; rekomendowane dostarczenie wersji produkcyjnej w pierwszym kwartale 2019, a najpóźniej do końca 2019 roku.

Schemat komunikacji pomiędzy komponentami technicznymi oraz schemat komunikacji z Terminalem POS pokazują diagramy na końcu dokumentu.

1.6.1. Analiza dotycząca wykorzystana standardów ICAO

W trakcie analiz nad e-Dowodem przyjęto zgodność z normami i zaleceniami ICAO. Jak wynika z definicji dowodu osobistego, zawartej w art. 4 ust. 1 ustawy o dowodach osobistych, jest to dokument stwierdzający tożsamość i obywatelstwo polskie osoby na terytorium Rzeczypospolitej Polskiej oraz innych państw członkowskich EU, państw Europejskiego Obszaru Gospodarczego nienależących do UE oraz państw niebędących stronami umowy o Europejskim Obszarze Gospodarczym, których obywatele mogą korzystać ze swobody przepływu osób na podstawie umów zawartych przez te państwa ze Wspólnotą Europejską i jej państwami członkowskimi oraz na podstawie jednostronnych decyzji innych państw, uznających ten dokument za wystarczający do przekraczania granic. Skoro dowód osobisty uprawnia do przekraczania granic w/w państw, powinien być zgodny z normami i zaleceniami ICAO, zarówno pod względem formatu dokumentu (ID-1 adekwatnie do normy ISO 7810), jak i układu danych identyfikacyjnych po stronie awersu i rewersu dowodu. Przewiduje się więc zachowanie zgodności dowodu z wymaganiami ICAO dla warstwy graficznej

Założono też zastosowanie w dowodzie osobistym z warstwą elektroniczną aplikacji ICAO, która pełni funkcję elektronicznego dokumentu podróży, stanowiąc powtórzenie elektronicznej funkcjonalności paszportu biometrycznego, zgodnego z wymaganiami ICAO.

Zgodnie z rozporządzeniem Rady Unii Europejskiej (WE) NR 2252/2004 z dnia 13 grudnia 2004 r. w sprawie norm dotyczących zabezpieczeń i danych biometrycznych w paszportach i dokumentach podróży wydawanych przez Państwa Członkowskie dokumenty podróży powinny zawierać na nośniku pamięci obraz twarzy (Artykuł 1 pkt 2). Państwa Członkowskie mogą również dołączyć odciski palców w interoperacyjnych formatach.

Wymogi dokumentu podróży ICAO zawiera Doc 9303 Machine Readable Travel Documents. W 9 rozdziale znaleźć można jakie cechy biometryczne zawiera ICAO:

- zdjęcie twarzy (300dpi) – wymagane,
- odciski palców – opcjonalne,
- wzór tęczówki – opcjonalne

Należy zaznaczyć, że wymagania na certyfikację warstwy graficznej dowodu osobistego pod kątem spełnienia norm i zaleceń ICAO, będą spełnione w tym zakresie, gdyż e-Dowód będzie przechodzić certyfikację Common Criteria na poziomie EAL4+.

Inną korzyścią dostosowania do standardu ICAO (mowa o technicznych rozwiązaniach a nie notyfikacji) jest możliwość zastosowania gotowych bibliotek programistycznych dla rozwiązań dotyczących dokumentów zgodnych z ICAO (np. http://jmrtd.org) co m.in. przełoży się skrócenie czasu dostarczenia rozwiązań informatycznych korzystających z eDowodu. Poza tym, wykorzystanie standardu, ułatwi powstawanie na rynku nowych rozwiązań biznesowych dla wykorzystania eDowodu.

1.6.2. Aspekty bezpieczeństwa e-Dowodu

Jedną z podstawowych funkcji warstwy elektronicznej e-Dowodu będzie zapewnienie autentyczności dowodu osobistego (czyli dokumentu, zawierającego dane uwidocznione w warstwie graficznej), o ile bowiem elementy graficzne są podatne na modyfikacje (fałszerstwa), o tyle poprawnie zbudowana warstwa elektroniczna (dzięki zastosowanej kryptografii) uniemożliwia modyfikację chronionych informacji. Dlatego też w warstwie elektronicznej będzie komplet unikalnych dla każdego konkretnego dowodu informacji (imię, nazwisko, imiona rodziców, nr blankietu, PESEL, itd.), zawartych w warstwie graficznej – w tym zdjęcie posiadacza, ale w wysokiej rozdzielczości, niedostępnej w warstwie graficznej. Udostępnieniu danych towarzyszyć będzie poświadczenie ich autentyczności realizowane tak, że:

- niemożliwe będzie sklonowanie tej funkcjonalności,
- nie będzie możliwości nielegalnego wykorzystania poświadczenia przez osobę weryfikującą i poświadczania autentyczności tych danych wobec osób trzecich już bez udziału dowodu osobistego.

Kontener przechowujący dane obywatela będzie chroniony dzięki zastosowaniu protokołu PACE, który jest dostępny dla interfejsów bezstykowych. Dodatkowo warstwa elektroniczna z danymi klienta po personalizacji będzie zablokowana do edycji.

Warstwa elektroniczna dowodu osobistego musi spełniać najwyższe standardy bezpieczeństwa, zweryfikowane przez niezależne instytucje, dlatego też przeprowadzona będzie certyfikacja jej zgodności ze standardowym profilem ochrony dla bezpiecznych urządzeń do składania podpisu elektronicznego, przeprowadzona według normy ISO 15408 (Common Criteria). Planowany poziom certyfikacji to EAL4+ (Evaluation Assurance Level).

Dla zmitygowania ryzyka uzależnienia od jednego dostawcy planowane jest zagwarantowanie w Umowie z PWPW, aby układy scalone warstwy elektronicznej, w tym użyty system operacyjny był dostarczone przez 2 różnych producentów.

Do uwierzytelnienia za pomocą e-Dowodu planowane jest użycie protokołu 2-way (dwustronnego) TLS/SSL, którego celem jest ustanowienie bezpiecznego połączenia pomiędzy klientem a serwerem, które się wzajemnie uwierzytelniają. Protokół oparty jest o kryptografię asymetryczną i łączy w sobie zarówno proces ustanowienia bezpiecznego kanału komunikacyjnego

zapewniającego poufność jak i potwierdzenia, że na obu końcach tego kanału są osoby/podmioty przedstawiające się certyfikatami.

Pierwszą fazą procesu uwierzytelnienia TLS/SSL jest nawiązanie bezpiecznego kanału pomiędzy klientem a serwerem, następnie następuje uwierzytelnienie oparte o szyfrowanie klucza ze strony serwera oraz uwierzytelnianie oparte o podpis cyfrowy ze strony klienta. Dane które są wymieniane w protokole uwierzytelnienia są danymi poufnymi, co zapewnia że jedynie strony komunikacji po nawiązaniu bezpośredniego połączenia są w stanie prawidłowo zakończyć proces uwierzytelniania. Konstrukcja protokołu TLS/SSL zapewnia odporność przed atakami man-in-the-middle.

W wyniku analizy bezpieczeństwa połączonej z analizą poziomu skomplikowania projektu i potencjału rozwoju, zdecydowano się na rezygnację z certyfikatu na karcie do podpisu. Proponowane jest rozwiązanie, w którym dowód osobisty zawiera najbardziej potrzebną funkcję uwierzytelniania do usług on-line zarówno administracji publicznej jak i innych instytucji (i połączenie jej z węzłem krajowego schematu identyfikacji elektronicznej).

W proponowanym wariancie podpis elektroniczny (wcześniej nazywany „podpisem osobistym") realizowany jest jako podpis serwerowy. W szczególności będzie to mógł być zmodernizowany Podpis Elektroniczny Potwierdzony Profilem Zaufanym (zadanie w ramach prac zleconych do COI przez MC). Dodatkowo możliwe jest też realizowanie podpisu kwalifikowanego serwerowego przez państwowego lub komercyjnych dostawców usługi zaufania funkcjonujących na rynku polskim. Takie podejście umożliwia realizację kwalifikowanego podpisu dla obywateli bez koniecznego certyfikowania blankietu dowodu osobistego pod kątem nośnika podpisu kwalifikowanego.

Nowo powstające standardy podpisu pozwalają na uzależnienie możliwości złożenia podpisu serwerowego od dostępności tokenu (w przypadku e-Dowodu – podpisu cyfrowego z certyfikatu do potwierdzenia obecności) w trakcie procesu podpisywania, który tworzy Dane aktywujące podpisu. Te dane aktywujące podpis mogą być dynamiczne, bo uzależnione od podpisywanej treści, co zabezpiecza łańcuch dowodowy dla takiego podpisu.

1.6.3. **Analiza dotycząca podpisu kwalifikowanego**

Główną trudnością w implementacji podpisu kwalifikowanego na karcie jest konieczność zapewnienia możliwości współpracy z dowolnym podmiotem kwalifikowanym działającym w obrębie Wspólnego Rynku. Ze względu na wymagania bezpieczeństwa niezbędna jest wstępna weryfikacji uprawnień podmiotu kwalifikowanego do dokonania zapisu na karcie. To z kolei wymusza możliwość weryfikacji przez dowód osobisty aktualnego statusu podmiotu. To okazuje się jednak nie do końca proste – wymaga współpracy karty z międzynarodową infrastrukturą PKI (która nie została jeszcze w pełni zbudowana). Alternatywnie wymagane jest zbudowanie dedykowanej infrastruktury z użyciem kluczy CVC (ang. Card Verifiable Certificates).

Innym rozwiązaniem jest pozwolenie na umieszczenie w e-Dowodzie podpisu kwalifikowanego tylko wybranemu podmiotowi, co rodzi obawy co do nieuprawnionej pomocy Państwa albo naruszenia zasad wolnego rynku.

W każdym przypadku, przy klasycznej implementacji należałoby zwrócić szczególną uwagę na aspekty odpowiedzialności Państwa wobec podmiotów kwalifikowanych i wobec podpisujących – Państwo staje się bowiem podmiotem świadczącym usługi zaufania – z wszystkimi tego konsekwencjami wynikającymi m.in. z rozporządzenia eIDAS.
Dotyczy to w szczególności przypadków uszkodzenia/niesprawności dowodu osobistego i utraty zawartych tam kluczy prywatnych.

Rozporządzenie eIDAS stwarza możliwość generowania podpisów kwalifikowanych jako podpisów
serwerowych. Opcja ta stosowana jest w Austrii.
Klasyczna implementacja podpisu kwalifikowanego jako podpisu serwerowego nie jest przez niektórych ekspertów rekomendowana ze względów bezpieczeństwa – daje bowiem możliwość generowania wiążących prawnie podpisów w imieniu obywatela przez operatora serwera.
Wspomniane krytyczne wady bezpieczeństwa mogą być wyeliminowane poprzez zastosowanie certyfikatu dowodu do stworzenia danych aktywizujących podpis dla danej treści przedstawionej do podpisania (patrz rozdział wyżej).

2. OPIS KARTY SPECJALISTY MEDYCZNEGO (KSM)

2.1. Zastosowanie biznesowe KSM

Karta Specjalisty Medycznego (KSM) będzie służyła pracownikowi medycznemu przede wszystkim do składania elektronicznego podpisu pod dokumentacją medyczną oraz do identyfikacji i uwierzytelniania posiadacza karty w systemach teleinformatycznych, w tym będzie stanowiło elektroniczne prawo wykonywania zawodu; karta będzie pozwalała ponadto w przyszłości na dostęp do medycznych danych ratunkowych pacjenta.

2.2. Zakres danych w KSM

2.2.1. Warstwa graficzna KSM

Jest planowane, że dokument KSM jako "Prawo wykonywania zawodu lekarza" i „Prawo wykonywania zawodu lekarza dentysty” (w przyszłości, planowane jest poszerzenie o kolejne zawody medyczne) powinien być w dwóch wersjach graficznych (kolorystycznych) dotyczących wersji: na czas odbywania stażu podyplomowego i wersji na czas nieokreślony (biorąc pod uwagę, że dostęp do warstwy elektronicznej nie będzie w pierwszym okresie powszechnie dostępny) i co do zasady zawierać powinien (do uszczegółowienia/modyfikacji na etapie prac legislacyjnych):

1) nazwę dokumentu - Prawo wykonywania zawodu lekarza i odpowiednio lekarza dentysty;

2) nazwę dokumentu w języku angielskim – The right to practice the profession of a physician (of a dentist);

3) numer prawa wykonywania zawodu lekarza;

4) datę uzyskania prawa wykonywania zawodu lekarza;

5) wskazanie organu przyznającego prawo wykonywania zawodu lekarza;

6) imię i nazwisko lekarza;

7) numer PESEL, lub w przypadku braku numeru PESEL numer paszportu lub innego dokumentu tożsamości;

8) tytuł zawodowy;

9) fotografię lekarza, przedstawiającą go bez nakrycia głowy i okularów z ciemnymi szkłami, z naturalnym wyrazem twarzy;

10) podpis lekarza;

11) numer seryjny dokumentu;

12) okres ważności dokumentu – w wersji pierwszej adnotacja o przyznaniu prawa wykonywania zawodu na czas odbywania stażu podyplomowego lub stażu adaptacyjnego albo przystąpienia do testu umiejętności

13) adnotację o charakterze prawnym dokumentu - Prawo wykonywania zawodu lekarza jest dokumentem stwierdzającym uprawnienie do wykonywania zawodu lekarza na terytorium Rzeczypospolitej Polskiej;

14) wizerunek orła z koroną;

15) miejsce na mikroprocesor,

16) zabezpieczenia w druku i w tworzywie

Analogiczny zestaw danych dotyczyć będzie także fizjoterapeutów, diagnostów laboratoryjnych oraz farmaceutów, a także pielęgniarki i położnej, z uwzględnieniem ew. różnic wynikających ze specyfiki poszczególnych zawodów.

2.2.2. **Warstwa elektroniczna KSM**

Dane zapisane w treści certyfikatu:

1) imię (imiona) i nazwisko;
2) numer PESEL, a w przypadku osoby, która nie ma nadanego numeru PESEL - numer paszportu lub innego dokumentu stwierdzającego tożsamość;
3) numer prawa wykonywania zawodu;
4) zawód;
5) specjalizacja, jeżeli dotyczy;
6) data wygaśnięcia uprawnień do wykonywania zawodu, jeżeli dotyczy;
7) dane służące do składania kwalifikowanego podpisu elektronicznego, weryfikowanego przy pomocy kwalifikowanego certyfikatu podpisu elektronicznego, który jest wydany przez kwalifikowanego dostawcę usług zaufania.

Ostateczny zakres danych zostanie ustalony na etapie prac legislacyjnych i projektu technicznego.

KSM w warstwie elektronicznej powinna zawierać:

- kontener na certyfikat kwalifikowalny do podpisywania dokumentacji medycznej; certyfikat ten będzie zawierał w dedykowanym polu lub polach (decyzja na etapie projektu technicznego) w postaci jawnej dodatkowe informacje: numer prawa wykonywania zawodu, tytuł, zawód, specjalizacja (jeżeli dotyczy).
- kontener na certyfikat CV do komunikacji z planowaną w przyszłości Kartą Pacjenta (poza zakresem tego projektu),
- kontener na certyfikat do identyfikacji i uwierzytelnienia NFZ/MZ i w systemach placówek medycznych.

Ostateczny zakres danych zostanie ustalony na etapie projektu technicznego i będzie wynikał z brzmienia właściwych przepisów oraz ewentualnych różnic wynikających ze specyfiki poszczególnych zawodów, dla których będą docelowo wydane KSM.

Dodatkowo elementami rozwiązania będą system informatyczny do wydawania KSM (system produkcji i personalizacji kart, portal do obsługi zamówień, moduł wydawania certyfikatów) oraz czytniki kart.

Karta będzie posiadała tylko interfejs stykowy.

2.3. Założenia co do wielkości produkcji oraz procesu dystrybucji i terminów

Wg danych własnych MZ, opartych o dane z rejestrów zawodów medycznych, przekazanych przez samorządy zawodowe oraz CSIOZ liczba KSM, czyli osób z Prawem Wykonywania Zawodu (PWZ) będzie się kształtowała następująco:

Zawód	Liczba osób z PWZ	Średni roczny przyrost osób z PWZ	Średni roczny przyrost osób z PWZ na okres stażu
lekarz	145 895	2 000	3 300
lekarz dentysta	41 415	600	1 000
farmaceuta	33 220	1 200	0

Zawód	Liczba osób z PWZ	Średni roczny przyrost osób z PWZ	Średni roczny przyrost osób z PWZ na okres stażu
diagnosta laboratoryjny	15 050	400	0
fizjoterapeuta (wyż.wykszt.)	50 000	5 000	0
fizjoterapeuta (technik fizj.)	15 000	0	0
ratownik medyczny	13 000	2 500	0
felczer	1 000	0	0
pielegniarka	285 380	2 670	2 670
położna	36 095	615	615
Suma	**636 055**	**14 985**	**7 585**

Należy podkreślić, że intencją MZ jest wydanie w pierwszej kolejności KSM dla lekarzy i lekarzy dentystów (ok. 187 tys. osób), a następnie poszerzanie kręgu posiadaczy kart o kolejne z ww. zawodów medycznych. Przedstawione w Koncecji koszty zakładają wydanie KSM na razie tylko dla pierwszych 2 grup.

W zakresie procesu dystrybucji, w odniesieniu do zawodu lekarza i lekarza dentysty założono istotny udział samorządu zawodowego, który odpowiadałby zarówno za przekazanie danych z rejestrów zawodów medycznych do PWPW na potrzeby personalizacji kart jak i potem za dystrybucję kart do jej przyszłych posiadaczy. Rozważanym dodatkowym elementem jest wskazanie samorządu jako Zamawiającego (strona umowy z PWPW) z przekazaniem samorządowi środków finansowych na realizację zadania poprzez odpowiednie zwiększenie przekazywanej corocznie z budżetu państwa dotacji.

W oparciu o ofertę PWPW w zakresie KSM dla lekarzy i lekarzy dentystów przyjęto, iż pierwsze wydanie KSM nastąpi do końca 2018 roku. Następnie będą realizowane coroczne dodruki kart, wynikające ze zgubienia/zniszczenia karty itp. oraz uzyskania prawa wykonywania zawodu przez kolejne osoby, a także na okres odbywania stażu podyplomowego.

3. OTOCZENIE ORGANIZACYJNO-PRAWNE

3.1. Otoczenie prawne

3.1.1. Legislacja dla e-Dowodu

Do wprowadzenia do obiegu nowego dowodu osobistego z warstwą elektroniczną, niezbędne będzie prowadzenie równolegle szeregu działań o charakterze legislacyjnym, technicznym oraz organizacyjnym.

Konieczne będą zmiany w ustawie z dnia 6 sierpnia 2010 r. o dowodach osobistych oraz wydanie aktów wykonawczych dotyczących dowodów osobistych z warstwą elektroniczną. Nowy wzór dowodu osobistego zostanie przekazany krajom, z którymi RP utrzymuje stosunki dyplomatyczne, KE oraz w ramach właściwych grup roboczych Rady Unii Europejskiej zgodnie z przyjętą praktyką.

Natomiast dowód osobisty z warstwą elektroniczną jako środek identyfikacji będzie podlegał notyfikacji zgodne z wymogami rozporządzenia PE i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE – zgodnie z art. 9 co najmniej 6 miesięcy przed jego notyfikacją pozostałe państwa członkowskie Unii Europejskiej powinny mieć możliwość zapoznania się z takim systemem. Podmiotem odpowiedzialnym za notyfikację będzie MC we współpracy z MSWiA.

Rozporządzenia wykonawcze do ustawy o dowodach osobistych o charakterze technicznym powinny podlegać procedurze notyfikacji na podstawie rozporządzenia Rady Ministrów z dnia 23 grudnia 2002 r. w sprawie sposobu funkcjonowania krajowego systemu notyfikacji norm i aktów prawnych (Dz. U. Nr 239, poz. 2039, z późn. zm.); minimalny czas na tę procedurę to 3 miesiące, ale może ona ulec wydłużeniu o kolejne 3 miesiące w przypadku uwag Komisji Europejskiej.

W ustawie o dowodach osobistych powinny zostać uregulowane m.in.:

1) zakres danych posiadacza dowodu zawartych w warstwie graficznej i elektronicznej, a także funkcjonalności warstwy elektronicznej,
2) zasady wymiany i unieważnienia dowodu osobistego bądź zawieszania funkcjonalności warstwy elektronicznej,
3) zakres danych gromadzonych w Rejestrze Dowodów Osobistych,
4) kwestie związane z udostępnianiem danych,
5) ustanowienie narodowego nadzoru nad PKI dla dowodu z warstwą elektroniczną (a w rozporządzeniu opis polityk certyfikacji i bezpieczeństwa)

3.1.2. Legislacja dla zastosowań e-Dowodu w e-Administracji

Zakłada się, że na moment wdrożenia e-Dowodu będą już przyjęte przepisy i rozporządzenia regulujące funkcjonowanie Węzła Krajowego i Urzędu do spraw cyfrowej tożsamości. Uregulowania wymaga natomiast wprowadzenie e-Dowodu z mocy ustawy jako środka identyfikacji elektronicznej o poziomie wysokim oraz wprowadzenia nowej formy podpisu – Podpis potwierdzony środkiem identyfikacji. Dopuszczonym środkiem identyfikacji do potwierdzania tego podpisu będzie Profil Zaufany (PZ) i e-Dowód. Dlatego wymagane są też zmiany przepisów szczegółowych dotyczących możliwości składania Podpisu potwierdzonego środkiem identyfikacji (e-Dowodem); uzupełni on obecnie funkcjonujący Podpis potwierdzony Profilem Zaufanym, oprócz dopuszczonego do tej pory Podpisu kwalifikowanego.

Rozważa się też umocowanie prawne wprowadzenia obowiązku potwierdzania PZ w Urzędach Gmin przy wydawaniu dowodów obywatelom. Pod kątem tego planuje się przeprowadzenie konsultacji z samorządami i przygotowanie przepisów w ustawie o informatyzacji działalności podmiotów realizujących zadania publiczne.

3.1.3. Legislacja dla KSM

Wprowadzenie funkcjonalności potwierdzania odbioru świadczenia medycznego i udzielania zgody na dostęp do dokumentacji medycznej do dowodów osobistych z warstwą elektroniczną, a także wydanie KSM wymagać będzie również zmiany szeregu przepisów obowiązujących w systemie ochrony zdrowia, w tym m.in. ustawy o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych i ustaw dotyczących poszczególnych zawodów medycznych.

3.1.4. Sprawy organizacyjne

Wprowadzenie warstwy elektronicznej będzie wiązało się z opracowaniem poziomu zabezpieczeń dla warstwy graficznej. Dotychczas Zespół Ekspertów do spraw zabezpieczeń dokumentów, organ pomocniczy działający przy Ministrze Spraw Wewnętrznych i Administracji, nie stwierdził konieczności znaczącej zmiany katalogu zabezpieczeń zastosowanych w obecnym dowodzie osobistym. Choć interfejs bezstykowy nie jest widoczny na warstwie zewnętrznej dowodu, nie można wykluczyć konieczności przeprojektowania warstwy graficznej e-Dowodu. Położenie mikroprocesora i anteny może powodować konieczność zmian rozmieszczenia elementów zabezpieczających lub w skrajnym przypadku rezygnację z jakiegoś elementu zabezpieczającego.. Generalnie funkcjonujące od marca 2015 r. zabezpieczenia będzie można z powodzeniem wykorzystać na potrzeby dowodu osobistego z warstwą elektroniczną, choć możliwe są pewne zmiany w tym zakresie, związane z rozwojem technik zabezpieczania dokumentów jak i z analizą wpływu danego zabezpieczenia na koszt blankietu.

Etap wdrożenia nowych dowodów zakończy przekazanie innym państwom członkowskim UE oraz służbom informacji o nowym wzorze dowodu osobistego z warstwą elektroniczną. Jest to zadanie, które będzie realizowane na końcu całego procesu, do którego niezbędne jest posiadanie wyprodukowanych spersonalizowanych dowodów osobistych z warstwą elektroniczną.

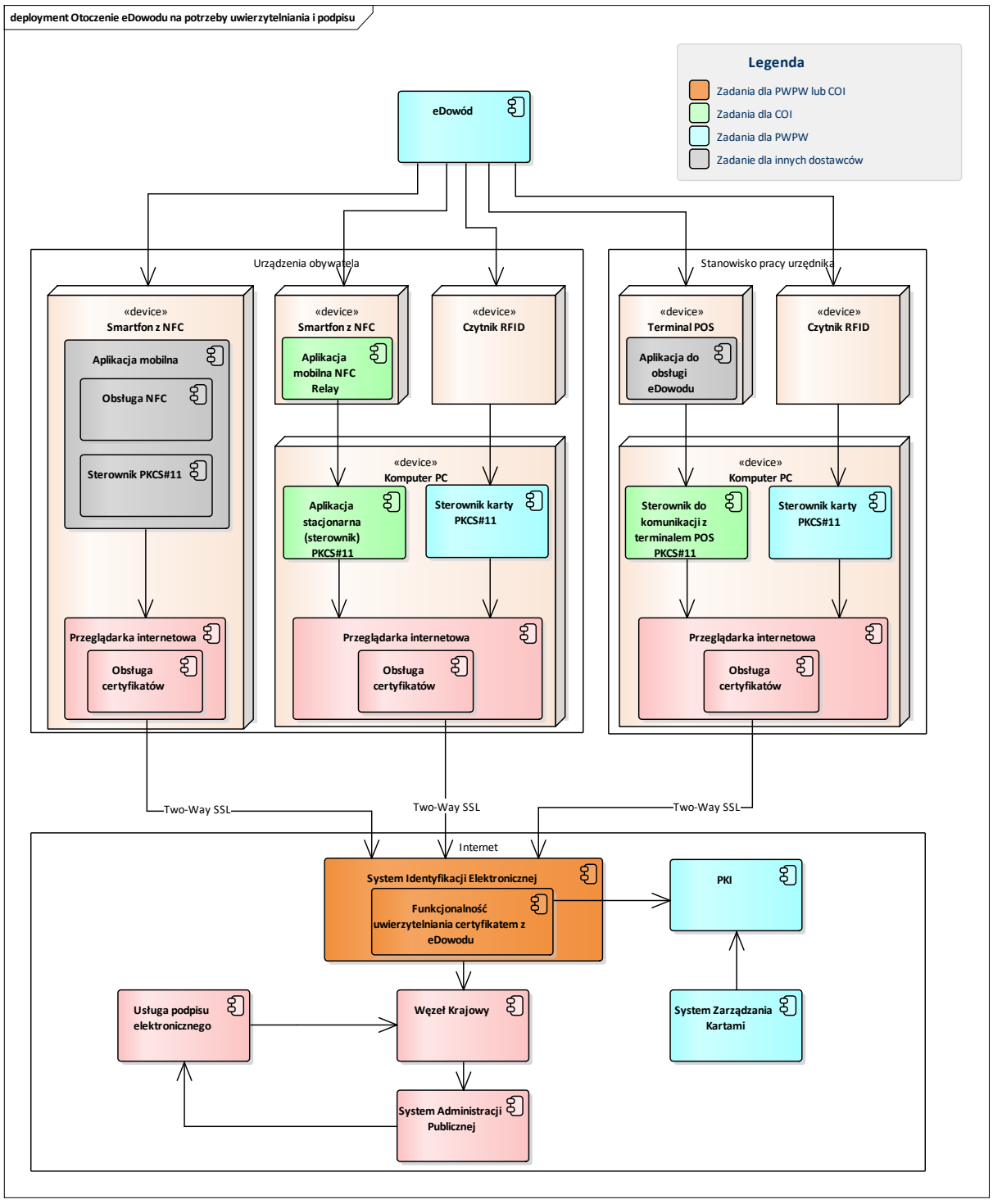
Zadanie to należy wykonać minimum na 2 miesiące przed wprowadzeniem do obrotu dowodów osobistych z warstwą elektroniczną.

Aktualnie dowody osobiste są produkowane przez Polską Wytwórnię Papierów Wartościowych S.A. (PWPW) i personalizowane przez Centrum Personalizacji Dokumentów MSWiA (CPD). CPD ma podpisaną umowę z PWPW na System Personalizacji Dokumentów oraz dostarczanie blankietów dowodów osobistych nr 118/14. Okres obowiązywania umowy upływa z dniem 31 grudnia 2024 roku. W związku z wdrożeniem dowodów osobistych z warstwą elektroniczną wskazane będzie aneksowanie przedmiotowej umowy lub podpisanie nowej umowy z PWPW w zakresie niezbędnym do wdrożenia e-dowodu, na mocy której zapewnione zostaną m.in. blankiety niezbędne do wydawania dowodów elektronicznych.

Wymagane jest też przeprowadzenie certyfikacji na Common Criteria warstwy elektronicznej i niezbędnego do jej obsługi oprogramowania.

4. Diagramy

4.1. Komponenty architektury aplikacji IT dla eDowodu



4.2. **Komponenty architektury aplikacji IT dla obsługi eDowodu na Terminalu POS**