Wymagania dla warstwy elektronicznej Dowodu Osobistego

(karty o funkcjonalności Karty Ubezpieczenia Zdrowotnego KUZ i funkcjonalności Karty Specjalisty Medycznego KSM)

wyciąg z wymagań przygotowanych w ramach projektu RUM II na potrzeby postępowania o zamówienie publiczne

DEFINICJE

Certyfikat	Elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.
CVC	(ang. Card Verifiable Certificate) certyfikat umożliwiający uwierzytelnienie do dostępu do medycznych danych ratunkowych, znajdujących się na karcie KUZ.
ECC	Asymetryczny algorytm kryptograficzny oparty na krzywych eliptycznych (ang. Elliptic Curve Cryptosystem) zgodny z RFC5639 „Elliptic curve cryptography (ECC) Brainpool Standard Curves and Curve Generation”, marzec 2010, albo normą FIPS 186-4 Digital Signature Standard, lipiec 2013.
Klucze podpisu elektronicznego i identyfikacji on-line	Dane służące do składania podpisu elektronicznego pod losowym wyzwaniem i zestawienia bezpiecznego połączenia - niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tę osobę do uwierzytelnienia i identyfikacji w systemach informatycznych.
Klucz zarządzający	Klucz algorytmu symetrycznego (AES lub TDES), składający się z kluczy K_{ENC} i K_{MAC}, służących do uwierzytelnienia i zestawiania szyfrowanego połączenia warstwy elektronicznej karty z otoczeniem, zgodnie z pkt. 8.9 normy PN-EN 419212-1:2015 - „Symmetric authentication scheme”.
KUZ	Karta Ubezpieczenia Zdrowotnego, o której mowa w Ustawie z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135 z późn. zm.).
Medyczne dane ratunkowe	Medyczne dane ratunkowe są zbiorem danych medycznych dotyczących pacjenta, których dostępność dla lekarza lub ratownika może mieć istotne znaczenie przy podejmowaniu decyzji o sposobie postępowania w warunkach nagłego przypadku medycznego. Dane mogą obejmować m.in.: • informacje o diagnozach, • informacje o podawanych lekach i dawkach, • informacje o alergiach, • inne szczegółowe wskazówki dotyczące danego pacjenta (np. obecność implantów).
Middleware	Oprogramowanie będące w zakresie realizacji Umowy, zapewniające możliwość wykorzystania Kart w systemach Świadczeniodawców. Middleware stanowi jeden z elementów Oprogramowania.
NFZ	Narodowy Fundusz Zdrowia.
PIN	4-znakowy kod, pozwalający na odblokowanie dostępu do możliwości użycia danego klucza prywatnego.
PKI	(ang. Public Key Infrastructure) Infrastruktura Klucza Publicznego.

Podpis elektroniczny	Nazwa technologii składania podpisu przy pomocy algorytmów asymetrycznych z certyfikatami klucza publicznego.
Podpis elektroniczny w celu identyfikacji	Podpis elektroniczny składany przy pomocy dedykowanego klucza umieszczonego na karcie, służący do uwierzytelnienia on-line Użytkownika Karty w systemach informatycznych; stosowany również w protokołach SSL/TLS do dystrybucji/uzgadniania kluczy algorytmów zapewniających poufność.
Podpis elektroniczny w celu składania różnego rodzaju oświadczeń	Podpis elektroniczny składany przy pomocy dedykowanego klucza umieszczonego na karcie, służący do potwierdzania integralności i autentyczności dokumentów.
Podpis medyczny	Podpis elektroniczny składany przy pomocy dedykowanego klucza umieszczonego na KUZ, do złożenia którego nie jest wymagane podanie PIN-u.
PUK	6-8-znakowy kod, pozwalający na ustanowienie nowej wartości kodu PIN.
RSA	Asymetryczny algorytm kryptograficzny RSA (Rivest, Shamir, Adleman) zgodny z normą PKCS#1, wersja 1.5 lub wyższa.
RUM	Rejestr Usług Medycznych.
Ustawa o świadczeniach	Ustawa z dnia 27 sierpnia 2004 r. o świadczeniach opieki zdrowotnej finansowanych ze środków publicznych (Dz.U. 2004 nr 210 poz. 2135 ze zm.).
X.509	Standard generowania, zarządzania i używania certyfikatów klucza publicznego. Definiuje m.in. zawartość certyfikatu i listy certyfikatów unieważnionych, zarówno co do informacji obligatoryjnych, jak i opcjonalnych.

WYMAGANIA DLA WARSTWY ELEKTRONICZNEJ DOWODU OSOBISTEGO (KARTY O FUNKCJONALNOŚCI KUZ I KARTY O FUNKCJONALNOŚCI KSM)

Wymagania dla kart

Struktura warstwy elektronicznej kart jest zawarta w poniższych tabelach przy czym nazwy obiektów mają charakter orientacyjny.

Uwaga 1. Symetryczne klucze zarządzające opisane w tabeli nie mogą mieć uprawnień do zmiany wartości PIN i PUK. Wartość inicjalna odpowiednich PIN i PUK jest wprowadzana na etapie personalizacji lub w ramach post-issuingu.

Uwaga 2. Symetryczny klucz zarządzający A opisany w poniższych tabelach, nie może mieć uprawnień do zmiany wartości obiektów w apletach (w szczególności wartości PIN, PUK i kluczy), a jedynie do dodawania i usuwania apletów.

Uwaga 3. Karta nie może umożliwiać, za pomocą kluczy zarządzających B, D, E w poniższych tabelach wprowadzania do pamięci nieulotnej karty innych obiektów, w tym w szczególności plików wykonywalnych (np. obiektów typu „aplet") oraz nie pozwala na zmianę wartości kluczy zarządzających, odpowiednio B,D,E.

Tabela 1 Struktura Karty o funkcjonalności KSM

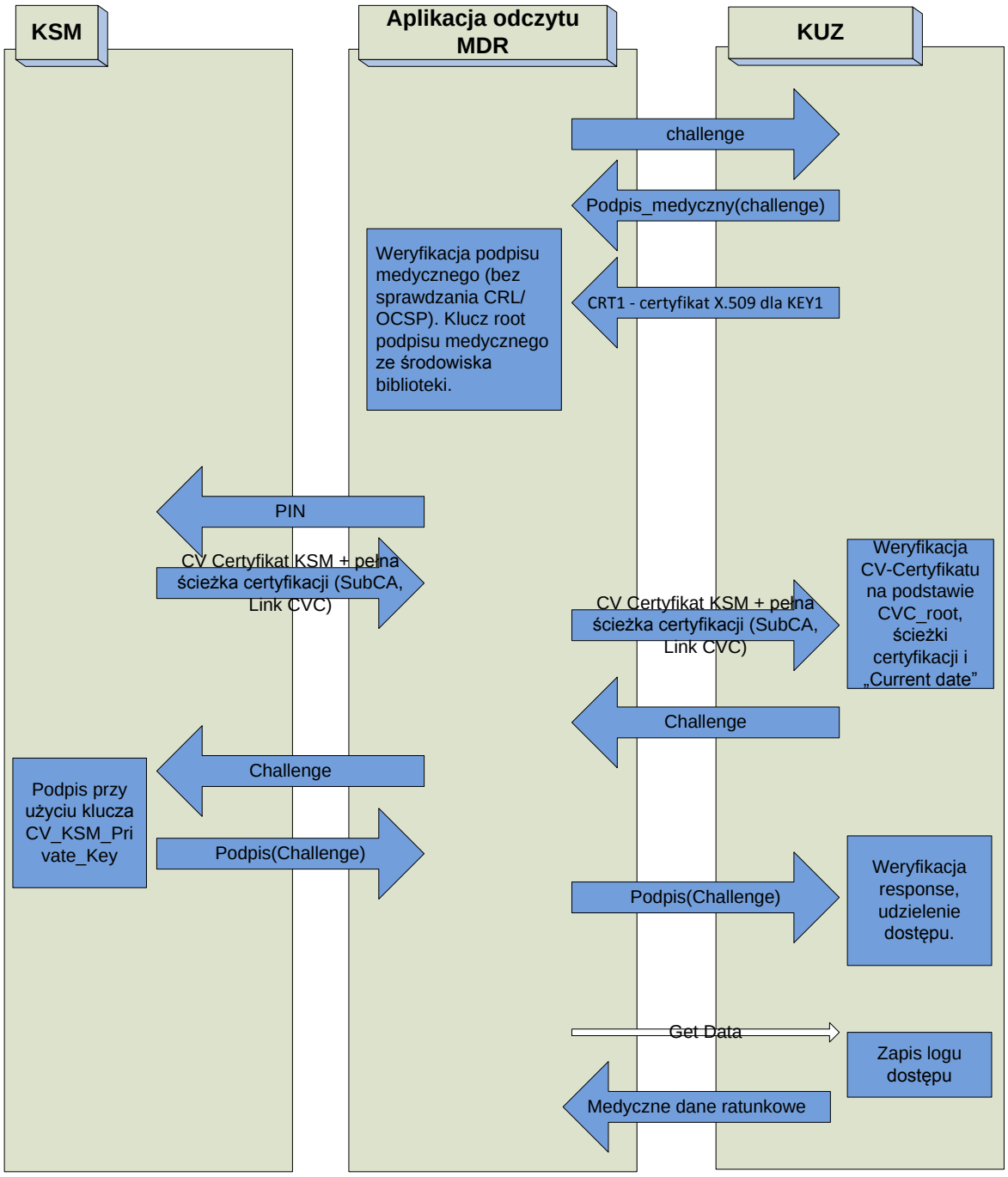
Instancja Apletu (AID)		zawartość	Symetryczne klucze zarządzające		Uwagi
SSCD NFZ	MF	EF.SN.ICC EF1 dane użytkownika (ang. administrative data) EF2 dane użytkownika (ang. identification data) CRT- certyfikat X.509	B (dodawanie, usuwanie, modyfikacja obiektów)	A (dodawanie, usuwanie apletów)	
	DF1	KEY1 - para kluczy asymetrycznych do podpisu, CRT1 - certyfikat X.509 dla KEY1 PIN1 PUK1	B (dodawanie, usuwanie, modyfikacja obiektów poza PIN i PUK)	A (dodawanie, usuwanie apletów)	Wartość inicjalna PIN i PUK na etapie personalizacji.
	DF2	KEY2 – para kluczy asymetrycznych do identyfikacji i uwierzytelnienia CRT2 – certyfikat X.509 dla KEY2 PIN2 PUK2	B (dodawanie, usuwanie, modyfikacja obiektów poza PIN i PUK)	A (dodawanie, usuwanie apletów)	
	DF3	KEY3– para kluczy asymetrycznych do dostępu do medycznych danych ratunkowych CRT3 – certyfikat CVC specjalisty	B (dodawanie, usuwanie, modyfikacja obiektów	A (dodawanie, usuwanie apletów)	

		medycznego dla KEY3 (EE certificate) CRT_CROSS – certyfikat dla SubCA wystawiony przez root (Cross Certificate) w ramach infrastruktury CVC CRT_LINK – certyfikat dla „nowego" klucza root, podpisany „starym" kluczem root (Link Certificate) w ramach infrastruktury CVC PIN3 PUK3	poza PIN i PUK)		
SSCD QCA	DF4	KEY4 – para kluczy asymetrycznych do składania podpisów kwalifikowanych lub identyfikacji i uwierzytelnienia KEY5 – para kluczy asymetrycznych do składania podpisów kwalifikowanych lub identyfikacji i uwierzytelnienia CRT4 – certyfikat kwalifikowany X.509 dla KEY4 CRT5 – certyfikat kwalifikowany X.509 dla KEY5 PIN4 PUK4 Opis wymagań dla obszaru DF4 jest opcjonalny i w odniesieniu do wymagań dla obszaru DF1	C (modyfikacja obiektów poza PIN i PUK)	A (dodawanie, usuwanie apletów)	Klucz C nie pozwala na zmianę wielkości obszaru DF4 oraz nie pozwala na zmianę swojej wartości. Wartość inicjalna PIN i PUK na etapie personalizacji.
Pozostały obszar karty				A (dodawanie, usuwanie apletów)	

Tabela 2 Struktura Karty KUZ

Instancja Apletu		zawartość	Symetryczne klucze zarządzające		Uwaga
SSCD NFZ	MF	EF.SN.ICC EF1 dane użytkownika (ang. administrative data) EF2 dane użytkownika (ang. identification data) CRT- certyfikat X.509	B (dodawanie, usuwanie, modyfikacja obiektów)	A (dodawanie, usuwanie apletów)	
	DF1	KEY1 - para kluczy asymetrycznych do podpisu medycznego, CRT1 - certyfikat X.509 dla KEY1	B (dodawanie, usuwanie, modyfikacja obiektów)	A (dodawanie, usuwanie apletów)	
	DF2	KEY2 - para kluczy asymetrycznych do podpisu, CRT2 - certyfikat X.509 dla KEY2 PIN2 PUK2	B (dodawanie, usuwanie, modyfikacja obiektów poza PIN i PUK)	A (dodawanie, usuwanie apletów)	Wartość inicjalna PIN i PUK w ramach post-issuing
	DF3	KEY3 – para kluczy asymetrycznych do identyfikacji i uwierzytelnienia CRT3 – certyfikat X.509 dla KEY3 PIN3 PUK3	B (dodawanie, usuwanie, modyfikacja obiektów poza PIN i PUK)	A (dodawanie, usuwanie apletów)	
SSCD QCA	DF4	KEY4 – para kluczy asymetrycznych do składania podpisów kwalifikowanych lub identyfikacji i	C (modyfikacja obiektów poza PIN i PUK)	A (dodawanie, usuwanie	Klucz C nie pozwala na zmianę

		uwierzytelnienia KEY5 – para kluczy asymetrycznych do składania podpisów kwalifikowanych lub identyfikacji i uwierzytelnienia CRT4 – certyfikat kwalifikowany X.509 dla KEY4 CRT5 – certyfikat kwalifikowany X.509 dla KEY5 PIN4 PUK4 Opis wymagań dla obszaru DF4 jest opcjonalny		apletów)	wielkości obszaru DF4 oraz nie pozwala na zmianę swojej wartości. Wartość inicjalna PIN i PUK na etapie personalizacji
NFZ _Emergency _DATA	DF5	EF3 medyczne dane ratunkowe (ang. medical emergency data) EF4 plik logu (rejestracja dostępów do medycznych danych ratunkowych) CRT_Root_1 – certyfikat root dla infrastruktury CVC (kotwica zaufania nr 1) razem z datą CED CRT_Root_2 – certyfikat root dla infrastruktury CVC (kotwica zaufania nr 2) razem z datą CED PIN5 – dostęp do logu dostępów do medycznych danych ratunkowych PUK5	D (zarządzanie obiektami na karcie KUZ zawierającymi medyczne dane ratunkowe, dostęp do odczytu pliku logu) E (wprowadzanie „kotwicy zaufania” CRT_CA w karcie KUZ	A (dodawanie, usuwanie apletów)	
Pozostały obszar karty			B (dodawanie, usuwanie, modyfikacja obiektów)	A (dodawanie, usuwanie apletów)	



Rysunek 1. Schemat uwierzytelnienia przy dostępie do medycznych danych ratunkowych w oparciu o mechanizm certyfikatów CV

Uwaga 4: Wykonanie i poprawna weryfikacja podpisu medycznego są konieczne w celu zapewnienia ochrony karty KUZ przed kopiowaniem - aby można było mieć pewność, że karta pacjenta, z którą ma do czynienia lekarz, została wydana przez NFZ jako karta KUZ, a więc w konsekwencji – że zapisane na niej dane medyczne są wiarygodne.

1. WYMAGANIA OGÓLNE

Tabela 3. Wymagania ogólne

ID	Opis
WK-1	Karta musi być zgodna z profilem „SSCD” zawartym w standardzie CWA 14169 Secure Signature-Creation Devices "EAL 4+" dla typu 3 (generowanie kluczy na karcie) lub w normie PN-EN 419 211 „Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu”: część 2: “Urządzenie z generowaniem kluczy” lub część 4: “Rozszerzenie dla urządzenia z generowaniem kluczy i bezpiecznym kanałem z aplikacją generującą certyfikaty”. lub w przypadku wykorzystania możliwości importu kluczy na kartę, karta musi być zgodna z profilem „SSCD” zawartym w standardzie CWA 14169 Secure Signature-Creation Devices "EAL 4+" dla typu 2 (generowanie kluczy poza kartą) lub w normie PN-EN 419 211 „Profile zabezpieczeń dla bezpiecznego urządzenia do składania podpisu - Część 3: Urządzenie z importem kluczy”
WK-2	Karta musi posiadać certyfikat zgodności z profilem, o którym mowa w pkt. WK-1 wydany przez ciało wyznaczone (ang. *designated body*) w rozumieniu dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych.
WK-3	Certyfikat, o którym mowa w pkt. WK-2 musi obejmować zgodność z odpowiednim profilem zabezpieczeń warstwy elektronicznej, systemu operacyjnego i apletu łącznie (SSCD).
WK-4	Karta musi posiadać certyfikat zgodności z profilem zabezpieczeń „Java Card Protection Profile – Open Configuration” (wersja 2.6 lub nowsza), wydany przez akredytowany podmiot w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (WE) nr 765/2008 z dnia 9 lipca 2008 r., ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie (EWG) nr 339/93 (Dz. U. UE, L 218/30).
WK-5	Certyfikaty, o których mowa w pkt. WK-2, nie mogą zawierać ograniczeń dotyczących wykorzystywania karty, w zakresie generowania kluczy, osadzania certyfikatów i składania podpisów elektronicznych, w normalnym środowisku[1],

[1] Przez normalne środowisko rozumiane jest środowisko pracy typu „dom” i „biuro”

	w którym karta będzie użytkowana (certyfikaty i dokumenty typu „Certification Report" lub „Security Target", nie mogą zawierać zastrzeżeń dotyczących np. konieczności zapewnienia bezpiecznego środowiska pracy przy wykonywaniu powyższych operacji na karcie. Akceptowalne są zastrzeżenia bezpieczeństwa wymagające stosowania „biurowych" standardów bezpieczeństwa np. wymaganie aktualizacji systemów operacyjnych, wymaganie instalacji i aktualizacji oprogramowania antywirusowego).
WK-6	Karta musi umożliwiać osadzanie dodatkowych apletów (kodu wykonywalnego i instancji) po wydaniu karty (w ramach tzw. *post-issuing*). Osadzanie tych apletów musi spełniać następujące wymagania: a) dodawanie nowych apletów wymaga zastosowania klucza zarządzającego „A", o którym mowa w pkt. WK-17; b) dodanie nowego apletu po wydaniu karty nie narusza wymagań certyfikatów, o których mowa w pkt. WK-3 i WK-4, w szczególności certyfikaty te muszą zachować ważność po dodaniu apletu „NFZ_Emergency_Data", o którym mowa dalej. Karta musi zapewniać mechanizmy integralności i kontroli dodawania apletów, uniemożliwiające uszkodzenie jej funkcjonalności w przypadku błędu procesu dodawania apletu (np. wyjęcia karty z czytnika).
WK-7	Karta musi umożliwiać usuwanie dodanych apletów (kodu wykonywalnego, instancji i danych). Usuwanie tych apletów musi spełniać następujące wymagania: a) usuwanie dodanych apletów wymaga zastosowania klucza zarządzającego „A", o którym mowa w pkt. WK-17; b) usunięcie apletu powoduje brak możliwości dostępu do wszystkich danych zawartych w usuwanych apletach.
WK-8	Pierwotne założenie z projektu: Warstwa elektroniczna karty musi posiadać wolne zasoby pamięci nieulotnej - po osadzeniu systemu operacyjnego i apletu, objętych certyfikacją „SSCD", o której mowa w pkt. WK-3 oraz apletu „NFZ_Emergency_Data", o którym mowa dalej - nie mniejsze niż 60 kB. Na potrzeby Medycznych danych ratunkowych oraz danych administracyjnych niezbędnych do identyfikacji pacjenta w systemie opieki zdrowotnej wymagana ilość wolnych zasobów została oszacowana na 20kB.
WK-9	Karta jest formatu ID-1, o którym mowa w normie PN-ISO/IEC 7810 „Karty identyfikacyjne -- Charakterystyki fizyczne".

WK-10	Warstwa fizyczna karty jest zbudowana z wielowarstwowego poliwęglanu, przy czym warstwy zewnętrzne są przezroczyste, a warstwy środkowe nieprzezroczyste.
WK-11	Karta ma interfejs stykowy zgodnie z normą PN-ISO/IEC 7816-1 „Karty identyfikacyjne - Karty elektroniczne - Część 1: Karty stykowe - Charakterystyki fizyczne”.
WK-12	Gwarancja na użytkowanie karty musi być zapewniona przez krótszy z okresów: 10 lat od momentu wydania karty, 15 lat od momentu rozpoczęcia wydawania pierwszej karty w ramach Umowy.
WK-13	Po uruchomieniu procesu dystrybucji Wydawca może dokonać zmiany karty, przy czym zmiana ta jest możliwa pod następującymi warunkami: a) w przypadku zmiany warstw poliwęglanowych karty i/lub zmian w technologii personalizacji graficznej, nowa karta musi spełniać, jako minimalne, wszystkie wymagania zawarte w niniejszym dokumencie; b) karta z nową warstwą elektroniczną musi spełniać, jako minimalne, wszystkie wymagania zawarte w niniejszym dokumencie przy czym dla zmian wymagana jest akceptacja MZ/NFZ; c) karta z nową warstwą elektroniczną musi spełniać, jako minimalne, wszystkie wymagania zawarte w niniejszym dokumencie, w szczególności: • w zakresie wolnych zasobów pamięci nieulotnej, • zaimplementowanych algorytmów kryptograficznych, • czasu wykonywania podpisów elektronicznych i czasu generowania kluczy na karcie oraz • czasu dostępu do medycznych danych ratunkowych, o którym mowa w pkt. WK-41; d) w przypadku zmian w warstwie elektronicznej dostawca musi dostarczyć zmodyfikowaną wersję Middleware’u obsługującego jednocześnie nowe i stare karty, i tym samym musi zapewnić kompatybilność nowej karty we współpracy z istniejącymi aplikacjami;
WK-14	Dla dostarczanej karty zostanie dostarczona: • dokumentacja zawierająca wszystkie niezbędne informacje pozwalające na implementację własnych apletów do kart. Dokumentacja musi w szczególności zawierać: ○ Szczegółowy opis interfejsów systemu operacyjnego karty ○ Szczegółowy opis interfejsów komunikacji karty z otoczeniem

	dostępnych na poziomie apletów karty ○ Szczegółowy opis interfejsów współpracy apletów ze sprzętem, w szczególności koprocesorem kryptograficznym ○ Szczegółowy opis procesu przygotowywania, kompilowania, osadzania i aktywowania apletów ○ Szczegółowy opis struktur danych ○ Szczegółowy opis środowiska uruchomieniowego i dostarczonego SDK (patrz WK-15). • dokumentację osadzanych na karcie apletów wykorzystywanych w funkcjonalności KUZ i KSM dostarczanych w trakcie cyklu życia karty na poziomie specyfikacji struktur danych apletów i komend APDU. Dokumentacja ma umożliwiać samodzielną implementację interfejsu PKCS#11. NFZ ma prawo do udostępnienia dokumentacji podmiotowi wykonującemu oprogramowanie na rzecz NFZ pod warunkiem zachowania poufności dokumentacji.
WK-15	Dla karty należy dostarczyć SDK (ang. Software Development Kit) wraz ze środowiskiem uruchomieniowym, kompletem narzędzi i odpowiednimi licencjami dla 5 stanowisk, pozwalającym na implementację apletów .

2. ZARZĄDZANIE WARSTWĄ ELEKTRONICZNĄ KARTY

Tabela 4 Wymagania na zarządzanie warstwą elektroniczną karty

ID	Opis
WK-16	W ramach post-issuing'u karta musi umożliwiać zarządzanie warstwą elektroniczną tylko za pomocą kluczy zarządzających, o których mowa w pkt. WK-17 (Wdawca zobowiązany jest usunąć wszelkie inne klucze do zarządzania kartą). Zarządzanie to musi obejmować co najmniej: dodawanie i usuwanie dodanych apletów (kodu wykonywalnego, instancji i danych) oraz dodawanie, usuwanie i modyfikację obiektów znajdujących się na karcie.
WK-17	Karta musi umożliwiać ustanowienie następujących, oddzielnych (różnych) kluczy zarządzających: a) „A" – klucz umożliwiający zarządzanie apletami znajdującymi się na karcie, który umożliwia dodawanie nowych apletów, instancji już istniejących apletów, usuwanie dodanych apletów i instancji, w tym danych. Usunięcie dodanego apletu lub instancji apletu oznacza brak możliwości dostępu do wszystkich obiektów znajdujących się w usuwanym aplecie/instancji, w tym w szczególności obiektów typu klucz, PIN i PUK. b) „B" – klucz umożliwiający zarządzanie obiektami zawierającymi dane użytkownika karty („Dane administracyjne" i „Dane identyfikacyjne", o których mowa w normie PN-EN ISO 21549 „Informatyka w ochronie zdrowia -- Dane karty zdrowia pacjenta") oraz obiektami związanymi z identyfikacją on-line i podpisami elektronicznymi, c) „D" – klucz umożliwiający zarządzanie obiektami zawierającymi medyczne dane ratunkowe, umożliwiający dostęp do odczytu pliku logu. d) „E" – klucz umożliwiający wprowadzanie „kotwicy zaufania" dla mechanizmu uwierzytelnienia za pomocą CVC.

3. FUNKCJONALNOŚCI UŻYTKOWE

Tabela 5 Wymagania na funkcjonalności użytkowe karty

ID	Opis
WK-18	Certyfikat, o którym mowa w pkt. WK-3, musi obejmować funkcjonalność składania podpisów elektronicznych z wykorzystaniem funkcji skrótu SHA-256 oraz algorytmu RSA-2048 i ECC-256, z zastrzeżeniem pkt. WK-19 w zakresie ECC-256.
WK-19	Karta musi umożliwiać obliczanie funkcji skrótu poza kartą lub co najwyżej ostatnia runda funkcji skrótu (i podpis) może być wykonywana na karcie.
WK-20	Karta musi realizować komendę APDU „DIGITAL SIGNATURE" dla pewnych kluczy kryptograficznych bez konieczności podania kodu PIN, a dla innych kluczy kryptograficznych wyłącznie po podaniu kodu PIN przez użytkownika. NFZ określi, najpóźniej na etapie generowania struktury karty, czy klucz ma być zabezpieczony, czy nie.
WK-21	Karta musi wspierać mechanizm PIN, który ma następujące właściwości: a) posiada licznik kolejnych nieudanych prób podania poprawnego kodu PIN, po osiągnięciu którego dostęp do użycia klucza jest zablokowany; b) dopuszczalne wartości licznika nieudanych pod rząd prób podania kodu PIN to 3, 4 lub 5; c) każde podanie poprawnego kodu PIN zeruje licznik, o którym mowa w ppkt. a); d) zmiana kodu PIN wymaga podania starego kodu PIN; e) odblokowanie dostępu do użycia klucza karty, zablokowanego poprzez błędne podawanie pod rząd kodu PIN, polega na ustanowieniu nowego kodu PIN i musi być możliwe wyłącznie za pomocą kodu PUK.
WK-22	Karta musi wspierać mechanizm PUK, który ma następujące właściwości: a) posiada licznik kolejnych nieudanych prób podania kodu PUK, po osiągnięciu którego nie jest możliwe użycie kodu PUK; b) dopuszczalne wartości licznika nieudanych pod rząd prób podania kodu PUK to 3, 4 lub 5; c) każde podanie poprawnego kodu PUK zeruje licznik, o którym mowa w ppkt. a).
WK-23	Karta musi wspierać mechanizm PIN i PUK, o których mowa w pkt. WK-21 i WK-22, w stosunku do wszystkich odpowiednich kodów zawartych na karcie, a ponadto musi być zapewnione, że:

	a) w obiektach zarządzanych przy pomocy klucza zarządzającego „B”, każdy z kluczy prywatnych jest zabezpieczony osobnym kodem PIN i osobnym kodem PUK, przy czym może być zastosowana ta sama wartość inicjalna kodu PUK; b)
WK-24	Karta musi posiadać mechanizm, z zastrzeżeniem pkt. WK-25, wskazujący, że osadzone na karcie klucze prywatne (o ile ich użycie jest chronione kodem PIN) nie zostały użyte w sposób niewykrywalny. Próba użycia kluczy wymusza zmianę kodu PIN „inicjalnego”, wprowadzonego do karty podczas osadzania klucza prywatnego. Dla raz użytych kluczy nie ma możliwości niewykrywalnego oznaczenia kluczy jako nieużywane.
WK-25	Wymaganie, o którym mowa w pkt. WK-24 nie dotyczy zmiany wartości kluczy, które wcześniej były używane. W takim przypadku dostęp do użycia nowej wartości klucza prywatnego jest możliwy za pomocą stosowanego dla tego klucza kodu PIN.

4. ZARZĄDZANIE DANYMI RATUNKOWYMI

Tabela 6 Wymagania na zarządzanie danymi ratunkowymi na karcie

<table>
<tr><th>ID</th><th>Opis</th></tr>
<tr><td>WK-26</td><td>W ciągu 18 miesięcy od podpisania Umowy Wydawca musi dostarczyć aplet „NFZ_Emergency_Data”. Aplet umożliwia zapisywanie, usuwanie i odczyt danych ratunkowych zapisywanych na kartach KUZ. Dostarczenie apletu obejmuje również dostarczenie Middleware, obsługującego funkcjonalności związane z danymi ratunkowymi, w formie uaktualnienia poprzedniej wersji Middleware.</td></tr>
<tr><td>WK-27</td><td>Karta KUZ musi umożliwiać zapis danych ratunkowych w oddzielnym plik typu EF. Zapis danych ratunkowych do karty KUZ wymaga użycia klucza zarządzającego „D”, o którym mowa w pkt. WK-17.</td></tr>
<tr><td>WK-28</td><td>Odczyt danych ratunkowych wymaga uwierzytelnienia, przy pomocy komend APDU, o których mowa w pkt. WK-36, otoczenia wobec karty KUZ za pomocą algorytmu asymetrycznego i certyfikatów CV. Schemat dostępu do danych ratunkowych przedstawia Rysunek 1. Schemat uwierzytelnienia przy dostępie do medycznych danych ratunkowych w oparciu o mechanizm certyfikatów CV.</td></tr>
<tr><td>WK-29</td><td>W ciągu 5 miesięcy od podpisania umowy Wydawca uzgodni z NFZ szczegółowy profil Link certyfikatu, Cross certyfikatu i certyfikatu CV specjalisty medycznego (Tabela 1). Każda zmiana profili w trakcie umowy wymaga uzgodnienia z NFZ.

Każdy z profili musi zawierać podzbiór następujących pól (określonych w normie CEN -EN 419212:2014 Application interface for smart cards used as secure signature creation devices) - przy czym pewne pola są alternatywne z innymi, a niektóre obligatoryjne:
<table>
<tr><th>Znacznik</th><th>Długość</th><th>Obligato-ryjność</th><th>Element danych</th></tr>
<tr><td>‘5F4E’</td><td>Var.</td><td>alternat. z ‘7F4E’</td><td>Certificate content</td></tr>
<tr><td>‘7F4E’</td><td>Var.</td><td>alternat. z ‘5F4E’</td><td>Certificate content template</td></tr>
<tr><td>‘5F29’</td><td>‘01’</td><td>✓</td><td>Interchange profile descriptor, eg. Certificate Profile Identifier (CPI)</td></tr>
<tr><td>‘42’</td><td>‘08’</td><td>✓</td><td>Certificate authority reference (CAR)</td></tr>
<tr><td>‘5F20’</td><td>‘0C’</td><td>✓</td><td>Certificate holder reference (CHR)</td></tr>
</table>
</td></tr>
</table>

		‘5F4C’	Var.	✓	Certificate holder authorization (CHA)
		‘5F24’	‘06’	✓	Certificate Expiration Date (CXD)
		‘5F25’	‘06’	✓	Certificate Effective Date (CED)
		‘5F49’	Var.	alternat. z ‘7F49’	Certificate holder public key, eg. PuK.IFD (primitive DO)
		‘7F49’	Var.	alternat. z ‘5F49’	Certificate holder public key, eg. PuK.IFD (constructed DO)
		‘06’	Var.	✓	Object Identifier (OID) for signature algorithm of certificate holder
		‘5F37’	Var.	✓	Signature of a certificate, produced by related CA
		‘5F38’	Var.		PuK-Remainder
		‘65’	Var	✓[2]	Certificate extension
WK-30	W celu weryfikacji certyfikatów CV (i tym samym dostępu do odczytu danych ratunkowych) karta KUZ musi zawierać tzw. „kotwicę zaufania”, czyli klucz publiczny urzędu certyfikacji najwyższego w hierarchii infrastruktury PKI (ang. *Root CA*). Klucz ten jest osadzany w karcie KUZ przy pomocy klucza zarządzającego „E”, o którym mowa w pkt. WK-17.				
WK-31	Karta musi wspierać możliwość określenia i wykorzystania dwóch kotwic zaufania, o których mowa w pkt. WK-30, każda z kotwic posiada datę ważności typu CED, czyli „nie wcześniej niż” zgodnie z Technical Guideline TR-03110-3 „Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 – Common Specifications” wersja 2.20 z 3 lutego 2015 r., wydany przez BSI i ANSSI.				
WK-32	Karta musi umożliwiać wymianę „kotwicy zaufania” za pomocą zarówno mechanizmu „link certificate”, jak i klucza zarządzającego „E”. Mechanizm „link certificate” automatycznie zastępuje kotwicę, której data CED jest wcześniejsza.				
WK-33	Weryfikacja certyfikatu CV musi uwzględniać fakt, że infrastruktura PKI, o której mowa w pkt. WK-30, jest dwupoziomowa, tzn. certyfikat użytkownika wystawiany jest przez urząd certyfikacji CA, który z kolei posiada certyfikat wystawiony przez najwyższy urząd certyfikacji w hierarchii (Root CA).				
WK-34	Aplet „NFZ_EMERGENCY_DATA” posiada mechanizm aktualizacji „bieżącej daty”, w oparciu o pozytywnie zweryfikowany dowolny certyfikat CV, zgodny z				

[2] Pole obowiązkowe w certyfikatach dla użytkowników kart (EE)

	mechanizmem „current date”, o którym mowa w standardzie Technical Guideline TR-03110-3 „Advanced Security Mechanisms for Machine Readable Travel Documents and eIDAS Token – Part 3 – Common Specifications” wersja 2.20 z 3 lutego 2015 r., wydany przez BSI i ANSSI.
WK-35	Mechanizm weryfikacji CV certyfikatów negatywnie weryfikuje certyfikaty przeterminowane, czyli takie, w których data wygaśnięcia, zawarta w polu CXD jest wcześniejsza niż aktualna wartość „bieżąca data” w karcie KUZ.
WK-36	Mechanizm weryfikacji CV certyfikatów przez kartę KUZ i KUZ o funkcjonalności KSM wymaga w szczególności wykonania następujących komend APDU, o których mowa w normie ISO/IEC 7816: **Karta KUZ** • SELECT FILE; • MANAGE SECURITY ENVIRONMENT; • VERIFY CERTIFICATE; • GET CHALLENGE; • EXTERNAL AUTHENTICATE. **Karta** o funkcjonalności **KSM** • SELECT FILE; • VERIFY (PIN); • MANAGE SECURITY ENVIRONMENT; • INTERNAL AUTHENTICATE, przy czym realizacja tej komendy w karcie o funkcjonalności KSM musi odbywać się wyłącznie po odblokowaniu dostępu do użycia klucza prywatnego za pomocą odpowiedniego kodu PIN. Wydawca może zaproponować zrealizowanie oczekiwanej funkcjonalności w inny sposób, wówczas wymaga to akceptacji NFZ.
WK-37	Jedna para kluczy i stosowny certyfikat CV zawarte na karcie o funkcjonalności KSM, muszą umożliwiać uwierzytelnienie i dostęp do danych ratunkowych, zawartych na dowolnej karcie KUZ.
WK-38	Po pozytywnym uwierzytelnieniu karty o funkcjonalności KSM za pomocą certyfikatu CV wobec karty KUZ, karta KUZ musi przekazywać dane ratunkowe do aplikacji za pośrednictwem Middleware’u. Odczyt danych ratunkowych musi być logowany w pliku EF na karcie (pliku logu), bezpośrednio przez aplet karty i przed wydaniem danych na zewnątrz karty. Plik logu ma postać „bufora cyklicznego” o pojemności 50 rekordów (po zapełnieniu, najstarsze rekordy są nadpisywane).

WK-39	Rekord danych, o którym mowa w pkt. WK-38, musi zawierać aktualną „bieżącą datę” oraz: • pole ‘5F20’ (CHR) z numerem prawa wykonywania zawodu specjalisty medycznego oraz • pole ‘65’ (rozszerzenie certyfikatu) zawierające imię i nazwisko specjalisty medycznego, z certyfikatu CV specjalisty medycznego, który był podstawą mechanizmu uwierzytelnienia przy dostępie do danych ratunkowych.
WK-40	Dostęp do odczytu pliku logu, o którym mowa w pkt. WK-38 musi wymagać podania oddzielnego kodu PIN (Tabela 2) lub uwierzytelnienia z wykorzystaniem klucza zarządzającego „D”, o którym mowa w pkt. WK-17. Wybór w tym zakresie będzie dokonywany w momencie odczytu danych.
WK-41	Czas pobrania danych ratunkowych z karty KUZ licząc od momentu wprowadzenia kodu PIN do karty o funkcjonalności KSM (tj. PIN3, Tabela 1) , do momentu ich odebrania z Middleware, nie może przekraczać 12 sekund dla pliku o rozmiarze 5 kB.

5. MIDDLEWARE

Tabela 7 Wymagania na dostarczane oprogramowanie Middleware

ID	Opis
WK-42	Wydawca dostarczy moduł graficznego interfejsu użytkownika GUI pozwalający na: • Wizualizację obiektów znajdujących się na karcie z możliwością ich wyboru i dalszego zarządzania; • Automatyczne wywołanie funkcjonalności zmiany PIN-u transportowego przy pierwszym użyciu karty; • Weryfikację, czy klucze były użyte (status „operacyjny” lub „nieoperacyjny”); • Zmianę każdego z kodów PIN i PUK, których zmianę dopuszcza karta; • Odblokowanie każdego z kodów PIN przy pomocy odpowiedniego kodu PUK; • Wyświetlenie parametrów, tj. nazwy algorytmu i długości kluczy, każdego klucza asymetrycznego znajdującego się na karcie; • Wyświetlenie zawartości i wyeksportowanie do pliku każdego certyfikatu znajdującego się na karcie; • W wersji dla systemu Windows, rejestrację w magazynach systemowych wszystkich certyfikatów znajdujących się na karcie z wyjątkiem certyfikatu podpisu medycznego. Dla nowej wersji Middleware, o której mowa w pkt. WK-26, ponadto: • Dla karty KUZ, odczyt logu zapamiętanego przez kartę dostępów do medycznych danych ratunkowych i zapisanie ich w pliku tekstowym. Odczyt logu musi każdorazowo wymagać podania odpowiedniego kodu PIN przez użytkownika (Tabela 2).
WK-43	Middleware nie może przechowywać PIN ani PUK poza pamięcią operacyjną komputera. PIN, PUK w pamięci operacyjnej nie może być przechowywany dłużej niż przez czas niezbędny do wykonania operacji, dla której został wprowadzony.

ID	Opis
WK-44	Dostawca dostarczy bibliotekę interfejsu PKCS#11 do karty w zakresie umożliwiającym wykonanie wszystkich operacji wynikających z warunków niniejszego postępowania, a w szczególności następujące grupy funkcji (tytuły rozdziałów dokumentu z PKCS#11 v.2.10: Cryptographic Token Interface Standard December 1999): • General-purpose functions; • Slot and token management functions; • Session management functions; • Object management functions; • Decryption functions; • Signing and MACing function; • Functions for verifying signatures and MACs; • Key Management Functions w zakresie przynajmniej C_GenerateKeyPair, C_GenerateKey, C_UnwrapKey. Dostarczany moduł PKCS#11, dla wersji Middleware, o której mowa w pkt. WK-26, poza funkcjami standardowymi opisanymi w standardzie, musi realizować dodatkowe funkcjonalności w postaci rozszerzeń producenta (ang. *vendor specific extensions*): • Funkcja udostępniająca medyczne dane ratunkowe po uwierzytelnieniu (opisanym w rozdz. 4) w oparciu o CV certyfikat. • Funkcja pozwalająca na pobranie logu zapamiętanego przez kartę dostępów do medycznych danych ratunkowych. Dostęp do logu wymaga podania odpowiedniego kodu PIN użytkownika (Tabela 2) lub uwierzytelnienia za pomocą klucza zarządzającego „D", o którym mowa w wymaganiu WK-17. • Funkcja weryfikacji CV certyfikatu powodująca zmianę ustawień „bieżącej daty", którą pamięta karta, o której mowa w wymaganiu WK-34. • Funkcja wymiany „kotwicy zaufania", o której mowa w wymaganiu WK-32.
WK-45	Wydawca dostarczy bibliotekę interfejsu CSP lub Minidriver do karty umożliwiające wykonanie analogicznych jak dla PKCS#11 (z wyjątkiem vendor specific extensions) operacji z obiektami znajdującymi się na karcie, które to operacje leżą w zakresie specyfikacji CSP i Minidriver.

ID	Opis
WK-46	Każda z bibliotek, o której mowa w wymaganiach WK-44 i WK-45 musi obsługiwać wszystkie dostarczone karty, w tym karty po dodaniu apletu „NFZ_Emergency_Data”.
WK-47	Biblioteki Middleware mają być dostarczone na następujące systemy operacyjne: • Windows XP/Vista/7/8/8.1/10/2003/2008/2012 w wersjach 32- i 64-bitowych, dla polskiej i angielskiej wersji językowej systemu; • Linux Ubuntu 14.04 LTS oraz CentOS 7; • Mac OS 10.10. z wyjątkiem modułu CSP/Minidriver, który dostarczany jest w wyłącznie w wersji Windows.
WK-48	Wymagane jest aby moduły oprogramowania były dostarczane dla wszystkich nowo pojawiających się wersji systemu Windows, Mac OS oraz wymienionych dystrybucji systemów Linux, nie później niż 3 miesiące od daty oficjalnego wydania nowej wersji systemu.
WK-49	W czasie trwania Umowy Middleware dla innych niż wymienionych wersji i dystrybucji systemów Linux, mają być dostarczane na żądanie. Czas realizacji dostawy nie może przekroczyć 6 miesięcy od daty złożenia zamówienia.
WK-50	W przypadku konieczności aktualizacji oprogramowania Middleware, nowa wersja zostanie dostarczona dla każdego z systemów znajdujących się na publikowanej na stronie www przez NFZ liście wspieranych systemów, która będzie zawierać podzbiór systemów, wersji i dystrybucji wynikających z wymagań WK-47, WK-48, WK-49.
WK-51	Moduły oprogramowania muszą zostać dostarczone z dokumentacją użytkownika oraz ze szczegółową dokumentacją programistyczną interfejsów zawierającą: • szczegółowy opis działania poszczególnych funkcji, • szczegółowy opis parametrów wywołania, • szczegółowy opis wartości zwracanych przez funkcje, • szczegółowy opis ograniczeń i warunków użycia funkcji, • przykłady użycia poszczególnych funkcji.

ID	Opis
WK-52	Moduły Middleware muszą być wyposażone w mechanizm automatycznej aktualizacji (możliwy do wyłączenia przez użytkownika karty), który wykrywa istnienie nowszej wersji, pobiera ją z serwera zarządzanego przez Wydawcę i automatycznie aktualizuje oprogramowanie. Wydawca zobowiązany jest do powiadomienia NFZ o udostępnieniu kolejnej wersji (wraz z informacją różnicach między wersjami i powodzie opublikowania nowej wersji) przed jej opublikowaniem.
WK-53	Instalacja Middleware może wymagać uruchomienia z konta administratora jedynie za pierwszym razem. Aktualizacje automatyczne muszą pozwalać na aktualizację oprogramowania bez konieczności logowania administratora lub wprowadzania danych autoryzacyjnych dla konta administratora.
WK-54	Wymaga się, aby dostarczony Middleware był objęty licencją pozwalającą na użytek publiczny, na dowolnej liczbie stanowisk, przez dowolny podmiot.