Narodowy Fundusz Zdrowia

ENIGMA

4pi ANALYST

Projekt:

Zalecenia dla zamawiającego w zakresie projektu RUM II

Wersja: 2.50

Autor: *Zespół Wykonawcy*
Data: *16.12.2014*

4pi Sp. z o.o. 03-924 Warszawa, ul. Niekłańska 27/5, tel/fax (22) 616 33 42, www.4pi.pl
ENIGMA Systemy Ochrony Informacji Sp. z o. o., ul. Jutrzenki 116, 02-230 Warszawa, tel. 22 570 57 10, www.enigma.com.pl

SPIS TREŚCI

SPIS ILUSTRACJI

SPIS TABEL

Brak.

SŁOWNIK

Patrz dokument „Finalna koncepcja rozwiązań w zakresie Projektu RUM II”.

OKREŚLENIE ISTOTNYCH DLA WDROŻENIA ZAŁOŻEŃ I OGRANICZEŃ

Obszar prawny

1. Konieczność przyjęcia zmian prawnych w zakresie opisanym w dokumencie pt. „Założenia do projektu ustawy o zmianie ustawy o systemie informacji w ochronie zdrowia oraz niektórych innych ustaw".
2. NFZ podejmie starania o nałożenie na Urzędy Stanu Cywilnego obowiązku przesyłania do NFZ danych adresowych opiekunów prawnych dla nowonarodzonych dzieci, których uzyskanie jest niezbędne dla dystrybucji kart drogą pocztową.

   W przypadku braku takiej możliwości, karty KUZ dzieci będą tworzone na podstawie wniosku rodzica/opiekuna, weryfikowanego w oparciu o dostępne dla NFZ bazy danych. Należy również dodać, że przedstawiciel COI MSW (architekt projektu PL.ID w zakresie informatyzacji USC) stwierdził publicznie w październiku 2014 r., że formalnie od stycznia 2015 r., a praktycznie od marca-kwietnia 2015 r., będzie działał centralny rejestr USC, w ramach którego inne, uprawnione podmioty z administracji, będą mogły uzyskać informacje m.in. o nowonarodzonych dzieciach.
3. Oparcie się o standardowe rozwiązania technologiczne, stosowane od lat zarówno w administracji jak i w sektorze prywatnym, w dużym stopniu eliminuje ryzyka związane z kwestią ograniczeń patentowych. Konieczne jest przeniesienie na wykonawców oprogramowania i urządzeń do składania i weryfikacji podpisów elektronicznych zapewnienie, że nie naruszają ograniczeń patentowych.

Obszar technologiczny

1. Ze względu na konieczność weryfikacji podpisów elektronicznych, którymi opatrzone będą sprawozdawane dane, niezbędne jest zwiększenie mocy obliczeniowej systemów informatycznych w oddziałach wojewódzkich NFZ.
2. Niezbędne jest odpowiednio wczesne opracowanie i upublicznienie nowych formatów sprawozdawanych danych, udostępnienie testowych kluczy i certyfikatów KSM, KSA i KUZ, usług znakowania czasem, usług OCSP, a także systemu weryfikacji testowych danych sprawozdawczych, tak aby czas wytworzenia nowego oprogramowania przez firmy komercyjne nie były przyczyną opóźnienia wdrożenia systemu.

Obszar organizacyjny

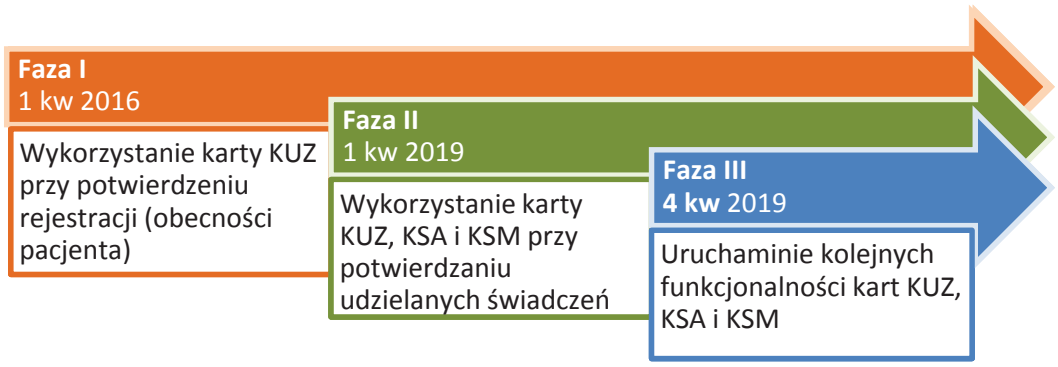
1. Harmonogram dystrybucji kart KUZ i KSA musi uwzględniać ich niezwłoczną eksploatację. Przewiduje się, że w pierwszej kolejności zostaną wydane karty KUZ i KSA dla dwóch województw, w miarę reprezentatywnych dla reszty kraju (np. łódzkie i podlaskie), w których zostanie uruchomione pilotażowe wdrożenie Fazy I RUM II („rejestracji"). Wymagać to będzie modernizacji sprzętu i aplikacji weryfikujących „schemat XML" w tych dwóch OW NFZ, jak również uruchomienia praktycznie wszystkich pozostałych elementów systemu po stronie NFZ, w szczególności Help

Desk'u i systemu SZUK, jak również modernizacji aplikacji świadczeniodawców, przygotowywanych przez wiele firm komercyjnych.

ZALECENIA DLA ZAMAWIAJĄCEGO DOTYCZĄCE PRZYGOTOWANIA I PRZEPROWADZENIA WDROŻENIA SYSTEMU

Fazy wdrożenia systemu

Wdrażanie wykorzystania rozwiązań w zakresie RUM II musi mieć charakter stopniowy, gdyż włączanie poszczególnych funkcji i kolejnych Świadczeniodawców będzie następowało sukcesywnie. Na poniższym diagramie przedstawiono kolejne fazy realizacji RUM II, dla których określono terminy rozpoczęcia każdej z faz, termin należy rozumieć, jako datę rozpoczęcia wykorzystywania przypisanych do faz funkcjonalności kart.



Rysunek 1. Fazy wdrożenia rozwiązań RUM II

Faza I „Rejestracja” - powszechne wprowadzenie kart KUZ i KSA, jako środka poprawiania jakości danych w systemach Świadczeniodawców, co podniesie jakość sprawozdawanych do NFZ danych. Nastąpi potwierdzanie rejestracji (obecności) pacjenta w placówce, przy pomocy karty KUZ oraz wprowadzona zostanie kontrola dostępu personelu świadczeniodawcy do eWUŚ z wykorzystaniem karty KSA i KSM.

Faza II „Potwierdzanie udzielonych świadczeń” - powszechne wprowadzanie kart KUZ, KSA oraz KSM do potwierdzania w systemach Świadczeniodawców faktu udzielania świadczeń na bieżąco. Użycie kart KUZ, KSA i KSM posłuży do uwiarygodnienia sprawozdawanych przez Świadczeniodawców do rozliczenia z NFZ udzielonych, świadczeń, w tym danych osoby udzielającej świadczenie.

Faza III „Rozszerzenie wykorzystania funkcjonalności” - polegałaby na wprowadzaniu dodatkowych funkcji karty kryptograficznej przez ich zdalne uruchomienie z poziomu systemu SZUK (nowe aplikacje), jak również na rozszerzaniu wykorzystania istniejących funkcjonalności kart.

Zasoby kadrowe po stronie NFZ dla realizacji projektu RUM II

Założenia w zakresie zarządzania projektem, w tym struktury organizacyjnej projektu opisano szczegółowo w dokumencie „Mechanizmy projektowe realizacji Projektu RUM II". Poniżej zgodnie z zaproponowaną strukturą, przedstawiono minimalne zasoby kadrowe zespołu projektowego po stronie NFZ, które powinny być zapewnione dla realizacji projektu RUM II:

- Kierownik Projektu - 1 osoba,
- Kierownicy Grup Zadań - 3 osoby,
- Grupa Zadań „Dostarczenie systemów, interfejsów oraz ewaluacja systemów" - 3 osoby (poza Kierownikiem Grupy Zadań),
- Grupa Zadań „Dostarczenie kart KUZ i KSA" - 3 osoby (poza Kierownikiem Grupy Zadań),
- Grupa Zadań „Kampania informacyjna" - 2 osoby (poza Kierownikiem Grupy Zadań),
- Zamówienie publiczne - 2 osoby (w okresie realizacji zamówień),
- Specjalista ds. zarządzania jakością - 1 osoba,
- Biuro projektu - 1 osoba.

Powyższe zestawienie dotyczy osób na stałe zaangażowanych w realizację Projektu, nie uwzględnia dodatkowych zasobów niezbędnych w okresie wzmożonych prac wdrożeniowych, gdzie należy przewidzieć szerszy udział pracowników NFZ. Dodatkowo niezbędna będzie współpraca pracowników OW NFZ, POZ oraz przedstawicieli Świadczeniodawców.

Zapewnienie wsparcia posiadaczom kart i rozwiązywanie problemów

Zapewnienie wsparcia w przybliżeniu 33 milionom użytkowników wymaga zbudowania bardzo licznie obsadzonej służby informacyjnej. Nowoczesny Help Desk zapewnia przy tym obsługę różnych kanałów zgłoszeń. Czyli oprócz linii telefonicznych, także kanały w postaci poczty elektronicznej i portali informacyjnych NFZ (obecnie eWUŚ i ZIP).

Możliwe są tu dwa zasadnicze rozwiązania:

- Zlecenie obsługi Help Desk jako usługi zewnętrznej firmie.

Wariant wiąże się z koniecznością wyspecyfikowania poziomu świadczenia usług w postaci umowy SLA. Konieczne jest również w tym przypadku zapewnienie dostępu do systemów NFZ dla firmy świadczącej usługę oraz dodatkowego porozumienia z dostawcami (firmami utrzymującymi) obecne i nowe systemy NFZ.

- Uruchomienie Help Desk po stronie NFZ.

Wariant wiąże się z koniecznością zbudowania dość kosztownej infrastruktury dla docelowo ok. 300 osób, przy czym dynamika narastania gęstości strumienia informacyjnego jest nie do przewidzenia.

Bez względu na to, czy usługa Help Desk-u będzie wykonywany realizowana„siłami własnymi" NFZ, czy w postaci outsource'ingu, należy kłaść bardzo duży nacisk na jakość usługi (szkolenia, testy wiedzy dopuszczające do realizacji usługi i testy w trakcie wykonywania zadań). Przypadek „Błękitnej Linii" ostrzega przed drastycznym pogorszeniem wizerunku NFZ, a przede wszystkim należy mieć na uwadze niedopuszczalne w ochronie zdrowia zablokowanie kanałów informacyjnych, tym samym niewykorzystania potencjału i funkcji kart.

Decyzja w zakresie wyboru wariantu zostanie podjęta w dalszym etapie prac.

Zasoby kadrowe po stronie NFZ dla utrzymania rozwiązań RUM II

W każdym z rozwiązań w zakresie usługi Help Desk-u dodatkowo należy zapewnić obsadę kadrową dla utrzymania systemu SZUK wraz z systemami PKI i administracji Help Desk.
Ponadto należy (w zakresie utrzymania systemów) zapewnić trwałe wsparcie utrzymania i rozwoju ze strony dostawców systemów.
Poniżej przedstawiono przewidywane zestawienie osobowe zespołów dedykowanych do utrzymania i rozwoju nowych systemów RUM II oraz Help Desk po stronie NFZ (dane należy zweryfikować w oparciu o informację o zaangażowaniu osobowym w NFZ obecnie eksploatowanych systemów, m.in. eWUŚ, RUM, ZIP).

PKI – minimum 7 osób:

a) Kierownik Utrzymania i Rozwoju Systemu – 1 osoba, (może dodatkowo pełnić rolę Audytora systemu)

b) Zespół Eksploatacji Aplikacji i Rozwoju – 4 osoby (Inspektor bezpieczeństwa (2 osoby), który może dodatkowo pełnić rolę Inspektora ds. Rejestracji, Operator systemu i Inspektor ds. Rejestracji)

c) Zespół Service Desk, Administratorzy – 2 osoby (mogą pełnić rolę Inspektora Rejestracji lub Operatora systemu).

Osoby określone w punktach b i c pracują w systemie zmianowym, tak aby zapewnić całodobową obsługę systemu przez co najmniej 1 operatora systemu i 1 inspektora ds. rejestracji na zmianę.

d) W oddziałach NFZ Punkty Rejestracji – Operatorzy Punktu Rejestracji, po 1,5 etatu osoby na oddział, w sumie 93 osoby.

SZUK – minimum 9 osób:

a) Kierownik Utrzymania i Rozwoju Systemu – 1 osoba,

b) Zespół Rozwoju – 2 osoby,

c) Zespół Eksploatacji Aplikacji – 4 osoby,

d) Zespół Service Desk, Administratorzy – 2 osoby.

Help Desk
1. Wariant zlecenia zewnętrznemu dostawcy – wymagana obsługa SLA dostawcy – 4 osoby:

a) Kierownik Umowy – 1 osoba,

b) Zespół – 3 osoby.

2. Wariant obsługi Help Desk po stronie NFZ – 300 osób:

a) Kierownik Help Desk – 1 osoba,

b) Koordynatorzy – 20 osób,

c) Zespół Konsultantów 1 linii wsparcia – ok. 240 osób,

d) Zespół Konsultantów 2 linii wsparcia – ok. 30 osób,

e) Zespół Konsultantów 3 linii wsparcia – ok. 9 osób.

Na podstawie powyższych założeń wstępnie można oszacować, że zespół 15-20 osób (+93 osoby do obsługi punktów rejestracji w Oddziałach) po stronie NFZ byłby wystarczający do utrzymania i administracji dostarczonych systemów oraz wsparcia użytkowników kart jeśli cała realizacja Help Desk zostanie przekazana w outsourcing. Przewidywany zespół ulegnie znacznemu zwiększeniu w przypadku wariantu uruchomienia Help Desk po stronie NFZ - w tym przypadku przewiduje się zaangażowanie dodatkowych 300 osób. Doświadczenie innych instytucji (zwłaszcza finansowych obsługujących karty płatnicze) wskazuje, że fazie stabilnego działania systemu można znacząco obniżyć ilość personelu w tym obszarze.

OPRACOWANIE REKOMENDACJI W ZAKRESIE WDROŻENIA KONCEPCJI ROZWIĄZANIA

„Podpisany zestaw danych”

Rekomenduje się zastosowanie struktury podpisanych danych, która została opisana w rozdz. 6.1 (pkt 9) dokumentu „Finalna koncepcja rozwiązań w zakresie Projektu RUM II”. Będzie to format zgodny z normą ETSI EN 319 132: “Electronic Signatures and Infrastructures (ESI); XML Advanced Electronic Signatures (XadES)” i zostanie użyty w Fazie I („rejestracji”) oraz Fazie II („potwierdzania udzielonych świadczeń”).

Personalizacja kart KUZ

Należy dokonać wyboru dwóch dostawców spersonalizowanych kart. Podział wielkości wolumenu personalizowanych kart między „pierwszego” i „drugiego” dostawcę powinien być w stosunku 60:40, czyli podmiot składający najlepszą ofertę otrzymuje „premię” w postaci większej liczby kart. Może to mieć korzystny wpływ na koszt przedsięwzięcia.

Centra personalizacji powinny spełniać analogiczne wymagania, które są stosowane na całym świecie w odniesieniu do emisji kart bankowych, akceptowanych przez organizacje płatnicze o zasięgu ogólnoświatowym.

Również wymagania co do czasu personalizacji i dystrybucji kart powinny być podobne do stosowanych aktualnie w Polsce przy personalizacji kart płatniczych, czyli od momentu udostępnienia danych do dostawy kart do punktu odbioru, powinno upłynąć nie więcej niż ok. 40 godzin. Rekomendowane są następujące parametry:

- D+0 – wysłanie *paczki rekordów* z danymi personalizacyjnymi do godz. 00:00;
- D+1 – wysłanie przez wykonawcę kart najpóźniej następnego dnia roboczego (poniedziałek-sobota, czyli z wyłączeniem tylko niedziel i świąt);
- D+2 do godziny 14:00 – dostawa na miejsce przeznaczenia do godz. 14 w kolejnym dniu roboczym.

Spełnienie tego typu wymagań nie będzie odbiegać od obowiązujących w europejskich centrach personalizacji reżimów pracy i pozwoli NFZ na szybką reakcję, gdyby okazało się, iż któryś z podmiotów ma kłopoty z realizacją kontraktu (w takiej sytuacji, poza przewidzianymi w umowie karami, powinna być możliwość czasowego powierzenia drugiemu podmiotowi personalizacji większej ilości kart).

Potwierdzenie tożsamości użytkownika karty KUZ

Wszystkie wydawane karty KUZ powinny mieć funkcjonalności podpisu medycznego (bez PIN-u) oraz podpisu elektronicznego oraz identyfikacji i uwierzytelnienia on-line (z PIN’ami odblokowującymi daną funkcjonalność). Jednak funkcja podpisu elektronicznego i identyfikacji będzie nieaktywna, a jej uruchomienie, w tym wygenerowanie kluczy i podpisanie certyfikatów, będzie możliwe za pomocą systemu SZUK, po zalogowaniu z wykorzystaniem mechanizmów ZIP i innych lub w oddziale NFZ.

Po zaktywowaniu funkcji „podpisu elektronicznego" i „identyfikacji" za pomocą karty KUZ, będzie możliwy późniejszy dostęp do konta ZIP i IKP również za pomocą tej karty.

Informowanie użytkowników o statusie wydania ich kart KUZ

Rekomenduje się, aby świadczeniobiorcy mogli być na bieżąco informowani o statusie wydania „swojej" karty KUZ. Do tego celu zasadne jest wdrożenie na portalu SZUK, dostępnego za pomocą ZIP, albo w inny sposób (ePUAP, ZUS itp.), specjalnej zakładki, na której uzyskiwano by informację o statusie karty w kontekście jej dostarczenia do użytkownika. Mogłyby tam być następujące komunikaty:

- Dokument przewidywany do produkcji w *grudniu 2016 r.*;
- Dokument jest w fazie produkcji;
- Dokument został wysłany na adres: xxxxx;
- Dokument jest przygotowany do odbioru w xxxxx;
- Dokument nie został wyprodukowany – został wycofany z produkcji, zawierał np. *błędne dane*;
- Dokument wydany w dniu *YYYYMMDD*;
- Na stronie wprowadzono błędne dane (np. popełniono błąd w trakcie wpisywania imienia, nazwiska lub numeru PESEL);
- Status nie został jeszcze wprowadzony do Systemu NFZ (w celu uzyskania wyjaśnień proszę skontaktować się z NFZ xxxxx);
- Karta o nr yyyyyyy unieważniona/zawieszona.

Powyższe rozwiązanie ma m.in. zapobiec sprzedaży lub wykorzystaniu kart świadczeniobiorców, które nie zostały odebrane przez właściciela, przez nieuczciwy personel podmiotu zaangażowanego w dystrybucję.

Zmiana adresu odbioru karty KUZ

Portal, o którym mowa w poprzednim pkt. powinien mieć dodatkową funkcję udostępniającą możliwość zmiany adresu odbioru kart. Zmiana na adres „z listy" przewidzianych adresów odbioru kart nie będzie się wiązała z uiszczaniem żadnej dodatkowej opłaty, natomiast zmiana na adres spoza „listy" (np. domowy) będzie możliwa po uiszczeniu dodatkowej, niewielkiej opłaty (w formie e-płatności) odpowiadającej kosztom wysłania listu poleconego za zwrotnym potwierdzeniem odbioru na dany adres.

W przypadku akceptacji rozwiązania „zmiana adresu za dodatkową odpłatnością" należy dokonać stosownych zmian w projekcie ustawy nowelizującej ustawę o świadczeniach (lub przynajmniej dać taką możliwość w ramach delegacji do wydania rozporządzenia wykonawczego), oraz dla takiego trybu musi być wdrożony dodatkowy mechanizm aktywacji karty, również w zakresie podpisu medycznego. Standardowa aktywacja karty KUZ w zakresie podpisu medycznego będzie wykonywana za pomocą sprawozdania, poprzez specjalny portal, faktu wydania karty i do tego celu zostanie wykorzystana karta KSA osoby wydającej kartę. Aktywacja będzie polegała na wskazaniu aplikacjom weryfikującym „schemat" w oddziałach wojewódzkich NFZ, iż należy akceptować podpisy medyczne zawarte w „podpisanym zestawie danych". Czas rozpoczęcia akceptacji powinien być przynajmniej jeden dzień wcześniejszy, niż data sprawozdania faktu wydania karty. W

przypadku zmiany adresu odbioru, aktywacja powinna zostać wykonana w systemie SZUK przez wysyłającego (podmiot personalizujący) już w momencie wysyłki karty listem poleconym, albo po otrzymaniu „zwrotnego potwierdzenia odbioru". Alternatywnie można dopuścić „standardową" aktywację kart KUZ wysłanych na adres domowy odbiorcy – taka karta byłaby aktywowana w momencie pierwszej bytności pacjenta u świadczeniodawcy, i do tego celu stosowano by kartę KSA osoby upoważnionej, która zgłaszałaby fakt „odebrania" karty na specjalnym portalu, po potwierdzeniu tożsamości świadczeniobiorcy.

Sugeruje się również rozważenie większego zaangażowania podmiotów personalizujących w proces dystrybucji kart. Poza „wysyłką" mogłyby te firmy również zająć się „zwrotami", tj. ich przechowywaniem i ponowną wysyłką na inny adres, wskazany przez NFZ, albo niszczeniem.

Warstwa elektroniczna kart KUZ i KSA

Karty KUZ i KSA powinny być kartami z certyfikatem SSCD wydanym przez *designated body* w rozumieniu regulacji UE dot. podpisu elektronicznego[1]. Ze względu na proces wydawania kart (centralne przygotowanie danych) i późniejsze instalowanie certyfikatów, np. certyfikatów kwalifikowanych wydawanych przez komercyjne centra, powinny to być SSCD typu 2 i 3 łącznie. Jeśli chodzi o typ 3 (generacja kluczy podpisu na karcie), to w zastrzeżeniach certyfikacyjnych nie może być żadnych ograniczeń typu „generowanie tylko w bezpiecznym środowisku", gdyż założono możliwość wywoływania tej funkcji na dowolnym komputerze, jedynie mającym połączenie on-line z systemem SZUK.

Ponadto powinny to być karty typu Java i w zastrzeżeniach do certyfikatu SSCD musi być dopuszczone osadzanie innych apletów bez naruszenia jego ważności. Tego typu karty oferuje kilku wiodących dostawców oraz nie bez znaczenia jest fakt, że brak „certyfikatu SSCD" naraża całe przedsięwzięcie na ryzyko używania kart, którym odmówiono wydania stosownej aprobaty ze względu na wykryte słabości.

System operacyjny i aplet podpisujący musi spełniać wymagania CEN/TS 15480 „European Citizen Card" oraz ISO/IEC 24727 „Identification cards". Szczegóły zakresu zgodności z tymi standardami zostaną określone w ramach dialogu technicznego.

Centra personalizacji NFZ

Wykonawca rekomenduje odstąpienie od pomysłu uruchomienia innych niż w zewnętrznych podmiotach, centrów personalizacji kart. Wiązałoby się to z niewspółmiernymi do ewentualnych korzyści kosztami dostosowania pomieszczeń, ich utrzymywania, a także budowy infrastruktury informatycznej oraz integracji z systemami centralnymi. Koszt adaptacji zależy od zakresu prac koniecznych do wykonania w konkretnej lokalizacji, czyli bez jej wskazania nie jest możliwy do oszacowania. Jednak należy zaznaczyć, że adaptacja nie będzie polegała na stworzeniu pomieszczenia „biurowego", a na zbudowaniu „produkcyjno-

[1] dyrektywa Parlamentu Europejskiego i Rady 1999/93/WE z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych oraz Decyzja Komisji z dnia 6 listopada 2000 r. w sprawie minimalnych kryteriów jakie powinny zostać wzięte pod uwagę przez Państwa Członkowskie przy wyznaczaniu organów zgodnie z art. 3 ust. 4 dyrektywy 1999/93/WE Parlamentu Europejskiego i Rady w sprawie wspólnotowych ram w zakresie podpisu elektronicznego

laboratoryjnego", z podwyższonymi wymaganiami w zakresie utrzymania stałej temperatury, wilgotności i zapylenia, z filtrami zarówno na wejściu, jak i na wyjściu (ozon).

Koszt profesjonalnego zestawu personalizującego, zintegrowanego z urządzeniem *mailingowym* (pakowanie kart i drukowanie listów oraz „bezpiecznych kopert") o wydajności rzędu 3-4 mln kart/rok, wynosi ok. 1,5 mln Euro. Urządzenie to będzie wymagało obsługi ze strony przynajmniej kilkunastu osób, czyli razem z personelem zarządzającym i pomocniczym, będzie to komórka NFZ z obsadą 20-25 osób. Stąd poza kosztami dostosowania i utrzymania pomieszczeń, zakupu i eksploatacji urządzeń, należy również wziąć pod uwagę wydatki na pensje pracowników na poziomie 150 tys. PLN/miesiąc (20 x 5000 zł x 1,5).

Okres ważności certyfikatów

Sugeruje się, aby okresy ważności wszystkich certyfikatów zapisywanych na karty KUZ, KSA i KSM (X.509 i CVC) były identyczne z czasem ważności kart, czyli 10 lat dla kart KUZ i 5 lat dla KSM/KSA. Uprości to zarządzanie certyfikatami (brak konieczności odnawiania), a nie wpłynie w sposób zasadniczy na bezpieczeństwo użytkowania.

Czytniki kart KUZ, KSA i KSM

Zastosowanie specjalnego („bezpiecznego") czytnika można by uzasadniać w następujący sposób:

a. Dostęp do danych KUZ (medycznych danych ratunkowych) wymaga bezpiecznego środowiska, z dodatkowymi mechanizmami zabezpieczającymi.

b. Czytnik pełni istotną rolę w określaniu momentu czasu realizacji świadczenia dla trybu off-line.

c. Czytnik stanowi istotne zabezpieczenie środowiska składania podpisów elektronicznych, czyli chroni przed atakami ze strony złośliwego oprogramowania.

Ad.a. Przyjęcie założenia z punktu a) o konieczności dodatkowego uwierzytelnienia karta-terminal oznacza - zdaniem autorów - zastosowanie środków przeciwdziałania nieadekwatnych do poziomu zagrożeń. Dostęp do medycznych danych ratunkowych jest ograniczany wyłącznie do posiadaczy KSM i ograniczony czasowo (poprzez zastosowanie uwierzytelnienia przy użyciu CV-certyfikatów odblokowywanych PIN-em – kwestia wykorzystania skradzionej karty KSM). Wprowadzanie trzeciego elementu bezpieczeństwa w postaci dedykowanego czytnika jest nieuzasadnione.

Dostęp do medycznych danych ratunkowych wymagany jest w szczególności poza placówkami służby zdrowia, np. w karetkach pogotowia, ale również przy wizytach domowych. W związku z tym czytnik podlega takim samym (o ile nie większym, gdyż nie jest przypisany do osoby) zagrożeniom, jak karta KSM. Przeciwdziałanie tym narażeniom wymagałoby częstej zmiany kluczy (certyfikatów) w czytnikach, aby uniewrażliwić je na kradzież/zgubienie. Jednak automatyczna wymiana kluczy musiałaby się odbywać w pewnym reżimie czasowym (którego naruszenie skutkowałoby wyłączeniem czytnika z eksploatacji do czasu manualnego osadzenia nowych kluczy), co - przy braku podłączenia czytników do sieci, ich mobilności i niewielkiej skali wykorzystania - oznaczałoby duże prawdopodobieństwo, że system w tym aspekcie nie będzie w ogóle funkcjonował.

Kolejnym argumentem przemawiającym za rezygnacją z dodatkowego uwierzytelnienia karta-terminal w przypadku ratowników medycznych (a jest to podstawowa grupa specjalistów w kontekście „danych ratunkowych") jest to, że – jak uzgodniono z odpowiednimi dep. merytorycznymi NFZ – dla tego rodzaju specyficznych świadczeń nie będzie wymagać się znakowania czasem sprawozdawanego rekordu, nawet w Fazie II projektu RUM II. Jest to podyktowane specyfiką działalności zespołów ratownictwa (mobilność, przypadkowe miejsce udzielenia świadczenia), gdzie używanie dodatkowych mechanizmów zabezpieczających (np. znaczników czasu) nie jest zasadne i powinno się odnosić tak samo do specjalnych czytników.

Ad. b. Przyjęcie argumentacji z punktu b) mogło by być zasadne, ale - zdaniem autorów – rozwiązania techniczno-organizacyjne, pozwalające na wykorzystanie standardowych czytników, są całkowicie wystarczające dla uruchomienia projektu RUM II, przy czym jednocześnie nie wyklucza się w przyszłości decyzji o obligatoryjności znakowania czasem każdego sprawozdawanego rekordu dot. udzielonego świadczenia medycznego, nawet w sytuacji, gdy nie będzie połączenia on-line z serwerem znakowania czasem w momencie udzielania świadczenia – czyli znakowanie czasem w trybie off-line za pomocą specjalnego czytnika (lub podobnego urządzenia).

W dokumencie „Finalna koncepcja rozwiązań w zakresie Projektu RUM II", w rozdz. „Wykorzystanie KUZ, KSA i KSM w procesach rozliczania świadczeń medycznych NFZ", zaproponowano model struktury XML raportującej zdarzenia medyczne. Jest to opis XML'owy **zestawu podpisanych danych**, o którym mowa w Koncepcji. Niektóre z elementów struktury XML mają charakter obligatoryjny, inne fakultatywny, co czyni ją uniwersalną, tj. możliwą do zastosowania również w sytuacjach niestandardowych, typu: brak karty KUZ lub KSM, tryb off-line (brak bieżącego „znacznika czasu"). Określono, że w przypadku braku dostępu do serwera znakowania czasem, udostępnionego świadczeniodawcom przez NFZ, można użyć „daty pewnej", czyli kwalifikowanego znacznika czasu, wystawionego przez podmiot komercyjny, a w ostateczności „deklarowanej daty", czyli daty systemowej, która określa moment wykonywania świadczenia, i która jest poświadczana podpisem elektronicznym specjalisty medycznego, udzielającego świadczenia.

„Znacznik czasu" wystawiany przez NFZ lub kwalifikowany podmiot w rozumieniu ustawy o podpisie elektronicznym, potwierdza czas udzielenia danego świadczenia medycznego w sposób nie budzący wątpliwości. Inaczej jest z „deklarowaną datą", jednak również w tym przypadku można mówić o znacznym bezpieczeństwie stosowania. Mianowicie, gdy NFZ rozpozna, że pewna grupa świadczeniodawców istotnie częściej stosuje „deklarowaną datę" (lub np. „brak karty KUZ") niż pozostali, zostanie objęta szczególnym nadzorem i będą wobec niej stosowane w pierwszej kolejności „celowane kontrole"; można założyć, że takie procedury kontrolne NFZ bardzo skutecznie ograniczą pomysły sprawozdawania nieistniejących świadczeń.

Gdyby po 2-3 latach działania systemu RUM II okazało się, że ilość nadużyć z powodu braku znaczników czasu uzyskiwanych w trybie on-line, jest istotna, to będzie można wprowadzić (poprzez zmianę zarządzenia Prezesa NFZ) wymaganie, iż „schemat XML" MUSI zawierać znaczniki czasu NFZ, kwalifikowanych CA lub pochodzące ze specjalnych czytników, pod groźbą odrzucenia na etapie wstępnej weryfikacji. Dopiero wtedy świadczeniodawcy zostaną zmuszeni do zakupu urządzeń, które zapewnią im znaczniki czasu uzyskiwane w trybie off-line. Spotka się to z pewnością ze sprzeciwem różnych grup interesu, **ale wtedy**

NFZ będzie dysponował rzeczowymi argumentami, przemawiającymi za wprowadzeniem takiego wymagania i w konsekwencji koniecznością wyłożenia dodatkowo min. kilkuset zł przez każdego ze świadczeniodawców.

Ad.c. Ataki *malware* na systemy podpisu elektronicznego w ogromnej większości są typu „GUI[2]", czyli *co innego jest prezentowane, a co innego podpisywane*. Specjalne czytniki nie są w stanie temu przeszkodzić, a podstawową funkcją zabezpieczającą takiego czytnika jest dzisiaj jedynie ochrona PIN-ów. Polega to na tym, że czytnik ma wbudowany pinpad (klawiaturę numeryczną) i nie pozwala na wykonanie rozkazów APDU, które są związane z PIN-em, a które pochodzą od aplikacji podpisującej. Każdy taki rozkaz jest blokowany i zamiast niego wymuszane jest podanie kodu PIN za pomocą wbudowanego pinpad'a. Wadą takiego rozwiązania jest konieczność podawania PIN-u przy każdym podpisie. Gdyby podpis medyczny świadczeniobiorcy wymagał PIN-u, to zastosowanie takich czytników byłoby być może zasadne. Jednak w projekcie RUM II pacjent nie podaje PIN-u, a jedynie lekarz. Dla tego drugiego konieczność pracy w trybie „jeden podpis = jeden PIN" byłaby dodatkowym utrudnieniem i argumentem za odstąpieniem w ogóle od stosowania kart KSM dla potwierdzania udzielanych świadczeń („zamiast leczyć lekarze muszą tracić czas na niepotrzebne procedury techniczne"). Sugerujemy, aby – podobnie jak to jest w przepisach dot. kwalifikowanych podpisów elektronicznych – wybór trybu: „jeden PIN = jeden podpis" lub „jeden PIN = wiele podpisow", pozostawić do decyzji lekarza. W związku z tym stwierdzamy, że specjalne czytniki w nieznacznym stopniu chronią przed atakami ze strony złośliwego oprogramowania i bardziej racjonalne jest, dla przeciwdziałania takiemu zagrożeniu, instalowanie oprogramowania typu „personal firewall" monitorującego całe środowisko aplikacji, niż specjalnego czytnika.

Reasumując: rekomendujemy zastosowanie typowych czytników kart KUZ, KSA i KSM w Fazie I („rejestracja") i w pierwszym okresie Fazy II („potwierdzania świadczeń"). Po 2-3 latach Fazy II należy dokonać weryfikacji, czy pozostawienie „deklarowanej daty" w sytuacji braku połączenia on-line z serwerem znakowania czasem jest słabością wykorzystywaną przez nieuczciwych świadczeniodawców. Dopiero na takiej podstawie należy w przyszłości podjąć decyzję o ewentualnym wprowadzeniu obligatoryjności znakowania czasem każdego sprawozdawanego rekordu, czyli wykonywania znakowania czasem również w trybie off-line za pomocą specjalnego urządzenia (np. „bezpiecznego czytnika"). Takie podejście pozwoli to na istotne ograniczenie kosztów na pierwszym etapie wdrożenia kart KUZ, KSA i KSM po stronie świadczeniodawców.

[2] ang. *Graphical User Interface*

OCENA POPRAWNOŚCI OSZACOWANIA BUDŻETU

Oszacowania zawarte w koncepcji NFZ dot. kosztów wydania kart KSM, KSA i KUZ, na poziomie 1,8 EUR za kartę w 2010 roku (co po uwzględnieniu inflacji w strefie euro daje 1,96 euro za kartę w 2014 roku), są zbliżone do wykonanego przez doradcę rozeznania rynku, które wskazuje, że należy oczekiwać w przetargu kwoty rzędu 2 euro/kartę netto.

Zwracamy uwagę, że w koncepcji NFZ koszty zostały policzone bez podatku VAT, który w oszacowaniu budżetu należy doliczyć.

Oszacowane przez doradcę koszty nabycia, personalizacji i dystrybucji kart KUZ i KSA dla etapu masowego wynoszą łącznie 358,3 mln zł wobec 303,4 mln zł przyjętych w koncepcji NFZ (wzrost o 18%), a dla „dodruków" - 188,7 mln zł wobec 177,4 mln zł w koncepcji NFZ (wzrost o 6,4%). Wzrost szacowania kosztów budżetowych wynika przede wszystkim z doliczenia podatku VAT do ceny karty.

W związku z tym, że w chwili obecnej nie planuje się wdrażania „specjalnego czytnika", koszt czytników będzie zdecydowanie niższy, zależny od liczby sztuk nabywanych przez świadczeniodawcę. Koszt ten można szacować na ok. 15-35 EUR za szt. (przy zakupie od 1 do 50 czytników jednoszczelinowych) lub ok. 45 EUR za szt. (przy pojedynczych zakupach) dla czytników dwuszczelinowych - zamiast planowanego kosztu 90 EUR. Zmniejszy to zdecydowanie obciążenie finansowe świadczeniodawców.

Koniec dokumentu