Narodowy Fundusz Zdrowia

ENIGMA

4pi ANALYST

Projekt: *Usługa doradztwa eksperckiego w ramach programu wdrożenia silnych mechanizmów identyfikacji i uwierzytelniania na potrzeby systemu Rejestru Usług Medycznych II (RUM II) dla Centrali Narodowego Funduszu Zdrowia*

Specyfikacja zmian systemów obsługi transakcji po stronie NFZ i Świadczeniodawców

Wersja: *1.10*
Autor: *Zespół Wykonawcy*
Data: *17.12.2014*

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

1. WPROWADZENIE

Dokument zawiera wysokopoziomową specyfikację zmian w systemach NFZ oraz systemach świadczeniodawców jaka będzie wymagana w ramach wprowadzenia systemu RUM II. W dokumencie znajduje się również szczegółowa specyfikacja komunikatów sprawozdawczych oraz algorytm weryfikacji i walidacji danych sprawozdawczych w zakresie podpisów elektronicznych.

2. SPOSÓB OPISU WYMAGAŃ

Dla wszystkich wymagań funkcjonalnych i niefunkcjonalnych zastosowana zostanie ta sama forma opisu wymagań. Znaczenie poszczególnych kolumn tabeli wymagań zostało opisane w poniższej tabeli.

Tabela 1. Definicja informacji w tabelach wymagań

Nazwa kolumny	Opis
ID	Kolejny numer wymagania (WF – dla wymagań funkcjonalnych i WN – dla wymagań niefunkcjonalnych).
Opis wymagania	Opis wymagania.

3. WYSOKOPOZIOMOWA SPECYFIKACJA ZMIAN SYSTEMÓW OBSŁUGI TRANSAKCJI ROZLICZENIOWYCH NFZ

3.1. Porównanie funkcjonalności RUM II z budowanym systemem PKI

Tabela poniżej zawiera zestawienie wymaganych interfejsów do systemu PKI z wymaganiami SIZW. Wszystkie niezbędne interfejsy mają pokrycie w wymaganiach SIWZ.

Tabela 2. Porównanie wymaganych interfejsów systemu PKI z zapisami SIWZ dla systemu PKI

Wymagane interfejsy	Zapis SIWZ dla PKI
Funkcja generowania kluczy dla algorytmu RSA i ECC.	FN.23 […] Pobranie wygenerowanego certyfikatu wraz z kluczami kryptograficznymi,
Funkcja wystawiania certyfikatów X.509 na podstawie określonego profilu	FN.23 […]Wprowadzanie danych niezbędnych do wydania certyfikatu zgodnie z profilem certyfikatu
Funkcja zwracająca wszystkie certyfikaty danego użytkownika wraz z ich statusem.	FN.48 Reguły publikacji FN 41. […] wyszukanie certyfikatu i pobranie informacji o jego statusie
Funkcja zwracająca status (ważny/unieważniony/zawieszony) certyfikatu o danym numerze seryjnym.	FN 41. […] wyszukanie certyfikatu i pobranie informacji o jego statusie.
Funkcja unieważniania wszystkich certyfikatów użytkownika jednoznacznie wskazanego przez podzbiór jego atrybutów.	FN 41. […] Wykonanie operacji zmiany statusu certyfikatu: unieważnienie, czasowe zawieszenie, uchylanie zawieszania
Funkcja unieważniania wskazanego certyfikatu.	FN 41. […] Wykonanie operacji zmiany statusu certyfikatu: unieważnienie, czasowe zawieszenie, uchylanie zawieszania
Funkcja wystawiania CV certyfikatu dla podanych danych.	FN 62 […] wydawanie certyfikatów CVC zgodnie z wybranym profilem
Funkcja znakowania czasem.	FN.9 Znakowanie czasem

Interfejsy zrealizowane są w technologii WebServices za wyjątkiem funkcji znakowania czasem.	FN.23 […] Wykorzystanie usług sieciowych (ang. webservices) do komunikacji z zewnętrznymi systemami.

Tabela poniżej zawiera porównanie wymagań wydajnościowych systemu RUM II z wymaganymi parametrami systemu PKI. Na czerwono zaznaczone są wymagania RUM II nie spełniane przez system PKI

Tabela 3. Porównanie wymagań wydajnościowych systemu RUMII z wymaganiami wydajnościowymi systemu PKI

Wymagane interfejsy	Zapis SIWZ dla PKI
Liczba jednocześnie ważnych kart KUZ, każda karta zawiera 3 klucze i certyfikaty: poniżej 40 mln	NF.21 Zakładana liczba certyfikatów dla karty KUZ Usługi rejestracji certyfikatów, wydawania certyfikatów, unieważnienia certyfikatów, powinny umożliwiać obsługę 40 mln ważnych certyfikatów dla każdego z wymienionych rodzajów: - dla pieczęci elektronicznej KUZ, - do uwierzytelnienia dla ubezpieczonego (KUZ), - do weryfikacji podpisu elektronicznego (KUZ).
Liczba jednocześnie ważnych kart KSA zawierających jeden klucz i certyfikat: poniżej 100 tyś.	NF.22 Zakładana liczba certyfikatów dla karty SM Usługi rejestracji certyfikatów, wydawania certyfikatów, unieważnienia certyfikatów powinny umożliwiać obsługę 500 tyś. ważnych certyfikatów dla każdego z wymienionych rodzajów: - do uwierzytelnienia dla SM, - do podpisu dla SM.
Liczba dziennie wydawanych kart KUZ: 100 tyś.	NF.23 Wydajność usługi rejestracji/wydawania certyfikatów dla karty KUZ Usługi rejestracji certyfikatów, wydawania certyfikatów powinny zapewniać wydajność w trybie ciągłym na poziomie 20 certyfikatów na sekundę dla kluczy RSA o długości 2048bit lub ECC o długości kluczy 224bit na sekundę dla każdego z rodzajów certyfikatów. Brak jest wymagań na wydajność generowania kluczy dla kart KUZ, co oznacza że klucze dla kart KUZ nie mogą być generowane w systemie PKI i funkcja ta musi być realizowana po stronie podmiotu personalizującego karty.

Liczba dziennie wydawanych kart KSA: poniżej 1000	NF.24 Wydajność usługi rejestracji/wydawania certyfikatów dla karty SM Usługi rejestracji certyfikatów, wydawania certyfikatów powinny zapewniać wydajność w trybie ciągłym na poziomie 4 certyfikatów na sekundę dla każdego z rodzajów certyfikatów: - do uwierzytelnienia dla SM, - do podpisu dla SM.
Oszacowanie liczby niezbędnych znaczników czasu i odpowiedzi OCSP przy następujących założeniach: • 150 mln zdarzeń medycznych rocznie • Każde zdarzenie medyczne opatrywane jest znacznikiem czasu • Zdarzenia medyczne zachodzą w trybie 365/8h Zakładając równomierny rozkład wymagane jest 14 znakowań czasem na sekundę.	NF.29 Wydajność usługi znakowania czasem. Usługi znakowania czasem powinny zapewniać wydajność na poziomie 200 zapytań na sekundę (zakładany pik dzienny). NF.28 Wydajność usługi weryfikacji ważności certyfikatów Usługi weryfikacji ważności certyfikatów (OCSP) powinny zapewniać wydajność na poziomie 200 zapytań na sekundę (zakładany pik dzienny).

3.2. Modyfikacje aplikacji świadczeniodawców

Tabela 4. Opis wymagań funkcjonalnych

ID	Opis
WF-1	Składanie podpisów elektronicznych zgodnie z algorytmem określonym w rozdziale 4 pod danymi sprawozdawanymi do NFZ.
WF-2	Wykrywanie (za pomocą middleware systemu SZUK) konieczności modyfikacji struktury karty KUZ i informowanie o tym świadczeniobiorcy.
WF-3	Odczytu danych świadczeniobiorców z karty KUZ.
WF-4	Wykorzystania kart KSA/KSM do uwierzytelnienia w systemie eWUS.

3.3. Modyfikacje systemów rozliczeniowych NFZ

Tabela 5. Opis wymagań funkcjonalnych

ID	Opis

ID	Opis
WF-1	Przyjmowanie komunikatów XML o nowej strukturze.
WF-2	Weryfikacja i walidacja podpisanych danych sprawozdawczych zgodnie z algorytmem opisanym w rozdziale 5.
WF-3	Gromadzenie danych zawartych w nowych elementach struktury komunikatów XML.

3.4. Modyfikacje Portalu Świadczeniodawcy

Tabela 6. Opis wymagań funkcjonalnych

ID	Opis
WF-1	Osadzenie na stronach portalu podstron systemu SZUK.
WF-2	Dodanie mechanizmu logowania przy pomocy karty KSA.

3.5. Modyfikacje ZIP

Tabela 7. Opis wymagań funkcjonalnych

ID	Opis
WF-3	Osadzenie na stronach portalu podstron systemu SZUK.
WF-4	Dodanie mechanizmu logowania przy pomocy karty KUZ i kluczy do uwierzytelnienia.

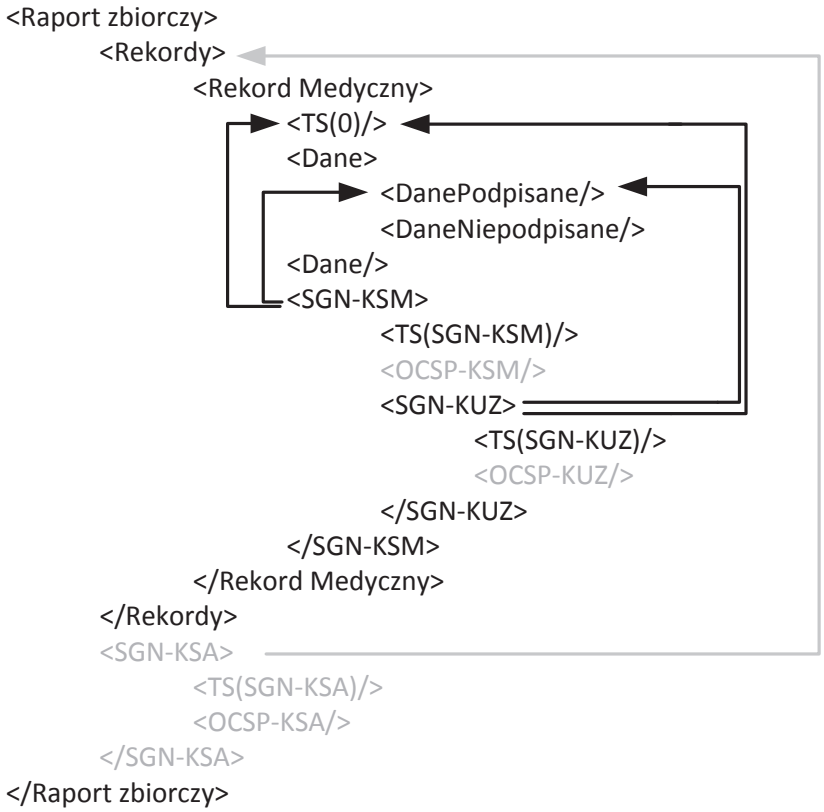
3.6. Modyfikacje eWUŚ

Tabela 8. Opis wymagań funkcjonalnych

ID	Opis
WF-1	Dodanie mechanizmu logowania przy pomocy karty KSA
WF-2	Osadzenie apletu pozwalającego na pobieranie danych świadczeniobiorcy z karty KUZ

4. ZAKRES I FORMATY DANYCH

1. Poglądowy model struktury XML raportującej zdarzenia medyczne przedstawiony jest na rysunku poniżej.

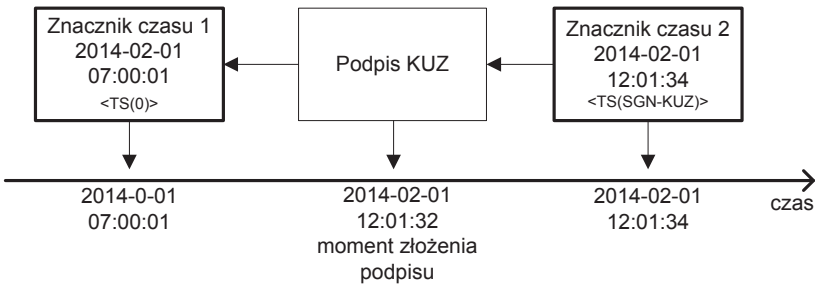


Rysunek 1. Model dokumentu sprawozdawczego zdarzeń medycznych

Na rysunku powyżej elementy opcjonalne oznaczono kolorem szarym. Strzałki wskazują te elementy danych, które zostaną podpisane przez dany podpis. Zwraca się uwagę, że podpisy obejmują jednocześnie kilka rozłącznych fragmentów dokumentu XML. W Fazie II zagnieżdżony podpis <SGN-KUZ> jest kontrpodpisem i obejmuje również podpis <SGN-KSM>, natomiast w Fazie I <SGN-KUZ> jest podpisem samodzielnym – podpisu <SGN-KSM> w ogóle nie ma.

Ideą schematu jest wprowadzenie mechanizmu pozwalającego na stwierdzenie, że dane zdarzenie medyczne wystąpiło w pewnym przedziale czasu. Granice tego przedziału wyznaczane są za pomocą kryptograficznych znaczników czasu (patrz Rysunek 2), zawierających dokładną datę i godzinę. Podpisanie przy pomocy karty KUZ znacznika czasu <TS(0)> dowodzi, że podpis KUZ wykonany został po dacie wystawienia znacznika (ponieważ znacznik czasu istniał wcześniej niż złożony pod nim podpis). Oznakowanie drugim znacznikiem czasu (<TS(SGN-KUZ)>) istniejącego już podpisu KUZ dowodzi, że podpis ten został złożony wcześniej niż czas i data zawarta w drugim znaczniku. Stosując

oba mechanizmy jednocześnie uzyskujemy pewność, że podpis elektroniczny KUZ został złożony w przedziale pomiędzy oboma znacznikami czasu. Analogiczny mechanizm stosuje się dla podpisu złożonego przy pomocy karty KSM.



Rysunek 2. Wyznaczanie przedziału czasu dla zdarzenia medycznego

Funkcje znacznika czasu <TS(0)> ograniczającego przedział czasu „od dołu", mogą również pełnić odpowiedzi systemu eWUŚ (zawiera dokładną datę i godzinę), a nawet data systemowa w sytuacji niedostępności serwerów znakowania czasem i systemu eWUŚ.

Semantyka poszczególnych struktur z ***Rysunek 1*** jest następująca:

- <Raport zbiorczy> - struktura przysyłki służącej do raportowania zdarzeń medycznych do NFZ
- <Rekordy> - lista rekordów medycznych.
- <Rekord medyczny> - struktura opisująca pojedyncze zdarzenie medyczne.
- <TS(0)> stempel czasu w postaci (alternatywa):
    - odpowiedź systemu eWUŚ dotycząca danego pacjenta;
    - znacznik czasu uzyskiwany dla pustych danych, w pierwszym kroku procedury rejestracji zdarzenia medycznego przez lekarza lub pracownika administracji (jeśli dotyczy rejestracji pacjenta);
    - data systemowa (o ile nie było możliwe uzyskanie odpowiedzi eWUŚ ani znacznika czasu).
- <Dane> - dane zdarzenia medycznego. Dane są strukturą złożoną z dwóch części: części stałej <DanePodpisane>, która podlega podpisowi elektronicznemu KSM (Faza II) i podpisowi medycznemu KUZ (Faza I i II) oraz części możliwej do modyfikacji <DaneNiepodpisane>, która podpisom nie podlega.
- <DanePodpisane> identyfikator świadczeniodawcy oraz miejsce wykonywania świadczenia.
- <SGN-KUZ> - podpis medyczny złożony przy pomocy karty KUZ, obejmuje on: <DanePodpisane>, <TS(0)> oraz – w Fazie II – <SGN-KSM>, przy czym w przypadku, gdy występuje <SGN-KSM> to podpis KUZ nie musi obejmować <TS(0)>, aczkolwiek jest to dopuszczalne.
- <SGN-KSM> - podpis elektroniczny wykonywany w Fazie II, złożony przy pomocy karty KSM obejmujący <DanePodpisywane> oraz <TS(0)>.
- <SGN-KSA> - opcjonalny podpis elektroniczny świadczeniodawcy, który złożono przy pomocy karty KSA pracownika administracji, obejmujący całość sprawozdawanych danych.
- <TS(SGN-KUZ)> - znacznik czasu, którym opatrzono podpis <SGN-KUZ>.
- <TS(SGN-KSM)> - znacznik czasu, którym opatrzono podpis <SGN-KSM>.
- <TS(SGN-KSA)> - znacznik czasu, którym opatrzono <SGN-KSA>.
- <OCSP-KUZ> - odpowiedź OCSP dla certyfikatu do weryfikacji <SGN-KUZ>.
- <OCSP-KSM> - odpowiedź OCSP dla certyfikatu do weryfikacji <SGN-KSM>.

- <OCSP-KSA> - odpowiedź OCSP dla certyfikatu do weryfikacji <SGN-KSA>.

Zwraca się uwagę na następujące aspekty:

- Podpisy pacjenta i lekarza w ramach pojedynczego rekordu medycznego są podpisami zagnieżdżonymi w sensie struktur podpisu elektronicznego zdefiniowanych w specyfikacji technicznej ETSI TS 101 903 „XML Advanced Electronic Signatures (XAdES)", tj. najpierw jest składany podpis KSM, a następnie KUZ.
- Obecność podpisów KUZ i KSM w ramach pojedynczego rekordu medycznego nie jest obowiązkowa dla poprawności struktury. W przypadku niedostępności kart KUZ lub KSM, dowolny z podpisów (lub oba na raz) może nie występować.
- Znaczniki czasu <TS(SGN-KSM)>, <TS(SGN-KSA)>, <TS(SGN-KUZ)> są zwykłymi znacznikami czasu wg ETSI i są osadzane w strukturach podpisu elektronicznego.
- Znacznik czasu <TS(0)> jest zwykłym znacznikiem czasu, tyle że uzyskanym dla pustego ciągu danych wejściowych lub może to być odpowiedź eWUŚ.
- Jeżeli w rekordzie medycznym występują oba podpisy (KSM i KUZ – Faza II), to wystarczy, aby tylko podpis KUZ był oznakowany czasem.
- Odpowiedzi OCSP będą podstawowym mechanizmem wspierającym weryfikację ważności podpisów elektronicznych, przy czym będą mogły być stosowane zamiennie lub uzupełniająco z listami CRL. Dla potrzeb długoterminowej ważności podpisów elektronicznych należałoby, w przypadku braku odpowiedzi OCSP, wykorzystywać listy CRL dot. KUZ i KSM (ewentualnie również KSA).

2. Algorytm podpisywania pojedynczego rekordu medycznego, przy założeniu, że ze strony świadczeniodawcy wykorzystywana będzie karta KSM (Faza II) oraz że przed udzieleniem świadczenia uzyskano odpowiedź systemu eWUŚ dla świadczeniobiorcy:
    a) przygotuj <DanePodpisywane> tj. identyfikator świadczeniodawcy, wskazanie lokalizacji;
    b) przyjmij jako <TS(0)> posiadaną odpowiedź eWUŚ;
    c) podpisz <DanePodpisane>, <TS(0)> przy pomocy KSM albo wprowadź informację o oświadczeniu lekarza dotyczącą braku karty KSM;
    d) opcjonalnie uzyskaj dla podpisu <SGN-KSM> odpowiedź OCSP i osadź ją w strukturach podpisu;
    e) jeżeli karta KUZ jest dostępna to:
        i. Jeżeli podpis KSM został złożony to:
            a. Podpisz <SGN-KSM> przy pomocy KUZ
        ii. W przeciwnym wypadku:
            a. Podpisz <DanePodpisane> oraz <TS(0)> przy pomocy KUZ,
        iii. Uzyskaj dla podpisu KUZ odpowiedź OCSP i osadź ją w strukturach podpisu;
    f) jeżeli karta KUZ nie jest dostępna to wprowadź informację o oświadczeniu pacjenta dot. braku karty KUZ.
    g) oznakuj czasem ostatni złożony podpis (<SGN-KSM> lub <SGN-KUZ>).

3. Algorytm przygotowania raportu zbiorczego:
    a) przygotuj dokument raportu poprzez dołączenie wszystkich rekordów medycznych;

b) opcjonalnie podpisz dokument podpisem elektronicznym pracownika administracyjnego świadczeniodawcy (przy pomocy karty KSA)
    i. oznakuj podpis czasem;
    ii. opcjonalnie uzyskaj dla podpisu odpowiedź OCSP i osadź ją w strukturach podpisanej wiadomości.

Szczegółowa specyfikacja komunikatów sprawozdawczych znajduje się w załączniku do dokumentu.

5. ALGORYTM WERYFIKACJI I WALIDACJI PODPISÓW

5.1. Faza 1

W Fazie I (rejestracja) *podpisany zestaw danych* będzie ograniczony do potwierdzenia faktu bytności pacjenta u świadczeniodawcy. Na tym etapie „schemat XML" dot. sprawozdania pojedynczego zdarzenia medycznego, zostanie rozszerzony jedynie o podpis medyczny kartą KUZ świadczeniobiorcy, gdzie w „body" podpisywanej wiadomości będzie kod świadczeniodawcy, wskazanie miejsca wykonywania świadczenia i data świadczenia. Poszczególne elementy będą następującej postaci:

a) kod świadczeniodawcy: „KŚ: xxxxx", gdzie xxxx oznacza numer nadany przez NFZ w ramach realizacji stosownej umowy.

b) miejsce wykonywania świadczenia składa się z pola „MUS" kodowanego jako *string*, postaci: „MUS: yyyyy", gdzie łańcuch yyyyy jest zgodny z kodem określonym w ramach stosownej umowy na wykonywanie świadczeń.

c) data_świadczenia_1 – może to być (alternatywnie):

- znacznik czasu (wydany przez NFZ lub komercyjny, kwalifikowany podmiot);
- odpowiedź eWUŚ dotycząca danego świadczeniobiorcy (wydana przez NFZ) lub
- „deklarowana data" w postaci: „Data świadczenia: YYMMDD GGMM".

W przypadku braku podpisu KUZ, zostanie wprowadzona informacja postaci: „Kod braku KUZ: xxx", gdzie xxx będzie przyjmować następujące wartości: „zapomniana", „awaria", „zgubiona", „nigdy nie posiadana".

Podpis kartą KUZ, zawierający powyższe dane, jest znakowany czasem przez NFZ lub kwalifikowany komercyjny podmiot. Ten znacznik czasu zawiera datę_świadczenia_2. W przypadku braku znacznika czasu (NFZ lub „kwalifikowanego komercyjnego"), datą_świadczenia_2 może być też „deklarowana data". Data_świadczenia_1 i data_świadczenia_2 pełnią rolę typu: „nie wcześniej niż" i „nie później niż", tj. rzeczywisty podpis kartą KUZ odbywa się w przedziale czasu ograniczony tymi wskazaniami czasu.

Implikacje dla aplikacji weryfikującej

- Kotwice zaufania: weryfikacja podpisów elektronicznych (podpis kartą KUZ, odpowiedzi OCSP i znaczników czasu) wymaga określenia (skonfigurowania) tzw. *kotwic zaufania*, którymi będą klucze publiczne: CA NFZ dla weryfikacji podpisów struktur danych tworzonych przez NFZ i root'a krajowego dla znaczników czasu wydawanych przez komercyjne, kwalifikowane podmioty.
- Status certyfikatu KUZ: jeśli w *podpisanym zestawie danych* nie ma odpowiedzi OCSP (lub jest inna niż „valid"), to aplikacja weryfikująca powinna pobrać bieżącą odpowiedź OCSP dla certyfikatu lub bieżącą listę CRL. Jeśli odpowiedź OCSP zawiera

wskazanie „valid", to uznaje się, że dany certyfikat podpisu medycznego KUZ jest ważny, natomiast w przeciwnym przypadku aplikacja musi sięgnąć do listy CRL, wydanej po data_świadczenia_2 i określić status certyfikatu na jej podstawie. Należy uznać, że status jest „valid", jeśli lista CRL nie zawiera numeru certyfikatu lub stosowny wpis o unieważnieniu wskazuje, że nastąpiło ono po data_świadczenia_2.

- Status certyfikatu znacznika czasu: aplikacja weryfikująca powinna pobrać bieżącą listę ARL (lub CRL, zawierającą ARL) NFZ lub komercyjnego CA, i na tej podstawie zweryfikować certyfikat klucza publicznego znacznika czasu.
- Status certyfikatu odpowiedzi OCSP – aplikacja weryfikująca powinna pobrać bieżącą listę ARL (lub CRL, zawierającą ARL) NFZ.

Zakres weryfikacji

- Weryfikacja poprawności struktury *podpisanego zestawu danych* i weryfikacja ważności podpisanych wewnętrznych struktur (TS, OCSP, kod eWUŚ, podpis medyczny KUZ). W przypadku negatywnego wyniku – nieprzyjęcie całego schematu i wskazanie kodem błędu powodu. Kod błędu powinien być odpowiednio zróżnicowany i dotyczyć „pierwszej niezgodności".
- Rozdzielczość czasowa

  Między data_świadczenia_1 i data_świadczenia_2 nie może upłynąć więcej niż wymagany i ustalony z góry okres czasu. Dla potrzeb Fazy 1, wartość ta powinna wynosić 24 godziny i to powinno podlegać weryfikacji.
- Kod świadczeniodawcy – weryfikacja, czy podpisany kod świadczeniodawcy (*body* wiadomości podpisanej kartą KUZ) jest zgodny z umową; w przypadku wykorzystywania „odpowiedzi eWUŚ" jako daty_świadczenia_1, to dodatkowo sprawdzanie, czy kod zawarty w odpowiedzi eWUŚ jest taki sam, jak w *body* podpisanej wiadomości.
- Miejsce udzielenia świadczenia – odczytana z *podpisanego zestawu danych* wartość powinna być zgodna z deklarowanym przez świadczeniodawcę potencjałem i zgodna z innymi informacjami zawartymi w schemacie XML danego świadczenia.
- W przypadku braku pewnych elementów, tj. użycie „deklarowanej daty" i/lub braku podpisu medycznego, aplikacja weryfikująca odnotowuje ten fakt w stosownych rejestrach (z rozdzielczością pozwalającą na określenie, czy chodzi o data_świadczenia_1, data_świadczenia_2, czy podpis medyczny), które służą do tworzenia statystyk. Gdy audyt NFZ uzna, że liczba „wyjątków" w sprawozdaniach danego świadczeniodawcy budzi wątpliwości, podejmuje działania wyjaśniające.

5.2. Faza 2

W Fazie II podpisy kartą KSM pozwolą na zweryfikowanie, czy świadczenie zostało wykonane przez właściwego specjalistę medycznego. Na tym etapie „schemat XML" dot. sprawozdania

pojedynczego zdarzenia medycznego nie będzie zawierał podpisu wykonanego w rejestracji, a zamiast niego taki podpis będzie wykonywany w gabinecie lekarskim (lub w podobnych lokalizacjach, np. miejscach zabiegów fizjoterapeutycznych). Pozostałe zasady dot. czasu określania zdarzenia medycznego, miejsca udzielania świadczenia i wskazywania świadczeniodawcy, nie ulegają zmianie w stosunku do Fazy 1, co pozwoli na potwierdzenie faktu przyjęcia pacjenta przez konkretnego specjalistę medycznego u danego świadczeniodawcy.

Podpisy pacjenta i lekarza w ramach pojedynczego rekordu medycznego są podpisami zagnieżdżonymi (kontrpodpisy) w sensie struktur podpisu elektronicznego zdefiniowanych w specyfikacji technicznej ETSI TS 101 903 „XML Advanced Electronic Signatures (XAdES)", i podpis KSM jest składany wcześniej niż KUZ.

W przypadku braku podpisu KSM musi być wprowadzona odpowiednia informacja o powodach, czyli „Kod braku KSM: yyy", analogicznie jak dla podpisu KUZ.

Wymagania dla aplikacji podpisującej są wobec tego w Fazie 2 praktycznie identyczne, jak w Fazie 1. Jedyne nieznaczne różnice są wymienione niżej.

Implikacje dla aplikacji weryfikującej

- Kotwice zaufania: mimo, że podpis specjalisty medycznego może być wykonany również za pomocą narzędzi wydanych przez komercyjny, kwalifikowany podmiot, to nie ma to wpływu na zakres „kotwic zaufania", gdyż będzie to w takim przypadku klucz root'a krajowego, jak dla komercyjnych znaczników czasu; jedynie w treści certyfikatu można sprawdzić, czy znajduje się adnotacja o prawie wykonywania zawodu.

Zakres weryfikacji

- Weryfikacja poprawności struktury *podpisanego zestawu danych* i weryfikacja ważności podpisanych wewnętrznych struktur musi dodatkowo zawierać „podpis KSM".
- Rozdzielczość czasowa

  W Fazie 2 zasadne jest przyjęcie zróżnicowanych wymagań dla określenia dokładności czasu wykonywania świadczenia medycznego. W związku z tym dla niektórych świadczeń maksymalny okres czasu między data_świadczenia_1 i data_świadczenia_2 może zostać utrzymany na poziomie 24 godzin, natomiast dla innych zostanie narzucone bardziej restrykcyjne wymaganie, np. sesje psychoterapeutyczne – 2 godziny, co będzie podlegało weryfikacji.
- Do listy „braku pewnych elementów" w *podpisanym zestawie danych* zostanie dodany element „podpis KSM", którego brak będzie również podlegał analizom statystycznym.
- Lekarz udzielający świadczenie odczytany z certyfikatu, którym weryfikujemy podpis KSM powinien być zgodny z deklarowanym przez świadczeniodawcę potencjałem oraz z innymi informacjami zawartymi w schemacie XML danego świadczenia.

KONIEC DOKUMENTU