Zachodniopomorski Uniwersytet Technologiczny w Szczecinie

WI

Metoda długookresowego przechowywania elektronicznych dokumentów zdrowotnych w rozproszonych rejestrach medycznych

Rozprawa doktorska

mgr inż. Tomasz Hyla

promotor:
prof. dr hab. inż. Włodzimierz Bielecki

Szczecin 2011

Spis treści:

SŁOWNIK SKRÓTÓW ..... - 5 -

1. WSTĘP ..... - 7 -

1.1. CHARAKTERYSTYKA PROBLEMU ..... - 7 -
1.2. PODSTAWOWE DEFINICJE ..... - 8 -
1.3. CEL I TEZA ROZPRAWY ..... - 11 -
1.4. MIEJSCE WYNIKÓW ROZPRAWY ..... - 13 -
1.5. METODYKA BADAŃ ..... - 14 -
1.6. KORZYŚCI Z WDROŻENIA WYNIKÓW ROZPRAWY ..... - 15 -
1.7. STRUKTURA ROZPRAWY ..... - 17 -

2. ELEKTRONICZNE DOKUMENTY ZDROWOTNE ..... - 18 -

2.1. DEFINICJA ELEKTRONICZNEGO DOKUMENTU ZDROWOTNEGO (EHR) ..... - 18 -
2.2. MODELE INFORMACYJNE EHR ..... - 18 -
2.2.1 Model jednopoziomowy/dwupoziomowy ..... - 19 -
2.2.2 Standardy dotyczące struktury EHR ..... - 20 -
2.2.2.1 CEN ENV 13606:2000 ..... - 20 -
2.2.2.2 GEHR/openEHR ..... - 21 -
2.2.2.3 CEN/ISO EN13606:2009 ..... - 22 -
2.2.2.4 HL7 CDA R2 ..... - 24 -
2.2.2.5 DICOM Strutured Reporting ..... - 25 -
2.2.3 Podsumowanie ..... - 26 -
2.3. SYSTEMY EHR ..... - 27 -
2.3.1 Wpływ na poprawę jakości ochrony zdrowia ..... - 27 -
2.3.2 Rejestry i repozytoria ..... - 28 -
2.3.3 Rejestr ebXML ..... - 28 -
2.3.4 Profil IHE – Wymiana Dokumentów Pomiędzy Przedsiębiorstwami ..... - 29 -
2.3.5 Narodowe systemy ochrony zdrowia ..... - 32 -
2.3.5.1 System kanadyjski ..... - 32 -
2.3.5.2 System brytyjski ..... - 33 -
2.3.5.3 System estoński ..... - 33 -
2.3.5.4 System niemiecki ..... - 33 -
2.3.5.5 System turecki ..... - 34 -
2.4. WYMAGANIA ODNOŚNIE DŁUGOTERMINOWEGO PRZECHOWANIA EHR ..... - 34 -
2.5. INFRASTRUKTURA KLUCZA PUBLICZNEGO ..... - 35 -
2.5.1 Podpis cyfrowy ..... - 36 -
2.5.2 Certyfikaty ..... - 36 -
2.5.3 Tworzenie i weryfikacja podpisu cyfrowego ..... - 37 -
2.5.4 Dodatkowe źródła zaufania ..... - 38 -
2.5.4.1 Algorytmy kryptograficzne ..... - 38 -
2.5.4.1 Lista statusu zaufanych usług ..... - 38 -
2.6. DŁUGOTERMINOWE PRZECHOWYWANIE PODPISANYCH DOKUMENTÓW MEDYCZNYCH ..... - 39 -
2.6.1 Podpis cyfrowy w długim okresie ..... - 39 -
2.6.2 Zaufane znaczniki czasu ..... - 39 -
2.6.3 Schematy wiązań binarnych ..... - 40 -
2.6.3 Słowniki uwierzytelniane ..... - 42 -
2.6.4 Przedłużanie ważności pojedynczych, podpisanych cyfrowo dokumentów ..... - 42 -
2.6.5 Przedłużanie ważności grup podpisanych cyfrowo dokumentów ..... - 42 -

2.6.6 Model zaufanego archiwalnego notariatu ..... *- 44 -*
2.6.7 Schemat skumulowanego notariatu ..... *- 45 -*
2.6.8 Specyfikacja składni rekordów dowodowych ..... *- 46 -*
2.6.9 Zaufana usługa archiwizowania ..... *- 47 -*
2.7. PODSUMOWANIE ..... - 49 -
2.7.1 EHR a pozostałe rodzaje dokumentów ..... *- 49 -*
2.7.2 Porównanie prac pokrewnych ..... *- 49 -*

3. METODA DŁUGOOKRESOWEGO PRZECHOWYWANIA ELEKTRONICZNYCH DOKUMENTÓW ZDROWOTNYCH ..... - 52 -

3.1. WSTĘP ..... - 52 -
3.2. DZIAŁANIA SKŁADOWE ..... - 53 -
3.3. OGÓLNA ARCHITEKTURA SYSTEMU EHR ..... - 54 -
3.3.1 Źródła dokumentów zdrowotnych ..... *- 54 -*
3.3.2 Architektura systemu EHR ..... *- 54 -*
3.3.3 Środki zabezpieczeń ..... *- 56 -*
3.4. ZALEŻNOŚCI POMIĘDZY IMPLEMENTACJAMI ALGORYTMÓW W SYSTEMIE EHR ..... - 59 -
3.5. REKORDY POŚWIADCZEŃ REJESTRÓW ..... - 61 -
3.5.1 Warianty użycia Rekordów Poświadczeń Rejestrów ..... *- 61 -*
3.5.2 Struktura Rekordów Poświadczeń Rejestrów ..... *- 63 -*
3.6. DZIAŁANIA SKŁADOWE METODY DPEDZ ..... - 65 -
3.6.1 Dodawanie nowego dokumentu do systemu EHR ..... *- 65 -*
3.6.2 Utworzenie tokenu potwierdzenia nadania ..... *- 67 -*
3.6.3 Utworzenie poświadczeń ..... *- 67 -*
3.6.4 Aktualizacja poświadczeń ..... *- 71 -*
3.6.5 Weryfikacja tokenu potwierdzenia nadania ..... *- 73 -*
3.6.6 Scalanie poświadczeń ..... *- 73 -*
3.6.7 Weryfikacja autentyczności zbioru metadanych z rejestrów ..... *- 75 -*
3.6.8 Weryfikacja niezaprzeczalności EHR ..... *- 77 -*
3.6.9 Weryfikacja niezaprzeczalności pojedynczego dokumentu ..... *- 80 -*
3.7. DODATKOWE ŹRÓDŁA ZAUFANIA ..... - 81 -
3.7.1 Centrum Informacji Długoterminowej ..... *- 81 -*
3.7.2 Lista Polecanych Algorytmów Kryptograficznych ..... *- 83 -*
3.7.3 Komunikacja CID z użytkownikami ..... *- 84 -*
3.8. METODA DPEDZ A PRACE POKREWNE ..... - 86 -
3.9. PODSUMOWANIE ..... - 89 -

4. BADANIA EKSPERYMENTALNE ..... - 90 -

4.1. TESTY WYDAJNOŚCI ..... - 90 -

4.1.1 Środowisko testowe ..... - 90 -

4.1.2 Dane testowe ..... - 92 -

4.1.3 Protokół PDNW ..... - 92 -

4.1.4 Algorytmy tworzenia i aktualizacji RPR ..... - 96 -

4.1.4.1 Algorytm AARPR ..... - 96 -

4.1.4.2 Algorytm APWATS ..... - 103 -

4.1.5 Algorytmy weryfikacji ..... - 104 -

4.1.5.1 Algorytmy AWNR i AWNEHR ..... - 104 -

4.1.5.2 Algorytm AWND ..... - 105 -

4.1.6 Algorytmy tworzenia i weryfikacji tokenu nadania ..... - 107 -

4.2. TESTY BEZPIECZEŃSTWA ..... - 109 -

5. WNIOSKI I PODSUMOWANIE ..... - 119 -

5.1. ODNIESIENIE DO TEZY ..... - 120 -

5.2. ELEMENTY NOWOŚCI ..... - 122 -

5.3. DALSZE PRACE ..... - 123 -

6. ODWOŁANIA ..... - 124 -

6.1. SPIS RYSUNKÓW ..... - 124 -

6.2. SPIS TABEL ..... - 125 -

6.3. BIBLIOGRAFIA ..... - 126 -

ZAŁĄCZNIKI ..... - 132 -

Słownik skrótów

EHR – Electronic Health Record – Elektroniczny Dokument Zdrowotny
ADL – Archetype Definition Language – Język Definiowania Archetypów
HL7 CDA 2 – Health Level 7 Clinical Document Architecture Release 2
ERS – Evidence Records Syntax
SNOMED CT – Systemized Nomenclature of Medicine Clinical Terms
LOINC – Logical Observation Identifiers Names and Codes
IHE XDS – IHE Cross-Enterprise Document Sharing
PKI – Public Key Infrastructure – Infrastruktura Klucza Publicznego
CA – Certification Authority - Urząd Certyfikacji
CRL – Certificate Revocation List – Lista Certyfikatów Odwołanych
TSL – Trusted-service Status List – Lista Statusu Zaufanych Usług
TSA – Timestamp Authority – Urząd Znacznika Czasu
DPEDZ – Metoda Długookresowego Przechowywania Elektronicznych Dokumentów Zdrowotnych
RPR – Rekordy Poświadczeń Rejestrów
SZRPR – System Zarządzania Rekordami Poświadczeń Rejestrów
SWEHR – System Weryfikacji EHR
BRPR – Baza Rekordów Poświadczeń Rejestrów
UZZ – Usługa Zintegrowanego Zarządzania
ZM – Zestaw Metadanych
ATS – Archive Timestamp – Archiwalny Znacznik Czasu
ATSCh – Archive Timestamp Chain – Łańcuch Archiwalnych Znaczników Czasu
TS – Timestamp – Znacznik Czasu
RT – Reduced hash Tree – Zredukowane Drzewo Skrótów
CID – Centrum Informacji Długoterminowej
LPAK – Lista Polecanych Algorytmów Kryptograficznych

Następująca notacja jest używana w przedstawianych poniżej opisach algorytmów:

$EHRS_d$ – domowy system EHR – system EHR w którym pacjent jest zarejestrowany, np.: system działający w miejscu zamieszkania pacjenta;

$EHRS_k$ – *k-ty* zewnętrzny system EHR – system EHR stowarzyszony z domowym system EHR pacjenta, np.: system w innym państwie/regionie;

UZZ_d – Usługa Zintegrowanego Zarządzania EHR w $EHRS_d$;

UZZ_k - Usługa Zintegrowanego Zarządzania EHR w $EHRS_k$;

$BRPR_d$ – Baza Rekordów Poświadczeń Rejestrów przy UZZ_d;

$BRPR_k$ – Baza Rekordów Poświadczeń Rejestrów przy UZZ_k;

$SZRPR_k$ – Menedżer Bezpieczeństwa – System Zarządzania RPR w $EHRS_k$;

$SZRPR_d$ – Menedżer Bezpieczeństwa – System Zarządzania RPR w $EHRS_d$.

P_{id_p} – pacjent o identyfikatorze *p*;

D_i – dokument medyczny *i* – dokument wysłany przez specjalistę ds. ochrony zdrowia do systemu EHR;

M_i – Metadane opisujące D_i lub metadane z $aRPR^k_{id_p}$;

URI_i – Ujednolicony Identyfikator Zasobu (*ang. Unified Resource Identifier*) do D_i w repozytorium;

$W^k_{id_p}$ – wiadomość z $EHRS_k$ do $EHRS_d$ z informacją, że P_{id_p} posiada dokumenty zdrowotne w $EHRS_k$;

M_n – zbiór wszystkich (w ilości *n*) M_i z jednej rundy;

GM_{id_p} – grupa M_i należących do jednego P_{id_p} z jednej rundy;

$ZM^k_{id_p}$ – zbiór wszystkich M_i przechowywanych w $EHRS_k$ należących do P_{id_p};

$ZM^d_{id_p}$ – zbiór wszystkich M_i przechowywanych w $EHRS_d$ należących do P_{id_p};

ZM_{id_p} – zbiór wszystkich $ZM^k_{id_p}$ z wszystkich $EHRS_k$ oraz z $EHRS_d$;

R_n – Rejestr o identyfikatorze n;

RPR_{id_p} – Rekordy Poświadczeń Rejestrów dotyczące P_{id_p};

$RPR^k_{id_p}$ – RPR_{id_p} dotyczące P_{id_p} w $EHRS_k$;

$aRPR^k_{id_p}$ – abstrakt z RPR_{id_p} z $EHRS_k$ (wiadomość składająca się z P_{id_p}, ostatniej wartości *L*, numeru dokumentu *j* i numeru systemu EHR *k);*

SW_{id_p} – element Sekwencja Wpisów z RPR_{id_p};

R_{rd} – element Runda z elementu SW_{id_p} z RPR_{id_p} o lokalnym, wewnętrznym numerze rundy *rd*;

W – element W z elementu Runda z elementu Sekwencja Wpisów z RPR_{id_p};

$RT^{id_p}_{tn+1}$ – zredukowane binarne drzewo skrótów dla P_{id_p} z globalnej rundy o numerze *tn+1;*

1. Wstęp

1.1. Charakterystyka problemu

Niniejsza rozprawa doktorska dotyczy bezpieczeństwa elektronicznych dokumentów zdrowotnych (*ang. EHR – Electronic Health Record*). EHR jest wirtualnym kontenerem przechowującym elektroniczne dokumenty medyczne związane z życiem jednego człowieka od urodzenia aż do śmierci. Głównym celem tworzenia systemów do zarządzania EHR jest zapewnienie ciągłości leczenia i poprawienie jakości ochrony zdrowia. Przez cały okres składowania EHR powinien zapewnić możliwość potwierdzenia, że jego zawartość jest oryginalna i kompletna. Ewentualne błędy, czy braki w dokumentacji medycznej, mogą spowodować postawienie niewłaściwej diagnozy, a tym samym wpłynąć na pogorszenie zdrowia pacjenta. Istotna jest również gwarancja poufności informacji, gdyż jej ujawnienie może nieść negatywne konsekwencje dla pacjenta zarówno w aspekcie ekonomicznym (np. wzrost kosztów ubezpieczenia na życie), jak i osobistym. Aktualnie nie istnieje gotowa metoda długoterminowego przechowywania EHR uwzględniająca wszystkie aspekty bezpieczeństwa.

Obecnie na świecie w trakcie realizacji jest wiele systemów informatycznych ochrony zdrowia implementujących EHR [59], na przykład w Kanadzie, Norwegii, czy w Wielkiej Brytanii. W projektach tych systemów stosuje się różne podejścia do przechowywania danych w zależności od uwarunkowań lokalnych. Dodatkowo istnieje kilkadziesiąt różnych norm opracowanych przez instytucje narodowe i międzynarodowe dotyczących bezpieczeństwa dokumentów medycznych. Z uwagi na wymagania bezpieczeństwa dokumenty medyczne muszą być podpisane cyfrowo. W literaturze naukowej istnieje klika metod pozwalających na długoterminowe przechowywanie podpisanych dokumentów elektronicznych. Metody te jednak nie są przystosowane do dokumentów medycznych i nie uwzględniają specyfiki EHR, na który składają się dokumenty znajdujące się w różnych repozytoriach oraz ich opisy (metadane) znajdujące się w wielu rejestrach.

W Europie i na świecie proces ochrony zdrowia obywateli stoi obecnie w obliczu radykalnych zmian. Ich istotą jest konieczność wdrożenia infrastruktury elektronicznego dokumentu zdrowotnego umożliwiającej przechowywanie, utrzymywanie i zarządzanie informacją kliniczną związaną z pacjentami. Tworzenie historii klinicznej pacjenta realizowane jest w oparciu o mechanizm elektronicznych dokumentów zdrowotnych. Idea tego typu dokumentów bazuje na dwóch podstawowych elementach: repozytoriach i rejestrach. W repozytoriach są przechowywane wszystkie medyczne obiekty danych, tj. dokumenty kliniczne, dane laboratoryjne, obrazy diagnostyczne i informacje o przepisanych lekach. Natomiast rejestry zawierają referencje do medycznych obiektów danych i umożliwiają tworzenie na żądanie różnych przekrojowych informacji zdrowotnych o pacjencie, włącznie z pełną informacją od urodzenia do śmierci. Architektura infrastruktury EHR jest całkowicie zorientowana na dokument i powinna być zgodna z modelem architektury IHE XDS (patrz [66]). W praktyce oznacza to, iż wymianie i przechowywaniu w

obrębie infrastruktury EHR podlegają jedynie podpisane dokumenty elektroniczne. Podpis elektroniczny może być złożony przez uprawnionego pracownika ochrony zdrowia, przez osoby akceptujące dokument, przez podmiot składający dokument do repozytorium lub przez system, w którym przechowywany jest dokument.

Elektroniczny dokument zdrowotny (EHR) pacjenta jest dokumentem wirtualnym, tzn. jest zawsze tworzony na żądanie z dokumentów składowych, w oparciu o podany identyfikator pacjenta oraz określone kryteria wyboru. W pracy termin „EHR" używany jest jako kontener (kontenerem może być także plik np. xml) zawierający wszystkich dokumenty składowe należące do jednego pacjenta. Natomiast termin „ekstrakt EHR" jest używany w odniesieniu do dokumentu złożonego z dowolnie wybranych dokumentów składowych należących do jednego pacjenta. W skrajnych przypadkach ekstrakt EHR może zawierać jeden dokument składowy lub wszystkie i wtedy jest tożsamy z EHR.

Wiarygodność EHR zależy zawsze od wiarygodności metadanych zawartych w rejestrach opisujących medyczne obiekty danych znajdujące się w repozytoriach. Przy ocenie tej wiarygodności należy wziąć pod uwagę także fakt, że metadane w rejestrach oraz dane w repozytoriach mogą należeć do różnych świadczeniodawców usług medycznych i znajdować się pod kontrolą organizacji, którym te dane zostały powierzone w celu ich przechowywania i przetwarzania.

1.2. Podstawowe definicje

Na potrzeby niniejszej rozprawy przyjęto następujące podstawowe definicje algorytmu, protokołu, metody, modelu i systemu:

- algorytm – „Algorytm jest uporządkowanym zbiorem jednoznacznych, wykonywalnych kroków, określającym skończony proces" (J. G. Brookshear [22]).
- metoda – „Metoda, czyli system postępowania, jest to sposób wykonywania czynu złożonego, polegający na określonym doborze i układzie jego działań składowych, a przy tym uplanowiony i nadający się do wielokrotnego stosowania" (T. Kotarbiński [75]).
- model informacyjny – „Model informacyjny jest reprezentacją koncepcji, relacji, ograniczeń, zasad oraz operacji, które określają semantykę danych dla wybranej domeny. Może dostarczyć udostępniane, stabilne i zorganizowane wymogi informacyjne w kontekście domeny" (R. Veryard [104]) .
- protokół – „Reguły według których odbywa się komunikacja między różnymi składowymi systemu komputerowego" (J. G. Brookshear [22]).
- system – „System jest pewną całością, w której współdziałają wyodrębnione części składowe. Funkcjonowanie systemu zależy od funkcji części składowych i związków między nimi. Powiązania części składowych określają strukturę systemu. Części składowe nazywamy często komponentami" (Z. Bubnicki [23]).

oraz przyjęto następujące znaczenie terminów dotyczących bezpieczeństwa (wg norm PN-I-02000 [94] i ISO/IEC 13888-1 [68]):

- autentyczność – właściwość polegająca na tym, że pochodzenie lub zawartość obiektu informatycznego są takie jak deklarowane;
- integralność (dokładniej integralność danych) – właściwość polegająca na tym, że dane nie zostały wcześniej zmienione lub zniszczone w nieautoryzowany sposób;
- niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie; niezaprzeczalność jest dzielona na typy m. in.:
    - niezaprzeczalność pochodzenia – usługa przeznaczona jest do ochrony przed fałszywym zaprzeczeniem przez inicjatora faktu utworzenia zawartości wiadomości oraz jej nadania;
    - niezaprzeczalność odbioru – usługa przeznaczona jest do ochrony przed fałszywym zaprzeczeniem przez odbiorcę faktu otrzymania wiadomości;

W Tab.1.1 zostały zebrane wymagania bezpieczeństwa wraz z ich opisami dotyczące długoterminowego przechowywania EHR. W tabeli Tab. 1.2 umieszczono wybrane wymagania z normy ISO 18306 [69] (L.p. 1-6) oraz z RFC 4810 [105] (L.p. 7, 8) wraz z opisami. W rozprawie sformułowanie „długi okres" oznacza okres wynoszący 100 i więcej lat będący maksymalnym okresem życia człowieka. W dalszej części rozprawy sformułowanie niezaprzeczalność EHR oznacza niezaprzeczalność odbioru i pochodzenia EHR.

Tabela 1.1: Wymagania bezpieczeństwa (źródło: opracowanie własne)

L.p.	Kod wymagania	Nazwa wymagania	Opis wymagania
1	AUT1.0	Autentyczność metadanych	Metoda musi umożliwiać stwierdzenie autentyczności zbioru metadanych z rejestrów opisujących dokumenty składające się na EHR;
2	NZP1.1	Niezaprzeczalność pochodzenia pojedynczego dokumentu	Metoda musi umożliwiać weryfikację w dowolnym momencie niezaprzeczalności pochodzenia pojedynczych dokumentów składających się na EHR;
3	NZP1.2	Niezaprzeczalność pochodzenia EHR	Metoda musi umożliwiać weryfikację w dowolnym momencie niezaprzeczalności pochodzenia EHR dla każdego pacjenta; przy czym uznaje się, że niezaprzeczalność pochodzenia EHR jest spełniona, gdy zbiór metadanych z rejestrów jest autentyczny i wszystkie dokumenty spełniają warunek niezaprzeczalności pochodzenia;

L.p.	Kod wymagania	Nazwa wymagania	Opis wymagania
4	NZO1.1	Niezaprzeczalność odbioru pojedynczego dokumentu	Metoda musi umożliwiać weryfikację w dowolnym momencie niezaprzeczalności odbioru przez system EHR pojedynczych dokumentów wysłanych do systemu przez specjalistę ds. ochrony zdrowia;
5	NZO1.1	Niezaprzeczalność odbioru EHR	Metoda musi umożliwiać weryfikację w dowolnym momencie niezaprzeczalności odbioru EHR dla każdego pacjenta; przy czym uznaje się, że niezaprzeczalność odbioru EHR jest spełniona, gdy EHR jest autentyczny i wszystkie dokumenty składowe spełniają warunek niezaprzeczalności odbioru;

Stwierdzenie autentyczności zbioru metadanych umożliwia stwierdzenie, że zawartość zbioru metadanych otrzymanych w wyniku zapytania jest taka jak deklarowana, tj. metadane dotyczące wszystkich dokumentów składowych należących do danego pacjenta są obecne i niezmienione oraz nie zostały dodane fałszywe wpisy. Stwierdzenie autentyczności oraz niezaprzeczalności wymaga stwierdzenia integralności. Niezaprzeczalność pochodzenia pojedynczego dokumentu zapewnia, że składowy dokument został utworzony przez określonego specjalistę ds. ochrony zdrowia i nie może on temu zaprzeczyć. Niezaprzeczalność odbioru pojedynczego dokumentu składowego umożliwia otrzymanie poświadczenia, któremu nie można zaprzeczyć, że dokument został odebrany od specjalisty ds. ochrony zdrowia w określonym czasie.

Tabela 1.2: Wymagania bezpieczeństwa (źródło: [69, 105])

L.p.	Kod wymagania	Nazwa wymagania	Opis wymagania
1	PRO2.7	Skalowalność	Architektura systemu EHR nie powinna utrudniać przetwarzania bardzo dużych rekordów lub bardzo dużej liczby rekordów.
2	PRS4.1	Integralność danych	Architektura systemu EHR powinna obsługiwać środki zapewniające integralność danych przechowywanych w, pobieranych z oraz wysyłanych do EHR.
3	MEL1.1	Wymagania prawne	Architektura systemu EHR powinna obsługiwać środki zapewniające dokładne odwzorowanie chronologii zdarzeń klinicznych i dostępności informacji w EHR.

L.p.	Kod wymagania	Nazwa wymagania	Opis wymagania
4	MEL2.7	Odpowiedzialność autora I	Architektura systemu EHR powinna obsługiwać środki zapewniające, że każdy wpis do rekordu jest oznaczony datą i można zidentyfikować jego autora.
5	MEL2.8	Odpowiedzialność autora II	Architektura systemu EHR powinna obsługiwać środki zapewniające istnienie bezwzględnego wymogu, aby każdy wpis do rekordu był przypisany do aktora ochrony zdrowia, będącego w roli aktora lub nie.
6	MEL2.9	Atestacja wpisów	Architektura systemu EHR powinna obsługiwać środki zapewniające, że każdy wpis do rekordu jest atestowany przez odpowiedzialną osobę.
7	LTA4.4	Poświadczenia	Długoterminowa usługa archiwum musi być zdolna dostarczyć poświadczenia, które mogą być użyte do zademonstrowania integralności danych których dotyczą, od czasu odebrania danych w archiwum do końca okresu archiwizacji;
8	LTA4.7	Obsługa grup dokumentów	Archiwum długoterminowe powinno obsługiwać przedkładanie grup obiektów archiwalnych; w przypadku operowania na grupach obiektów, dowód niezaprzeczalności musi być również dostępny osobno dla każdego obiektu archiwalnego.

1.3. Cel i teza rozprawy

Celem niniejszej rozprawy jest opracowanie metody, która w długim okresie umożliwia spełnienie wymagań autentyczności metadanych w rejestrach oraz niezaprzeczalności pochodzenia i odbioru elektronicznych dokumentów zdrowotnych jak i niezaprzeczalności pochodzenia i odbioru pojedynczych dokumentów wchodzących w ich skład.

Dodatkowo metoda powinna spełniać następujące wymagania bezpieczeństwa: skalowalność, integralność danych, wymagania prawne, odpowiedzialność autora, atestacja wpisów, poświadczenia oraz obsługa grup dokumentów.

W pracy zakłada się, że istnieje polityka organizacyjna wymagająca replikowanie danych (powielanie danych pomiędzy wieloma serwerami) z rejestrów i repozytoriów oraz tworzenie kopii zapasowych, tak aby nie istniała możliwość całkowitego usunięcia danych. Nie powinna istnieć opcja kasowania. Natomiast w przypadku skasowania danych (celowo

lub przez przypadek) z pojedynczego rejestru czy repozytorium, po wykryciu takiego incydentu, musi istnieć możliwość odtworzenia danych z kopii.

Badania prowadzone w ramach pracy służą do wykazania prawdziwości następującej tezy badawczej:

Opracowanie metody opartej na słownikach uwierzytelnianych i ich wiązaniach umożliwi zapewnienie autentyczności i niezaprzeczalności wirtualnego elektronicznego dokumentu zdrowotnego (EHR) w długim okresie.

W przeciwieństwie do dokumentu papierowego, wartość wirtualnego dokumentu elektronicznego jako środka dowodowego może zmniejszać się z upływem czasu. W szczególności wynika to z następujących przyczyn:

- algorytmy szyfrowe oraz klucze kryptograficzne użyte podczas tworzenia mechanizmów autentyczności zbioru metadanych jak i niezaprzeczalności pochodzenia i odbioru pojedynczych dokumentów składowych i EHR z upływem czasu stają się słabe i stąd mało odporne na ataki;
- niedostępne są informacje (zaświadczenia podmiotów świadczących usługi certyfikacyjne, listy certyfikatów unieważnionych, dokumenty elektroniczne, itp.) niezbędne do zweryfikowania autentyczności zbioru metadanych z rejestrów lub niezaprzeczalności medycznych obiektów danych.

Powyższe fakty mogą uniemożliwić zweryfikowanie wiarygodności wirtualnego dokumentu elektronicznego po upływie wielu lat od umieszczenia jego składowych w rejestrach i w repozytoriach. W efekcie może to doprowadzić do całkowitej utraty wartości dowodowej tego typu dokumentu (o ile taką wartość posiadały składowe dokumentu w momencie wysłania go do przechowania do systemu infrastruktury elektronicznego dokumentu zdrowotnego).

Opracowana innowacyjna metoda pozwala zapewnić autentyczność wpisów z metadanymi w rejestrach oraz niezaprzeczalność dokumentów składowych EHR umieszczonych w repozytoriach. Nowa metoda zapewnia poziom bezpieczeństwa praktycznie niedostępny dla dokumentacji papierowej, przy użyciu której nie można stwierdzić automatycznie w ciągu ułamku sekundy, że wszystkie dokumenty papierowe należące do jednego pacjenta, przechowywane w różnych miejscach świadczeń usług ochrony zdrowia, są obecne i oryginalne.

1.4. Miejsce wyników rozprawy

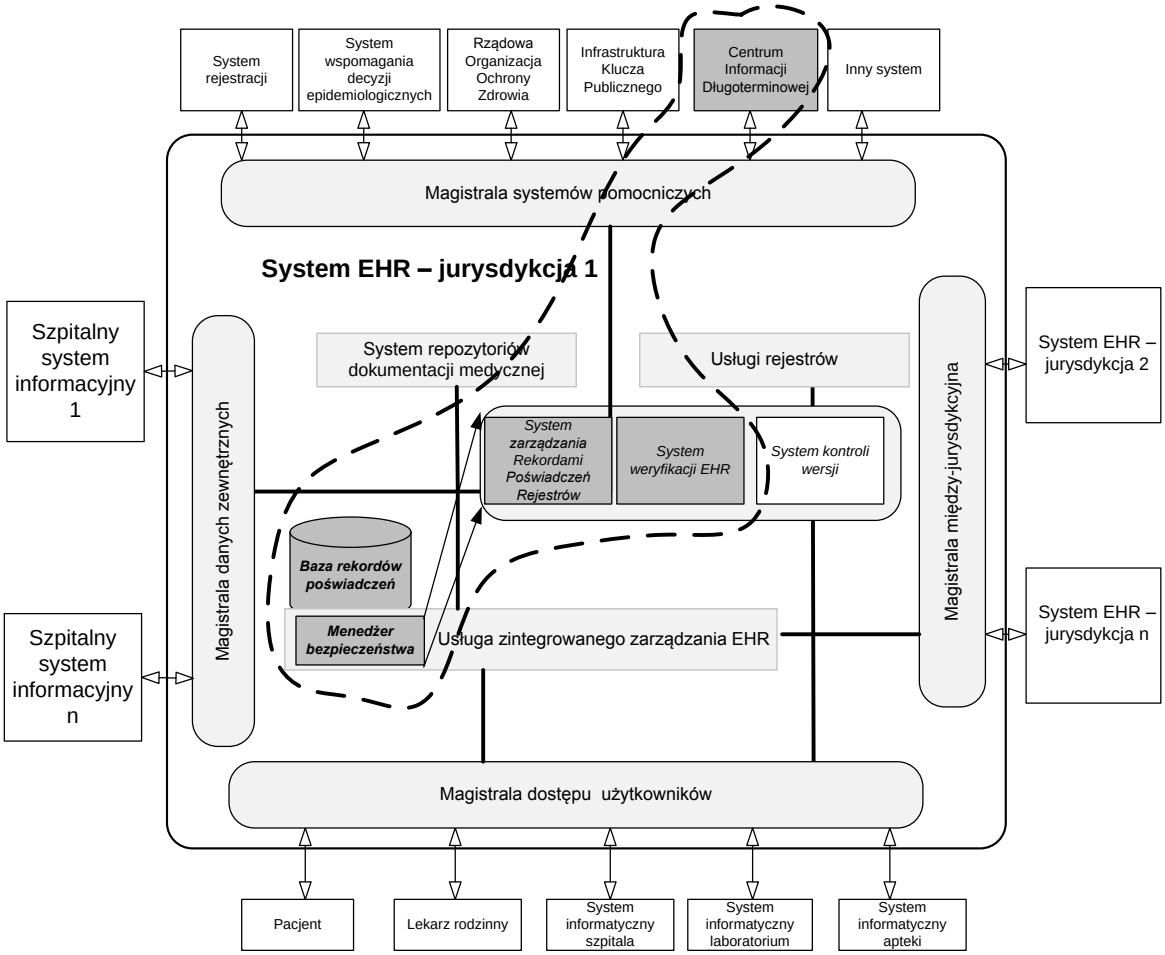
Wynik pracy doktorskiej są umiejscowione w następujących dziedzinach informatyki według międzynarodowej klasyfikacji ACM [1]:

- *E. Dane (ang. Data)*
  - *E.1 Struktury Danych (ang. Data Structures)* – w rozprawie przedstawiono Rekordy Poświadczeń Rejestrów, strukturę danych służącą do przechowywania poświadczeń dotyczących wpisów z metadanymi w rejestrach;
  - *E.3 Kryptografia Danych (ang. Data Encryption)* – Dziedzina dotyczy zagadnień m. in. związanych z krypto-systemami klucza publicznego. W rozprawie poruszane są zagadnienia związane z infrastrukturą klucza publicznego. Opracowana metoda wykorzystuje zaufane znaczniki czasu oraz konserwuje wartość podpisów cyfrowych w repozytoriach;
- *H. Systemy Informacyjne (ang. Information Systems)*
  - *H.3 Przechowywanie i Pozyskiwanie Danych (ang. Information Storage And Retrieval)*
    - *H.3.2 Przechowywanie Informacji (ang. Information Storage)* – opracowana w rozprawie metoda służy do zapewnienia długoterminowego bezpieczeństwa elektronicznych dokumentów zdrowotnych (EHR) przechowywanych w rejestrach i repozytoriach.

Uzyskane wyniki w dziedzinie Informatyki mają charakter ogólny i mogą być zastosowane do tworzenia nie tylko systemów bezpieczeństwa w ochronie zdrowia, ale również do tworzenia systemów informatycznych, które służą do przechowywania pogrupowanych dokumentów wraz z metadanymi w rejestrach i repozytoriach. Dokumenty mogą być dodawane w długim okresie.

System bezpieczeństwa implementujący metodę stworzoną w ramach niniejszej rozprawy doktorskiej może zostać umiejscowiony w systemie EHR tj. na Rys 1.1. i składa się z następujących komponentów:

- Menedżer Bezpieczeństwa (MB) – główny komponent zarządzający przepływem danych między pozostałymi komponentami;
- Baza danych przechowująca poświadczenia (BRPR);
- System zarządzania poświadczeniami (SZRPR) – odpowiedzialny za tworzenie i aktualizację poświadczeń;
- System weryfikacji EHR (SWEHR) – zawiera algorytmy umożliwiające weryfikacje autentyczności i niezaprzeczalności;
- Centrum Informacji Długoterminowej (CID) – umożliwia długoterminowe zarządzanie informacją o algorytmach i usługach PKI oraz zawiera protokół umożliwiający komunikację z systemem EHR.



Rysunek 1.1: Wyniki rozprawy doktorskiej na tle systemu EHR (źródło: opracowanie własne)

1.5. Metodyka badań

Utrzymywanie wiarygodności wirtualnego elektronicznego dokumentu zdrowotnego można zapewnić dzięki zastosowaniu odpowiednich środków organizacyjnych i technicznych. Co więcej, im bardziej rygorystyczne są środki organizacyjne, tym mniej surowe mogą być wymagania nakładane na zastosowane środki techniczne. Przedmiotem zainteresowania rozprawy są jednak tylko techniczne metody utrzymywania i weryfikowania wiarygodności wirtualnego elektronicznego dokumentu zdrowotnego.

Podstawą warsztatu naukowego opracowanej metody są metody kryptograficznej ochrony informacji (w tym w szczególności schematy wiązań binarnych, słowniki uwierzytelniane), z uwzględnieniem obecnego stanu wiedzy w zakresie kryptoanalizy (w tym metod analizy protokołów wymiany informacji). Punktem wyjścia badań jest analiza teoretycznych oraz praktycznych rozwiązań, przeznaczonych dla podobnej klasy problemów. Przykładami tego typu rozwiązań są podpisy elektroniczne przechowywane w formie archiwalnej CAdES-A [4] lub XAdES-A [41], Evidence Record Syntax (ERS) [50] grupy LTANS oraz specyfikacja i systemy zgodne ze specyfikacją ebXML Registry [37]. Na podstawie przeprowadzonej analizy zostały zaprojektowane struktury poświadczeń. Podczas projektowania została rozważona celowość zastosowania takich rozwiązań, aby:

- istniała możliwość dostarczenia poświadczenia dla całej grupy obiektów danych medycznych, np. powinno być możliwe zarejestrowanie obiektu i danych potwierdzających ich autentyczność i niezaprzeczalność w taki sposób, aby otrzymały to samo poświadczenie;
- w przypadku dostarczenia grupy obiektów danych dowód niezaprzeczalności był dostępny dla każdego z obiektów z osobna;
- usunięcie niektórych lub określonej liczby obiektów danych nie mogło stanowić zagrożenia dla innych przechowywanych obiektów danych;
- istniała możliwość umieszczenia wszystkich poświadczeń łącznie z zarejestrowanymi obiektami danych w pojedynczym elemencie danych lub umieszczenia pakietu i obiektów danych w oddzielnych elementach;
- istniała możliwość integracji dodatkowych informacji niezbędnych do weryfikacji danych wewnątrz rekordu poświadczenia lub samego obiektu danych, takich jak certyfikaty, listy CRL, elementy mające wpływ na bezpieczeństwo zastosowanych algorytmów.

Do zbudowania poświadczeń można zastosować słowniki uwierzytelniane [81]. Wersje trwałe tego typu struktur, stosowane do przechowywania historii zmian danych, stosowane są m.in. w infrastrukturze klucza publicznego w procesie przetwarzania dokumentów elektronicznych i długoterminowego utrzymywania ich wartości dowodowej [92] (m.in. w podpisie elektronicznym czy usłudze znakowania czasem).

Opracowana nowa metoda jest dostosowana do specyfiki elektronicznego dokumentu zdrowotnego, w tym do jego struktury, zasad przechowywania i przetwarzania oraz weryfikowania jego wiarygodności. W tym celu została przeprowadzona analiza obecnych standardów określających strukturę EHR oraz analiza struktury obecnie istniejących systemów.

Analiza i ocena uzyskanych efektów została przeprowadzona w przypadkach, gdy liczba wpisów do rejestru i repozytoriów jest rzędu kilku milionów i odpowiada rzeczywistej liczbie wpisów w systemie EHR. Do wykonania oceny efektywności opracowanych algorytmów oraz optymalizacji ich działania zostały wykorzystane wieloprocesorowe jednostki obliczeniowe. Na podstawie otrzymanych wyników zostały przeprowadzone dalsze działania mające na celu optymalizację działania opracowanej metody. Kolejnym krokiem było przeprowadzenie testów bezpieczeństwa, których celem było sprawdzenie odporności metody na ataki.

1.6. Korzyści z wdrożenia wyników rozprawy

Zgodnie z wytycznymi Komisji Europejskiej oraz Planem Działań Komisji Europejskiej (*ang. European Commision's Action Plan*) [44, 45] wprowadzenie usług związanych z eZdrowiem jest jednym z głównych priorytetów rozwoju społeczeństwa informacyjnego. Obecnie w Polsce nie istnieje spójny system zarządzania dokumentacją medyczną konkretnego pacjenta. Każdy pacjent odwiedzający kilku lekarzy posiada

dokumentacje w różnych miejscach w postaci papierowej lub elektronicznej. Dokumentacja papierowa jest często nieczytelna. Dodatkowo najczęściej sam pacjent musi przenosić swoją dokumentację pomiędzy jednostkami ochrony zdrowia, np.: wyniki badań z laboratoriów. Konsekwencją tego jest brak możliwości całościowego spojrzenia na historię medyczną pacjenta. Wyniki badań uzyskane w trakcie realizacji pracy doktorskiej pozwalają na stworzenie bezpiecznego systemu zarządzającego EHR, rozwiązującego powyższe problemy.

W przypadku wdrożenia systemu EHR, dzięki lepszej informacji o wykorzystaniu zasobów, możliwe jest poprawienie dostępu do usług ochrony zdrowia. Przykładowo, wprowadzenie systemu rejestracji elektronicznych do lekarzy specjalistów niweluje problem wielokrotnego zapisywania się pacjenta do tej samej kolejki, a także umożliwia monitorowanie ilości lekarzy i świadczonych przez nich usług, co umożliwia skrócenie kolejek. Badania naukowe dowodzą [5, 9], że natychmiastowy dostęp do kompletnych danych medycznych pacjenta podnosi jakość ochrony zdrowia.

Przykładowo, można sobie wyobrazić następujący przypadek użycia systemu EHR: pacjent w nocy ulega wypadkowi i jest nieprzytomny; zachodzi potrzeba podania w ciągu kilku minut jednego z dwóch leków, które wiadomo, że mogą u wielu pacjentów wywołać reakcję alergiczną; szybki dostęp do danych medycznych pacjenta (do jego EHR) umożliwia podanie właściwego leku i pacjent zostaje uratowany.

System EHR nie może być wdrożony bez odpowiednich mechanizmów bezpieczeństwa. Proponowana w pracy metoda umożliwia zaimplementowanie systemu umożliwiającego wykrycie wszelkich nieuprawnionych zmian w EHR danego pacjenta, tak aby celowe lub przypadkowe zamiany w dokumentach medycznych nie miały wpływu na diagnozę lekarza. Diagnoza oparta na nieprawidłowych danych może doprowadzić do pogorszenia stanu zdrowia, a nawet śmierci pacjenta. Równie ważne są aspekty prawne umożliwiające pacjentom rozstrzyganie sporów przed właściwym sądem. System zaimplementowany w oparciu o proponowaną metodę uniemożliwia danemu specjaliście ds. ochrony zdrowia wyparcia się utworzenia dokumentu, a także umożliwia udowodnienie, że dany dokument nie został dodany.

Podsumowując główną zaletą wdrożenia systemu implementującego proponowaną metodę jest zwiększenie bezpieczeństwa wirtualnych elektronicznych dokumentów zdrowotnych.

Niniejsza rozprawa doktorska została uznana za innowacyjną i uzyskała współfinansowanie przez Unię Europejską w ramach Europejskiego Funduszu Społecznego i Budżetu Państwa, Programu Operacyjnego Kapitał Ludzki Priorytetu VIII, Działanie 8.2 Transfer wiedzy Poddziałanie 8.2.2 „*Regionalne Strategie Innowacji*”, projektu systemowego realizowanego przez Wojewódzki Urząd Pracy w Szczecinie „*Inwestycja w wiedzę motorem rozwoju innowacyjności w regionie”*.

1.7. Struktura rozprawy

Niniejsza rozprawa doktorska zawiera sześć rozdziałów oraz załączniki dołączone na płycie CD. Rozdział pierwszy zawiera opis problemu, a także cel i tezę pracy wraz z metodyką badań oraz oceną korzyści uzyskanych w wyniku ich zrealizowania.

Rozdział drugi zawiera opis środowiska badawczego, a więc analizę modeli informacyjnych EHR (rozdz. 2.2) oraz standardów dotyczących struktury dokumentów zdrowotnych (rozdz. 2.2.2). W dalszej części rozdziału zostały przedstawione systemy EHR (rozdz. 2.3). Następnie omówiono wymagania odnośnie długoterminowego przechowywania EHR (rozdz. 2.3). Rozdział 2.5 wprowadza w tematykę infrastruktury klucza publicznego, a rozdział 2.6 zawiera przegląd prac pokrewnych związanych z długoterminowym przechowywaniem podpisanych dokumentów medycznych. Rozdział kończy się podsumowaniem i porównaniem prac pokrewnych.

Rozdział trzeci zawiera opis proponowanej metody DPEDZ. W rozdziale została przedstawiona ogólna architektura systemu EHR (rozdz. 3.3) oraz Rekordy Poświadczeń Rejestrów (rozdz. 3.5). Następnie została omówiona szczegółowo metoda DPEDZ wraz z wchodzącymi w jej skład działaniami (rozdz. 3.6). Rozdział 3.7 zawiera opis dodatkowych źródeł zaufania wraz z proponowanym Centrum Informacji. Rozdział kończy się porównaniem (rozdz. 3.8) z pracami pokrewnymi przedstawionymi w rozdz. 2 oraz podsumowaniem (rozdz. 3.9).

W rozdziale czwartym znajduje się opis przeprowadzonych badań eksperymentalnych. W rozdziale 4.1 zawarto opis i wyniki testów wydajności opracowanych działań wchodzących w skład proponowanej metody. Następnie zostały przeprowadzone testy bezpieczeństwa sprawdzające odporność opracowanej metody na ataki (rozdz. 4.2).

Rozdział piąty zawiera podsumowanie. Zostały wymienione także elementy nowości i kierunki dalszych prac.

Rozdział szósty zawiera zestawienie literatury przywoływanej w pracy oraz spisy tabel i rysunków.

Do pracy została dołączona płyta CD z załącznikami zawierająca m. in. oprogramowanie implementujące poszczególne działania wchodzące w skład proponowanej metody, które zostało wykorzystywane do przeprowadzenia testów.

2. Elektroniczne dokumenty zdrowotne

2.1. Definicja elektronicznego dokumentu zdrowotnego (EHR)

Elektroniczny dokument zdrowotny (*ang. EHR, Electronic Health Record*) jest wirtualnym kontenerem, na który składają się dokumenty związane ze zdrowiem pojedynczego podmiotu ochrony zdrowia – pacjenta. Jest to przechowywana cyfrowa informacja o zdrowiu jednego człowieka, od jego urodzenia aż do śmierci. Okres przechowywania dokumentów wchodzących w skład EHR może wynosić 100 lub więcej lat. Dokumenty medyczne wchodzące w skład EHR mogą być tworzone, przechowywane i używane w wielu różnych organizacjach ochrony zdrowia.

Standardy ISO i CEN zawierają wiele różnych definicji EHR. Jednakże tylko najnowszy ISO TR 20514 [70] zawiera wyczerpującą definicję, która określa zakres i kontekst EHR. ISO TR 20514 rozróżnia pomiędzy treścią a strukturą EHR, opisując EHR jako funkcję jego struktury. Taka podstawowa definicja jest nazwana BGEHR (*ang. Basic Generic EHR*), gdzie BGEHR jest zdefiniowane jako *kontener na przetwarzane dokumenty medyczne powiązane z jednym pacjentem*. Kolejny podział rozdziela EHR na udostępniane i nieudostępniane. Specjalizacją udostępnianego EHR jest ICEHR, który jest zdefiniowany w [70] następująco:

> *"ICEHR jest repozytorium informacji dotyczących stanu zdrowia podmiotu ochrony zdrowia w komputerowo przetwarzalnej formie, przechowywanej i transmitowanej bezpiecznie i dostępnej dla wielu upoważnionych użytkowników. Posiada standaryzowany i ogólnie uzgodniony logiczny model informacyjny, niezależny od systemów EHR. Jego podstawowym celem jest wspieranie ciągłej, efektywnej i jakościowo zintegrowanej ochrony zdrowia i zawiera informacje które są retrospektywne, jednoczesne i perspektywiczne".*

Zawarte w definicji stwierdzenie, że ICEHR musi być „przechowywany i transmitowany bezpiecznie" służy podkreśleniu ważności problemu zapewnienia bezpieczeństwa przechowywania informacji w EHR dotyczących ochrony zdrowia. Dalej w niniejszej pracy termin EHR używany jest w sensie ICEHR.

Oprócz wyżej wspomnianych definicji istnieje jeszcze wiele podobnych definicji dotyczących EHR i elektronicznej dokumentacji zdrowotnej. W artykule [54] zostały zestawione definicje dotyczące EHR używane w literaturze światowej.

2.2. Modele informacyjne EHR

Model informacyjny [106] EHR jest abstrakcyjnym modelem z dziedziny ochrony zdrowia, który jest związany z przechowywanymi informacjami o pacjencie. Model ten zawiera [40]:

- uczestników zdarzenia związanego z ochroną zdrowia i ich role funkcjonalne (uczestnikami mogą być ludzie, organizacje, jednostki organizacyjne, itd.);

- kontekst, w którym została stworzona informacja (kontekstem mogą być uczestniczący obserwatorzy, użyte urządzenia, język informacji, itd.);
- dokumenty i ich strukturę (sekcje, kodowane wpisy, itd.);
- referencje, czyli powiązania pomiędzy poszczególnymi wpisami;
- prawa własności i odpowiedzialność (wpisy do rejestrów zdarzeń na potrzeby audytu, podpisy cyfrowe, prawa dostępu, itd.).

Model informacyjny określa operacje, które dla danego typu informacji kompatybilna z modelem implementacja systemu EHR musi obsługiwać, jednakże nie określa sposobu implementacji. Z modelu może być odziedziczony format wiadomości służący do wymiany zawartości EHR.

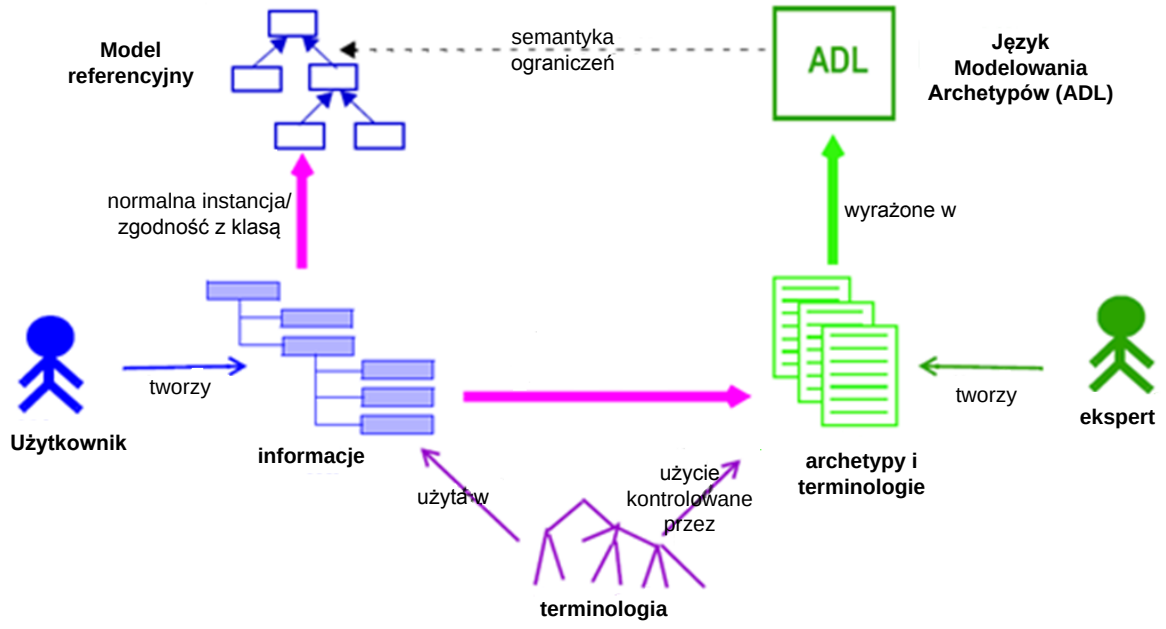
2.2.1 Model jednopoziomowy/dwupoziomowy

Długookresowy cykl życia EHR powoduje, że model informacyjny musi być bardzo stabilny, ponieważ informacje medyczne przeszłe, aktualne i przyszłe muszą być zapisywane w tym samym EHR pacjenta. Od modelu wymagana jest również elastyczność, ponieważ wiedza medyczna oraz procesy świadczenia usług opieki zdrowotnej zmieniają się w czasie. Model informacyjny musi być na tyle skuteczny, aby informacje o zdrowiu pacjenta z całego życia mogły być zapisane z użyciem jednego modelu, a jednocześnie musi być wystarczająco prosty do implementacji i zarządzania.

Aby spełnić przedstawione wyżej wymagania w wielu modelach informacyjnych do przedstawiania struktury EHR używane jest modelowanie dwupoziomowe [11]. Na pierwszym poziomie modelu istnieje ogólny model referencyjny dla dziedziny ochrony zdrowia. Model ten zawiera tylko kilka niezmiennych w czasie klas. Na drugim poziomie modelowane są archetypy (uszczegółowiające ograniczenia nałożone na model referencyjny) specyficzne dla ochrony zdrowia pojęcia, np. ciśnienie krwi czy wyniki badań laboratoryjnych. Archetypy otrzymuje się przez zastosowanie zasad ograniczających (*ang. constraint rules*), uszczegóławiających ogólne struktury danych, które mogą być zaimplementowane z użyciem modelu referencyjnego, na przykład można uszczegółowić ogólną klasę „Obserwacja” do archetypu „Ciśnienie Krwi”. Archetyp można by porównać do instrukcji klocków LEGO (np. budowy czołgu), która opisuje konfiguracje klocków LEGO tworzących czołg. Archetypy są elastyczne w podobny sposób do klocków LEGO, które mogą posiadać wiele opcji podczas budowy tego samego czołgu.

W modelowaniu dwupoziomowym tylko pierwszy poziom musi być zaimplementowany, co powoduje znaczące zmniejszenie zależności zainstalowanych systemów od zmiennych definicji zawartości (wyrażonych w postaci archetypów). Na Rys. 2.1 przedstawiono zależności danych w systemach jedno i dwupoziomowych. Dane stworzone przez użytkownika są zgodne z modelem referencyjnym systemu. Systemy stworzone za pomocą modelowania jednopoziomowego (cała semantyka z danej dziedziny jest zakodowana w oprogramowaniu lub w bazie danych) są ograniczone do architektury tego rodzaju. W przypadku użycia modelowania dwupoziomowego dane podczas wykonania są

zgodne z modelem referencyjnym oraz są zgodne semantycznie z archetypami. Archetypy są tworzone przez ekspertów z danej dziedziny i zawierają ograniczenia narzucone na model referencyjny.



Rysunek 2.1: Meta-architektura archetypu (źródło [13])

Zaletą modelowania dwupoziomowego jest separacja aspektów technicznych od aspektów medycznych. W takim podejściu technicy implementują system EHR bazując na modelu referencyjnym, a eksperci z dziedziny medycyny definiują odpowiednie definicje archetypów. Jedną z kwestii do końca nierozwiązanych jest to, kto ma być odpowiedzialny za tworzenie i utrzymanie bibliotek archetypów.

2.2.2 Standardy dotyczące struktury EHR

2.2.2.1 CEN ENV 13606:2000

Norma CEN ENV 13606:2000 „*Electronic Healthcare Record Comunication*" [29] jest następcą normy ENV 12265 i miała być pierwszym w pełni implementowanym standardem EHR. Składa się z czterech części definiujących: model informacyjny EHR, zbiór terminologii wspierającej różne poziomy interoperacyjności pomiędzy różnymi systemami EHR, zbiór obiektów reprezentujących zasady przyznawania praw dostępu do EHR oraz wiadomości żądania i odpowiedzi pozwalające na wymianę podzbiorów EHR pomiędzy systemami.

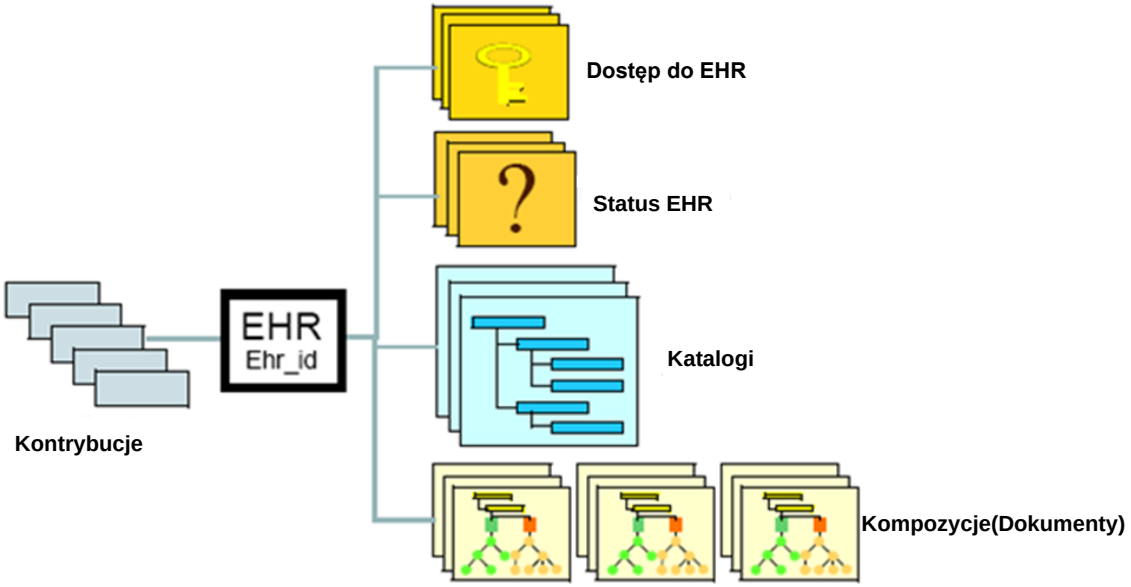
Norma ENV 13606:2000 bazuje na wiadomości służącej do przekazywania medycznych rekordów danych. Nie opisuje całego systemu EHR, tylko skupia się na interfejsach ważnych w komunikacji pomiędzy różnymi systemami. Model informacyjny ENV 13606:2000 należy do pierwszej generacji modeli informacyjnych EHR. Jest to bardzo złożony, jednopoziomowy model składający się z 90 klas podzielonych na 8 podsystemów. Pomimo dużej liczby dostępnych klas model jest niewystarczający [40].

Części ENV 13606 zostały zaimplementowane w różnych projektach dotyczących EHR w wielu krajach europejskich, m. in. w Danii, Holandii, Norwegii, Szwecji i w Wielkiej Brytanii [39]. W żadnym z wymienionych krajów nie użyto całości standardu. Wielokrotne implementacje ujawniły wiele słabości tego standardu ograniczających jego użyteczność. Główną przyczyną jest modelowanie jednopoziomowe, przez które model informacyjny jest bardzo złożony oraz trudny do implementacji i zrozumienia.

2.2.2.2 GEHR/openEHR

Inicjatywa GEHR/OpenEHR została stworzona w roku 1992 jako projekt badawczy Unii Europejskiej pod nazwą „*Good European Health Record*", a następnie była kontynuowana pod nazwą „*Good Electronic Health Record*". Obecnie rozwojem GEHR/OpenEHR zajmuje się fundacja non-profit OpenEHR [87] pracująca w kierunku wprowadzenia interoperacyjnego EHR zawierającego informacje o zdrowiu człowieka z całego jego życia.

Model informacyjny openEHR jest dwupoziomowy. Archetypy w openEHR bazują na modelu referencyjnym openEHR składającym się z pakietów i opisującym rekord medyczny. Każdy pakiet definiuje jeden dokument specyfikacji openEHR. Struktura wysokiego poziomu EHR w openEHR została zaprezentowana na Rys. 2.2.



Rysunek 2.2: Struktura wysokiego poziomu EHR w openEHR (źródło [88])

EHR w openEHR jest ustrukturyzowany według relatywnie prostego modelu. Główny obiekt EHR jest identyfikowany za pomocą *EHR_id*, zawiera referencje do wielu typów ustrukturyzowanej i wersjonowanej informacji oraz do obiektów *Contribution*, które zawierają informacje o wprowadzonych zmianach i służą do audytów. Główny obiekt EHR posiada globalny identyfikator *Ehr_id*, który jest różny dla każdego pacjenta. Dodatkowo posiada zapisany czas utworzenia oraz ID systemu, w którym został utworzony. Wszystkie te identyfikatory są niezmienne podczas życia EHR.

Kompozycje są podstawowym kontenerem danych w openEHR. Instancje klasy *Composition* mogą być uważane za samodzielne agregaty danych lub jako dokumenty w systemie zorientowanym na dokumenty. Kluczowe informacje w *composition* są umieszczone w atrybutach *content, context* i *composer*. Dane w *composition* są przechowywane w atrybucie *content* Istnieją cztery typy ustrukturyzowania danych w atrybucie *content* (może być on także pusty):

- może zwierać jedną lub więcej sekcji zdefiniowanych w archetypie kompozycji;
- może zawierać jedno lub więcej drzew sekcji, gdzie każde z nich jest oddzielnie archetypowaną strukturą;
- może zawierać jedną lub więcej wpisów bez użycia pośrednich sekcji;
- może być kombinacją powyższych.

Właściwe struktury używane w *Composition* podczas działania systemu są kontrolowane przez szablony, które kontrolują użycie określonej kombinacji archetypów. Do opisu archetypów został stworzony formalny język ADL *(ang. Archetype Definition Language*) [12]. Jest to formalny język do tworzenia archetypów należący do grupy języków opisujących wiedzę.

OpenEHR zawiera przygotowaną gotową bibliotekę archetypów, która zawiera archetypy gotowe do wykorzystania przy tworzeniu systemu EHR. W skład openEHR wchodzi także model referencyjny, język ADL, specyfikacje do implementacji (XML Schema, specyfikacje IDL itd.) oraz kilka implementacji typu *open-source* specyfikacji openEHR.

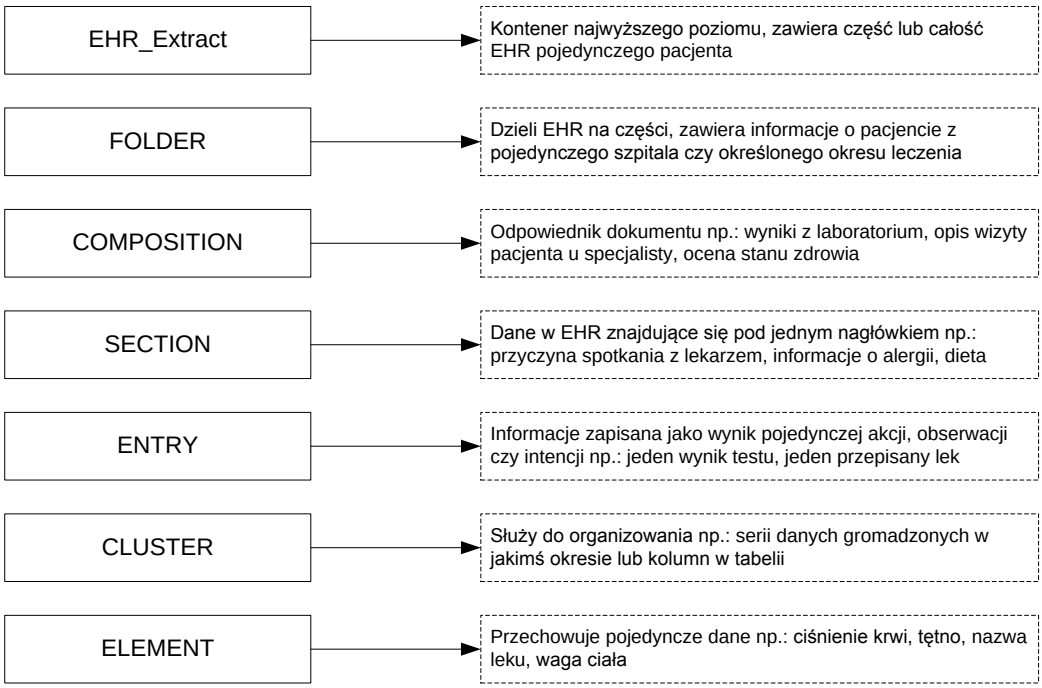
2.2.2.3 CEN/ISO EN13606:2009

Norma CEN/ISO EN13606:2009 [30] jest następcą normy ENV 13606:2000, przy jej tworzeniu wzięto pod uwagę doświadczenia z implementacji systemów EHR oraz zaadaptowano w nim metodologie archetypu z modelu openEHR przedstawionego w rozdz. 2.2.2.2. Norma ta, nazywana w skrócie EHRcom, składa się z pięciu części:

- Część 1: Model referencyjny (*ang. Reference Model)* – zawiera ogólny model informacyjny służący do przekazywania całości lub części EHR pomiędzy systemami;
- Część 2: Specyfikacja wzajemnej wymiany archetypów *(ang. Archetype Interchange Specification)* – zawiera ogólny model informacyjny oraz język do reprezentacji i przekazywania definicji indywidualnych instancji archetypów;
- Część 3: Referencyjne Archetypy i Lista Terminów *(ang. Reference Archetypes and Term Lists)* – zawiera początkowy zestaw archetypów wraz z mapowaniem do innych znaczących standardów oraz zawiera mikro-słowniki dla części pierwszej modelu;
- Część 4: Bezpieczeństwo *(ang. Security)* – opisuje zasady opisu kontroli dostępu, przyznawania uprawnień i audytów;
- Część 5: Specyfikacja interfejsów (*ang. Interface specification)* – opisuje interfejsy wiadomości i serwisów, które umożliwiają przekazywanie EHR i archetypów.

Celem normy EN13606 jest zdefiniowanie precyzyjnej i niezmiennej architektury informacji służącej do przekazywania części lub całości EHR pojedynczego pacjenta. Norma wspiera interoperacyjność systemów i komponentów, które przekazują EHR jako wiadomości elektroniczne lub jako rozproszone obiekty z zachowaniem znaczenia medycznego i poufności. Jednakże nie specyfikuje wewnętrznej architektury lub projektu bazy danych systemu EHR lub jego komponentów.

Norma EN13606 używa, podobnie jak openEHR, podejścia dwupoziomowego składającego się z modelu referencyjnego, opisanego w pierwszej części standardu, który reprezentuje ogólne właściwości rekordu z informacjami o zdrowiu oraz archetypów zawartych w części drugiej i trzeciej. Model referencyjny EHRcom składa się z pakietów *Extract, Demographics, Support* i *„Primitives”,* opisujących różne aspekty dotyczące EHR. Pakiet *Extract* definiuje klasę główną modelu referencyjnego (*EHR_EXTRACT*) i struktury danych dla zawartości EHR. Pakiet *Demographics* udostępnia minimalny zestaw danych służący do definiowania różnych osób, agentów programowych, urządzeń i organizacji, do których odnosi się *EHR_EXTRACT*. Pakiet *Support* - zawiera klasy pomocnicze tj. unikalny identyfikator, URI. Natomiast pakiet *Primitives* wymienia typy proste, które z założenia występują na każdej platformie implementacyjnej i nie są dalej definiowane (np.: List<T>, Double, String).



Rysunek 2.3: Hierarchia komponentów modelu referencyjnego EHR_Extract (źródło: [30])

Rysunek 2.4: Diagram hierarchii EHR_Extract (źródło: [30])

Na Rys. 2.3 oraz Rys. 2.4 przedstawiono hierarchię komponentów modelu referencyjnego Ekstraktu EHR (*EHR_Extract*). Na najwyższym poziomie znajduje się katalog z folderami pacjenta (*EHR_Extract*). Foldery mogą być zagnieżdżone i zawierają informacje o pacjencie z pojedynczej jednostki organizacyjnej opieki zdrowotnej, czy z określonego okresu leczenia. Foldery zawierają zero lub więcej kompozycji. Kompozycja (ogólnie odpowiednik dokumentu klinicznego) może zawierać sekcje z nagłówkami, w których skład wchodzą Wpisy (*Entries*) składające się z klastrów z elementami lub z elementów. Każdy element posiada pojedynczą wartość pojedynczego typu danych. Zawartość w ekstrakcie EHR jest zawsze dodawana lub zamieniana jako cała kompozycja (wersjonowanie, prawo własności, ślad audytu w EHRcom bazują na kompozycji).

Drugim ważnym blokiem składającym się na EHRcom jest metodologia archetypu. Model archetypów został zaadoptowany i jest zgodny z modelem archetypów openEHR. W EHRcom archetypy używane są do uszczegółowienia kompozycji. Docelowo koncepcja archetypu z EHRcom będzie zharmonizowana z koncepcją archetypu z HL7 CDA i HL7 Templates (patrz rozdz. 2.2.2.4). Z powodu użycia modelowania dwupoziomowego użyteczność systemu EHR zależy głownie od biblioteki dostępnych archetypów. Zawartość EHR może być wyświetlona bez wiedzy na temat archetypu, jednakże archetypy są potrzebne dla przetwarzania maszynowego zawartości i do zoptymalizowanego wyświetlania. Trzecia część normy EN 13606 zawiera bibliotekę archetypów.

2.2.2.4 HL7 CDA R2

Referencyjny model informacyjny HL7v3 (RIM) [55, 36] opracowany przez firmę Health Level 7, jest modelem z dziedziny medycyny składającym się z sześciu podstawowych klas (*Act, Participiption, Entity, Role, ActRelationship, RoleLink*) oraz z ich specjalizacji. RIM jest opisany w postaci notacji UML. Model HL7 RIM docelowo nie był projektowany jako model EHR [88]. Model ten jest zbiorem semantyki dla wielu systemów, które mogą istnieć w rozproszonym środowisku systemów służby zdrowia i nie jest tylko modelem EHR.

CDA R2 (HL7 CDA 2 – Clinical Document Architecture, Release 2 [36, 84] jest standardem HL7 zatwierdzonym przez ANSI w maju 2005 roku opisującym dokument za

pomocą znaczników określających strukturę i semantykę dokumentu klinicznego stworzonego do celów wymiany. Dokument CDA jest zdefiniowany jako obiekt zawierający kompletną informację, w skład którego może wchodzić tekst, dźwięki lub inne elementy multimedialne. Dokument CDA może być przesyłany wewnątrz wiadomości lub istnieć niezależnie poza wiadomością.

Dokumenty CDA są zakodowane z użyciem XML'a i wywodzą się z modelu RIM. Model CDA R2 jest bogaty w wyrażenia umożliwiające formalną reprezentację wyrażeń klinicznych, przez co mogą być automatycznie interpretowane przez komputer. Z drugiej strony CDA dostarcza mechanizm prostego opakowywania dokumentów nie XML'owych w nagłówek CDA oraz umożliwia tworzenie dokumentów, które posiadają ustrukturyzowany nagłówek, a w treści tylko tekst opisowy nie nadający się do automatycznego przetwarzania. Dokumenty nie nadające się do automatycznego przetwarzania są włączone w celu popularyzacji CDA i stopniowego dochodzenia do interoperacyjności semantycznej.

Dokumenty CDA posiadają nagłówek (*header*) oraz ciało (*body*). Nagłówek identyfikuje i klasyfikuje dokument. Ciało zawiera raport kliniczny zorganizowany w sekcje, których część narracyjna może być zakodowana z użyciem ustandaryzowanej terminologii. W CDA zarówno nagłówek jak i ciało są dziedziczone po klasach RIM. RIM oraz typy danych HL V3 używane przez CDA dostarczają potężny mechanizm umożliwiający włącznie do CDA koncepcji z standaryzowanych systemów kodowych tj. Systemized Nomenclature of Medicine Clinical Terms (SNOMED CT) [67] i Logical Observation Identifiers Names and Codes (LOINC) [97].

Specyfikacja CDA jest wystarczająco obszerna, aby objąć domenę dokumentów klinicznych. Szablony (*Templates* – odpowiedniki archetypu z openEHR) lub przewodnik implementacyjne mogą być użyte do uściślenia specyfikacji CDA wewnątrz określonej implementacji, a później do sprawdzenia zbioru zasad weryfikujących, które sprawdzają zgodność z tymi ograniczeniami.

2.2.2.5 DICOM Strutured Reporting

DICOM Structured Reporting (SR) [34, 57] jest ogólnym modelem kodowania za pomocą ustrukturyzowanego sposobu raportów medycznych bazującym na formacie tagów DICOM [106]. Jest rozszerzeniem standardu DICOM, za jego pomocą można kodować raporty medyczne, pomiary, rezultaty, logi procedur itd. SR bazuje podobnie jak inne współczesne standardy EHR na modelu dwupoziomowym [40], gdzie na drugim poziomie są szablony (*templates*), które są odpowiednikami archetypów. Każdy raport zawsze zawiera informacje o jednym badaniu jednego pacjenta.

SR składa się z nagłówka, także używanego do obrazów przesyłanych za pomocą DICOM, oraz zawartości dokumentu reprezentowanej za pomocą drzewa dokumentu (*document tree*). Każdy element (węzeł) drzewa zawiera część informacji np.: paragraf tekstu lub referencje do obrazu. Zbiór „dobrze zdefiniowanych" relacji określa jak element rodzic i element potomek w hierarchicznej strukturze są z sobą powiązane. Semantyka większości elementów z zawartością w drzewie dokumentu SR jest opisana przez kody do przetwarzania

maszynowego, przez co możliwe jest automatyczne przetwarzanie i ocena dokumentów przez komputer.

SR umożliwia użycie istniejących sieciowych usług infrastruktury DICOM umożliwiających archiwizacje, komunikacje, szyfrowanie oraz podpisywanie cyfrowe po wprowadzeniu tylko niewielkich zmian do istniejących systemów. Dokumenty SR w przeciwieństwie do innych standardów EHR są kodowane binarnie. Standard DICOM nie określa jak dokument SR ma być wyświetlony przez aplikacje, znajduję się to poza zakresem standardu.

W celu umożliwienia interoperacyjności standard DICOM określa klasy dokumentów i inne typy ograniczeń dla różnych aplikacji medycznych. Przykładowo, standard definiuje szablony (*templates* – odpowiedniki archetypów) w celu harmonizacji struktury oraz definiuje grupy kodów w celu ograniczenia możliwości dla określonego kontekstu. Kolekcja standardowych szablonów (*standard templates*), grup kontekstowych oraz kodów nazywa się DICOM Content Mapping Resource (DCMR).

DICOM SR jest bardzo potężną koncepcją, która zasadniczo pokrywa wszystkie rzeczy potrzebne dla EHR, jeżeli jest połączona z innymi usługami DICOM [40]. Natomiast jedną z wad DICOM SR jest skomplikowane kodowanie binarne i protokół komunikacyjny praktycznie nieznany poza dziedziną obrazowania. Dodatkowo, standard ten nie został zaprojektowany w celu używania pomiędzy różnymi przedsiębiorstwami, dlatego nie istnieje np. żaden główny indeks identyfikatorów pacjentów.

W ciągu ostatnich lat DICOM SR został zaimplementowany wiele razy, ale w większości w celach demonstracyjnych [39]. Od niedawna zaczęły się pojawiać produkty komercyjne wspierające dokumenty SR. Skupiają się one głownie na dziedzinach medycyny dobrze opisanych przez standard DICOM, dla których istnieją standardowe szablony dokumentów. Takimi dziedzinami są radiologia i kardiologia. W tych dziedzinach zajmujących się przechwytywaniem obrazów są aktualnie używane obiekty i usługi DICOM, dlatego DICOM Structured Reports wydaje się być brakującym ogniwem. DICOM jest mało popularny poza dziedzinami medycyny wykorzystującymi duże liczby obrazy.

2.2.3 Podsumowanie

Porównanie właściwości standardów ISO/IEC 13606, HL7 CDA, DICOM SR zamieszczono w Tab. 2.1. Właściwości 1-4 dotyczą logicznej struktury EHR. Wszystkie wymienione normy opisujące zawartość dokumentu zdrowotnego bazują na koncepcji dwupoziomowego modelowania zawartości EHR. W tej koncepcji zawartość dokumentu zdrowotnego opisywana jest za pomocą modelu referencyjnego oraz zbioru ograniczeń, pozwalających na jednoznaczne przedstawienie obserwacji klinicznych. W normie ISO/IEC13606 zbiór ograniczeń określany jest mianem archetypów. Równoważna koncepcja używana jest w normie ISO/HL7 CDA pod nazwą wzorców. Wzorce te nie są obecnie w większości określone, ale docelowo mają być spójne z archetypami normy ISO/IEC 13606. W normie DICOM SR ograniczenia są także nazywane wzorcami, których skutki wydają się być

bardzo podobne do archetypów normy ISO/IEC 13606. Wszystkie archetypy i wzorce tworzone są w formie bibliotek.

Tabela 2.1: Porównanie norm dotyczących struktury EHR (źródło: opracowanie własne na podstawie [39])

Lp.	Własność/norma	ISO/IEC 13606	HL7 CDA	DICOM SR
1	Najmniejszą wymienianą jednostką jest dokument	+	+	+
2	Może zawierać dane/referencje do danych multimedialnych	+	+	+
3	Strukturalizowana zawartość EHR przydatna do przetwarzania	+	+	+
4	Wspiera archetypy/ wzorce	+	+	+
5	Wspiera podpisy elektroniczne składane na dokumentach	+-	+-	+
6	Wspiera szyfrowanie w warstwie transportowej	-	+	+
7	Przesyłanie danych uwierzytelniających użytkownika	-	+	+
8	Wymuszanie polityki kontroli dostępu	+	-	-

Analiza norm wykazała, że struktura EHR jest dobrze określona i ogólna idea tworzenia EHR wg norm ISO/IEC 13606, HL7 CDA, DICOM SR jest podobna. Jednakże mechanizmy bezpieczeństwa nie są już tak dobrze opisane. Proces składania podpisu elektronicznego jest jawnie zdefiniowany jedynie w normie DICOM SR. W przypadku norm ISO/IEC 13606 i ISO/HL7 CDA dokument jest zapisywany zgodnie ze specyfikacją XML. Stąd domyślnie można przyjąć, że podpisy elektroniczne mogą być tworzone np. zgodnie z normą XAdES (patrz rozdz. 2.6.4). Żadna z tych norm nie określa jednak sposobu przechowywania podpisanych dokumentów elektronicznych w repozytoriach dokumentów (np. w systemie EHR).

W ostatnich trzech wierszach Tab. 2.1 przedstawiono cechy bezpieczeństwa związane protokołami przesyłania danych wbudowane w poszczególne normy i specyfikacje techniczne. Cechy te dotyczą szyfrowania przesyłanych danych w warstwie transportowej, uwierzytelniania podmiotów w oparciu przesyłane dane uwierzytelniające oraz kontroli dostępu do danych medycznych, których dotyczy zapytanie, pobranie lub przedłożenie. Zastosowane mechanizmy zabezpieczeń przesyłu danych medycznych muszą zapewnić nie tylko na uzyskanie wymienionych cech bezpieczeństwa, ale także interoperacyjność systemów, w które są wbudowane.

2.3. Systemy EHR

2.3.1 Wpływ na poprawę jakości ochrony zdrowia

Systemy informatyczne ochrony zdrowia zarządzające elektronicznymi dokumentami zdrowotnymi (Systemy EHR) są obecnie rozwijane w wielu państwach na świecie. Systemy te są wdrażane, gdyż informatyzacja ochrony zdrowia pozwala podnieść jakość opieki

zdrowotnej dla obywateli [5-7, 89], a także pozwala zoptymalizować [32] i zredukować koszty zarządzania.

Wyniki badań przedstawione w [8, 9, 31] wykazały, że systemy elektronicznych recept wraz ze wspomaganiem decyzji mogą zredukować poważne błędy medyczne nawet o 55%. Porównanie dwudziestu dziewięciu systemów e-recept pokazało, że w przypadku 66% z nich, ich użycie spowodowało poprawę wydajności lekarzy, chociaż większość z nich nie zmierzyła lub nie mogła zmierzyć bezpośrednich pozytywnych skutków oddziaływań systemu na pacjentów. Dodatkowo, systemy e-recept umożliwiają kontrolę niepożądanych interakcji między lekami (*ang. ADEs - adverse drug invents*); badania przeprowadzone w [108] wykazały, że możliwie jest zredukowanie takich błędów o połowę.

2.3.2 Rejestry i repozytoria

Model rejestru współpracującego z repozytorium jest przedstawiony w [48]. Rejestr może być opisany jako centralna lokalizacja, gdzie przechowywane są metadane dotyczące obiektów (dokumentów). Natomiast repozytorium jest miejscem przechowywania obiektów (dokumentów) zarejestrowanych w rejestrze. Rejestr dostarcza usługi umożliwiające odpytywanie metadanych. Wynik zapytania zawiera referencje do obiektów (dokumentów) znajdujących się w repozytoriach, skąd mogą być pobrane. W celu pobrania dokumentu z repozytorium konieczne jest posiadanie dokładnego identyfikatora dokumentu.

Rejestr jest zwykle zintegrowany z repozytorium. Jednakże w przypadku rozległych systemów może działać oddzielnie. W takim przypadku do jednego rejestru może być podłączonych kilka repozytoriów. W modelu rejestru/repozytorium, porównując do biblioteki, rejestr jest zbiorem kart indeksu, które wskazują konkretną półkę z książkami w bibliotece. A repozytorium jest półką na książki.

2.3.3 Rejestr ebXML

EbXML (*ang. Electronic Business using eXtensible Markup Language*) to rodzina norm opartych na języku XML zaproponowanych przez OASIS i UN/CEFACT. Ma ona na celu stworzenie otwartej, opartej na języku XML infrastruktury umożliwiającej globalne użytkowanie elektronicznej informacji biznesowej przy założeniu maksymalnej interoperacyjności, jednoznaczności i bezpieczeństwa. Na specyfikację ebXML [38] składa się kilka uzupełniających się norm:

- *ebXML Messaging Services* – usługi komunikacyjne,
- *ebXML Registry* – rejestr,
- *ebXML Business Process Specification Schema* – schemat opisu procesów biznesowych,
- *ebXML Collaboration Protocol Profile and Agreement* – profil protokołu współpracy i umowy.

Głównym zadaniem rejestru jest wspomaganie szybkiego wyszukiwania danych cyfrowych umieszczonych w repozytorium dzięki przeszukiwaniu dostępnych metadanych.

Rejestr może opisywać dowolne artefakty, czyli np.: dokumenty i schematy XML, opisy procesów, bazowe komponenty ebXML (*ang. ebXML Core Component*), modele UML, informacje o organizacjach czy komponenty programowe.

Praktycznie wszystkie zdefiniowane właściwości rejestru ebXML są rozszerzalne. Mogą one być dostosowywane do aktualnych wymagań lub normalizowane w postaci profili dla wybranych gałęzi przemysłu czy biznesu. Profile takie pozwalają na pełną interoperacyjność w danej dziedzinie przez precyzyjne określenie zbioru ograniczeń i rozszerzeń standardu ebXML. Kilka przykładowych profili przedstawiono poniżej (ostatni dotyczy ochrony zdrowia):

- ebXML Registry Profile for Web Services [85];
- ebXML Registry Profile for OWL [35];
- ebXML Registry Profile for ebXML Core Components [14];
- ebXML Registry Profile for IHE Cross-Enterprise Document Sharing (XDS) [patrz rozdz. 2.3.4].

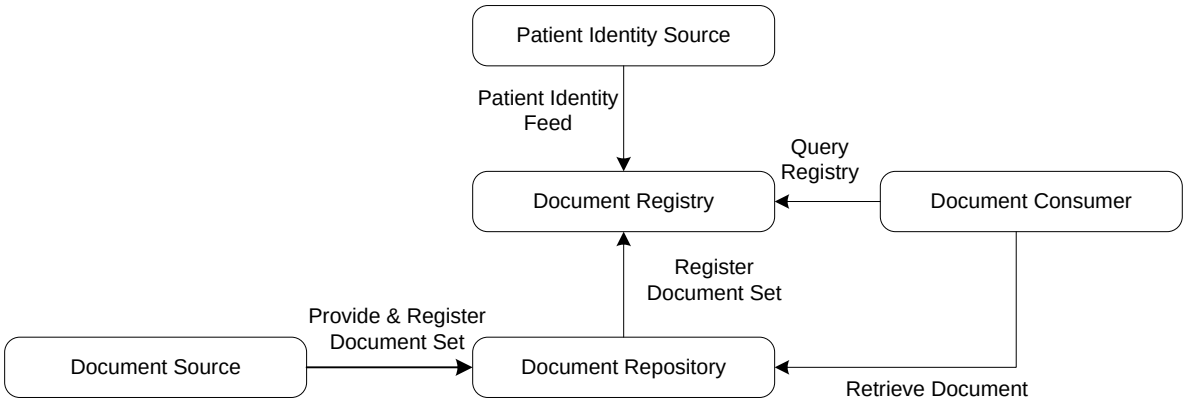
Model informacyjny rejestru ebXML (RIM) definiuje jakie dane i metadane mogą być przechowywane w rejestrze. EbXML umożliwia przechowywanie danych elektronicznych dowolnego typu, takich jak: dokumenty XML, dokumenty tekstowe, pliki graficzne i dźwiękowe. Instancje tego typu danych oznaczone są jako *RepositoryItems* i znajdują się w repozytorium, będącym częścią ebXML. Jako uzupełnienie dla *RepositoryItems* ebXML umożliwia przechowywanie standaryzowanych metadanych, które mogą być wykorzystane do opisania *RepositoryItems*. Instancje metadanych oznaczone są jako *RegistryObjects* (albo jeden z podtypów). *RegistryObjects* przechowywane są w rejestrze, będącym częścią ebXML. Każdy zarejestrowany obiekt (*RepositoryItem*) musi być opisany przez odpowiedni wpis w rejestrze (*RegistryObject*). Szczegółowy opis modelu wraz z diagramem UML znajduje się w [37].

2.3.4 Profil IHE – Wymiana Dokumentów Pomiędzy Przedsiębiorstwami

Większość obecnie tworzonych systemów EHR składa się z wielu repozytoriów i rejestrów. Profil stworzony przez organizację IHE – Wymiana Dokumentów Pomiędzy Przedsiębiorstwami (*IHE XDS – IHE Cross-Enterprise Document Sharing*) [66] zawiera, bazującą na aktualnych standardach, specyfikację do zarządzania współdzieleniem dokumentów pomiędzy jednostkami ochrony zdrowia, którymi może być prywatny gabinet lekarski, klinika, czy oddział szpitalny. XDS jest pierwszym krokiem IHE w celu stworzenia EHR zawierającego informacje o pacjencie z całego jego życia. Dokumenty medyczne składające się na EHR danego pacjenta są przechowywane w repozytorium, natomiast ich opis, czyli metadane są przechowywane w rejestrze.

Grupa jednostek ochrony zdrowia, które zdecydują się na współpracę w zakresie wymiany dokumentów medycznych pacjentów, w profilu IXE XDS jest nazywana *„Clinical Affinity Domain”*. W celu współpracy muszą zostać uzgodnione wspólne zbiory polityk, tj.: identyfikacja pacjentów, kontrola dostępu, czy wspólny zestaw terminów do reprezentowania

metadanych dokumentów. Dla specyfikacji IHE XDS nie ma znaczenia zawartość dokumentu, który może posiadać dowolną zawartość i być dowolnego typu, poczynając od dokumentów tekstowych do ustrukturalizowanych dokumentów, tj.: HL7 CDA, CEN EN 13606, czy DICOM SR. Jednakże, w celu zapewnienia interoperacyjności *„Clinical Affinity Domain”* musi również uzgodnić format dokumentu, jego strukturę oraz zawartość. Profil integracyjny XDS nie zapewnia wszystkich potrzeb związanych z komunikacją EHR. Niektóre scenariusze mogą wymagać użycia innych profili integracyjnych tj.: *Patient Identifier Cross-referencing* (PIX), *Audit Trail and Node Authentication* (ATNA), *Enterprise User Authentication* (EUA), czy *Retrive Information for Display* (RID) .



Rysunek 2.5: Aktorzy i transakcje w profilu IHE XDS (źródło: [66])

Aktorzy i transakcje zdefiniowane w profilu XDS zostali przedstawieni na Rys. 2.6. Repozytorium oraz rejestr dokumentów, znajdujący się w środkowej części diagramu stanowią razem archiwum dokumentów pochodzących z wielu źródeł, które tworzy EHR zawierający informacje medyczne z całego życia określonego pacjenta. Aktorzy *Document Source* oraz *Document Consumer* to systemy kliniczne działające w punkcie opieki zdrowotnej. Po zakończeniu epizodu opieki zdrowia informacje kliniczne są zamieniane w zbiór stałych dokumentów, które są następnie dostarczane do EHR. Aktorzy występujący w IHE XDS to:

- *Document Source* – reprezentuje punkt opieki zdrowotnej, w którym są zbierane dane medyczne. Wysyła dokumenty medyczne oraz metadane do jednego z repozytoriów, które dalej przesyła metadane do centralnego rejestru dokumentów;
- *Document Registry* – przechowuje i zarządza metadanymi wszystkich opublikowanych dokumentów dla pacjentów, o które może być odpytywane (jedną z metadanych jest referencja do repozytorium);
- *Document Repository* – przechowuje opublikowane dokumenty. Repozytorium nie obsługuje zapytań; aby pobrać dokument należy posiadać identyfikator dokumentu otrzymany z rejestru;
- *Document Consumer* – jest aplikacją działającą w miejscu dostarczania usług ochrony zdrowia;

- *Patient Identity Source* – to centralny system, który przydziela i zarządza identyfikatorami pacjentów wewnątrz *Clinical Affinity Domain.*

Dokument jest najmniejszą, przechowywaną jednostką informacji. IHE XDS definiuje dokument jako: *„zbiór atestowanych informacji medycznych (posiadających strukturę lub nie), które tworzą element rekordu pacjenta przeznaczony do współdzielenia”.* Każdy dokument jest przypisany do jednego pacjenta. W rejestrze foldery umożliwiają grupowanie dokumentów należących do jednego pacjenta. Folder zawiera dokumenty przez referencje. Jeden dokument może należeć do zera lub więcej folderów.

W profilu integracyjnym XDS zdefiniowanych jest pięć transakcji pomiędzy aktorami, które umożliwiają zapis i odczyt z rejestru i repozytoriów:

- *Patient Identity Feed* – zapewnia rejestrowi identyfikatory pacjentów zarejestrowanych w *Clinical Affinity Domain.* Transakcja bazuje na HL7 wersja 2.3.1 i używa wiadomości ADT *(admision, discharge, transfer)* z wieloma zdarzeniami obsługującymi rejestracje, aktualizacje oraz łączenie danych pacjenta;
- *Provide and Register Document Set* – jest używana w celu wysłania zbioru dokumentów wraz z metadanymi do repozytorium. Do wysyłania wiadomości jest używane *ebXML messaging framewrok,* którym jest SOAP z załącznikami MIME;
- *Register Document Set* – to transakcja wywoływana przez repozytorium dokumentów, które tworzy URI dla każdego otrzymanego dokumentu i przesyła je do centralnego rejestru wraz z metadanymi;
- *Query Documents* – to transakcja umożliwiająca wyszukiwanie dokumentów w rejestrze. Zapytania są tworzone z użyciem języka SQL według specyfikacji *ebXML Registry Services*;
- *Retrive Document* – to transakcja umożliwiająca pobranie dokumentu z użyciem HTTP URI z repozytorium dokumentów. Repozytorium zwraca żądany dokument w odpowiedzi HTTP.

Istnieje wiele możliwych strategii implementacyjnych dla profilu XDS [66]. Wybór strategii implementacyjnej zależy od konkretnego przypadku użycia. Źródło dokumentów i repozytorium mogą być zintegrowane, czyli każda organizacja należąca do domeny przechowuje dokumenty w własnym repozytorium i tylko rejestruje dokumenty w centralnym, dostępnym dla całej domenie rejestrze. Może zostać ustanowione także zewnętrzne repozytorium, do którego kopiowane są wszystkie dokumenty z lokalnego repozytorium organizacji.

Rejestr dokumentów jest faktycznie rejestrem ebXML, do którego dołączono rozszerzenia IHE tj. „*XDS registry adaptor function”* [66] , które zajmuje się m.in. weryfikacją metadanych przez umieszeniem ich w rejestrze. Dokument XDS przechowywany w repozytorium jest reprezentowany w rejestrze jako „*ebXML ExtrinsicObject*”. *ExtrinsicObjects* w ebXML są używane, aby dostarczyć metadane opisujące zawartość dokumentu, którego typ nie jest znany wewnątrz rejestru. Dokumenty XDS mogą być

grupowane w foldery, które są stworzone w rejestrze ebXML z użyciem pojęcia *„ebXML RegistryPackage”,* które jest używane do logicznego grupowania instancji *RegistryObject*. Foldery nie mogą być zagnieżdżane, dlatego że *RegistryPackag*e nie mogą być zagnieżdżane w ebXML.

2.3.5 Narodowe systemy ochrony zdrowia

Systemy EHR są wdrażane głównie w krajach europejskich, w Ameryce Północnej oraz w Australii i Japonii. Poziom wdrożenia oraz funkcjonalność systemów jest różna [21, 65, 80, 95], jednak żaden z systemów nie jest w pełni skończony i nadal trwają pracę nad zwiększeniem ich funkcjonalności i poziomu bezpieczeństwa. W każdym z państw występują różne warunki lokalne, polityki i wymagania [64] , które przekładają się na różne podejścia do projektowania systemów EHR.

We wszystkich państwach papierowa dokumentacja jest zastępowana przez elektroniczną w różnym tempie. W niektórych przychodniach, czy szpitalach mogą być wdrożone różne systemy do przechowywania dokumentów medycznych w postaci cyfrowej wewnątrz danej jednostki ochrony zdrowia. Jednakże stopień informatyzacji jednostek ochrony zdrowia, rodzaj i liczba przechowywanych dokumentów zależy od uwarunkowań lokalnych. W związku z tym dane w systemach EHR (które muszą połączyć wszystkie jednostki ochrony zdrowia w swoim zakresie działania) mogą być przechowywane [62]:

- lokalnie – w repozytoriach lokalnych systemach i tylko są rejestrowane w centralnym rejestrze systemu;
- centralnie – wyłącznie w repozytoriach krajowego systemu EHR (nic nie jest przechowywane lokalnie);
- hybrydowo – dane są przechowywane zarówno lokalnie jak i centralnie.

Dodatkowo dany system EHR może pobierać dane medyczne należące do pacjenta z innych systemów EHR (z innych regionów, państw) w przypadku, gdy systemy są ze sobą połączone. Problem budowy bezpiecznej architektury systemów EHR oraz modelu współpracy miedzy nimi jest poruszany m. in. w [18, 20, 52, 99].

2.3.5.1 System kanadyjski

W Kanadzie system EHR jest rozwijany przez organizację non-profit o nazwie Infoway [26]. Do końca 2016 100% Kanadyjczyków powinno mieć dostępny EHR [28]. Kanadyjski system EHR jest podzielony na wiele (nawet do 40) regionalnych infostruktur. Pojedyncza infostruktura EHR składa się z pięciu ogólnych repozytoriów danych klinicznych (repozytorium wspólnych danych zdrowotnych, repozytorium z wynikami laboratoryjnymi, repozytorium z informacjami o przepisanych lekach, repozytorium z obrazami medycznymi i repozytorium z informacją o szczepieniach) [27] i składa się z kilku rejestrów (rejestru klientów (pacjentów), rejestru dostawców, rejestru użytkowników, rejestru lokalizacji), które przechowują informacje na temat pacjentów, specjalistów ds. ochrony zdrowia czy miejsc

świadczenia usług zdrowotnych. Istnieje także kilka dodatkowych rejestrów, np. repozytorium technologii, baza danych struktur wiadomości.

Struktura wewnętrzna systemu jest ukryta przed użytkownikami i dostęp do informacji jest tylko możliwy przez HIAL. Wszystkie dokumenty przechowywane w systemie są indeksowane przez rejestr lokalizacji. Istnieje także rejestr posiadający informacje, czy inne infostruktury EHR posiadają informacje na temat konkretnego pacjenta. Po wprowadzeniu dokumentu klinicznego do systemu dostępowego PoS (system szpitalny, lekarza rodzinnego czy apteki), system ten wysyła informacje do HIAL. HIAL analizuje wiadomość, wydobywa wszystkie ważne informacje i wstawia nowe rekordy do odpowiednich rejestrów i repozytoriów.

2.3.5.2 System brytyjski

Inne podejście do struktury systemów EHR zostało zastosowane w Wielkiej Brytanii, gdzie został utworzony jeden ogólnokrajowy rejestr medyczny [56] przechowujący podstawowe informacje o pacjentach, np.: imię, nazwisko, grupę krwi, alergie i przebyte operacje. Rejestr ten nazywa się *Summary Care Record (SCR)* i umożliwia dostęp do podstawowych danych na terenie całego kraju, np.: w sytuacjach awaryjnych. Jednakże uznano, że jest potrzebny system do przechowywania bardziej szczegółowej informacji klinicznej i wprowadzono system rejestrów *Detailed Care Records (DCR).* System DCR nie posiada ogólnokrajowego rejestru, a w zamian system jest złożony z regionalnych rejestrów DCR oraz z głównego rejestru posiadającego odnośniki do rejestrów regionalnych. Miejsca opieki zdrowotnej (np.: szpitale, lekarze rodzinni) mogą nadal przechowywać informacje w swoich rejestrach lokalnych. Rejestry muszą spełniać uznane standardy i muszą umożliwiać komunikację i transfer danych klinicznych do rejestrów i innych miejsc opieki zdrowotnej.

2.3.5.3 System estoński

Idea systemu estońskiego jest podobna do brytyjskiego [90, 96]. Centralna baza danych zawiera trzy typy podstawowych informacji klinicznych o pacjencie, katalog odnośników do innych rejestrów w lokalnych miejscach opieki zdrowotnej. System estoński umożliwia podłączenie istniejących lokalnych rejestrów, jedynie wymagane jest spełnienie określonych standardów i możliwość podłączenia do ogólnokrajowego systemu EHR.

2.3.5.4 System niemiecki

W Niemczech większość dostawców usług ochrony zdrowia posiada lokalne systemy elektronicznej dokumentacji zdrowotnej [49]. Obecnie nie istnieje pojedynczy system informatyczny, który połączyłby systemy lokalne. W planach jest zbudowanie ogólnokrajowego infrastruktury e-Zdrowia, która umożliwi komunikacje miedzy systemami lokalnymi dzięki użyciu standaryzowanych interfejsów.

2.3.5.5 System turecki

Turecki system EHR ma scentralizowaną architekturę [74]. Celem systemu jest przechowywanie wszystkich danych z miejsc opieki zdrowotnej, rozproszonych po kraju, w repozytoriach ministerstwa zdrowia. Dane są przechowywane lokalnie, a ich kopia jest wysyłana do centralnego rejestru. System jest zbudowany na bazie sieci e-Zdrowia łączącej podstawowe komponenty. W celach komunikacyjnych użyty jest protokół HL7 v3. Jednym z komponentów systemu jest narodowy słownik danych zdrowotnych, który umożliwia określenie formatu i definicji danych, przez co umożliwia interoperacyjność semantyczną pomiędzy różnymi aplikacjami. Przepływ danych nie jest wyłącznie jednokierunkowy, autoryzowane osoby mogą odpytywać i pobierać informacje z centralnego rejestru. W przyszłości, po wprowadzeniu odpowiedniego ustawodawstwa, planowane jest umożliwianie współdzielenia dokumentów klinicznych pomiędzy dostawcami usług ochrony zdrowotnej.

2.4. Wymagania odnośnie długoterminowego przechowania EHR

Obecne możliwość zarządzania i przechowywania danych elektronicznych na poziomie fizycznym, jak i również długoterminowe strategie umożliwienia odczytu są udokumentowane i implementowane w aktualnych systemach informacyjnych [16, 46, 71]. Obecne badania w tym obszarze skupiają się głównie na problemach zachowania integralności obiektów cyfrowych oraz tworzenia dowodów ich istnienia. Problemy te są szczególnie ważne dla dokumentów wiążących prawnie. Wyzwania związane z badaniami nad przechowywaniem EHR opisano również w [79].

Ogólne wymagania odnośnie bezpieczeństwa systemów EHR zostały zebrane w ISO TS 18308 [69]. Celem ISO TS 18308:2004 „*Health Informatics – Requirments for an electronic health record architecture*" jest zebranie i zestawienie zbioru wymagań technicznych jak klinicznych dla architektury systemów EHR umożliwiających wymianę i udostępnianie EHR w różnych systemach państw i modelach dostarczania usług zdrowotnych. Specyfikacja wymienia tylko wymagania, jednocześnie nie podaje jak mają być zaimplementowane. Zbiór najważniejszych wymagań i ich definicji dotyczących bezpieczeństwa zawartych w ISO TS 18308 został przedstawiony przez H. Linden w [78] i jest następujący:

- uwierzytelnianie – weryfikacja deklarowanej tożsamości – osoby lub systemu;
- autoryzacja – przyznawanie praw, które zawiera przydzielanie dostępu bazując na prawach dostępu;
- integralność – zachowanie spójności danych i wykrywanie zmian;
- niezaprzeczalność – brak możliwości wyparcia się swego uczestnictwa w całości lub części wymiany danych przez jeden z podmiotów uczestniczących w tej wymianie;
- poufność – dane nie mogą zostać ujawnione niepowołanym osobom czy systemom;
- zgoda – uzyskiwanie, zapisywanie i śledzenie świadomej zgody pacjenta na dostęp do jego danych medycznych w określonym przedziale czasu;

- odpowiedzialność autora – zapewnienie, że każdy stworzony dokument może mieć jednoznacznie określonego autora;
- dzienniki zdarzeń na potrzeby audytu – wszystkie działania powinny być rejestrowane w porządku chronologicznym;
- zarządzanie wersjami – obsługa wersjonowania na poziomie granulacji, na którym informacje są atestowane, obsługujące środki pozwalające dostrzec modyfikacje lub uaktualnienia; musi istnieć możliwość odtworzenia stanu EHR w dowolnym przeszłym momencie.

Spełnienie tych wymagań dla systemu znajdującego się w jednej organizacji, może być stosunkowo proste. Jednakże dla złożonych systemów, tj. systemów EHR, które obejmują wiele organizacji i znajdują się w wielu regionach czy państwach często pod różnymi lokalnymi jurysdykcjami prawnymi, spełnienie tych wymagań urasta do bardzo trudnych problemów. W literaturze istnieje ogólny konsens co do wymagań stawianych systemom informatycznym zarządzającym dokumentami medycznymi.

Elektroniczne dokumenty zdrowotne muszą być przechowywane przez całe życie pacjenta [77], czyli nawet ponad 100 lat. Aby zapewnić takie cechy bezpieczeństwa jak integralność, autentyczność, niezaprzeczalność używa się podpisów cyfrowych oraz znaczników czasu. Z infrastrukturą klucza publicznego obsługującą podpisy cyfrowe związane są następujące problemy w przypadku długoterminowego przechowywania:

- klucze używane do tworzenia i weryfikacji podpisu mają ograniczony czas użycia, zwykle urzędy certyfikacji wydają certyfikaty klucza publicznego na 2 lata;
- algorytmy używane do tworzenia podpisu mogą być w przyszłości złamane lub znacznie osłabione;
- klucze użyte w podpisie mogą zostać skompromitowane;
- informacje konieczne do weryfikacji podpisu tj. łańcuchy certyfikatów, czy listy certyfikatów odwołanych mogą być niedostępne w przyszłości;
- zaufana trzecia strona (TTP) może w przyszłości nie być zaufana ze względu na zaprzestanie działalności, czy brak spełnienia wymagań bezpieczeństwa;

Rozwiązania zapewniające długoterminową ważność podpisów cyfrowych muszą rozwiązywać powyższe problemy. Niniejsza rozprawa zajmuje się problemem zapewnienia integralności, autentyczności i niezaprzeczalności (definicje patrz rozdz. 1.2.).

Problem uwierzytelniania, autoryzacji w kontekście dostępu do EHR oraz mechanizmu wyrażania przez pacjenta zgody na dostęp do EHR są opublikowane m. in. w [3, 19, 33, 86 101, 102, 107]. Problem zarządzania ryzykami związanymi z danymi zdrowotnymi jest poruszony w [73]. Natomiast zagadnienie transmisji rekordów medycznych przez Internet w [25].

2.5. Infrastruktura klucza publicznego

Infrastruktura klucza publicznego (*ang. PKI – Public Key Infrastructure*) [2] to oprogramowanie, sprzęt, polityki, protokoły i prawo potrzebne, aby możliwe było powiązanie

klucza publicznego z daną osobą oraz zweryfikowanie podpisu cyfrowego [47, 76]. PKI jest wykorzystywana obecnie powszechnie w Internecie (np. do bezpiecznych połączeń ze stronami internetowymi banków) oraz do podpisywania dokumentów. W wielu państwach podpis cyfrowy złożony z użyciem PKI jest uznawany za równoważny podpisowi własnoręcznemu.

2.5.1 Podpis cyfrowy

Podpis cyfrowy z załącznikiem to informacja dołączona do danych, umożliwiająca weryfikację ich autentyczności i integralności [82]. Norma ISO 7498-2 [72] definiuje podpis cyfrowy jako: *„dane dołączone do danych lub ich przekształcenie kryptograficzne, które pozwala odbiorcy danych udowodnić pochodzenie danych i zabezpieczyć je przed fałszerstwem”*. Ważny podpis cyfrowy umożliwia stwierdzenie, że dokument został stworzony przez określonego autora oraz nie został zmieniony podczas przesyłania. Każdy podpis cyfrowy składany przez tego samego użytkownika jest inny (wyjątek stanowi podpisywanie tego samego dokumentu z wykorzystaniem dopełnienia nielosowego). Natomiast podpis własnoręczny powinien być zawsze taki sam. Podpis cyfrowy jest wielokrotnie trudniejszy do podrobienia [47] od podpisu własnoręcznego.

Do tworzenia podpisów cyfrowych używa się kryptografii asymetrycznej, w której wykorzystuje się dwa klucze stworzone w taki sposób, że kryptogram zaszyfrowany za pomocą jednego klucza może być odszyfrowany tylko za pomocą drugiego. Kluczem szyfrującym nie można przeprowadzić operacji deszyfrowania i odwrotnie kluczem deszyfrującym nie można przeprowadzić operacji szyfrowania. W PKI jeden klucz (klucz prywatny), trzymany przez użytkownika w sekrecie, służy do podpisywania. Natomiast drugi klucz (klucz publiczny), dostępny dla każdego zainteresowanego, służy do weryfikacji podpisu.

2.5.2 Certyfikaty

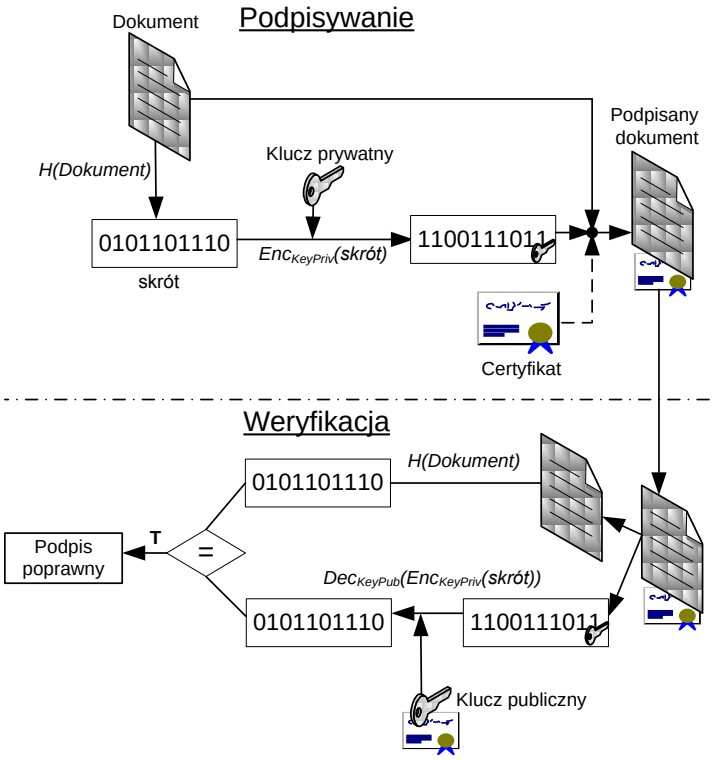
Aby powiązać klucz publiczny i prywatny z osobą fizyczną wykorzystuje się certyfikaty klucza publicznego. Certyfikat to dane osoby powiązane z kluczem publicznym oraz dane i podpis cyfrowy urzędu certyfikacji (*ang. CA – Certification Authority*) wystawiającego dany certyfikat. Certyfikat zawierający klucz publiczny jest dostępny dla wszystkich i umożliwia weryfikacje podpisu.

Zaufanie do ważności certyfikatów cyfrowych, potwierdzających przynależność klucza publicznego do osoby fizycznej, wynika z zaufania do urzędu certyfikacji wydającego dany certyfikat. Proces sprawdzania ważności podpisu cyfrowego jest kilku etapowy. Pierwszym krokiem jest sprawdzeniu matematycznej poprawności podpisu. Następnym krokiem jest sprawdzenie łańcucha certyfikatów (tworzących tzw. ścieżkę certyfikacji), aż do certyfikatu głównego, zaufanego urzędu certyfikacji oraz sprawdzenie listy certyfikatów unieważnionych (*ang. CRL – Certificate Revocation List*). W infrastrukturze PKI pierwszorzędne źródło zaufania do ważności podpisu cyfrowego stanowi właśnie sprawdzenie ścieżki certyfikacji.

Dzięki wykorzystaniu infrastruktury PKI istnieje możliwość stwierdzenia integralności, autentyczności, poufności oraz niezaprzeczalności pochodzenia dokumentów cyfrowych. Ważność certyfikatów trwa zwykle dwa lata. W przypadku, gdy dokument musi być przechowywany przez dłuższy okres czasu, konieczny jest jeden z sposobów przedłużenia okresu ważności podpisu cyfrowego, np. z użyciem znacznika czasu.

2.5.3 Tworzenie i weryfikacja podpisu cyfrowego

Proces tworzenia i matematycznej weryfikacji podpisu cyfrowego przedstawia Rys. 2.6. W celu utworzenia podpisu obliczany jest skrót z dokumentu z wykorzystaniem kryptograficznej funkcji skrótu. Następnie skrót jest szyfrowany z użyciem klucza prywatnego użytkownika. Podpisany dokument zawiera dokument wraz z zaszyfrowanym skrótem oraz opcjonalnie certyfikatem. Aby zweryfikować dokument oblicza się z niego skrót, który porównuje się ze skrótem otrzymanym po odszyfrowaniu kluczem publicznym skrótu z dokumentu zaszyfrowanego kluczem prywatnym. Gdy oba skróty są identyczne to podpis jest poprawny matematycznie.



Rysunek 2.6: Tworzenie i weryfikacja podpisu cyfrowego (źródło: opracowanie własne)

Następnym krokiem sprawdzania podpisu jest weryfikacja ścieżki certyfikacji. Później można opcjonalnie zweryfikować tzw. dodatkowe źródła zaufania, czyli czy aktualnie używane algorytmy są obecnie zalecane oraz czy CA wydające certyfikat znajduje się na liście statusu usług zaufanych opisanych w następnym podrozdziale. Dodatkowe usługi zaufania mają szczególne znaczenie podczas sprawdzania ważności archiwalnych podpisów

cyfrowych, gdyż wraz z upływem czasu algorytmy mogą zostać przełamane lub znacznie osłabione, a przez to nie polecane oraz CA mogą zaprzestać działalności lub utracić zaufanie.

2.5.4 Dodatkowe źródła zaufania

2.5.4.1 Algorytmy kryptograficzne

Wszystkie usługi wykorzystujące infrastrukturę klucza publicznego wykorzystują algorytmy kryptograficzne. Z uwagi na szybki przyrost mocy obliczeniowej komputerów oraz postęp w dziedzinie kryptografii, projektanci systemów PKI muszą określić, czy dany algorytm uważany jest za bezpieczny i czy spełnia wymogi prawne, aby podpis cyfrowy był równoważny odręcznemu. W różnych państwach mogą być zalecane/wymagane różne algorytmy o różnych parametrach. W Polsce załącznik nr 3 Rozporządzenia Rady Ministrów [98] do ustawy o podpisie elektronicznym [103] zawiera informacje na temat minimalnych wymagań dotyczących algorytmów szyfrowych służących do składania podpisu elektronicznego. Natomiast specyfikacja techniczna ETSI TS 102 176-1 [42] zawiera dokładne zalecenia na temat stosowania algorytmów w infrastrukturze klucza publicznego.

W normie ETSI TS 102 176-1 zdefiniowano listę polecanych algorytmów funkcji skrótu oraz listę algorytmów używanych do podpisu elektronicznego, a także ich kombinacji nazwanych zestawem do podpisu (*ang. signature suite*). Głównymi parametrami powodującymi włączenie danego algorytmu do tej specyfikacji technicznej są:

- uznanie algorytmu za bezpieczny;
- popularność stosowania algorytmu;
- łatwa możliwość referencji do jego specyfikacji.

W przypadku, gdy algorytm nie jest umieszczony na liście nie oznacza, że nie można go używać, a oznacza że algorytm nie spełnił wyżej wymienionych wymagań. Można założyć rozsądny poziom bezpieczeństwa jeżeli polecane algorytmy zostaną użyte z wykorzystaniem polecanych parametrów w kontekście ich rekomendacji. Lista tych algorytmów jest aktualizowana co pewien okres czasu, aby uwzględnić zmiany w dziedzinie kryptografii.

2.5.4.1 Lista statusu zaufanych usług

Standard ETSI TS 102 231 [43] zawiera informacje o sposobie tworzenia list statusu zaufanych usług (*ang. TSL - Trusted-service Status List*) udostępniających informacje na temat statusu zaufanych usług, aby zainteresowane strony mogły ustalić, czy usługa zaufania (*ang. trust service*) działała lub działa według uznanych zasad lub czy działała według uznanych zasad w czasie, w którym transakcja zależna od tej usługi miała miejsce. Celem TSL jest określenie zharmonizowanego sposobu publikacji informacji na temat statusu usług zaufanych i ich dostawców. Listy TSL są zarządzane przez operatorów, którzy postępują według określonych zasad oceny.

W ETSI TS 102 231 zdefiniowano tylko typ, rodzaj i znaczenie informacji, które mogą być prezentowane za pomocą TSL, natomiast nie definiuje się w jaki sposób informacje mają być zbierane przez operatorów. Standard nie określa jakie zasady oceny operator

powinien użyć w celu ustalenia statusu usługi zaufanej, którą nadzoruje. Nie definiuje także sposobu prezentacji statusu i informacji powiązanych z zasadami poza kontekstem TSL, np. na stronie zasad. Operator TSL musi być w stanie dostarczać informacje na temat jej zawartości w formie, która umożliwia użytkownikowi łatwy odczyt, pozyskanie i drukowanie w formie do umożliwiającej automatyczną weryfikację statusu .

Informacje zawarte w TSL powinny stanowić dodatkowe źródło zaufania; podstawowe źródło zaufania powinno wynikać ze sprawdzenia ścieżki certyfikacji. Lista TSL jest podpisana cyfrowo w celu umożliwienia sprawdzenia autentyczności i oprócz aktualnego statusu usług zaufanych musi zawierać także informacje o historii ich statusu. TSL składa się z czterech głównych komponentów:

1. Zawierającego informacje na temat zasad wydawania (*ang. issuing scheme*).
2. Identyfikującego TSP (*ang. Trusted-service Provider*) uznawanego przez zasady.
3. Identyfikującego usługi dostarczane przez TSP i ich aktualny status.
4. Zawierającego historię statusu usług.

2.6. Długoterminowe przechowywanie podpisanych dokumentów medycznych

Dokumenty zdrowotne w celu spełnienia wymagań bezpieczeństwa przedstawionych w rozdz. 2.4 muszą być podpisywane cyfrowo. Długoterminowe przechowywanie wymaga zastosowania rozwiązań pozwalających na przedłużenie ważności podpisów cyfrowych. Przedłużanie ważności każdego podpisu oddzielnie wymaga dużej mocy obliczeniowej. Szczególnie w systemach EHR, które z założenia służą do przechowywania miliardów dokumentów. Z tego powodu zaproponowano rozwiązania pozwalające zoptymalizować proces utrzymywania ważności podpisanych dokumentów zdrowotnych.

2.6.1 Podpis cyfrowy w długim okresie

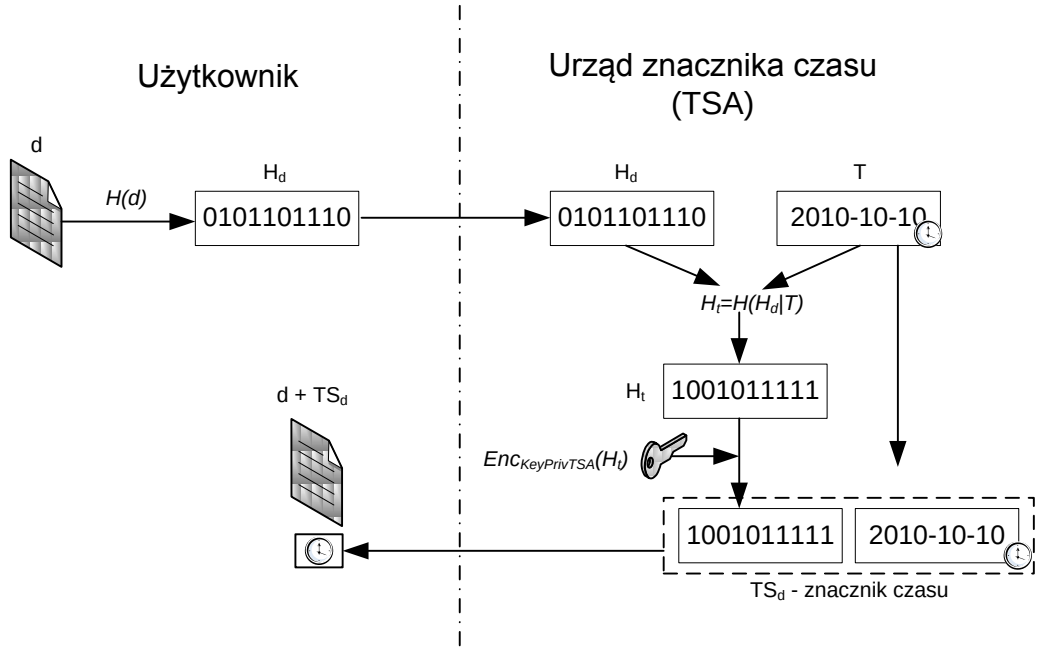
Podpis cyfrowy, w przeciwieństwie do podpisu odręcznego, po upływie czasu ważności certyfikatu z nim powiązanego traci ważność. Jeśli podpisany dokument musi być przechowywany w okresie dłuższym niż ważność certyfikatu klucza publicznego, to należy przedłużyć jego ważność stosując np. znaczniki czasu. Weryfikacja podpisu cyfrowego przebiega kilku etapowo. Na początku należy sprawdzić matematyczną ważność podpisu. Następnie należy sprawdzić łańcuch certyfikatów. Podczas weryfikacji certyfikatów należy sprawdzić listy certyfikatów odwołanych (CRL). Dodatkowo, gdy okres przechowywania podpisanego dokumentu jest długi, to metoda przedłużania jego ważności musi uwzględniać możliwość utraty zaufania do urzędu certyfikacji (CA) oraz możliwość przełamania lub osłabienia użytych algorytmów kryptograficznych.

2.6.2 Zaufane znaczniki czasu

Zaufane znaczniki czasu są tworzone przez zaufane urzędy znacznika czasu (*ang. TSA – Timestamp Authority*). Znaczniki czasu są używane, aby potwierdzić istnienie danych (np. danych medycznych, kontraktów) przed pewnym momentem czasu. Samo zawarcie daty w

podpisie nie powoduje, że trzecia strona może zaufać, że dana data jest prawidłowa. Podmiot tworzący podpis mógłby wpisać dowolną datę. Zaufane znaczniki czasu zapobiegają wstecznemu datowaniu dokumentów. W celu zwiększenia wiarygodności i redukcji podatności można użyć wielokrotnych znaczników czasu.

Stworzenie wiarygodnego znacznika czasu wymaga przesłanie jedynie skrótu dokumentu do TSA. Skrót oblicza się z wykorzystaniem jednokierunkowej kryptograficznej funkcji skrótu. Umożliwia to zachowanie poufności dokumentów. TSA aby stworzyć znacznik czasu (patrz Rys. 2.7) tworzy znacznik czasu (dane zawierające zaufany czas i swoje dane identyfikacyjne). Następnie oblicza skrót ze skrótu z przesłanego dokumentu i ze znacznika czasu. Kolejnym krokiem jest podpisanie obliczonego skrótu kluczem prywatnym TSA. Do użytkownika, który wysłał żądanie utworzenia podpisu przesyłany jest podpisany znacznik czasu zawierający podpisany skrót i znacznik czasu.

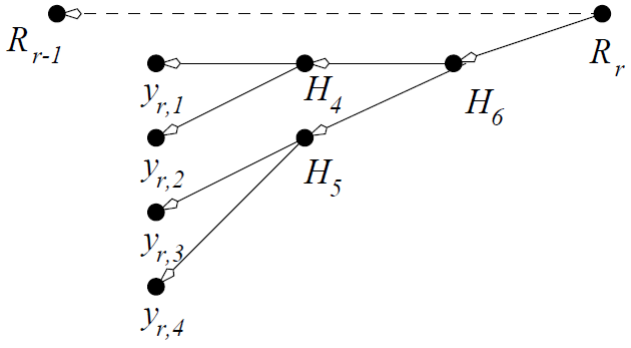


Rysunek 2.7: Tworzenie zaufanego znacznika czasu (źródło: opracowanie własne)

2.6.3 Schematy wiązań binarnych

Podsumowując, aby utworzyć znacznik czasu TSA dołącza aktualny czas *t* do przedłożonego dokumentu *X*, podpisuje dokument złożony z (*t*, *X*) i zwraca dwie wartości *t* i *s* = sig_{TSA} *(t, X)* do klienta. TSA musi być w pełni zaufane, gdyż nie ma możliwości zweryfikowania, czy znacznik czasu faktycznie został wydany w czasie *t*. Aby wyeliminować tą niedogodność tak aby system znakowania czasem nie polegał wyłącznie na kluczach czy innych tajnych informacjach, zaproponowano schematy powiązań binarnych (*ang. binary linking schmes*) [24].

W celu zmniejszenia konieczności zaufania do TSA, TSA może powiązać razem wszystkie znaczniki czasu w łańcuch (*ang. linear linking schemes*) używając odpornej na kolizje funkcji skrótu [53]. W takim przypadku n-ty znacznik dla czasu t_n dla dokumentu X_n jest następujący: $s = sig_{TSA}\ (n, t_n, ID_n, X_n, L_n)$, gdzie tn to aktualny czas, ID_n to identyfikator użytkownika, a L_n jest informacją wiążącą z poprzednimi wydanymi znacznikami i jest określona wzorem rekurencyjnym: $L_n=(\ n\text{-}1,\ t_{n-1},\ ID_{n-1},\ X_{n-1},\ H(L_{n-1}))$. W praktycznej implementacji wadą tego schematu jest duży nakład obliczeń koniecznych do przeprowadzenia weryfikacji. Liczba kroków koniecznych do weryfikacji jednokierunkowej relacji pomiędzy dwoma znacznikami czasu jest liniowy w stosunku do ilości znaczników miedzy nimi.



Rysunek 2.8: Przykład schematu Haber-Stornetta (źródło: [10, 24])

Wady tej nie posiadają schematy „drzewo-podobne" (*ang. tree-like schemes*). Dwa podobne schematy, używające drzewa, zostały zaproponowane przez Benaloh de Mare [15] i przez Haber-Stornetta [10, 24]. W schemacie Haber-Stornetta (patrz Rys. 2.8) procedura znakowania czasem jest podzielona na rundy. Znacznik czasu R_r dla rundy r jest skumulowanym skrótem z znacznika czasu R_{r-1} dla rundy $r\text{-}1$ oraz wszystkich dokumentów wysłanych do TSA w czasie rundy r. Po ukończeniu rundy r tworzone jest binarne drzewo T_r. Każdy uczestnik rundy P_i, który chce uzyskać znacznik czasu przynajmniej dla jednego dokumentu w rundzie r, wysyła do TSA skrót $y_{r,i}$ będący skrótem z R_{r-1} oraz z wszystkich dokumentów, które P_i chce oznakować czasem. Liście drzewa T_r są oznakowane przez różne $y_{r,i}$. Każdy wewnętrzny węzeł T_r jest rekurencyjnie oznaczony jako $H_k=H(H_{kL},H_{kR})$, gdzie kL i kR są odpowiednio lewym i prawym węzłem k, a H jest funkcją skrótu odporną na kolizje. TSA musi przechowywać tylko znaczniki czasu R_r dla rund. Cała pozostała informacja konieczna do zweryfikowania dokumentu jest przechowywana wewnątrz struktury znacznika czasu.

Schemat Benaloh de Mare różni się od schematu Haber-Stornetta brakiem bezpośredniego wiązania pomiędzy R_r a R_{r-1}. Zamiast tego każdy $y_{r,i}$ jest wiązany z R_{r-1}. Weryfikator bez sprawdzenia pojedynczych znaczników czasu nadesłanych dokumentów nie ma możliwości sprawdzenia jednokierunkowej zależności pomiędzy R_i.

2.6.3 Słowniki uwierzytelniane

W sytuacji w której mamy trzy strony: zaufane *źródło*, niezaufany *katalog* i użytkowników oraz *źródło* chce udostępnić informację za pomocą *katalogu* użytkownikom. *Źródło* definiuje skończony zbiór *S* elementów, które zmieniają się z czasem poprzez operacje wstawiania lub usuwania elementów. *Katalog* zarządza kopią zbioru *S* i otrzymuje z *źródła* oznakowane czasem aktualizacje wraz z *informacją aktualizującą uwierzytelnienie.* Użytkownik przeprowadza zapytania o członkostwo elementu *e* w zbiorze *S* . Jednak zamiast bezpośredniego odpytywania *źródła,* odpytuje *katalog*. *Katalog* dostarcza użytkownikowi odpowiedź typu tak/nie wraz z *informacją aktualizującą uwierzytelnienie*, która dostarcza dowód złożony przez złączenie oświadczeń podpisanych przez *źródło*. Następnie użytkownik weryfikuje dowód polegając wyłącznie na zaufaniu do *źródła* i na dostępności informacji publicznej umożliwiającej sprawdzenie podpisu *źródła*. Struktura danych używana przez *katalog* do zarządzania zbiorem *S* wraz z protokołem do aktualizacji i zapytań jest nazywana słownikiem uwierzytelnianym [51].

2.6.4 Przedłużanie ważności pojedynczych, podpisanych cyfrowo dokumentów

Specyfikacja formatu podpisu cyfrowego jest zawarta w XMLDSig [4] oraz w XAdES [41]. XMLDSig pozwala tworzyć podpisy cyfrowe w formacie xml, które jednakże są ważne tylko w okresie ważności certyfikatu. Natomiast XAdES jest rozszerzeniem XMLDSig używającym zaufane znaczniki czasu w celu zapewnienia wiarygodności podpisu po upływie normalnego czasu jego ważności i w celu wspierania niezaprzeczalności. Umożliwia również opcjonalne stosowanie dodatkowych znaczników czasu, aby zapewnić bardzo długą ochronę przeciwko kompromitacji kluczy lub osłabieniu algorytmów.

Specyfikacja XAdES zawiera kilka form podpisu cyfrowego. Każda kolejna forma to dodanie kolejnych wymagań do poprzedniej. Najbardziej podstawową formą jest XAdES-BES, która rozszerza XML-DSig włączając do właściwości objętych podpisem dodatkowe właściwości kwalifikowane – minimum certyfikat podpisującego. XAdES-EPES rozszerza XAdES-BES o identyfikator polityki (określającej jakie właściwości muszą być zawarte), zgodnie z którą został wydany certyfikat. Polityka musi być używana przy weryfikacji podpisu. XAdES-T rozszerza podpis o znacznik czasu i dzięki czemu można udowodnić istnienie podpisu w określonym momencie czasu. XAdES-C dodaje referencje do danych weryfikacyjnych (certyfikaty, listy CRL). XAdES-X tworzy znacznik czasu nad referencjami z XAdES-C. XAdES-X-L zamiast referencji do certyfikatów i list CRL wymaga umieszczenia ich w całości. XAdES-A dodaje możliwość stosowania okresowego znacznika czasu, aby przedłużyć ważność podpisów, gdy okres ich ważności dobiega końca.

2.6.5 Przedłużanie ważności grup podpisanych cyfrowo dokumentów

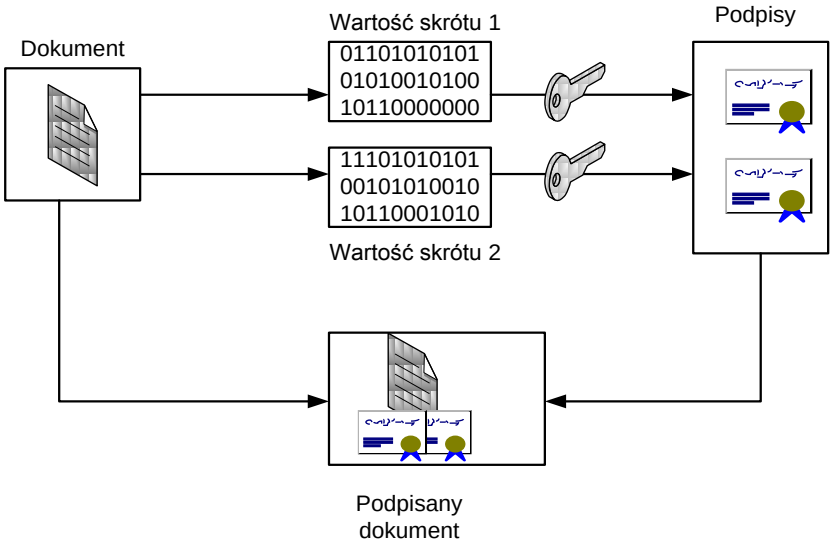
P. Pharow i B. Blobel w [93] rozważyli różne propozycje przedłużania ważności dla grup podpisów cyfrowych zawartych w dokumentach medycznych. Ponowne podpisywanie można wykonać na dwa sposoby. Pierwszy sposób wymaga „odpakowania” dokumentów z aktualnych podpisów i podpisania na nowo dokumentu. Natomiast drugi sposób wymaga

„opakowania” aktualnego podpisu w nowy (tak jak jest to robione w XAdES-A). Ze względów prawnych tylko drugi sposób może być brany pod uwagę. W tym sposobie kolejne warstwy są dodawane podobnie jak kolejne warstwy cebuli. Wszystkie poprzednie podpisy można zweryfikować, ale należy przechowywać wszystkie poprzednie powiązane certyfikaty i listy CRL.

W zarekomendowanym mechanizmie, nowo złożony podpis w celu przedłużenia poprzedniego podpisu, musi zawierać wszystkie poprzednie podpisy cyfrowe jak i znaczniki czasu. W celu umożliwienia weryfikacji poprzednich podpisów wszystkie poprzednie certyfikaty powiązane z podpisami muszą być również przechowywane. EHR przechowują wiele dokumentów. Wiele z tych dokumentów jest powiązanych ze sobą tj. badania krwi, dlatego autorzy rekomendują, aby przechowywać te dokumenty jako zbiór wraz z definicją zależności między nimi. Na Rys. 2.9 został zaprezentowany proces ponownego podpisywania tych dokumentów, w którym przed upływem czasu grupa powiązanych dokumentów jest ponownie podpisywana kwalifikowanym podpisem i/lub znakowana czasem.

Rysunek 2.9: Ponowne podpisywanie i składanie znacznika czasu dla zbioru dokumentów (źródło: [93])

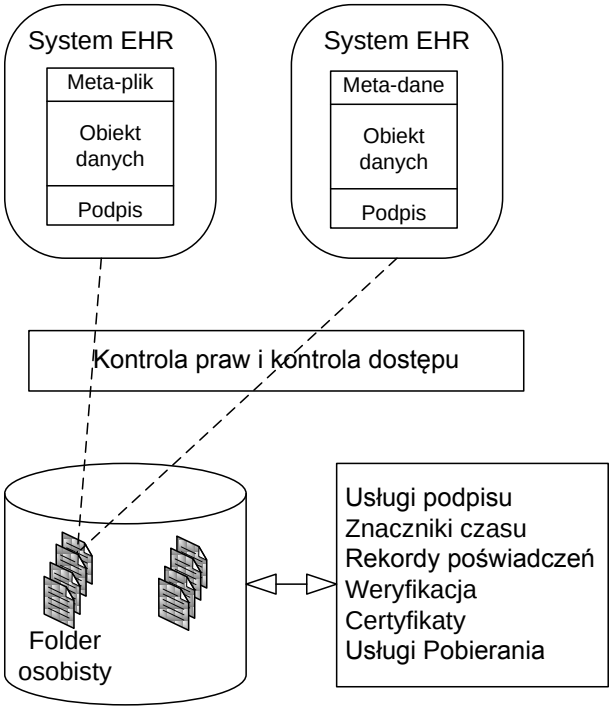
W celu uniknięcia sytuacji, że w czasie obowiązywania podpisu cyfrowego (lub znacznika czasu) zestaw używanych algorytmów kryptograficznych zostanie przełamany lub znacząco osłabiony stosuje się rozwiązanie (patrz Rys. 2.10) polegające na tworzeniu dwóch podpisów (lub znaczników czasu) z wykorzystaniem dwóch różnych zestawów algorytmów i certyfikatów wystawionych przez różne CA (lub różnych TSA w przypadku znaczników czasu).



Rysunek 2.10: Tworzenie podpisów cyfrowych z wykorzystaniem dwóch zestawów algorytmów (źródło: [93])

2.6.6 Model zaufanego archiwalnego notariatu

Ogólny model zaufanego archiwum notarialnego (*ang. TNA – Trusted Notary Archive*) przedstawił P. Routsalainen w [100]. TNA jest pojedynczą zaufaną organizacją, połączoną z urzędem znacznika czasu, która odbiera jednostkowe dane o zdrowiu z różnych systemów EHR. Przechowuje dane razem z powiązanymi metadanymi w długim okresie i dystrybuuje dane o zdrowiu. TNA komunikuje się z systemami EHR (patrz Rys. 2.11) i użytkownikami zewnętrznymi za pomocą wiadomości żądania i dystrybucji. TNA może przechowywać obiekty w formacie XML i istnieje możliwość udowodnienia niezaprzeczalność i integralność przechowywanych danych za pomocą struktur dowodowych, znaczników czasu i archiwalnych podpisów cyfrowych. Przedstawiony model TNA ma tą zaletę, że tylko klucze używane przez TNA muszą być przechowywane przez okres składowania dokumentów medycznych.



Rysunek 2.11: Współpracujące TNA i systemy EHR (źródło: P. Routsalainen [100])

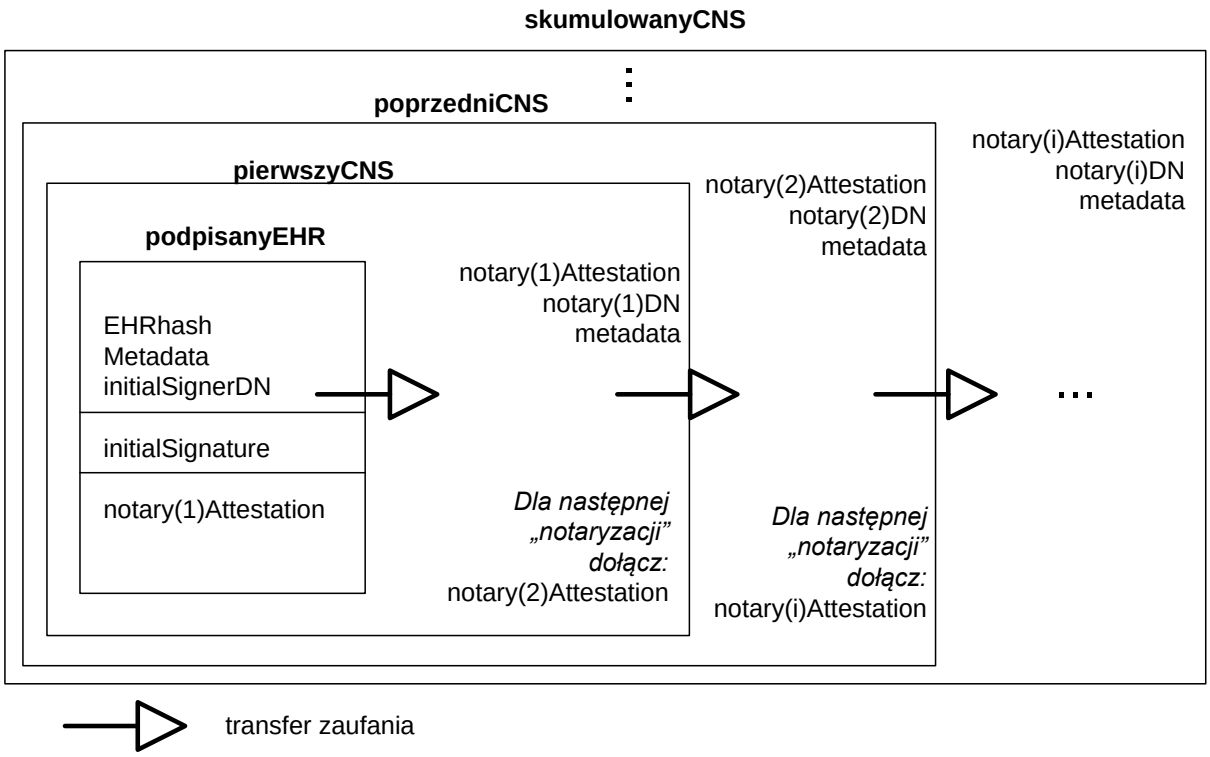
Archiwum notarialne jest zaufaną organizacją dostarczającą usługi długoterminowego przechowywania rekordów zdrowotnych i usługi zapewniające niezaprzeczalność oryginalnych danych. TNA zbiera dowody, tworzy struktury dowodowe, tworzy i odnawia znaczniki czasu, podpisuje dokumenty, tworzy logi audytu. TNA zbiera obiekty posiadające taki sam kod identyfikacyjny i przechowuje je w pojedynczym wirtualnym folderze pacjenta. TNA służy jako centralny, logiczny punkt przechowywania dokumentów, do którego mają zaufanie użytkownicy systemów EHR należących do poszczególnych przedsiębiorstw ochrony zdrowia.

2.6.7 Schemat skumulowanego notariatu

W modelu skumulowanego notariatu [77] podpisany cyfrowo EHR musi być regularnie weryfikowany przez zaufaną jednostkę zwaną przez autorów notariuszem. Notariusz atestuje ważność EHR, podpisuje go i odświeża siłę początkowego podpisu cyfrowego. Strona sprawdzająca (musi ufać notariuszowi) powinna sprawdzić tylko ostatni podpis notariusza. Taka procedura może być powtarzana okresowo i wykonywana w nieskończoność. W następnym okresie nowy notariusz musi sprawdzić tylko atestację złożoną przez poprzedniego notariusza, bez sprawdzenia początkowego podpisu i stworzyć kolejną atestację. Taki schemat kulminacyjnego notariatu może być powtarzany w nieskończoność.

Przedstawiona idea zakłada, że weryfikowalność EHR jest sukcesywnie przenoszona w kierunku nowych zaufanych notariuszy (patrz Rys. 2.12). Ponowną atestację może złożyć też ten sam notariusz. W przyszłości, strona weryfikująca musi ufać tylko ostatniemu notariuszowi, przez co wyeliminowana jest zależność od starych i słabych technologii algorytmicznych oraz od niedziałających czy nieobecnych urzędów notarialnych. Schemat nie wymaga bezpiecznego systemu archiwum. Tokeny stworzone przez notariusza są

podpisanymi strukturami danych, odpornymi na zamiany i mogą być przechowywane na osobistym nośniku lub w centralnym katalogu czy archiwum.

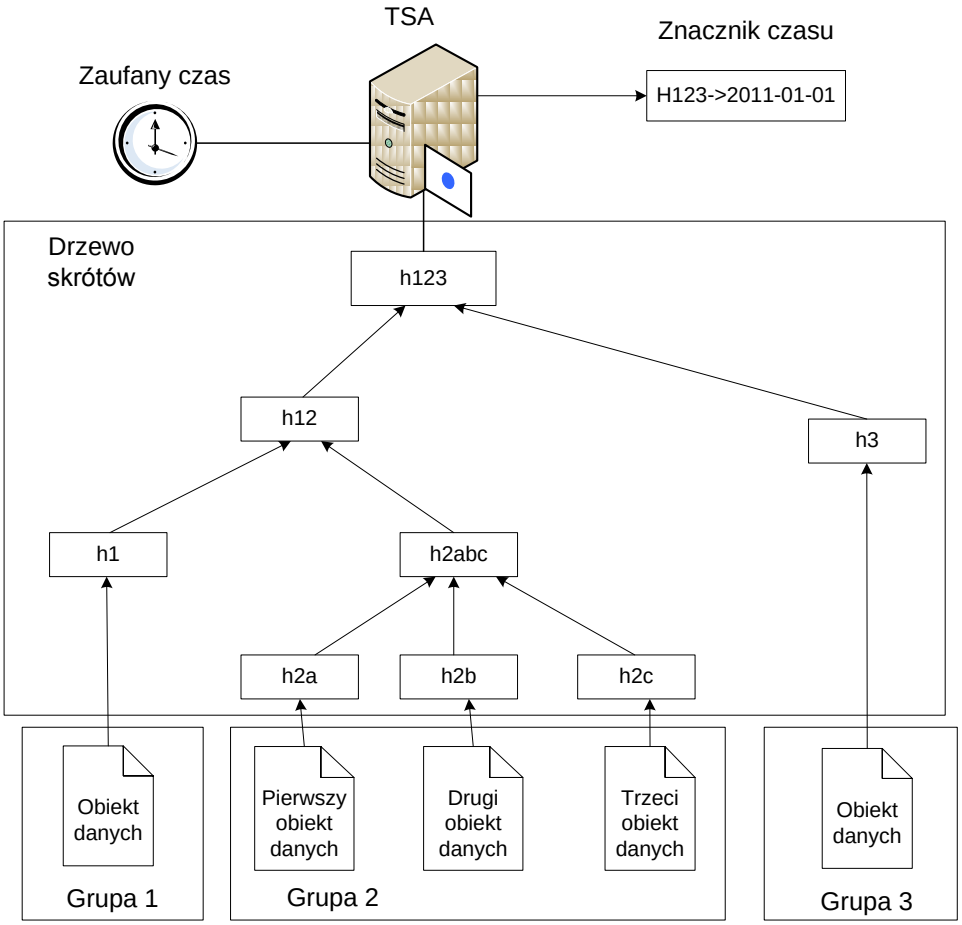


Rysunek 2.12: Kolejne enkapsulacje podpisu i skumulowana notaryzacja (źródło: [77])

2.6.8 Specyfikacja składni rekordów dowodowych

Specyfikacja składni rekordów dowodowych (*ang. ERS – Evidence Record Syntax*) zamieszona w RFC 4998 [50] i w [17] opisuje strukturę do przechowywania rekordów poświadczeń, czyli danych koniecznych do udowodnienia istnienia danych i metod do ich przetwarzania. Według ERS obiekt danych musi być oznakowany czasem najpóźniej przed upływem ważności jego podpisu cyfrowego. Rekordy poświadczeń zawierające archiwalne znaczniki czasu mogą być przechowywane w osobnym pliku lub mogą być zintegrowane jako np. atrybuty.

Archiwalny znacznik czasu tworzy się dla wielu dokumentów za jednym razem (w tym grup powiązanych dokumentów jak i dokumentów pojedynczych) z użyciem drzewa skrótów Merkle'a [83]. Obiekty danych (dokumenty) stanowią liście drzewa skrótów. Po obliczeniu korzenia drzewa, obliczany jest dla niego przez TSA zaufany znacznik czasu jak na Rys. 2.13. Dla każdego z obiektów danych zapisywane jest zredukowane drzewo skrótów. Użycie drzewa skrótów zmniejsza znacząco liczbę koniecznych do wykonania znaczników czasu oraz umożliwia udowodnienie istnienia grupy dokumentów w danym momencie czasu.



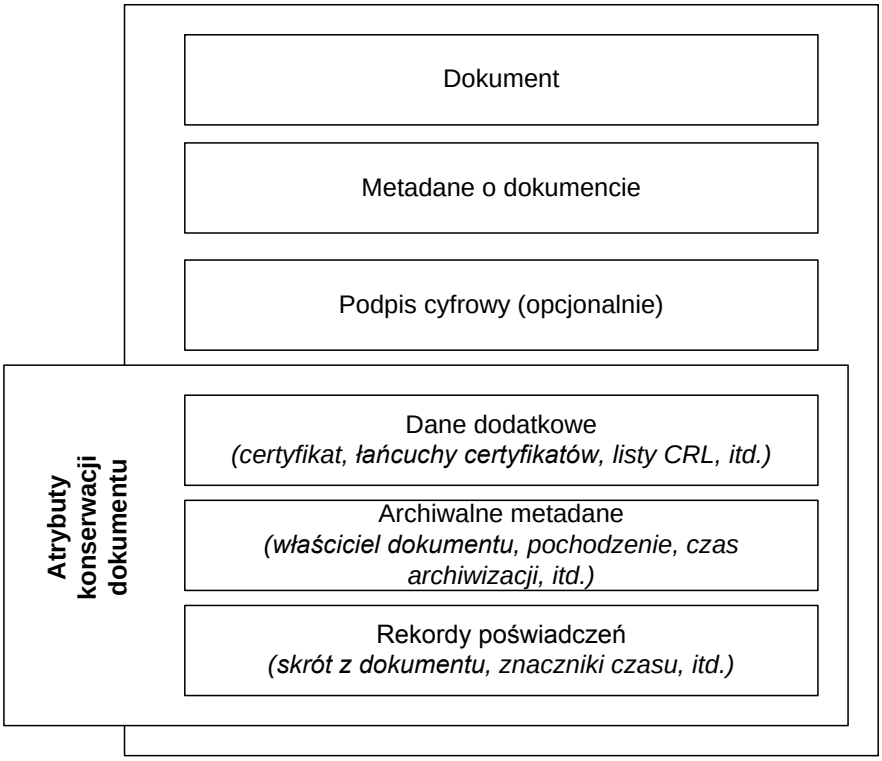
Rysunek 2.13: Generowanie znacznika czasu (źródło: [50])

Ponieważ ważność znacznika czasu tj. podpisu cyfrowego kończy się zazwyczaj po 2 latach, ERS przewiduje dwie procedury do odświeżania ważności archiwalnego znacznika czasu: *TimeStamp Renewal* and *Hash-tree Renewal*. Procedura *TimeStamp Renewal* jest uruchamiana wtedy, gdy aktualnie używany algorytm kryptograficznej funkcji skrótu jest nadal uważany za bezpieczny. W tej procedurze tworzony jest znacznik czasu obejmujący poprzedni znacznik czasu. Procedura *Hash-tree Renewal* jest uruchamiana, gdy zachodzi konieczność zmiany algorytmu funkcji skrótu i wymaga dostępu do źródłowych, z których tworzone jest jeszcze raz drzewo skrótów, którego korzeń jest łączony ze skrótem z poprzedniego znacznika czasu. Tak otrzymany skrót znakuje się czasem w celu otrzymania aktualnego archiwalnego znacznika czasu. Aby zapewnić redundancję w przypadku utraty zaufania do TSA, bądź przełamania funkcji skrótu, zaleca się tworzenia dwóch zestawów rekordów dowodowych z użyciem różnych TSA i funkcji skrótu.

2.6.9 Zaufana usługa archiwizowania

Usługa długoterminowa zaufanego archiwum (*ang. TAS – long-term Trusted Archive Service*) została zaprezentowana w [16]. TAS jest usługą zapewniającą dowód integralności i ważności oraz usług certyfikatowych dla danych archiwalnych. TAS traktuje dane jako ciąg danych i nie wnika do ich zawartości. Zarchiwizowane dane i powiązane z nimi informacje

nazywane są obiektami archiwalnymi, które są skonstruowane z trzech podstawowych elementów (patrz Rys. 2.14): z danych zarchiwizowanych, z metadanych powiązanych z danymi archiwizowanymi i z informacji dowodowej demonstrującej integralność i istnienie w określonym momencie czasu.



Rysunek 2.14: Struktura obiektu archiwalnego (źródło: [16])

Architektura TAS zawiera kilka podstawowych elementów. Do interakcji z usługą używany jest protokół LTAP (*ang. Long-Term Archive Protocol)*, który jest opisany przez typy i strukturę wiadomości wymienianych pomiędzy użytkownikiem a TAS. Kolejnym elementem jest moduł zarządzania danymi, który zapewnia mechanizmy związane z fizycznym przechowywaniem danych. Kolejnym modułem jest moduł służący do generowania i zarządzania rekordami dowodowymi. TAS zawiera także moduły interpretacji i weryfikacji danych.

Informacje dowodowe są generowane przez TAS lub pobierane z wspierających usług (np. znacznika czasu) na żądanie TAS przy użyciu specyfikacji Evidence Record Syntax. Po stworzeniu, obiekt archiwalny podlega ciągłemu konserwowaniu w celu utrzymania integralności i zapewnienia istnienia w określonym momencie czasu.

2.7. Podsumowanie

2.7.1 EHR a pozostałe rodzaje dokumentów

Elektroniczny dokument zdrowotny (EHR) jest dokumentem wirtualnym tworzonym na żądanie i w zależności od potrzeb składa się ze wszystkich lub wybranych rzeczywistych dokumentów zdrowotnych należących do jednego pacjenta. EHR jest dokumentem wirtualnym w sensie przechowywania, gdyż jest tworzony w locie na podstawie żądania i dostarczany do użytkownika jako pojedynczy dokument złożony z dokumentów składowych (plik XML w przypadku HL7 CDA2). Cała idea opiera się na utworzeniu jednego punktu dostępowego do dokumentacji medycznej. Poszczególne dokumenty wchodzące w skład EHR mogą znajdować się w rejestrach/repozytoriach różnych organizacji zajmujących się świadczeniem usług ochrony zdrowia (przychodni, szpitali, laboratoriów, itd.). Struktura EHR jest dobrze określona przez obecne standardy (m. in. ISO13606, OpenEHR).

Ogólnokrajowe systemy EHR przetwarzają dane wszystkich obywateli państwa co daje dziesiątki, setki milionów przetwarzanych EHR, a to przekłada się na miliardy dokumentów zdrowotnych. Duża liczba przetwarzanych danych wymusza dużą złożoność systemów EHR.

Systemy EHR w porównaniu do systemów przetwarzających inne dokumenty np. finansowe, wyróżniają się dużą złożonością, większym zakładanym okresem przechowywania, większą ilością podmiotów mających dostęp do systemu (lekarze, pacjenci, pracownicy ochrony zdrowia), a także dużą wrażliwością danych w przypadku ujawniania. Obecnie poza EHR nie ma określonych wirtualnych dokumentów o podobnej strukturze, funkcjonalności i złożoności.

2.7.2 Porównanie prac pokrewnych

W Tab. 2.2 zebrano metody przedstawione w niniejszym rozdziale wraz z ich właściwościami. Wszystkie istniejące metody pozwalają przedłużać ważność podpisów cyfrowych zawartych w pojedynczych dokumentach lub grupach dokumentów. Jednakże tylko kilka zapewnia niezaprzeczalności każdej z wielu grup podpisanych dokumentów w określonym momencie czasu (inaczej mówiąc, można wykryć czy wszystkie dokumenty z grupy są obecne i oryginalne oraz żaden nie został dodany do grupy w późniejszym czasie). Natomiast żadna z metod nie zapewnia niezaprzeczalności dla wielu grup dokumentów dodawanych przez długi okres, np. wielu EHR należących do wielu pacjentów, do których dodawane są dokumenty przez cały okres ich życia. Dla każdego EHR powinna istnieć możliwość sprawdzenia jego kompletności. Jedynie SLW, SHS i SBM umożliwiałyby zapewnienie takiej funkcjonalności, gdyby dla każdego EHR zastosować osobno schemat. Takie rozwiązanie spowodowałby, że w praktyce należałoby po każdym dodanym dokumencie składowym publikować wartość skrótu, co byłoby trudne do zrealizowania w praktyce i w automatycznej weryfikacji.

Kilka metod zostało opracowanych na potrzeby dokumentów medycznych. Jednakże brakuje kompleksowej metody traktującej EHR jako wirtualny kontener (tj. w ISO/IEC

13606). Analizowane metody nie są przystosowane do współpracy z dokumentami przechowywanymi w repozytoriach, których metadane są umieszczane w rejestrach. Brakuje takiej cechy w istniejących metodach, która umożliwi sprawdzenie autentyczność wpisów z metadanymi przechowywanymi w rejestrach, które zawierają informacje o dokumentach medycznych wchodzących w skład EHR.

Wszystkie metody umożliwiają weryfikację przez zewnętrznego arbitra oraz zapewnieją niezaprzeczalności dokumentu przez długi okres czasu. Zaufanie do tworzonych poświadczeń wywodzi się z zaufania do TTP (XADES, ERS/TAS, Metody P. Pharow i B. Blobel, Schemat skumulowanego notariatu) lub z wiary, że nie można sfalsyfikować wszystkich wartości skrótów opublikowanych, na przykład w codziennej gazecie (SLW, SHS, SBM). Model zaufanego archiwalnego notariatu wymaga ponadto, aby archiwum było TTP, co dla dużych systemów tj. systemy EHR jest dużo bardziej kosztowne niż umieszczenie archiwum w strefie niezaufanej i wywodzenie zaufania z zaufania do TTP.

Tabela 2.2: Porównanie dostępnych metod/rozwiązań (źródło: opracowanie własne)

Lp.	Właściwość \ Metoda	XADES-A	Schemat liniowego wiązania poświadczeń (SLW)	Evidence Record syntax (ERS) / TAS	Schemat Haber-Stornneta (SHS)	Schemat Benaloh de Mare (SBM)	Metody P. Pharow i B. Blobel	Model zaufanego archiwalnego notariatu	Schemat skumulowanego notariatu
1	Zapewnia niezaprzeczalność podpisanego dokumentu w długim okresie.	+	+	+	+	+	+	+	+
2	Zapewnia integralność, autentyczność podpisanego dokumentu.	+	+	+	+	+	+	+	+
3	Zapewnia niezaprzeczalność każdej z wielu grupy podpisanych dokumentów w określonym momencie czasu.	-	-	+	+	+	+	-	-
4	Zapewnia niezaprzeczalność każdej z wielu grup dokumentów dodawanych przez długi okres.	-	+-	-	+-	+-	-	-	-

5	Uwzględnia długi okres przechowywania, tj. 100 lat i więcej.	+	+	+	+	+	+	+	+
6	Weryfikacja przez zewnętrznego arbitra.	+	+	+	+	+	+	+	+
7	Wymaga współpracy z TTP.	+	-	+	-	-	+	-	+
8	Wymaga aby archiwum było TTP	-	-	-	-	-	-	+	-
9	Wymaga upubliczniania wartości na koniec rundy.	-	+	-	+	+	-	-	-
10	Zaprojektowana do dokumentów medycznych		-	-	-	-	+	+	+
11	Zaprojektowana do EHR o strukturze zdefiniowanej wg normy ISO/IEC 13606 – traktującej EHR jako wirtualny kontener	-	-	-	-	-	-	-	-
12	Uwzględnia składowanie danych w rejestrach/repozytoriach	-	-	-	-	-	-	-	-

Istnieje zapotrzebowanie na opracowanie metody, która uwzględnia strukturę EHR określoną w normie ISO/IEC 13606, a także uwzględnia składowanie danych i metadanych w rejestrach i repozytoriach, które należą do wielu organizacji ochrony zdrowia, które mogą się znajdować pod różnymi jurysdykcjami prawnymi. Opracowana metoda powinna powiększyć obecny stan wiedzy o rozwiązania umożliwiające zapewnienie autentyczności i niezaprzeczalności wielu grup dokumentów (wielu EHR) podczas długoterminowego przechowywania.

3. Metoda Długookresowego Przechowywania Elektronicznych Dokumentów Zdrowotnych

3.1. Wstęp

Celem metody Długookresowego Przechowywania Elektronicznych Dokumentów Zdrowotnych (DPEDZ) jest zapewnienie autentyczności oraz niezaprzeczalności EHR w długim okresie. Dokumenty zdrowotne są dodawane do EHR danego pacjenta przez specjalistów ds. ochrony zdrowia przez całe jego życie. Dokument wraz z metadanymi jest na początku sprawdzany pod kątem prawidłowości podpisu cyfrowego, a następnie umieszczany w odpowiednich rejestrach i repozytoriach.

Metadane dotyczące każdego dokumentu są zbierane i gdy ich ilość osiągnie określoną wartość *n* lub upłynie okres *t* (zakończy się runda) to następuje aktualizacja Rekordów Poświadczeń Rejestrów (RPR). Rekordy Poświadczeń Rejestrów są strukturą, w której przechowywane są poświadczenia. Każdy pacjent posiada oddzielne RPR. W danej rundzie metadane mogą pochodzić od jednego lub więcej pacjentów. Podczas dodawania nowych rekordów do RPR tworzone są wiązania liniowe pomiędzy kolejnymi rekordami w RPR, a także wykorzystywane są binarne drzewa skrótów Merkle'a, które umożliwiają zredukowanie liczby znaczników czasu do jednego na rundę.

Ponieważ czas trwania rundy może być długi, np. jeden dzień to dla każdego odebranego dokumentu tworzony jest token potwierdzający nadanie dokumentu. Sprawdzenie tokenu po zakończeniu rundy umożliwia potwierdzenie, że operacja aktualizacji RPR została wykonana prawidłowo.

Rekordy Poświadczeń Rejestrów są sprawdzane co *n* dni pod kątem ważności ostatniego znacznika czasu. RPR, których ważność ostatniego znacznika czasu jest bliska końcowi, poddawane są operacji ponownego znakowania czasem z użyciem drzewa skrótów, tak aby zminimalizować wymaganą ilość znaczników czasu. Ponieważ aktualizacja RPR przedłuża także ich ważność (ważność ostatniego znacznika czasu), działanie to nie jest wykonywane w przypadku, gdy dla każdego pacjenta przynajmniej raz na okres ważności znacznika czasu dodawany jest dokument. Działania, które aktualizują i przedłużają ważność RPR, konserwują również podpisy cyfrowe zawarte w dokumentach umieszczonych w repozytorium.

W sytuacji, w której dokumenty składające się na EHR danego pacjenta są przechowywane w wielu stowarzyszonych systemach EHR, każde żądanie weryfikacji autentyczności lub niezaprzeczalności EHR wymusza podejmowanie działania polegającego na scaleniu wszystkich części RPR odpowiadających częściom EHR przechowywanym w danych systemach. Algorytmy umożliwiające sprawdzenie autentyczności EHR, oraz niezaprzeczalności EHR, bądź pojedynczego dokumentu wchodzącego w jego skład, sprawdzają kolejno powiązania pomiędzy metadanymi oraz poprawność kolejnych znaczników czasu.

3.2. Działania składowe

Metoda DPEDZ składa się z następujących działań składowych mających na celu zapewnienie autentyczności wpisów w rejestrach i niezaprzeczalności pochodzenia i odbioru EHR oraz możliwość ich weryfikacji w długim okresie, wynoszącym nawet 100 i więcej lat:

1. Dodanie dokumentu wraz z metadanymi do systemu EHR (nowego wpisu z metadanymi do rejestru, dokumentu do repozytorium) – działanie wykonywane każdorazowo podczas utworzenia nowego dokumentu przez specjalistę ds. ochrony zdrowia. Działanie jest realizowane przez **Protokół Dodawania Nowych Wpisów (PDNW)**.
2. Utworzenie tokenu poświadczenia nadania – działanie wykonywane po zakończeniu działania nr 1. Działanie jest realizowane przez **Algorytm Tworzenia Tokenów Potwierdzenia Nadania (ATTPN)**.
3. Utworzenie poświadczeń – działanie wykonywane raz na rundę (każdorazowo gdy działanie 1 zostanie wykonane *n* razy lub upłynie określony okres czasu *t*). Działanie jest realizowane przez **Algorytm Aktualizacji Rekordów Poświadczeń Rejestrów (AARPR)**.
4. Aktualizacja poświadczeń – działanie wykonywane raz na określony okres czasu *t*. Działanie jest realizowane przez **Algorytm Przedłużania Wartości Archiwalnych Znaczników Czasu (APWATS)**.
5. Zweryfikowanie tokenu poświadczenia nadania – działanie wykonywane po ukończeniu działania 3. Działanie jest realizowane przez **Algorytm Weryfikacji Tokenu Potwierdzenia Nadania (AWTPN)**.
6. Scalenie poświadczeń – działanie realizowane na żądanie mające na celu zebranie poświadczeń z wielu systemów EHR. Działanie jest realizowane przez **Protokół Scalania Rekordów Poświadczeń Rejestrów (PSRPR)**.
7. Zweryfikowanie autentyczności zbioru metadanych z rejestrów, tj. zbioru wpisów z metadanymi dotyczącymi jednego pacjenta – działanie realizowane na żądanie użytkownika podczas każdego pobrania ekstraktu EHR. Działanie jest realizowane przez **Algorytm Weryfikacji Autentyczności Rejestrów (AWAR)**.
8. Zweryfikowanie niezaprzeczalności EHR lub ekstraktu EHR – działanie realizowane na żądanie użytkownika. Działanie jest realizowane przez **Algorytm Weryfikacji Niezaprzeczalności EHR (AWNEHR)**.
9. Zweryfikowanie niezaprzeczalności pojedynczego dokumentu wchodzącego w skład EHR pacjenta – działanie realizowane na żądanie użytkownika. Działanie jest realizowane przez **Algorytm Weryfikacji Niezaprzeczalności Dokumentu (AWND)**.

Metoda podczas działania wykorzystuje strukturę poświadczeń – Rekordy Poświadczeń Rejestrów (RPR), będącą słownikiem uwierzytelnianym oraz Centrum Informacji Długoterminowej (CID) świadczące dodatkowe usługi PKI. Zaufanie do działania

metody DPEDZ wynika z zaufania do Zaufanej Trzeciej Strony (TTP), m. in. z zaufanych znaczników czasu wystawianych przez urząd znacznika czasu (TSA).

W niniejszym rozdziale na początku przedstawiono ogólną architekturę systemu EHR (rozdz. 3.3) oraz Rekordy Poświadczeń Rejestrów (rozdz. 3.5). Następnie została omówiona szczegółowo metoda DPEDZ wraz z wchodzącymi w jej skład działaniami (rozdz. 3.6). Później zostało przedstawione Centrum Informacji Długoterminowej (rozdz. 3.7). Rozdział kończy się porównaniem (rozdz. 3.8) z pracami pokrewnymi przedstawionymi w rozdz. 2 oraz podsumowaniem (rozdz. 3.9).

Pierwsze idee działania algorytmów AARPR i AWAR, AWD zostały opublikowane przez autora niniejszej rozprawy w [63] oraz w [61]. Protokoły PDNW oraz PSRPR zostały również opublikowane w [60].

3.3. Ogólna architektura systemu EHR

3.3.1 Źródła dokumentów zdrowotnych

Dokumenty medyczne, które są umieszczane w EHR pacjenta, pochodzą od lekarzy rodzinnych, z laboratoriów medycznych, od lekarzy specjalistów, ze szpitali, a także z każdego innego miejsca, gdzie świadczone są usługi ochrony zdrowia. Przykładowo podczas leczenia zwykłej alergii, pacjent z symptomami zgłasza się do lekarza rodzinnego (informacja o spotkaniu z lekarzem rodzinnym jest przesyłana do EHR). Następnie pacjent odwiedza alergologa, wykonując wcześniej wymagane badania krwi (laboratorium umieszcza badania krwi w EHR pacjenta). Alergolog dokonuje dalszych badań, diagnozuje chorobę pacjenta i wystawia receptę (rezultaty testów, diagnoza i recepty są wysyłane do EHR). Nawet prosty proces leczenia pacjenta wymaga pracy wielu specjalistów, którzy umieszczają dokumenty w EHR. Specjaliści ds. ochrony zdrowia mogą pracować w różnych organizacjach świadczących usługi zdrowotne, które mogą znajdować się w różnych regionach, a nawet państwach, które mogą być pod inną jurysdykcją prawną.

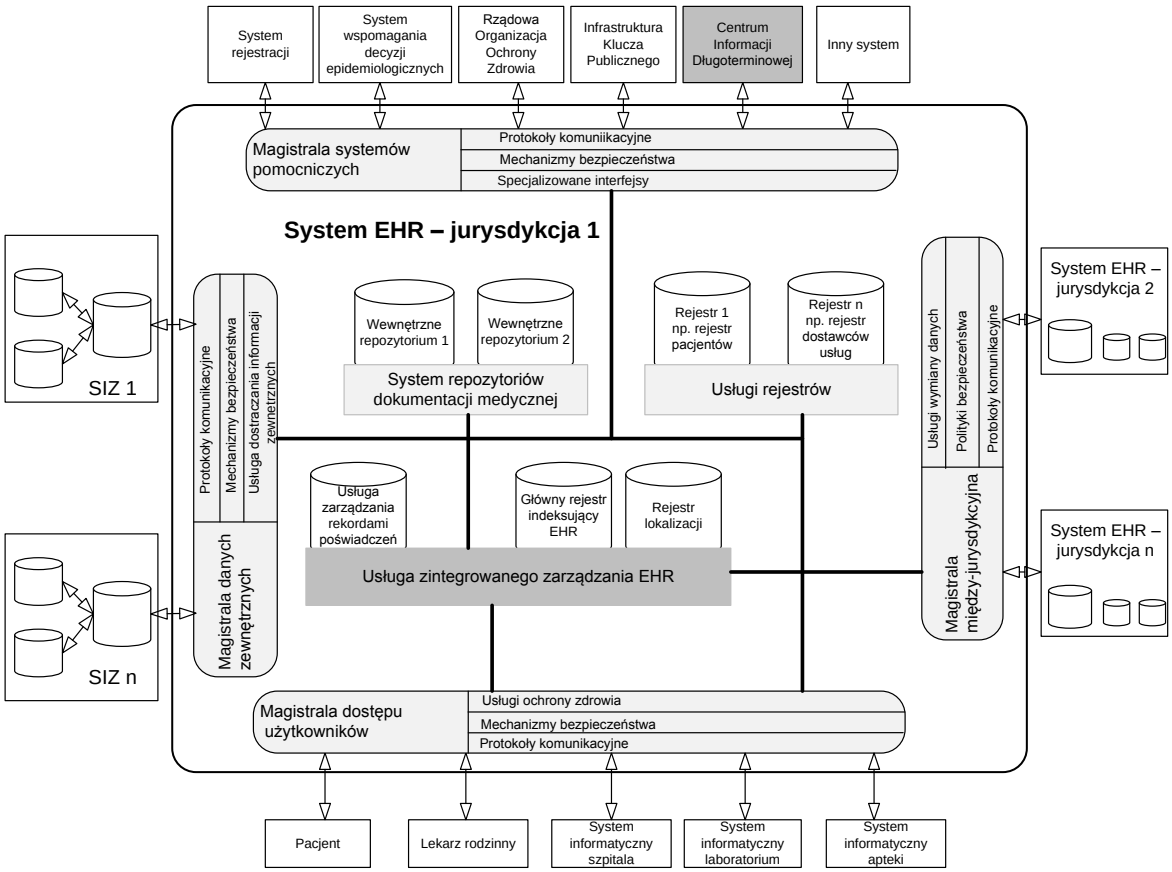
3.3.2 Architektura systemu EHR

Proponowaną ogólną architekturę między-jurysdykcyjnego systemu EHR przedstawia Rys. 3.1 (architektura ta została przedstawiona przez autora rozprawy w artykule [62]). Pracownicy ochrony zdrowia i pacjenci mogą połączyć się z systemem z wykorzystaniem Magistrali dostępu użytkowników. Wewnętrzna struktura systemu jest ukryta przed użytkownikami. Usługa Zintegrowanego Zarządzania (UZZ) EHR agreguje informacje na temat EHR'ów wszystkich pacjentów i jest w stanie dostarczyć w odpowiedzi na zapytanie obecną zawartość EHR lub taką, która była utworzona w dowolnym przeszłym punkcie czasu. UZZ zawiera Główny rejestr indeksujący EHR, w którym znajdują się odnośniki do dokumentów w repozytoriach i rejestrach, a także zawiera informacje na temat dokumentów pacjenta przechowywanych w innych systemach EHR.

Dokumenty zdrowotne zawarte w EHR mogą być przechowywane w:

- wewnętrznych repozytoriach i rejestrach systemu – dokumenty wraz z metadanymi są przechowywane wewnątrz systemu EHR;
- repozytoriach zewnętrznych – dokumenty są przechowywane w lokalnym systemie informatycznym szpitala i tylko metadane są rejestrowane w Głównym rejestrze indeksującym; Magistrala danych zewnętrznych wraz z usługą dostawcy pośredniczy pomiędzy systemem EHR a lokalnym systemem informatycznym szpitala;
- w stowarzyszonych systemach EHR; rejestr lokalizacji zawiera informacje, czy dane pacjenta znajdują się w stowarzyszonym systemie EHR; magistrala między-jurysdykcyjna pośredniczy pomiędzy systemami EHR.

Magistrala systemów pomocniczych pośredniczy pomiędzy systemem EHR i systemami bezpośrednio lub pośrednio biorącymi udział w procesie ochrony zdrowia np.: systemami rejestracji wizyt, systemami wspomagania decyzji epidemiologicznych, czy systemami Infrastruktury Klucza Publicznego w celu wspierania mechanizmów kryptograficznych, m.in. podpisów cyfrowych. Każdy z systemów jest podłączany przez specjalizowany interfejs.



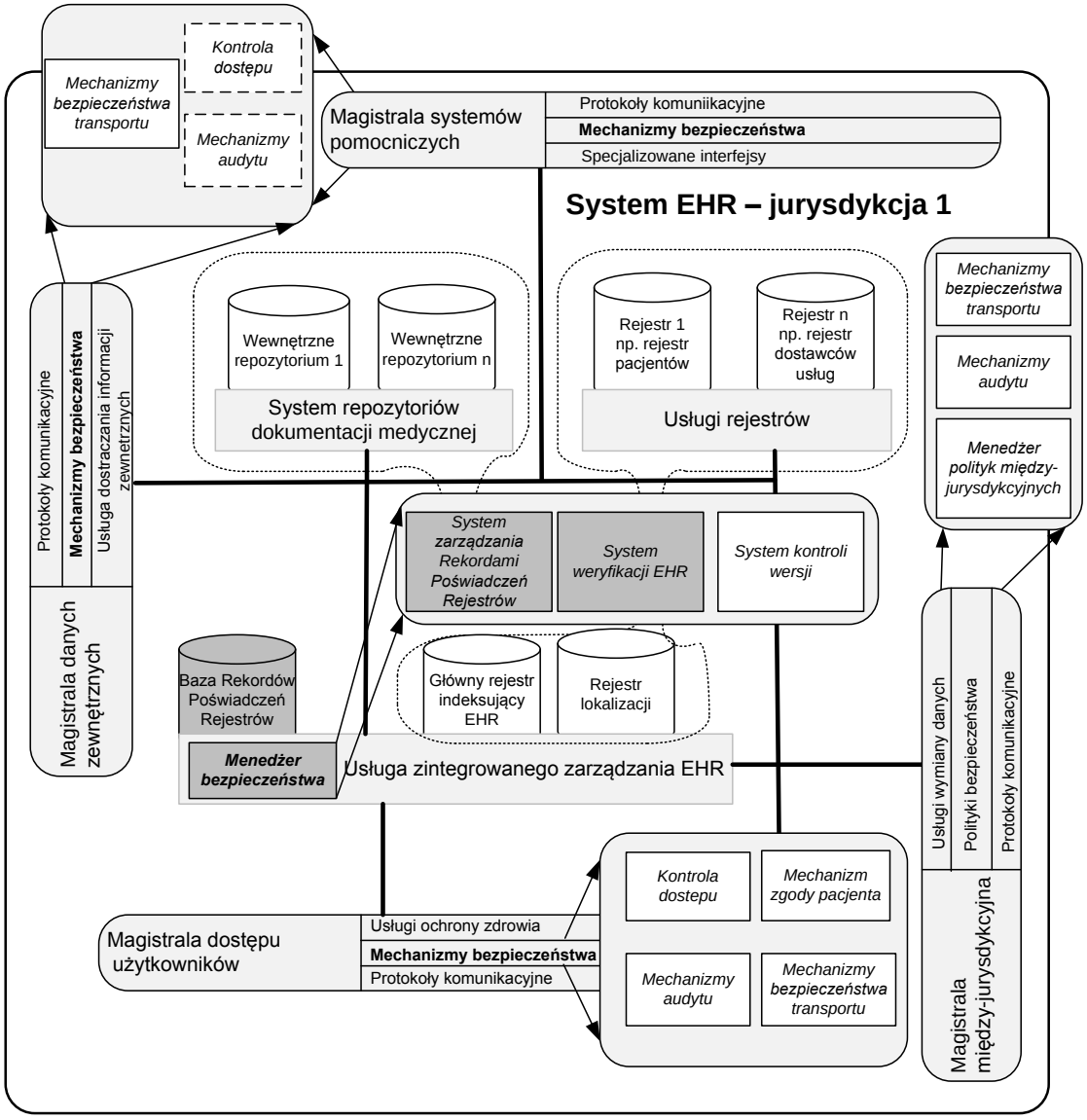
Rysunek 3.1: Ogólna architektura systemu EHR (źródło: [62])

3.3.3 Środki zabezpieczeń

Środki zabezpieczeń użyte w systemie EHR mogą być podzielone na wiele oddzielnych mechanizmów. Rys. 3.2 przedstawia proponowane mechanizmy bezpieczeństwa. Cała komunikacja z systemem odbywa się przez odpowiednie magistrale posiadające wbudowane środki bezpieczeństwa. Wszystkie magistrale posiadają mechanizmy audytu, bezpiecznego transportu i kontroli dostępu. Magistrala dostępu użytkowników posiada również wbudowany mechanizm zgody, który jest odpowiedzialny za zarządzanie zgodą pacjenta na udostępnianie całości lub części EHR. Magistrala między-jurysdykcyjna posiada również wbudowany mechanizm menedżera polityk między-jurysdykcyjnych, który jest odpowiedzialny za zarządzanie problemami bezpieczeństwa związanymi z wymianą rekordów pomiędzy różnymi systemami w tej samej lub w innych jurysdykcjach prawnych. Usługa zintegrowanego zarządzania EHR zawiera Menedżer Bezpieczeństwa, który zawiera System zarządzania Rekordami Poświadczeń Rejestrów, System Weryfikacji EHR oraz System Kontroli Wersji.

System kontroli dostępu jest połączony z mechanizmem zgody. System ten jest też odpowiedzialny za awaryjny dostęp do EHR pacjenta (w przypadkach nagłych, gdy pacjent jest nieprzytomny, a wymagany jest dostęp do jego EHR). Poufność jest zapewniona poprzez te systemy. Mechanizm audytu przechowuje informacje o dostępie do EHR. Poza potrzebą sprawdzenia kto i kiedy do czego miał dostęp, czasami istnieje potrzeba sprawdzenia, czy ktoś nie spojrzał do EHR pacjenta w czasie procesu leczenia. Bezpieczne połączenie sieciowe do zewnętrznych źródeł danych i do innych systemów EHR jest zapewnione przez mechanizmy bezpieczeństwa transportu.

Dokumenty kliniczne umieszczone w EHR są podpisywane cyfrowo, aby zapewnić ich integralność, autentyczność i niezaprzeczalność. System zarządzania Rekordami Poświadczeń Rejestrów (RPR) jest odpowiedzialny za utrzymywanie ważności podpisów cyfrowych i zapewnienie autentyczności oraz niezaprzeczalności pochodzenia i odbioru EHR, jak i jego składowych. System weryfikacji EHR umożliwia weryfikację EHR w oparciu o RPR w dowolnym momencie podczas długookresowego przechowywania. Umożliwia to stwierdzenie, czy jakikolwiek dokument został dodany, zmieniony lub skasowany z EHR. Menedżer wersji zbiera informacje o wersji dokumentów i może przywrócić widok EHR z każdego poprzedniego punktu w czasie (dokumenty nigdy nie są usuwane – zgodnie z wymaganiami ISO TS18308). Jest także odpowiedzialny za powiadomienia lekarzy w przypadku, którzy widzieli nieprawidłową wersję dokumentu klinicznego.



Rysunek 3.2: Środki zabezpieczeń w architekturze systemu EHR (źródło: [62])

Poszczególne działania wchodzące w skład metody DPEDZ mogą zostać zaimplementowane wewnątrz komponentów systemu. Działanie te przedstawiono w Tab. 3.1.

Tabela 3.1: Implementacja działań metody w komponentach systemu (źródło: opracowanie własne)

Kod komponentu	**Nazwa komponentu**	**Nr działania**	**Realizacja działania**
MB	Menedżer Bezpieczeństwa	1	PDNW
		6	PSRPR
SZRPR	System zarządzania RPR	2	ATTPN
		3	AARPR
		4	APWATS
SWRPR	System weryfikacji EHR	5	AWTPN
		7	AWAR
		8	AWNEHR
		9	AWND

Wykorzystywane przez metodę Rekordy Poświadczeń Rejestrów są przechowywane w Bazie Rekordów Poświadczeń (BRPR). System EHR zbudowany z wykorzystaniem metody DPEDZ odzwierciedla obecne trendy w budowaniu systemów informatycznych zarządzających EHR. EHR może znajdować się w jednym systemie EHR lub w wielu stowarzyszonych systemach EHR. System wykorzystujący metodę może współpracować z obecnie istniejącymi standardami dotyczącymi struktury EHR, tj. CEN/ISO 13606, IHE XDS, HL7 CDA2.

System EHR zbudowany w oparciu o metodę DPEDZ służy również do konserwowania okresu ważności podpisanych dokumentów znajdujących się w repozytoriach. Ważność podpisów cyfrowych jest zapewniana podczas przeprowadzania operacji umożliwiających stwierdzenie niezaprzeczalności dokumentów składowych. Natomiast Centrum Informacji Długoterminowej (CID) rozwiązuje problem dostępu do informacji o statusie usług infrastruktury klucza publicznego w przeszłości jak i statusie algorytmów kryptograficznych.

3.4. Zależności pomiędzy implementacjami algorytmów w systemie EHR

Menedżer Bezpieczeństwa (MB) zawiera System Zarządzania Rekordami Poświadczeń Rejestrów (SZRPR), System Weryfikacji EHR (SWEHR) oraz Bazę Rekordów Poświadczeń Rejestrów (BRPR). SZRPR jest odpowiedzialny za aktualizację RPR oraz długoterminowe utrzymywanie ich ważności. SWEHR zawiera natomiast implementacje algorytmów koniecznych do weryfikacji autentyczności oraz niezaprzeczalność EHR jak i również poszczególnych dokumentów składowych.

Powiązania pomiędzy oprogramowaniem implementującym protokoły i algorytmy zawartymi w MB, SZRPR i w SWEHR przedstawia Rys. 3.3, gdzie oznaczenie *Algorytm x* lub *Protokół x* oznacza oprogramowanie implementujące *Algorytm x* lub *Protokół x*. Podczas dodawania nowych wpisów do rejestrów (para dokument D_i, metadane M_i) używany jest Protokół Dodawania Nowych Wpisów (PDNW, opis działania patrz rozdz. 3.5.1). Po zakończeniu tego protokołu wpis M_i uzupełniony o URI zostaje umieszczony w rejestrze (z wpisów w rejestrach można wygenerować ZM) oraz D_i zostaje umieszczony w repozytorium. M_i jest przekazywane do oprogramowania implementującego Algorytm Tworzenia Tokenów Poświadczenia Nadania (ATTPN, opis działania patrz rozdz. 3.5.2) oraz Algorytmu Aktualizacji RPR (AARPR, opis działania patrz rozdz. 3.5.3).

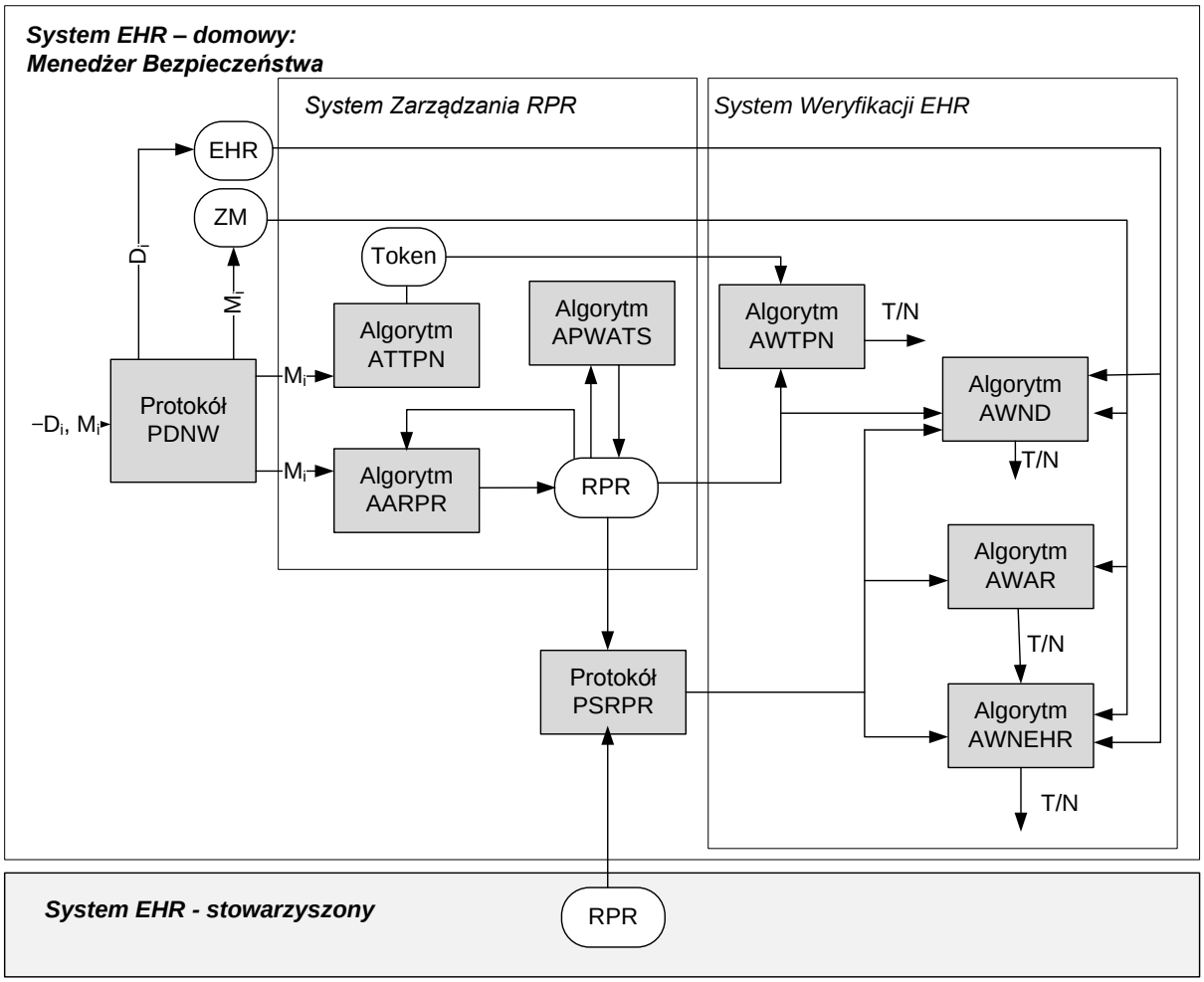
ATTPN służy do tworzenia znaczników poświadczenia nadania. Natomiast AARPR zbiera wszystkie M_i z jednej rundy (długość rundy określona jest przez interwał czasu lub przez liczbę przychodzących M_i) i aktualizuje lub tworzy nowy RPR dla każdego EHR do którego został dodany nowy dokument. W długim okresie do utrzymywania ważności RPR używane jest oprogramowanie implementujące Algorytm Przedłużania Ważności archiwalnych znaczników czasu (APWATS, opis działania patrz rozdz. 3.5.4).

Menedżer Bezpieczeństwa zawiera implementację Protokołu Scalania RPR (PSRPR, opis działania patrz rozdz. 3.5.5), który służy do scalania RPR z systemów stowarzyszonych EHR i z systemu domowego w jeden plik.

System Weryfikacji EHR zawiera oprogramowanie implementujące Algorytm Weryfikacji Autentyczności Rejestrów (AWAR, opis działania patrz rozdz. 3.5.7) umożliwiający sprawdzenie autentyczności zbioru wpisów zawierających metadane opisujące EHR należące do jednego pacjenta (na wejściu: ZM i RPR; na wyjściu: wynik weryfikacji). Oprogramowanie jest uruchamiane za każdym razem, gdy aplikacja specjalisty ds. ochrony zdrowia pobiera ekstrakt EHR stworzony na podstawie zapytania do rejestru. Celem jest sprawdzenie czy wszystkie dokumenty, z których jest zbudowany ekstrakt EHR, zostały w nim umieszone. W Systemie Weryfikacji EHR jest również zaimplementowany Algorytm Weryfikacji Niezaprzeczalności EHR (AWNEHR, opis działania patrz rozdz. 3.5.8) służący do weryfikacji niezaprzeczalności pochodzenia i odbioru EHR (na wejściu: ZM, EHR, wynik działania AWAR; na wyjściu: wynik weryfikacji).

Dodatkowo, gdy zachodzi konieczność weryfikacji niezaprzeczalności pochodzenia i odbioru pojedynczego dokumentu wchodzącego w skład EHR, uruchamiane jest oprogramowanie implementujące Algorytm Weryfikacji Niezaprzeczalności Dokumentu

(AWND, opis działania patrz rozdz. 3.5.9) (na wejściu: D_i, ZM->M_i, RPR; na wyjściu: wynik weryfikacji). Oprogramowanie zawierające Algorytm Weryfikacji Tokenów Poświadczenia Nadania (AWTPN, opis działania patrz rozdz. 3.5.6) służy do weryfikacji poprawności obliczenia rundy (na wejściu: Token, RPR, na wyjściu: wynik weryfikacji). Algorytmy weryfikacji są również dostępne dla zewnętrznego arbitra.

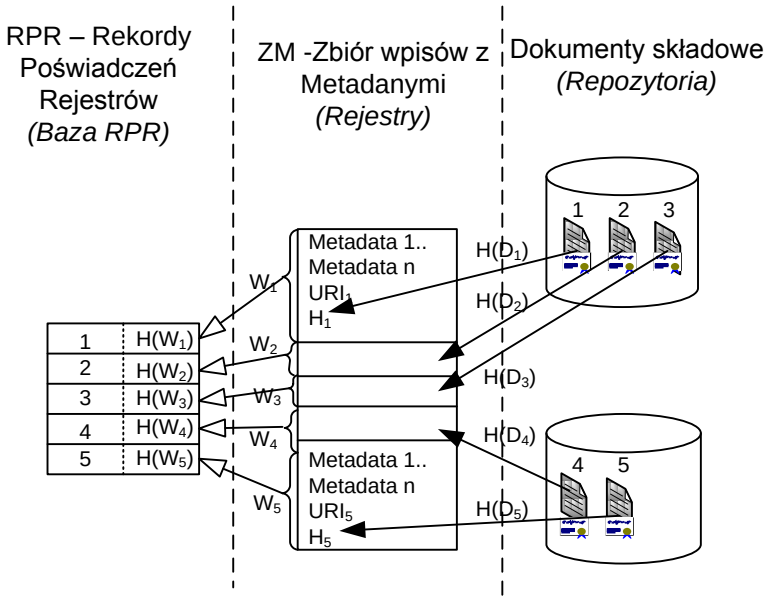


Rysunek 3.3: Powiązania pomiędzy oprogramowaniem implementującym algorytmy (źródło: opracowanie własne)

3.5. Rekordy Poświadczeń Rejestrów

3.5.1 Warianty użycia Rekordów Poświadczeń Rejestrów

Elektroniczny Dokument Zdrowotny (EHR) jest wirtualnym kontenerem na dokumenty medyczne należące do jednego pacjenta. W praktyce do przechowywania EHR używa się rejestrów i repozytoriów. Przesyłane dokumenty umieszcza się w repozytoriach, a opisujące je metadane w rejestrach. Rejestry umożliwiają wyszukiwanie odpowiednich części EHR, a także wygenerowanie na żądanie użytkownika ekstraktu EHR zawierającego całość lub część EHR. Dodatkowo dany pacjent może posiadać EHR w systemie działającym w jego miejscu zamieszkania (systemie domowym) oraz kilku/kilkunastu systemach działających w innych regionach/państwach (systemach stowarzyszonych).

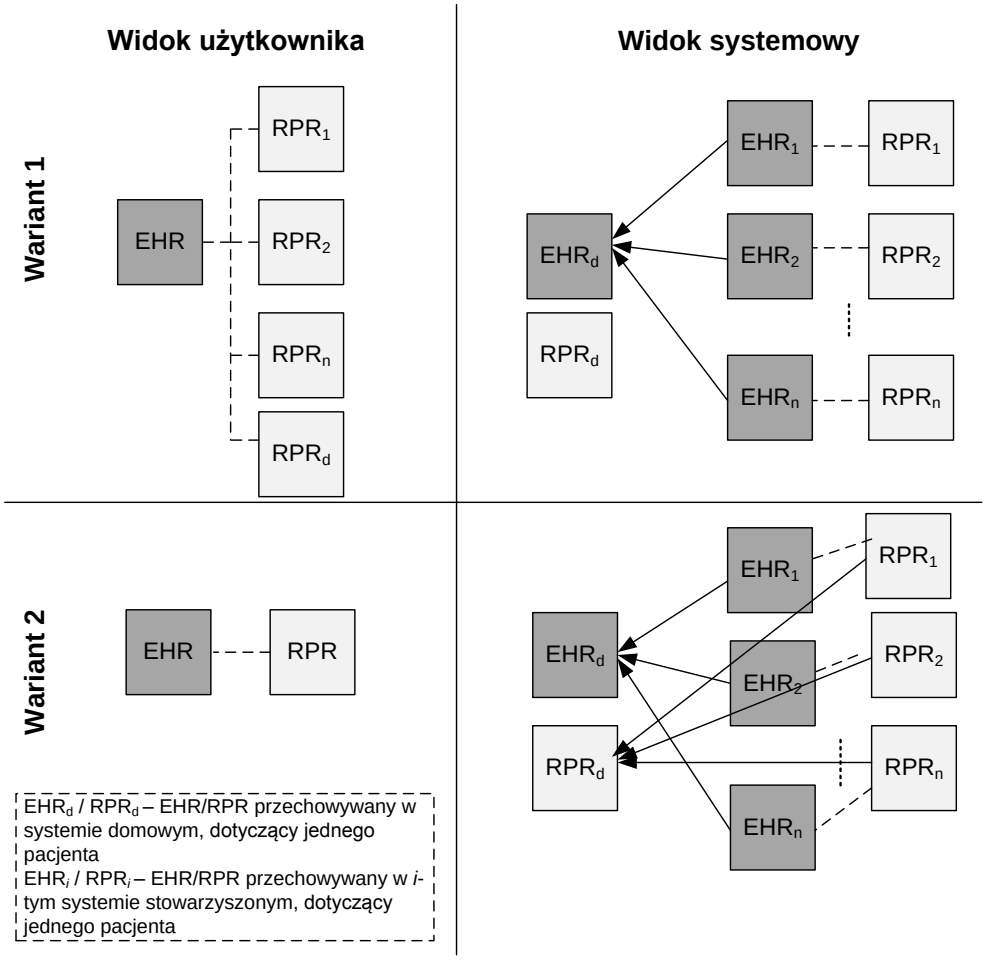


Rysunek 3.4: Relacje pomiędzy RPR, ZM a dokumentami w repozytoriach (źródło: opracowanie własne)

W systemie EHR dane dotyczące EHR znajdują się w kilku miejscach (patrz Rys. 3.4). Dokumenty składowe EHR są umieszczone w repozytoriach. Każdy wpis w rejestrze zawiera metadane opisujące konkretny podpisany dokument w repozytorium. W skład metadanych wchodzi informacja o lokalizacji (URI) oraz skrót z podpisanego dokumentu. W bazie RPR przechowywane są RPR. Jeden RPR zawiera poświadczenia dla jednego EHR, a w nich identyfikator dokumentu i skrót z wpisu z metadanymi

Z punktu widzenia użytkownika (patrz Rys. 3.5) EHR zawsze jest widziany jako całość, niezależnie od wewnętrznej struktury systemu jak, również liczby podłączonych systemów. Natomiast RPR mogą być zaprojektowane według dwóch wariantów. Pierwszy wariant zakłada, że każdy system tworzy osobny RPR dla części EHR zawartych w tym systemie. Innymi słowy, wariant zakłada, że wystarczy zapewnić autentyczność EHR w poszczególnych systemach a wtedy zapewniona będzie autentyczność całego EHR. Drugi wariant zakłada konieczność powiązania RPR z systemów stowarzyszonych z RPR z systemu domowego, aby zapewnić autentyczność EHR rozproszonego na kilka systemów EHR. W

tym wariancie wszystkie dokumenty składowe ze wszystkich systemów są ze sobą powiązane.



Rysunek 3.5: Warianty zastosowania RPR (źródło: opracowanie własne)

Podstawową zaletą wariantu drugiego w porównaniu do wariantu pierwszego jest zwiększenie bezpieczeństwa. W przypadku utraty informacji w rejestrze lokalizacji (trzymającym informacje o systemach stowarzyszonych, które posiadają informacje o danym EHR) lub utraty wszystkich danych w stowarzyszonym systemie EHR, istnieje poświadczenie pozwalające wykryć braki w dokumentach z innych systemów. Natomiast wadą wariantu drugiego w porównaniu do wariantu pierwszego jest: konieczność dodatkowej transmisji danych pomiędzy systemami EHR w przypadku dodawania dokumentu do systemu stowarzyszonego; nieznacznie zwiększony rozmiar RPR systemu domowego; zwiększona liczba operacji podczas weryfikacji autentyczności EHR.

Struktura RPR umożliwia realizację obu wariantów. Z punktu widzenia użytkownika docelowe warianty zakładają dostarczenie w celach weryfikacji trzech podstawowych elementów: RPR dotyczących konkretnego EHR, ZM zawierającego zbiór wpisów z metadanymi oraz EHR złożonego z dokumentów składowych.

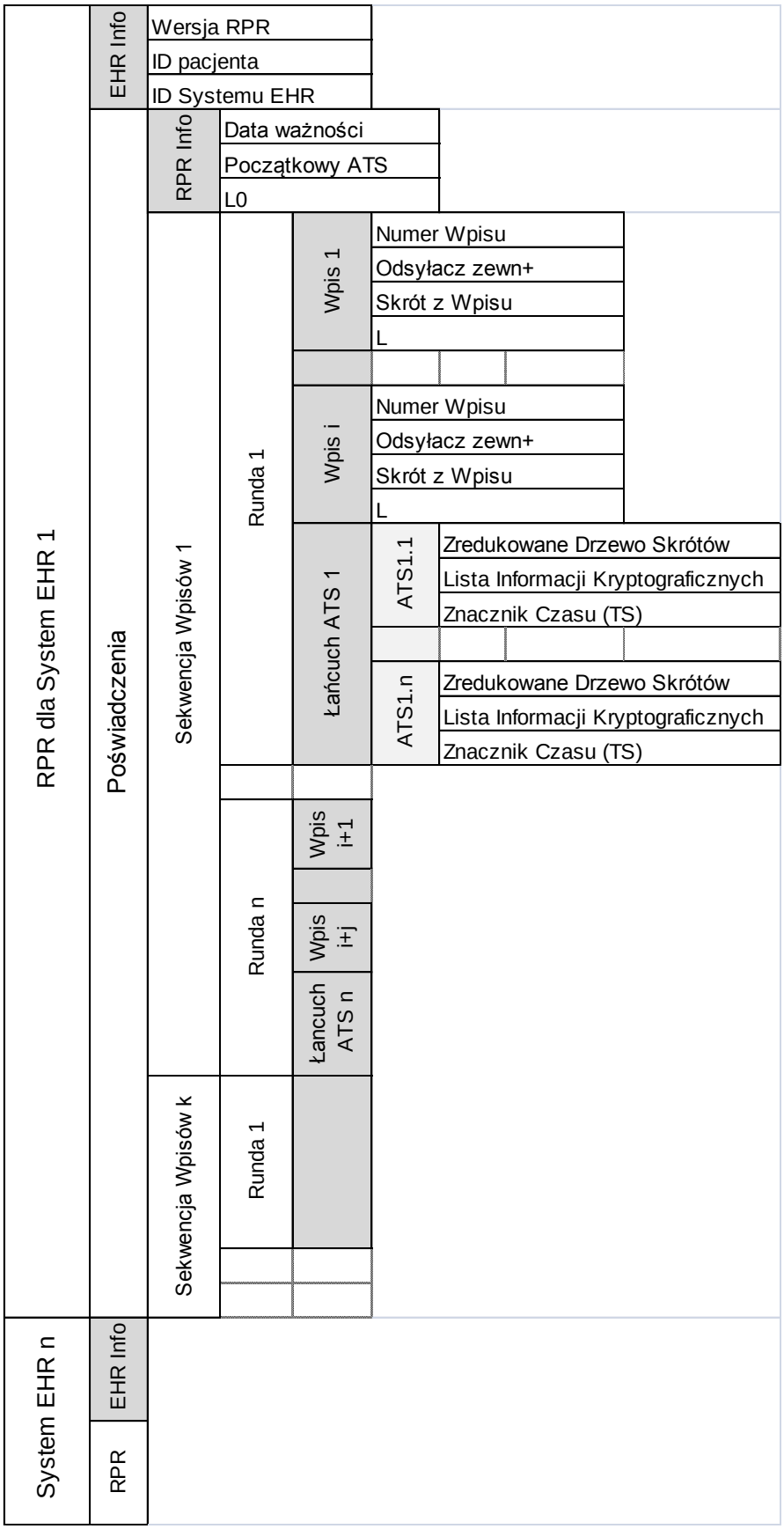
3.5.2 Struktura Rekordów Poświadczeń Rejestrów

Rekordy Poświadczeń Rejestrów (RPR) umożliwiają weryfikację niezaprzeczalności EHR w przypadku, gdy EHR jest rozproszony pomiędzy wiele systemów EHR lub znajduje się w jednym systemie EHR. Jeżeli EHR danego pacjenta jest rozproszony na wiele systemów EHR (w każdym systemie pacjent ma osobny EHR) to za pomocą RPR można zapewnić niezaprzeczalność EHR w każdym z systemów osobno. Jednakże, aby spełnić definicję EHR która zakłada, że w skład EHR wchodzą wszystkie dokumenty należące do danego pacjenta RPR umożliwiają powiązanie RPR z różnych systemów. RPR przedłużają również ważność podpisów cyfrowych zawartych w dokumentach medycznych wchodzących w skład EHR. Dla każdego EHR, każdy system EHR przechowuje osobny RPR. Jednakże w przypadku żądania przez użytkownika zewnętrznego, RPR są agregowane w jeden RPR zawierający niepowiązane lub powiązane RPR.

Struktura RPR bazuje częściowo na specyfikacji XML Evidence Record Syntax [17]. Logiczna struktura RPR jest zaprezentowana na Rys. 3.6. RPR jest podzielony pomiędzy systemy EHR. RPR dla systemu EHR zawiera nagłówek *EHR info,* na który składa się informacja o wersji oraz *Poświadczenia*. *Poświadczenia* zawierają nagłówek z datą ważności (datę wraz z którą upływa ważność ostatniego znacznika czasu), początkowy ATS (Archiwalny Znacznik Czasu generowany podczas tworzenia RPR, używany jako wartość początkowa do mechanizmu wiązań liniowych) oraz L0, która również jest losową wartość inicjalizacyjną.

Następnie w skład poświadczeń wchodzi *Sekwencja Wpisów*, która jest tworzona, gdy zmieniony jest zestaw używanych algorytmów kryptograficznych. W skład *Sekwencji Wpisów* wchodzą *Rundy*. Jedna *Runda* odpowiada wpisom do rejestrów dodanym podczas jednej rundy działania algorytmu AARPR. *Runda* zawiera jeden lub więcej *Wpisów* oraz *Łańcuch Archiwalnych Znaczników Czasu* (*Łańcuch ATS*). W skład *Łańcucha ATS* wchodzą Archiwalne Znaczniki Czasu (ATS). Natomiast w skład ATS wchodzi *Zredukowane Drzewo Skrótów*, *Lista Informacji Kryptograficznych* (certyfikaty, listy CRL i inne pomocne przy weryfikacji znaczników czasu) oraz *Znacznik Czasu*.

Element *Wpis* zawiera kolejny numer, skrót z wpisu w rejestrze którego dotyczy oraz opcjonalny odsyłacz zewnętrzny. W przypadku, gdy RPR są powiązane, odsyłacz zewnętrzny pokazuje, że dany *Wpis* nie dotyczy wpisu w rejestrze, a zawiera wartość wiążącą do innego systemu. Odsyłacze zewnętrzne są umieszczane tylko w systemie domowym EHR. W przypadku, gdy dokument jest dodawany w systemie stowarzyszonym, to po wykonaniu algorytmu AARPR w tym systemie, ostatnia wartość L jest przesyłana do systemu domowego, który umieszcza ją jako wpis z odsyłaczem zewnętrznym. Zamiast skrótu z wpisów w rejestrze wstawiana jest otrzymana wartość L, a odsyłacz zewnętrzny zawiera informacje o identyfikatorze systemu źródłowego.



Rysunek 3.6: Struktura Rekordów Poświadczeń Rejestrów (źródło: opracowanie własne)

3.6. Działania składowe metody DPEDZ

3.6.1 Dodawanie nowego dokumentu do systemu EHR

Protokół Dodawania Nowego Wpisu (PDNW), przedstawiony niżej, jest uruchamiany, gdy dokument zdrowotny jest dodawany do EHR danego pacjenta. Dokument może być dodany w domowym systemie EHR pacjenta lub stowarzyszonym systemie EHR. Dokumenty mogą być dodawane również przez rejestrowanie wpisów (metadanych o dokumentach w rejestrach) z podłączonych systemów szpitalnych. W przypadku dodawania dokumentu do systemu stowarzyszonego, RPR są aktualizowane w tym systemie i informacja o dodaniu dokumentu jest przesyłana do domowego systemu pacjenta. PDNW dla dodawania dokumentu do stowarzyszonego systemu EHR i dodawania wpisów w rejestrach jest następujący (patrz Rys. 3.7, objaśnienia skrótów patrz Słownik skrótów):

Protokół PDNW:

Początek: Dokument D_i wraz z M_i

Koniec: D_i , M_i umieszczone w systemie EHR

1. Specjalista ds. ochrony zdrowia wysyła nowy dokument D_i wraz z M_i dotyczące pacjenta P_{id_p} do UZZ_k w $EHRS_k$;

2. UZZ_k sprawdza poprawność M_i, oraz poprawność podpisu cyfrowego dołączonego do D_i:

   2.1. Sprawdź czy podpis cyfrowy jest poprawny pod względem matematycznym

   2.2. Sprawdź ścieżkę certyfikacji;

   2.3. Sprawdź listę TSL i LPAK.

   Następnie wysyła D_i wraz z M_i do Głównego Rejestru Indeksującego EHR oraz tworzy i wysyła wiadomość $W_{id_p}^k$ zawierająca informacje, że pacjent P_{id_p} posiada dokumenty zdrowotne w $EHRS_k$, na szynę między-jurysdykcyjną;

3. Używając magistrali między-jurysdykcyjnej, pośredniczącej pomiędzy systemami EHR, $W_{id_p}^k$ jest wysyłany do UZZ_d a następnie do Rejestru Lokalizacji w $EHRS_d$;

4. Główny Rejestr Indeksujący EHR wysyła D_i, M_i do rejestru R_n i dodaje informacje o docelowym rejestrze R_n do rekordów P_{id_p} ;

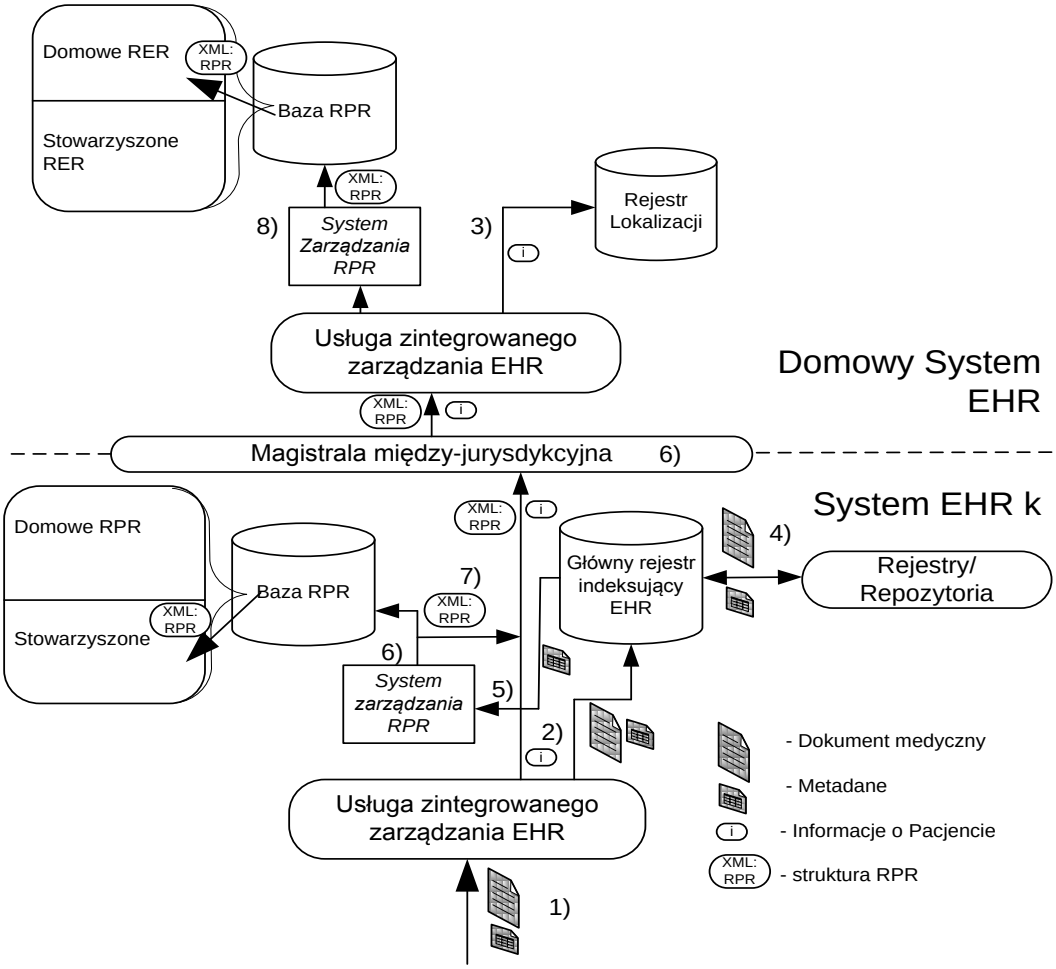
5. Główny Rejestr Indeksujący EHR modyfikuje M_i (poprzez ekstrakcję dodatkowych metadanych i wstawienie URI_i) i przez to tworzy M_i^k , które wysyła do $SZRPR_k$;

6. $SZRPR_k$ pobiera RPR_{id_p} z $BRPR_k$ z tabeli *Stowarzyszone EHR*, w przypadku, gdy nie istnieje – tworzy nowy; $SZRPR_k$ inicjuje algorytm AARPR, który ma za zadanie zaktualizować strukturę RPR_{id_p} używając przychodzących M_i;

7. (*po aktualizacji przez AARPR = po ukończeniu rundy*) $SZRPR_k$ wysyła zmodyfikowany RPR_{id_p} do $BRPR_k$ oraz tworzy $aRPR^k_{id_p}$, który wysyła na magistralę między-jurysdykcyjną; $aRPR^k_{id_p}$ zawiera P_{id_p}, ostatnią wartość L wyliczoną przez AARPR, numer dokumentu j i numer systemu EHR k;

8. Używając magistrali między-jurysdykcyjnej, pośredniczącej pomiędzy systemami EHR, $aRPR^k_{id_p}$ jest wysyłany do UZZ_d w $EHRS_d$;

9. UZZ_k wysyła $aRPR^k_{id_p}$ do $SZRPR_d$, który inicjuje algorytm AARPR, używając M_i, które tworzy z $aRPR^k_{id_p}$;



Rysunek 3.7: Dodawanie nowych wpisów (dokumentów) do EHR (źródło: [60])

W przypadku, gdy dokument jest dodawany do systemu domowego, to powyższy protokół jest uruchamiany bez kroków 6-8 oraz w krokach 2,5 bez wysyłania danych na szynę między-jurysdykcyjną. Również w kroku 5 tabela *Domowe RPR* używana jest zamiast tabeli *Stowarzyszone RPR*.

3.6.2 Utworzenie tokenu potwierdzenia nadania

Algorytm Tworzenia Tokenów Potwierdzenia Nadania (ATTPN), przedstawiony niżej, umożliwia wysłanie tokenu potwierdzającego nadanie dokumentu do systemu. W przypadku, gdy czas dodawania dokumentów do rundy jest długi, to jednostka wysyłająca dokument do Systemu EHR może zażądać tokenu potwierdzającego wysłanie dokumentu. Za pomocą tokenu można sprawdzić po ukończeniu rundy, czy runda została obliczona prawidłowo. Token jest wydawany natychmiast po otrzymaniu dokumentu.

Algorytm ATTPN:

Wejście: D_i , RPR_{id_p}

Wyjście: token TK^{id_p}

1. Weź $ATSCh_{rd-1}^{id_p}$ z poprzedniej rundy dla RPR_{id_p};
2. Dla *n* dodanych dokumentów D_i dla P_{id_p} :
   a. Oblicz $L_j^{id_p} = H\left(j \,|Hw_j^{id_p}\left|L_{j-1}^{id_p}\right.\right)$, gdzie *j* oznacza kolejny numer dokumentu w EHR pacjenta;
3. Wyślij token $TK^{id_p} = (ATSCh_{rd-1}^{id_p},\ L_j^{id_p},...,L_{j+n}^{id_p})$ do nadawcy dokumentów;

3.6.3 Utworzenie poświadczeń

Algorytm Aktualizacji Rekordów Poświadczeń Rejestrów (AARPR), przedstawiony na następnej stronie, aktualizuje RPR z użyciem rund. Informacje o wszystkich przychodzących dokumentach z działania 1 (z protokołu PDNW) są zbierane. Runda kończy się po upływie określonego czasu lub gdy zostanie dodane *n* dokumentów. Na wejściu do algorytmu jest zbiór wpisów z metadanymi lub $aRPR_{id_p}^k$ (wiadomość składająca się z ostatniej wartości *L*, numeru dokumentu *j* i numeru systemu EHR *k* służąca do powiązania wpisu z systemu stowarzyszonego z wpisami w systemie domowym). Na wyjściu są zmodyfikowane RPR lub nowe RPR, w przypadku gdy dla danego pacjenta został dodany pierwszy dokument do systemu EHR. Algorytm jest następujący:

Algorytm AARPR:

Wejście: M_i w liczbie *n, RPR'ów*

Wyjście: Zaktualizowane *RPR'ów*

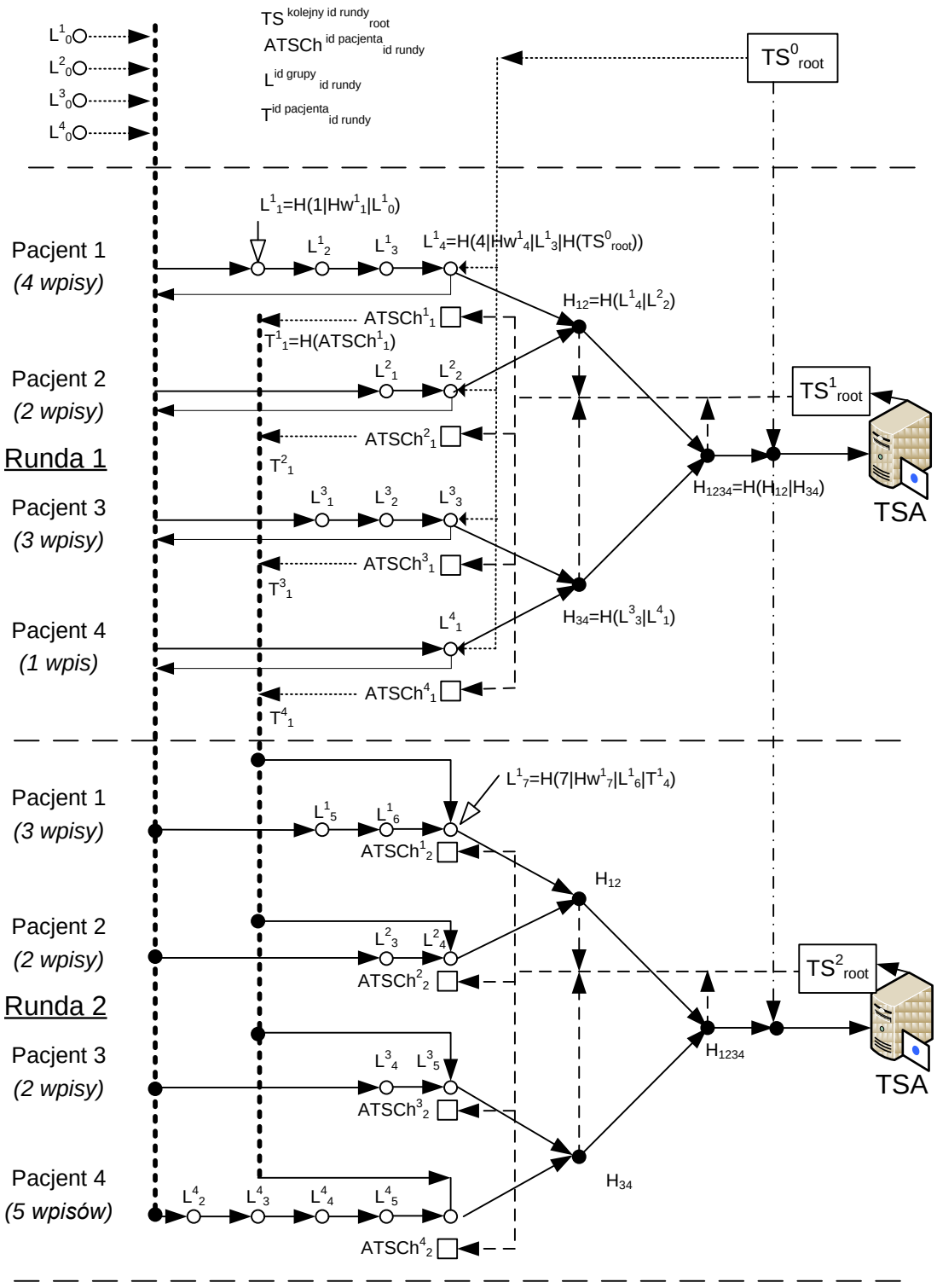
1. Podziel wszystkie M_i z obecnej rundy zgodnie z identyfikatorem pacjenta, $GM_{id_1} \cup \ldots \cup GM_{id_k} = M_n$, gdzie $\sum_{p=1}^{k} \left| GM_{id_p} \right| = n$.
2. Dla każdej GM_{id_p}, dla danej Sekwencji Wpisów SW_{id_p} =*null* oraz numeru rundy *rd=null* wykonaj:
   2.1. Pobierz *RPR* dla pacjenta z id_p (RPR_{id_p}) lub gdy nie istnieje, stwórz nowy;
   2.2. Przypisz SW_{id_p} ostatni element Sekwencja Wpisów z RPR_{id_p} i rd przypisz numer ostatniego elementu Runda R_{rd}.
   2.3. W RPR_{id_p} stwórz nowy element Runda o numerze R_{rd+1};
   2.4. Wewnątrz elementu R_{rd+1} utwórz element Wpis *W* dla każdego M_i z GM_{id_p}:
      2.4.1. Oblicz numer *W: j = j+1* (*j=1* dla pierwszego M_i w RPR_{id_p});
      2.4.2. Oblicz skrót $Hw_j^{id_p} = H(M_i)$, w przypadku gdy M_i zawiera dane z $aRPR_{id_p}^k$, to $Hw_j^{id_p} = M_i \text{->} L$;
      2.4.3. Jeżeli element W_j jest ostatni w R_{rd+1} i w kroku 2.1 został utworzony nowy RPR_{id_p} to oblicz $T_j^{id_p} = H\left(TS^0{}_{root}\right)$;
      2.4.4. W przeciwnym razie, gdy W_j jest ostatni w R_{rd+1} to $T_j^{id_p} = H\left(ATSCh_{rd}^{id_p}\right)$;
      2.4.5. W przeciwnym razie $T_j^{id_p} = null$;
      2.4.6. Oblicz $L_j^{id_p} = H\left(j \left| Hw_j^{id_i} \right| L_{j-1}^{id_p} \right| T_j^{id_p}\right)$.
3. Stwórz binarne drzewo skrótów używając ostatnich wartości $L_j^{id_p}$ dla każdego GM_{id_p} jako liści drzewa i oblicz korzeń drzewa H_{root}^{tn+1};
4. (*Opcjonalny*) Oblicz $T_{root}^{tn+1} = H\left(H_{root}^{tn+1} \middle| H\left(TS_{root}^{tn}\right)\right)$, ten opcjonalny krok łączy wartość skrótu korzenia drzewa H_{root}^{tn+1} z aktualnej rundy z wszystkimi poprzednimi znacznikami czasu.
5. Stwórz znacznik czasu TS_{root}^{tn+1} dla korzenia drzewa skrótów (wyślij żądanie do zaufanego urzędu znacznika czasu (TSA).
6. Dla każdego RPR_{id_p} stwórz zredukowane drzewo skrótów $RT_{tn+1}^{id_p}$:
   6.1. Przypisz *i* numer liścia (z poziomu *0*) odpowiadającemu RPR_{id_p};
   6.2. Dla poziomu drzewa *p =0* do *p=n* (*n* – liczba poziomów):
      6.2.1. Jeżeli *i%2==0* to wstaw do $RT_{tn+1}^{id_p}$ element *i+1* z *p* poziomu;
      6.2.2. Jeżeli *i%2==1* to wstaw do $RT_{tn+1}^{id_p}$ element *i-1* z *p* poziomu;
      6.2.3. *i=i/2*;

7. Dla każdego RPR_{id_p} w ostatnim elemencie Runda R stwórz łańcuch archiwalnych znaczników czasu $ATSCh_{rd+1}^{id_p}$ i wewnątrz jego element ATS; wewnątrz ATS zapisz zredukowane drzewo skrótów $RT_{tn+1}^{id_p}$ i znacznik czasu TS_{root}^{tn+1}.

Rozpatrzmy przykład działania algorytmu na podstawie Rys. 3.8 w celu zobrazowania jego działania. Przykład zawiera 2 rundy. W pierwszej rundzie dla pacjenta 1 zostały dodane cztery wpisy, dla pacjenta 2 – dwa, 3 – trzy, 4 – jeden. Na początku generowane są wartości inicjalizujące L^1_0, L^2_0, L^3_0, L^4_0 , gdzie indeks górny to identyfikator pacjenta a indeks dolny jest kolejnym numerem dokumentu w grupie. Następnie obliczany jest $L^1_1=H(1|Hw^1_1|L^1_0)$. L^1_2 i L^1_3 są obliczane za pomocą tej samej formuły. Wartość L^1_4 jest obliczana dla ostatniego elementu pacjenta 1 za pomocą formuły $L^1_4=H(4|Hw^1_4|L^1_3|H(TS^0_{root}))$. W ten sam sposób dokonywane są obliczenia dla pacjenta 2, 3 i 4.

Ostatnie wartości z każdej grupy wpisów (L^1_4, L^2_2, L^3_3, L^4_1) są wykorzystywane jako liście do budowy drzewa skrótów. Następnie budowane jest drzewo skrótów: $H_{12}=H(L^1_4|L^2_2)$, $H_{34}=H(L^3_3|L^4_1)$, $H^1_{root}=H_{1234}(H_{12}|H_{34})$, H^1_{root} jest połączone z poprzednim TS, tzn. $T^1_{root}=H(H^1_{root}|H(TS^0_{root}))$. T^1_{root} jest wysyłane do TSA z żądaniem wygenerowania znacznika czasu. Po otrzymaniu znacznika czasu TS^1_{root} dla każdego pacjenta generowane jest drzewo skrótów, np.: dla pacjenta 1 zredukowane drzewo to $(L^2_2, H_{34}, H(TS^0_{root}))$. Zredukowane drzewo skrótów wraz znacznikiem czasu zapisywane jako archiwalny znacznik czasu (ATS) wewnątrz łańcucha ATS – dla pacjenta 1 – $ATSCh^1_1$.

W rundzie drugiej do pacjenta 1 należą 3 dokumenty. Na początku obliczany jest $H(5|Hw^1_5|L^1_4)$, później $L^1_6= H(6|Hw^1_6|L^1_5)$ i na końcu $L^1_7= H(7|Hw^1_7|L^1_6|T^1_1)$, gdzie $T^1_1=H(ATSCh^1_1)$. Obliczenia dla pozostałych pacjentów są przeprowadzane w taki sam sposób. Po obliczeniu ostatniej wartość L dla każdej grupy wpisów pacjenta (L^1_7, L^2_4,L^3_5, L^4_6), obliczane jest drzewo skrótów. Korzeń drzewa skrótów połączony z poprzednim TS $T^2_{root}=H(H^2_{root}|H(TS^1_{root}))$ jest znakowany czasem przez zewnętrzną TSA i tak jak w poprzedniej rundzie, zredukowane drzewo skrótów wraz z znacznikiem czasu jest zapisywane dla każdego pacjenta, np. dla pacjenta 1 $ATSCh^1_2$.



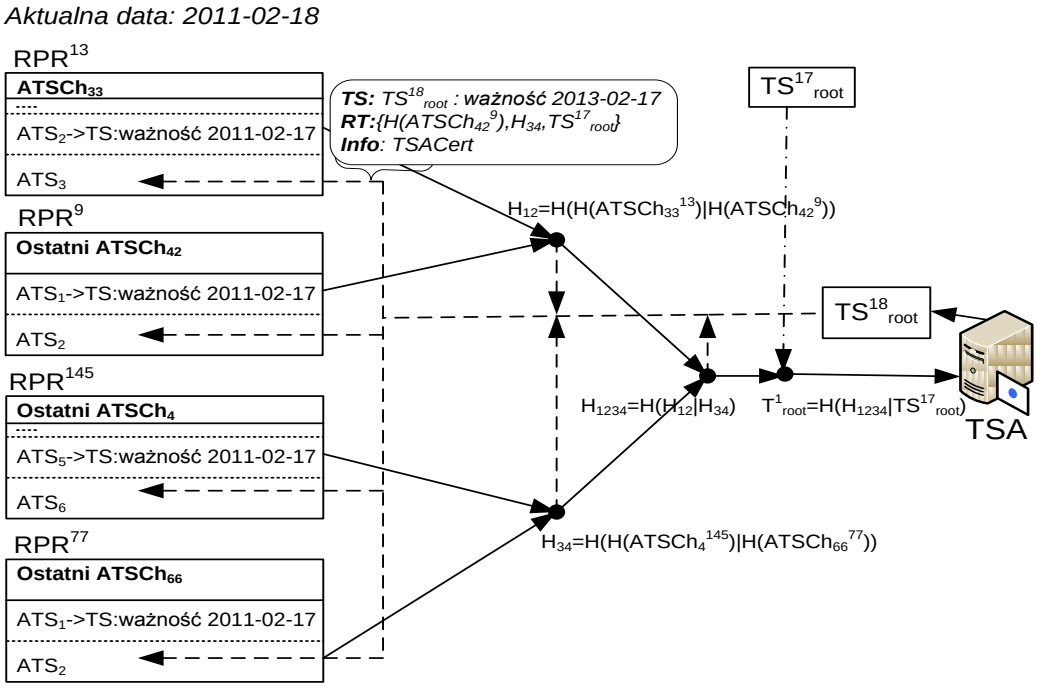
Rysunek 3.8: Przykład działania algorytmu AARPR (źródło: opracowanie własne)

3.6.4 Aktualizacja poświadczeń

Znaczniki czasu wymagają ponownego oznakowania czasem przed upływem ich okresu ważności (np. co dwa lata). Jednakże w strukturze RPR wiązania między dokumentami składającymi się na EHR powodują, że jeśli jeden dokument jest dodawany do EHR (czyli wpis do rejestrów) w okresie ważności ostatniego znacznika czasu, to wcześniejsze znaczniki czasu są automatycznie odnawiane i ponowne znakowania czasem nie jest wymagane.

Algorytm Przedłużania Ważności Archiwalnych Znaczników Czasu (APWATS), przedstawiony na następnej stronie, raz na rundę sprawdza ważność ostatniego znacznika czasu (ważność RPR). Jeżeli pozostały okres ważności jest mniejszy niż *n* dni, obliczany jest skrót z wszystkich poprzednich archiwalnych znaczników czasu (ATS) z ostatniego łańcucha ATS. Następnie wykorzystując obliczone skróty, tworzy się drzewo skrótów. Korzeń drzewa jest wiązany z poprzednim znacznikiem czasu i tak jest tworzony nowy znacznik czasu. Drzewo jest redukowane i zapisywane w każdym z przedłużanych RPR jako kolejny ATS w ostatnim łańcuchu ATS.

Rys. 3.9 zawiera przykład działania algorytmu w przypadku, gdy ostatnie znaczniki czasu z czterech RPR wymagają przedłużenia ważności. Na początku obliczane są skróty z ostatnich łańcuchów archiwalnych znaczników czasu z każdego RPR: $H(ATSCh_{33}^{13})$, $H(ATSCh_{42}^{9})$, $H(ATSCh_{4}^{145})$, $H(ATSCh_{66}^{77})$. Z tych wartości obliczane jest drzewo skrótów tj. H_{12}, H_{34} i H_{1234}. Korzeń drzewa jest wiązany z poprzednim znacznikiem czasu TS^{17}_{root}: $T^{1}_{root}=H(H_{1234}|TS^{17}_{root})$. Dla każdego RPR tworzone jest zredukowane drzewo skrótów, np. dla RPR^{13}: $H(ATSCh_{42}^{9})$, H_{34}, TS^{17}_{root}. Zredukowane drzewo skrótów wraz z otrzymanym znacznikiem czasu TS^{18}_{root} i certyfikatem TSA są zapisywane w kolejnym archiwalnym znaczniku czasu ATS_3 umieszczonym wewnątrz $ATSCh_{33}$.



Rysunek 3.9: Przykład działania algorytmu APWATS (źródło: opracowanie własne)

Algorytm APWATS działa w powyższy sposób tylko, gdy zestaw wykorzystywanych algorytmów kryptograficznych pozostaje ten sam. Kiedy zestaw algorytmów zostaje zmieniony, konieczne jest stworzenie nowego ATS, który obejmuje wszystkie stare znaczniki czasu, jak i również dokumenty. Algorytm wymaga ponownego dostępu do metadanych w rejestrach, a także do dokumentów źródłowych w repozytoriach. Procedura ta jest zawsze wymagana, gdy algorytm funkcji skrótu traci swoje właściwości bezpieczeństwa. W takim przypadku APWATS oblicza skrót L_p z poprzednich *Sekwencji Wpisów* z RPR. Następnie uruchamiany jest algorytm AARPR dla wszystkich wpisów w rejestrze z użyciem L_p jako L_0 i nowy element *Sekwencja Wpisów* jest tworzony i przechowywany wewnątrz właściwego RPR (patrz rozdz. 3.4.2). Algorytm wymaga dostępu do wszystkich dokumentów w repozytoriach.

Szczegółowy opis algorytmu APWATS jest następujący:

Algorytm APWATS:

Wejście: RPR'ów, których okres ważności jest mniejszy niż *n* dni.

Wyjście: Zaktualizowane RPR'ów.

1. Jeżeli zestaw algorytmów kryptograficznych pozostaje taki sam to:
   1.1. Dla każdego RPR_{id_p} sprawdź, czy okres ważności *t* jest mniejszy niż *n*:
      1.1.1. Jeżeli tak to dla RPR_{id_p}:
         1.1.1.1. Wyszukaj w RPR_{id_p} ostatni element Runda R_{rd};
         1.1.1.2. Oblicz skrót $H_p = H(ATSCh_{rd}^{id_p})$;
   1.2. Stwórz binarne drzewo skrótów używając wszystkich obliczonych wartości H_p jako liści drzewa i oblicz korzeń drzewa H_{root}^{tn}(*tn* to kolejny, globalny numer rundy, natomiast *rd* jest lokalnym, kolejnym numerem rundy w RPR_{id_p});
   1.3. *(Opcjonalny)* Oblicz $T_{root}^{tn} = H\left(H_{root}^{tn} \middle| H\left(TS_{root}^{tn-1}\right)\right)$, ten opcjonalny krok łączy wartość skrótu korzenia drzewa H_{root}^{tn} z aktualnej rundy z wszystkimi poprzednimi znacznikami czasu.
   1.4. Stwórz znacznik czasu dla korzenia drzewa skrótów (wyślij żądanie do zaufanego urzędu znacznika czasu) TS_{root}^{tn}.
   1.5. Dla każdego RPR_{id_p} stwórz zredukowane drzewo skrótów $RT_{tn}^{id_p}$ (patrz Algorytm 2, krok 6).
   1.6. Dla każdego RPR_{id_p} w ostatnim elemencie Runda *R* w $ATSCh_{rd}^{id_p}$ stwórz nowy ATS, a wewnątrz jego zapisz zredukowane drzewo skrótów $RT_{tn}^{id_p}$ i znacznik czasu TS_{root}^{tn}.
2. W przeciwnym przypadku:
   2.1. W takim przypadku dla każdego RPR_{id_p}:
      2.1.1. Dla każdego P_p wyślij do UZZ_d żądanie przysłania zaktualizowanych metadanych M_i zawierających nowe skróty z dokumentów w repozytoriach.
      2.1.2. Oblicz $L_0^{id_p} = H(SW_{id_p})$.

2.2. Uruchom algorytm AARPR z $GM_{id_1} \cup \ldots \cup GM_{id_k} = M_n$ i $L_0^{id_1} \cup \ldots \cup L_0^{id_p} = L_0$ na wejściu.

3.6.5 Weryfikacja tokenu potwierdzenia nadania

Algorytm Weryfikacji Tokenu Potwierdzenia Nadania (AWTPN), przedstawiony niżej, umożliwia weryfikację po zakończeniu rundy, czy została obliczona prawidłowo z wykorzystaniem tokenu potwierdzenia nadania jest następujący:

Algorytm AWTPN:

Wejście: TK^{id_p}, RPR_{id_p}

Wyjście: wynik weryfikacji – prawd/fałsz

1. Weryfikator posiada TK^{id_p}, RPR_{id_p};
2. Sprawdź ostatni $ATSCh_{rd}^{id_p}$ z RPR_{id_p}, jeżeli wynik jest negatywny, zwróć błąd;
3. Porównaj przedostatni $ATSCh_{rd-1}^{id_p}$ z RPR_{id_p} z $ATSCh_{rd-1}^{id_p}$ z TK^{id_p}, jeżeli wynik jest negatywny, zwróć błąd;
4. Porównaj wartości $L_j^{id_p},\ldots,L_{j+n}^{id_p}$ z odpowiadającymi i wartościami L z RPR_{id_p}, jeżeli wynik jest negatywny, zwróć błąd;
5. Dla W_j do W_n z RPR_{id_p} :
    a. Oblicz wartość $L_j^{id_p}$ (tj. w kroku 2.1.1.1 algorytmu AWAR) i porównaj z wartością $L_j^{id_p}$ z RPR_{id_p}, jeżeli wynik jest negatywny, zwróć błąd;
6. **sprawdźATS**(*ATSCh->ATS*), jeżeli wynik jest pozytywny to weryfikacja poprawna

3.6.6 Scalanie poświadczeń

Systemy EHR przechowują RPR'ów dla części EHR znajdującej się w ich systemie, a do weryfikacji konieczny jest RPR zawierający wpisy ze wszystkich systemów EHR. RPR'ów z różnych systemów są scalane w jeden RPR za pomocą działania realizowanego przez Protokół Scalania Rekordów Poświadczeń Rejestrów (PSRPR).

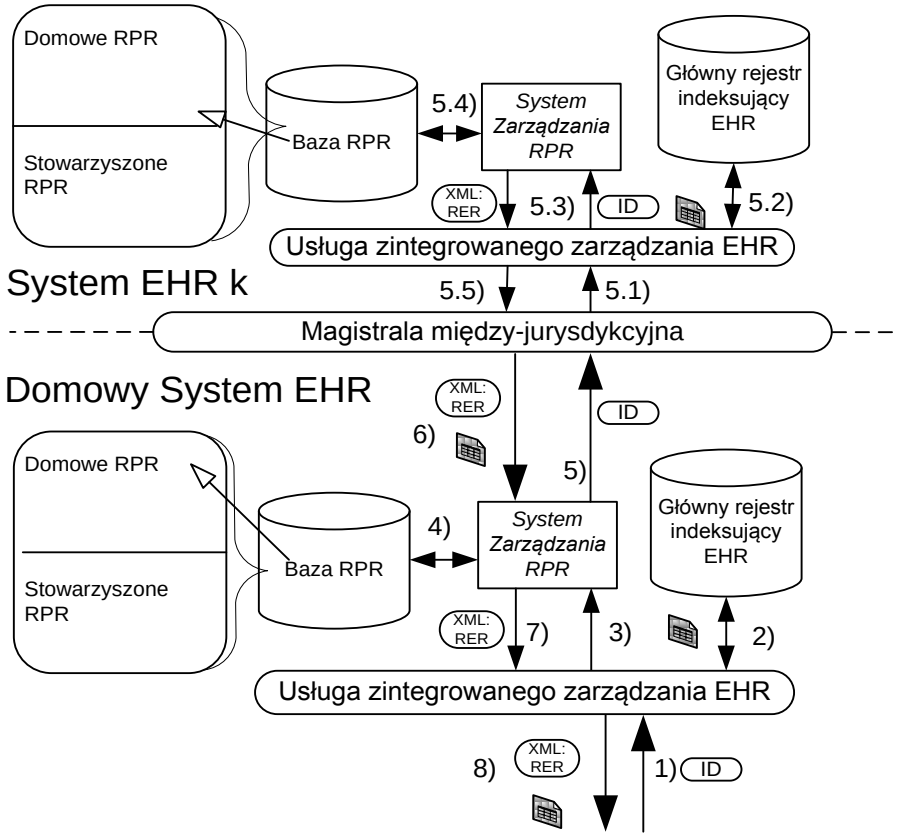
Protokół PSRPR, przedstawiony na następnej stronie, jest realizowany w trzech podstawowych etapach. W pierwszym następuje sprawdzenie, czy w systemach stowarzyszonych znajdują się RPR dotyczące danego pacjenta. W drugim etapie następuje wysłanie żądań i pobranie żądanych danych z systemów stowarzyszonych. Trzeci, ostatni etap to scalenie wszystkich RPR w jeden plik (struktura RPR umożliwia przechowywanie rekordów dotyczących jednego pacjenta pochodzących z jednego lub więcej systemów EHR) i wysłanie wraz z zbiorem wpisów z metadanymi z rejestrów, których dotyczą RPR, do strony inicjującej protokół.

Protokół PSRPR:

Początek: Zapytanie o RPR

Koniec: RPR

1. Użytkownik wysyła zapytanie do UZZ_d o RPR_{id_p};
2. UZZ_d wysyła żądanie do *Głównego Rejestru Indeksującego EHR* o wszystkie M_i powiązane z pacjentem P_{id_p};
3. UZZ_d wysyła żądanie do $SZRPR_k$ o RPR_{id_p};
4. $SZRPR_d$ pobiera RPR_{id_p} z $BRPR_d$;
5. $SZRPR_d$ pobiera z *Rejestru Lokalizacji* informacje w których $EHRS_k$ są przechowywane dokumenty pacjenta P_{id_p}; bazując na tej informacji $SZRPR_d$ wysyła żądanie przysłania $RPR^k_{id_p}$ do każdego z $EHRS_k$:
   5.1. Używając magistrali między-jurysdykcyjnej wyślij żądanie do UZZ_k;
   5.2. UZZ_k wysyła żądanie do *Głównego Rejestru Indeksującego EHR* o wszystkie o metadane $ZM^k_{id_p}$ opisujące wszystkie wpisy w rejestrach dotyczących P_{id_p};
   5.3. UZZ_k wysyła żądanie do $SZRPR_k$ for $RPR^k_{id_p}$;
   5.4. $SZRPR_k$ pobiera z $BRPR_k$ $RPR^k_{id_p}$ i wysyła do UZZ_k;
   5.5. UZZ_k wysyła poprzez magistralę $ZM^k_{id_p}$ i $RPR^k_{id_p}$ między-jurysdykcyjną do UZZ_d; UZZ_d, które przesyła dalej $RPR^k_{id_p}$ do $SZRPR_d$;
6. $SZRPR_d$ integruje wszystkie $RPR^k_{id_p}$ w RPR_{id_p} i przesyła z powrotem do UZZ_k;
7. UZZ_k integruje wszystkie $ZM^k_{id_p}$ oraz $ZM^d_{id_p}$ do ZM_{id_p}, które wysyła do weryfikatora wraz z RPR_{id_p};



Rysunek 3.10: Schemat działania protokołu scalania Rekordów Poświadczeń Rejestrów (źródło: [60])

3.6.7 Weryfikacja autentyczności zbioru metadanych z rejestrów

Algorytm Weryfikacji Autentyczności Rejestrów (AWAR) umożliwia sprawdzenie przez arbitra autentyczności metadanych z rejestrów dotyczących jednego pacjenta. AWAR porównuje RPR_{idp} z ZM_{idp} i zwraca pozytywny rezultat, jeżeli zawartość metadanych w rejestrach opisująca dany EHR jest autentyczna.

Algorytm AWAR

Wejście: RPR, ZM

Wyjście: Wynik weryfikacji – prawda/fałsz

1. Na wejściu odczytaj RPR_{id_p} , ZM_{id_p} ;
2. Dla rekordów poświadczeń z RPR_{id_p} dla każdego $EHRS_k$ i na końcu dla $EHRS_d$ wykonaj:
   2.1. Sprawdź, czy ostatni ATS z $SW_{nr_{last}}^{sehr}$ jest ważny używając funkcji ***sprawdźATS***$(ATS, L_j^{id_p})$; jeżeli rezultat jest negatywny, zwróć błąd; (ten krok eliminuje przypadki, w których ostatni ATS jest nieważny);
   2.2. Dla każdej sekwencji wpisów $SW_{nr_i}^{EHRS_{k|d}}$ w RPR_{id_p} wykonaj:
      2.2.1. Dla każdej rundy R_{rd} w $SW_{nr_i}^{EHRS_{k|d}}$ wykonaj:

2.2.1.1. Dla każdego wpisu W_j w R_{rd} wykonaj:

2.2.1.1.1. Oblicz skrót $Hw_j^{id_p}$ = $H(ZM_{id_p}$ ->M_i), jeżeli M_i nie istnieje, to zwróć błąd; (indeks *j* numeruje kolejne wpisy dla pacjenta P, natomiast *i* to kolejny numer dokumentu w systemie EHR, zarówno w RPR jak i w ZM kolejne rekordy są dodawane po kolei, dzięki temu nie ma problemu z odnalezieniem *i* odpowiadającemu *j*)

2.2.1.1.2. Jeżeli W_j *->odsyłacz zewnętrzny = k i k>0* to sprawdź, czy wartość $Hw_j^{id_p}$ jest równa wartości $L_j^{id_p}$ z $SW_{nr_i}^{EHRS_k}$, jeżeli rezultat jest negatywny, zwróć błąd;

2.2.1.1.3. Porównaj obliczone $Hw_j^{id_p}$ z $Hw_j^{id_p}$ z R_{rd}, jeżeli rezultat jest negatywny, zwróć błąd;

2.2.1.1.4. Jeżeli numer SW *==1* i *j==1*, to $L_{j-1}^{id_p} = L_0^{id_p}$;

2.2.1.1.5. Jeżeli numer SW $\neq 1$ i *j==1*, to $L_{j-1}^{id_p} = H\left(SW_{prev}^{EHRS_k}\right)$;

2.2.1.1.6. Jeżeli element Wpis jest ostatni w R i numer rundy *rd==1*, to $T_j^{id_p} = H\left(TS^0{}_{root}\right)$;

2.2.1.1.7. Jeżeli element Wpis jest ostatni w R, to $T_j^{id_p} = H\left(ATSCh_{rd}^{id_p}\right)$;

2.2.1.1.8. W przeciwnym przypadku $T_j^{id_p} = null$;

2.2.1.1.9. Oblicz $L_j^{id_p} = H\left(j \,|Hw_j^{id_p}\left|L_{j-1}^{id_p}\right| T_j^{id_p}\right)$;

2.2.1.1.10. Porównaj obliczone $L_j^{id_p}$ z $L_j^{id_p}$ z Wpisu, jeżeli rezultat jest negatywny, zwróć błąd;

2.2.1.2. Dla każdego ATS z ATSCh:

2.2.1.2.1. Jeżeli ATS nie jest pierwszy w ATSCh to $L_j^{id_p}$ = $H(ATS_1|\ldots|ATS_{poprzedni})$;

2.2.1.2.2. **sprawdźATS(***ATS*, $L_j^{id_p}$ **)**;

2.3. Sprawdź, czy wszystkie M_i z ZM_{id_p} zostały wykorzystane, jeżeli nie, to zwróć błąd.

3. Zwróć pozytywny wynik.

Algorytm *sprawdźATS*, przedstawiony poniżej, umożliwia sprawdzenie archiwalnego znacznika czasu. Na wejściu algorytmu jest wartość skrótu oraz archiwalny znacznik czasu, a na wyjściu wynik weryfikacji. Algorytm sprawdza ATS pod względem matematycznym, sprawdza ścieżkę certyfikacji, a także dodatkowe źródła zaufania.

Algorytm sprawdźATS:

Wejście: $ATS, L_j^{id_p}$)

Wyjście: Wynik weryfikacji – prawda/fałsz

a. Sprawdź, czy $L_j^{id_p}$ jest równe pierwszemu skrótowi z $RT_{tn}^{id_p}$, jeżeli rezultat jest negatywny, zwróć błąd;
b. Oblicz korzeń drzewa skrótów H_{root}^{tn} używając zredukowanego drzewa skrótów $RT_{tn}^{id_p}$;
c. Oblicz $T_{root}^{tn} = H\left(H_{root}^{tn} \middle| H\left(TS_{root}^{tn-1}\right)\right)$;
d. Porównaj powiązany korzeń drzewa skrótów T_{root}^{tn} ze skrótem z TS_{root}^{tn}, jeżeli rezultat jest negatywny, zwróć błąd;
e. Sprawdź TS_{root}^{tn} pod względem matematycznym;
f. Sprawdź ścieżkę certyfikacji;
g. Sprawdź listę TSL i LPAK;

3.6.8 Weryfikacja niezaprzeczalności EHR

Algorytm Weryfikacji Niezaprzeczalności EHR (AWNEHR), przedstawiony poniżej, na wejściu przyjmuje ZM_{idp} oraz EHR_{idp} i zwraca informacje, czy zawartość EHR (lub ekstraktu EHR) jest niezaprzeczalna. Algorytm służy do weryfikacji niezaprzeczalności pochodzenia i odbioru EHR (lub ekstraktu EHR), czyli udowodnienia, że wszystkie dokumenty, które powinny wchodzić w skład EHR (lub w skład ekstraktu EHR) są oryginalne i niezmienione oraz, że zostały odebrane przez system w określonym czasie.

Algorytm AWNEHR

Wejście: EHR/ekstrakt EHR, ZM

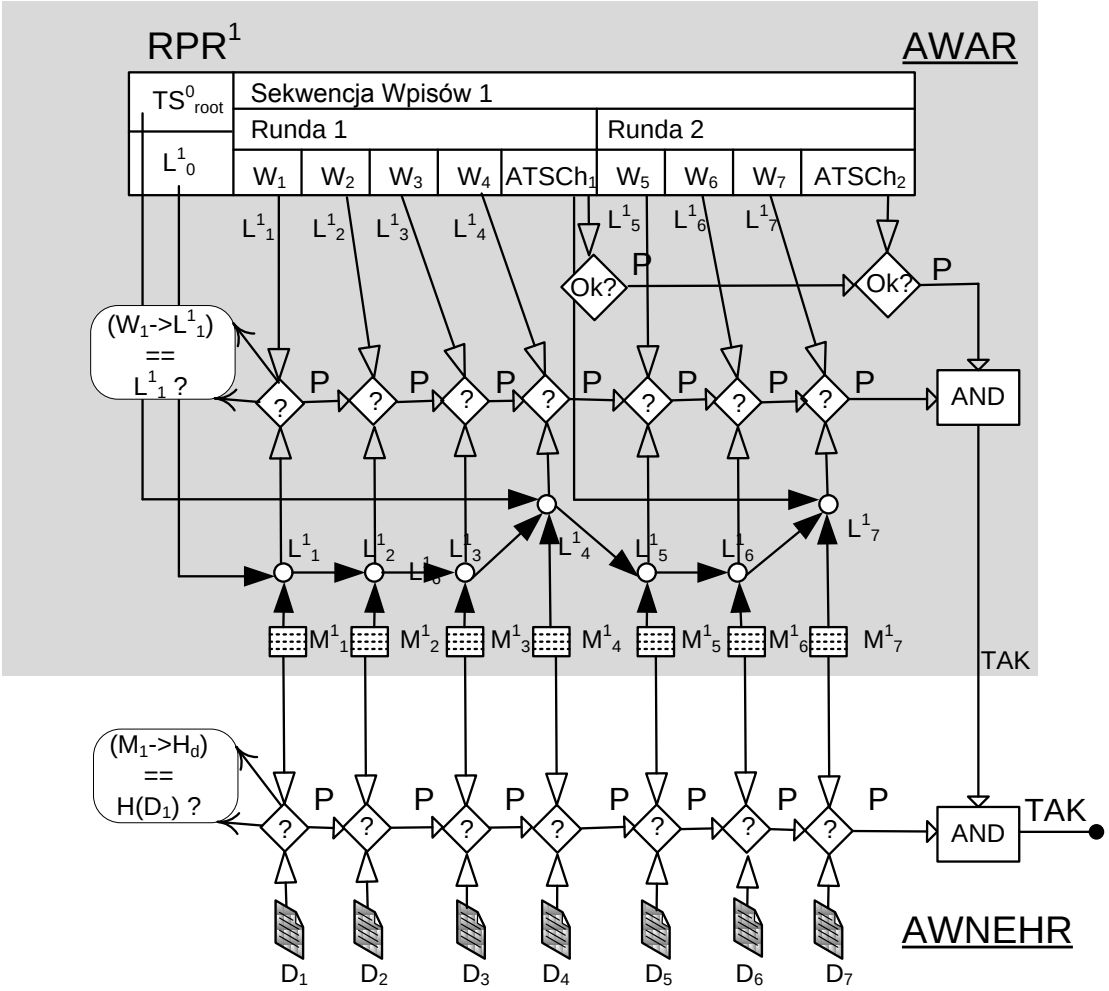
Wyjście: wynik weryfikacji – prawda/fałsz

1. Odczytaj EHR_{idp}, ZM_{id_p};
2. Uruchom algorytm AWAR, gdy wynik jest negatywny, zwróć błąd;
3. Dla każdego dokumentu D_i wchodzącego w skład EHR_{idp} wykonaj:
   3.1. Oblicz $H_d = H(D_i)$;
   3.2. Znajdź $H_d' = ZM_{id_p} \text{->} M_i \text{->} H_d$;
   3.3. Sprawdź czy $H_d = H_d'$, jeżeli wynik jest negatywny, zwróć błąd;
4. Sprawdź czy wszystkie M_i z ZM_{id_p} zostały wykorzystane, jeżeli nie to zwróć błąd;
5. Zwróć pozytywny wynik.

W celu weryfikacji niezaprzeczalności ekstraktu EHR, należy do algorytmu AWNEHR jako dane wejściowe zamiast EHR podstawić ekstrakt EHR.

Na Rys. 3.11 został zaprezentowany przykład działania algorytmów weryfikacji autentyczność rejestrów i niezaprzeczalności EHR. Przykład nawiązuje do przykładu działania algorytmu AARPR (patrz Rys. 3.5.2). Aby sprawdzić niezaprzeczalność EHR należy sprawdzić najpierw autentyczność metadanych w rejestrach. W tym celu z rejestrów pobierane są wpisy z metadanymi M^1_1 do M^1_7. Zaczynając od pierwszego wpisu, obliczana jest wartość $L^1_1=(1|H(M^1_1)|L^1_0)$, która jest porównywana z L^1_1 z wpisu W_1 z RPR^1. Analogicznie sprawdzane są kolejne wartości L, przy czym przy obliczaniu wartości L ostatniego wpisu w rundzie (L^1_4, L^1_7) do obliczania brany jest również pod uwagę łańcuch archiwalnych znaczników czasu z poprzedniej rundy. Następnie, po pozytywnej weryfikacji łańcucha wartości L, są sprawdzane kolejne archiwalne znaczniki czasu z każdej rundy ($ATSCh_1$, $ATSCH_2$). Zbiór metadanych jest uznawany za autentyczny po pozytywnej weryfikacji $ATSCH_2$;

Po otrzymaniu pozytywnego wyniku działania algorytmu AWAR, obliczane są skróty z dokumentów składowych EHR, które następnie są porównywane z skrótami z wpisów zawierających metadane z rejestrów. Wynik wszystkich porównań jest pozytywny oraz wynik działania algorytmu AWAR jest pozytywny, wiec wynik działania algorytmu AWNEHR jest pozytywny, czyli EHR jest niezaprzeczalny (wg definicji z rozdz. 1.2).



Rysunek 3.11: Przykład działania algorytmów AWAR i AWNEHR (źródło: opracowanie własne)

3.6.9 Weryfikacja niezaprzeczalności pojedynczego dokumentu

Algorytmu Weryfikacji Niezaprzeczalności Dokumentu (AWND), przedstawiony poniżej, służy do weryfikacji niezaprzeczalność pochodzenia i odbioru określonego dokumentu D_i jak powiązanych z nim wpisów w rejestrze M_i wchodzącego w skład EHR określonego pacjenta. W celu weryfikacji pojedynczego dokumentu z EHR nie jest konieczna weryfikacja wszystkich znaczników czasu z RPR, w przypadku gdy dokumenty są dodawane częściej niż raz na okres ważności znacznika czasu (np. dwa lata), wartość znaczników czasu w RPR ulega automatycznemu przedłużeniu. Algorytm jest następujący (przykład działania patrz na Rys. 3.12):

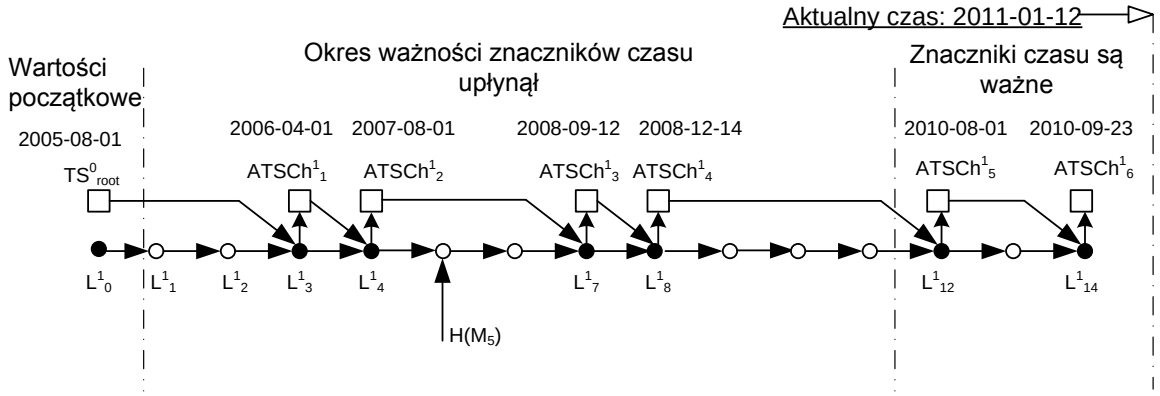
Algorytm AWND:

Wejście: D_i , M_i , RPR_{id_p}

Wyjście: wynik weryfikacji – prawda/fałsz

1. Przygotuj dokument D_i , M_i oraz RPR_{id_p};
2. Sprawdź czy M_i->$H_D = H(D_i)$, jeżeli wynik jest negatywny, zwróć błąd;
3. Znajdź w RPR_{id_p} rundę R_{rd} zawierającą $Hw_j^{id_p} = H(M_i)$;
4. Z rundy R_{rd-1} pobierz $ATSCh_{rd-1}^{id_p}$ ($ATSCh^1{}_2$ z przykładu na Rys. 3.12);
5. Zapisz czas *t* ostatniego ATS z $ATSCh_{rd-1}^{id_p}$ oraz $ATSCh_{rd-1}^{id_p}$ na tymczasowej liście TLST;
6. Dla rund R_{rd} do R_n:
   6.1. Dla wszystkich wpisów W_j z R_{rd}:
      6.1.1. Oblicz wartość $L_j^{id_p}$ (tj. w kroku 2.1.1.1 algorytmu AWAR);
      6.1.2. Porównaj obliczone $L_j^{id_p}$ z $L_j^{id_p}$ z W_j, jeżeli rezultat jest negatywny, zwróć błąd;
   6.2. Zapisz czas *t* ostatniego ATS z $ATSCh_{rd}^{id_p}$ oraz $ATSCh_{rd}^{id_p}$ na tymczasowej liście *TLST*;
   6.3. Jeżeli ostatni ATS z $ATSCh_{rd}^{id_p}$ jest ważny to przerwij; (np. $ATSCh^1{}_5$ z Rys. 3.12);
7. Dla *y=1* do liczby $ATSCh_{rd}^{id_p}$ w *TLST* wykonaj:
   7.1. Dla każdego *ATS* z $ATSCh_x = TLST(y)$:
      7.1.1. **sprawdźATS**(*ATS*, $L_j^{id_p}$) , jeżeli wynik jest negatywny, zwróć błąd;
   7.2. *z=2*;
   7.3. Dopóki okres $|TLST(y+z)-TLST(y)| < TS_{okres\ wazności}$ to:
      7.3.1. *z=z+1*;
   7.4. *y=y+z-1;*
8. Zwróć pozytywny wynik.

Jeżeli weryfikowany jest (D_i , M_i) przedstawiony na Rys. 3.12 to dla podanego przykładu zostaną zweryfikowane tylko $ATSCh^1{}_3$ and $ATSCh^1{}_5$.



Rysunek 3.12:Przykład działania algorytmu AWND (źródło: opracowanie własne)

3.7. Dodatkowe źródła zaufania

Niniejszy rozdział przedstawia propozycję Centrum Informacji Długoterminowej (CID), które zrządza listami TSL oraz Listą Polecanych Algorytmów Kryptograficznych (LPAK – zaproponowaną przez autora niniejszej rozprawy w [58]), będącą odpowiednikiem TLS w dziedzinie algorytmów kryptograficznych. Listy są wykorzystywane przez algorytm **sprawdźATS**(patrz rozdz. 3.5.6) do sprawdzania, czy dany urząd znacznika był certyfikowany przez krajową, rządową lub międzynarodową instytucję oraz czy użyto zalecanego zestawu algorytmów. Takie sprawdzenie jest szczególnie istotne przy weryfikacji długoterminowej, np.: po 20 latach trudno będzie określić jaki urząd był ówcześnie certyfikowany, szczególnie gdy zakończył już działalność operacyjną.

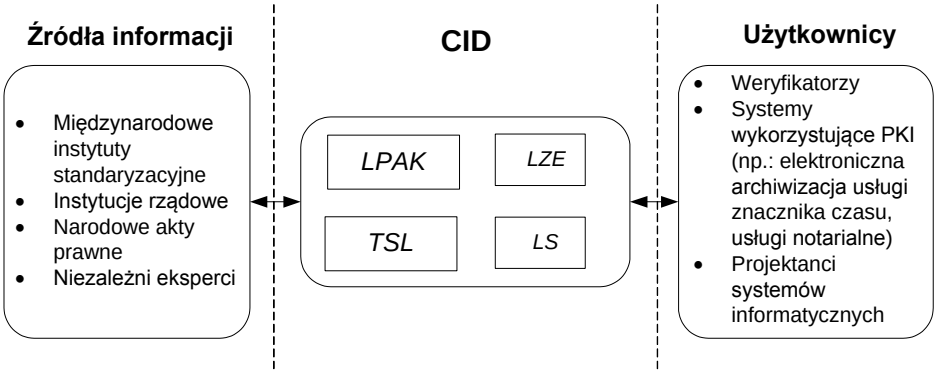
3.7.1 Centrum Informacji Długoterminowej

Centrum Informacji Długoterminowej (CID) (patrz Rys. 3.13) zajmuje się zarządzaniem Listą Polecanych Algorytmów Kryptograficznych (LPAK) oraz zestawem List Statusu Zaufanych Usług (TSL), czyli zarządzaniem informacjami na temat obecnych wymagań poszczególnych państw oraz instytucji standaryzacyjnych dotyczących algorytmów używanych w różnych usługach wykorzystujących infrastrukturę klucza publicznego oraz informacjami dotyczącymi statusu zaufanych usług (w tym znacznika czasu). CID zawiera:

- Listę Polecanych Algorytmów Kryptograficznych (LPAK);
- zestaw List Statusu Zaufanych Usług (TSL);
- Listę Zaufanych Ekspertów (LZE);
- Listę Subskrybentów (LS).

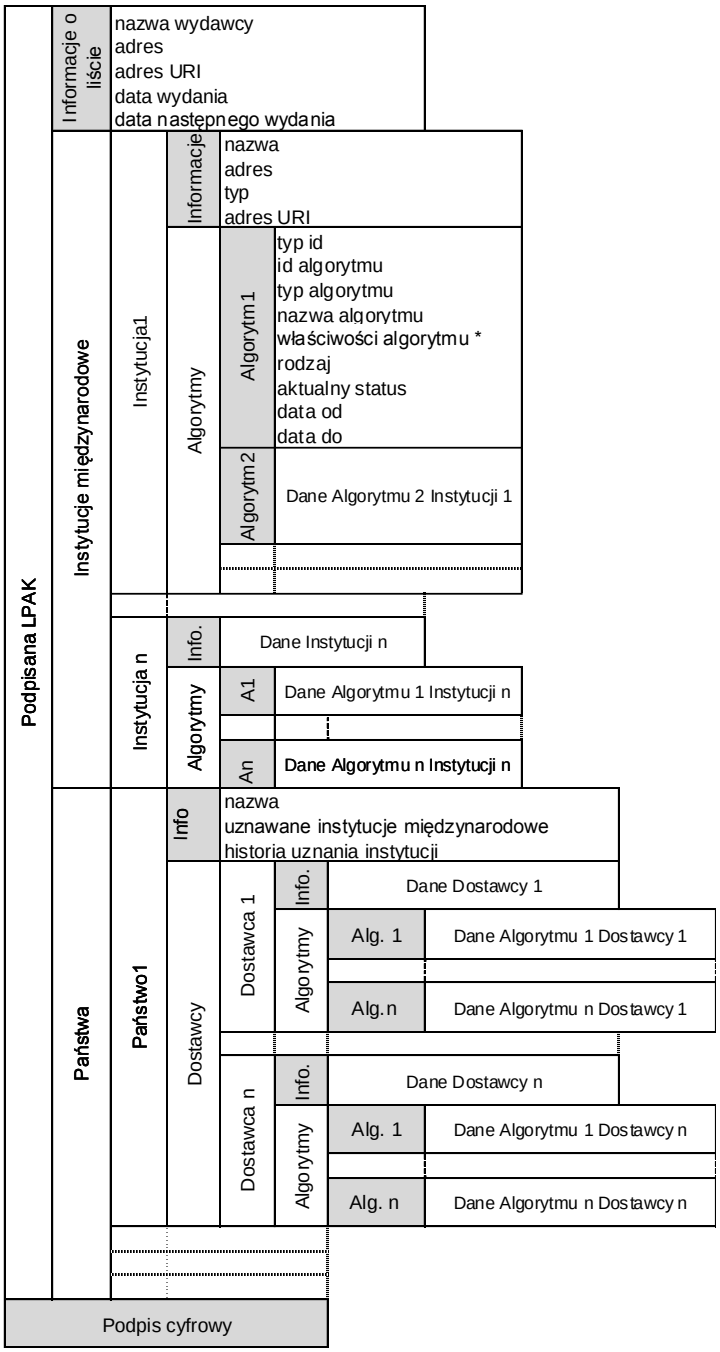
Lista TSL jest tworzona przez właściwą instytucję, np. Ministerstwo Gospodarki w Polsce, opis TSL zawiera rozdz. 2.5.4.1. niniejszej rozprawy. CID zawiera zestaw list TSL wydawanych przez uprawnione instytucje. LPAK przechowuje informację o aktualnie polecanych algorytmach wraz z ich parametrami oraz o historii polecanych algorytmów. LZE zawiera listę zaufanych, zatwierdzonych ekspertów, którzy mogą przesyłać informację o

przełamaniu algorytmów, a LS zawiera listę subskrybentów informowanych o przedterminowej utracie ważności algorytmu.



Rysunek 3.13 : Schemat Centrum Informacji Długoterminowej (źródło: opracowanie własne)

Dane o algorytmach są przesyłane przez organy tworzące prawo w poszczególnych krajach oraz przez narodowe i międzynarodowe instytucje standaryzacyjne. Dodatkowo informacje o algorytmach mogą umieszczać pracownicy CID na podstawie norm czy aktów prawnych. Lista LPAK jest podpisana cyfrowo przez CID i jest prezentowana na stronie WWW. CID udostępnia usługi pozwalające na przetwarzanie maszynowe LPAK i TSL opisane w rozdz. 2.5.4. Lista LPAK jest tworzona i zarządzana przez CID, natomiast listy TSL są jedynie zarządzane przez CID. Jeżeli lista TSL od określonego wystawcy zostaje zaktualizowana, to CID zastępuje ją nową wersją.



Rysunek 3.14: Model logiczny LPAK (źródło: [58])

3.7.2 Lista Polecanych Algorytmów Kryptograficznych

Lista Polecanych Algorytmów Kryptograficznych (LPAK) przechowuje informacje na temat algorytmów polecanych lub wymaganych przez instytucje normalizujące oraz przez narodowe akty prawne. W skład przechowywanych algorytmów wchodzą następujące rodzaje algorytmów: algorytmy funkcji skrótu (np. sha-1, Whirlpool), algorytmy podpisu (np. rsa, dsa), algorytmy generowania kluczy i parametrów, generatory liczb losowych, algorytmy tworzenia dopełnienia (*ang. padding*) oraz zestawy algorytmów wykorzystywanych w

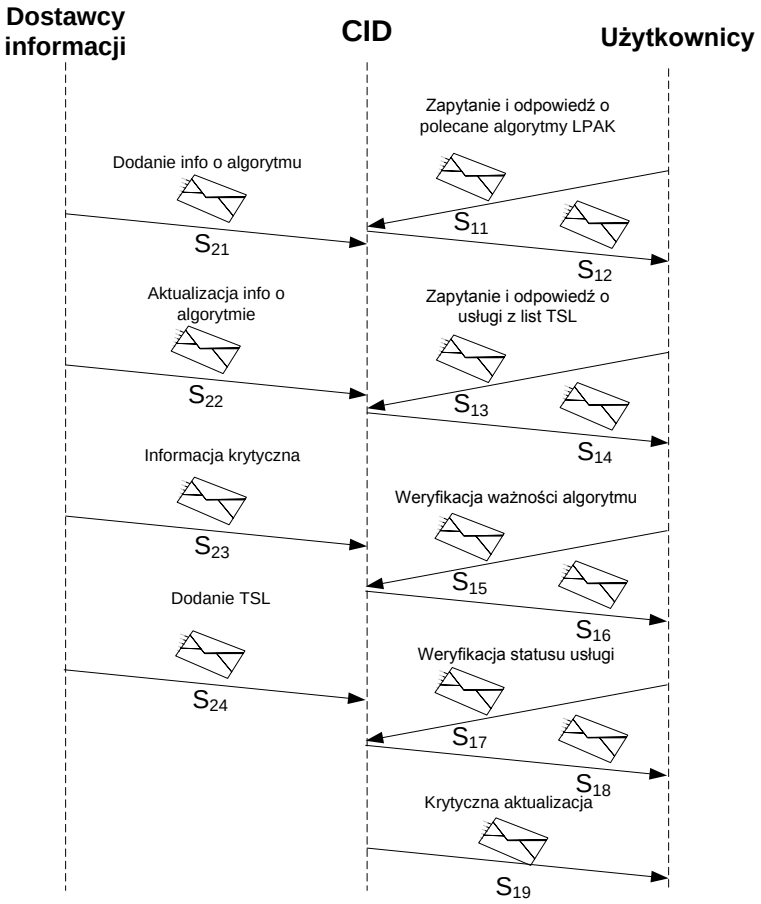
certyfikatach kluczy publicznych (*ang. signature suite*). Lista LPAK jest wydawana co pewien określony okres czasu, np. co 1 dzień.

Model logiczny LPAK został zaprezentowany na Rys. 3.14. Konstrukcja listy jest wzorowana na konstrukcji listy TSL określonej w ETSI TS 102 231 (opis w rozdz. 2.5.4.1). LPAK jest podpisana cyfrowo przez wystawcę. Lista zawiera, dla każdego dostawcy informacje o algorytmach, informacje o nim oraz listę algorytmów, które były lub są polecane czy wymagane (normy zwykle polecają wykorzystanie jakiegoś algorytmu, natomiast akty prawne wymagają stosowania algorytmów o określonych parametrach). Dostawcy informacji są uporządkowani według państw. Natomiast instytucje tworzące normy międzynarodowe są zebrane osobno, gdyż jeżeli dane państwo uznaje daną instytucję, to jednocześnie uznaje jej normy. Każde państwo podaje informacje o uznawanych przez siebie instytucjach międzynarodowych. Konstrukcja listy jest zoptymalizowana pod kątem efektywnego dostępu do polecanych algorytmów w danym państwie. Wyodrębnienie instytucji międzynarodowych pozwala uniknąć powtarzających się wpisów o danym standardzie w wielu państwach.

Informacja o konkretnym algorytmie zawiera dane umożliwiające jego jednoznaczną identyfikację (typ identyfikatora, identyfikator, nazwę, rodzaj). Dodatkowo może być zawarta informacja o dodatkowych parametrach (np. dla rsa minimalna długość modułu). Jest to pole opcjonalne zależne od konkretnego algorytmu, gdyż np. dla algorytmu sha-512 nie jest konieczne. Pole „aktualny status" określa, czy algorytm jest aktualnie polecany, czy już nie jest uważany za bezpieczny i nie jest polecany. Pole „data od" zawiera informacje o dacie dodania przez dostawcę algorytmu do listy. Natomiast pole „data do" zawiera informacje, w przypadku algorytmów aktualnie polecanych, o dacie do której zaleca się jego stosowanie, a w przypadków algorytmów już nie ważnych, o dacie w której algorytm stracił ważność.

3.7.3 Komunikacja CID z użytkownikami

Centrum Informacji Długoterminowej do komunikacji z użytkownikami i dostawcami informacji używa protokołu zawierającego dwa typów wiadomości. Wiadomości typu S_{1x}, gdzie $x \subset [1,9]$ służą do sprawdzania, czy dany algorytm jest ważny, a także do pobierania listy LPAK oraz list TSL. Natomiast wiadomości typu S_{2y}, gdzie $y \subset [1,4]$ służą do aktualizacji informacji na temat algorytmów i dostawców usług. Schemat protokołu komunikacji z CID przedstawia Rys. 3.15.



Rysunek 3.15: Typy wiadomości używanych do komunikacji z CID (źródło: opracowanie własne)

W skład grupy S_{1x} wchodzą następujące wiadomości:

- S_{11} – zapytanie do CID o aktualnie polecane algorytmy wskazanych typów przez wskazanych dostawców informacji lub o całą listę LPAK;
- S_{12} – odpowiedź CID zawierająca polecane algorytmy przez wskazanych dostawców informacji. W przypadku wskazania wszystkich algorytmów od wszystkich dostawców we wszystkich państwach przesyłana jest cała LPAK;
- S_{13} – zapytanie do CID o certyfikowane usługi określonego typu lub o całą listę TSL wystawioną przez określonego wystawcę;
- S_{14} – odpowiedź CID zawierająca listę dostawców usług lub listę(y) TSL;
- S_{15} – zapytanie weryfikatora odnośnie ważności algorytmu lub algorytmów w określonym przedziale czasu według określonych dostawców informacji;
- S_{16} – odpowiedź na zapytanie S_{15};
- S_{17} – zapytanie weryfikatora odnośnie statusu usługi w określonym przedziale czasu ;
- S_{18} – odpowiedź na zapytanie S_{17};
- S_{19} – wiadomość zawierająca informacji o przełamaniu algorytmu, jest wysyłana automatycznie do wszystkich zapisanych na Liście Subskrybentów (LS).

W skład grupy S_{2y} wchodzą następujące wiadomości:

- S_{21} – dodanie do Centrum informacji o nowym algorytmie zalecanym od dostawcy informacji (np. od instytucji normalizacyjnej, czy od ustawodawcy krajowego);
- S_{22} – aktualizacja informacji w Centrum odnośnie zalecanych algorytmów;
- S_{23} – wiadomość od zaufanego eksperta z LZE do systemu zawierająca informację o przełamanym algorytmie.
- S_{24} – przesłanie do CID listy TSL przez upoważnioną instytucję;

3.8. Metoda DPEDZ a prace pokrewne

Metoda DPEDZ zawiera szereg powiązanych działań, które wykonywane kolejno zgodnie z napływem nowych dokumentów składowych do EHR oraz żądań pobrania ekstraktów EHR umożliwiają zarządzanie RPR, za pomocą których można udowodnić niezaprzeczalność EHR. Pacjentowi rejestrującemu się w systemie (najczęściej przy urodzeniu) zostaje założony EHR. Podczas dodawania do EHR pierwszego dokumentu wraz z metadanymi zostaje uruchomiony protokół PDNW oraz algorytm AARPR, które tworzą Rekordy Poświadczeń Rejestrów. RPR zawierają rekordy w których znajduje się m. in. skrót z wpisów z rejestru zawierającego zestaw metadanych. Jedną z metadanych jest skrót z podpisanego cyfrowo dokumentu umieszczonego w repozytorium. Każdy rekord jest powiązany z rekordem poprzednim. Rekordy są pogrupowane wg rund w których zostały dodane. Na końcu rundy znajduje się archiwalny znacznik czasu, który zawiera m. in. zredukowane binarne drzewo skrótów Merkle'a. Taka konstrukcja RPR umożliwia wykrycie wszelkich zamian w metadanych w rejestrach i dokumentach w repozytoriach należących do konkretnego EHR.

Każdy następny dodawany dokument z metadanymi aktualizuje i „odświeża" okres ważność RPR. W przypadku, gdy dokumenty do EHR są dodawane częściej niż raz na okres ważności znacznika czasu, RPR nie wymagają użycia algorytmu APWATS przedłużającego jego ważność. Aktualizacja RPR odbywa się w rundach. Jeżeli czas trwania rundy jest długi, to istnieje możliwość utworzenia tokenu umożliwiającego nadawcy stwierdzenie czy runda została obliczona prawidłowo. Algorytmy AWAR, AWNEHR i AWND umożliwiają weryfikację autentyczności zbioru metadanych z rejestrów, niezaprzeczalności pochodzenia i odbioru EHR, niezaprzeczalności EHR, a także niezaprzeczalności pojedynczego dokumentu wchodzącego w jego skład (wg definicji z rozdz. 1.2).

W systemach archiwizujących dokumenty do przedłużenia ważności podpisów cyfrowych, a także zapewniania niezaprzeczalności pojedynczych dokumentów lub grup dokumentów, można użyć rozwiązań tj.: XADES-A, Schemat liniowego wiązania, Evidence Record Syntax, Schemat Haber-Stornetta, czy Schemat Benaloh de Mare. Porównanie właściwości tych rozwiązań w stosunku do właściwości proponowanej metody DPEDZ zawiera Tab. 3.2.

Tabela 3.2: Porównanie metody DPEDZ z innymi rozwiązaniami (źródło: opracowanie własne)

Lp.	Właściwość \ Rozwiązanie	XADES-A	Schemat liniowego wiązania (SLW)	Evidence Record syntax (ERS)	Schemat Haber-Storrneta (SHS)	Schemat Benaloh de Mare (SBM)	DPEDZ
1	Zapewnia niezaprzeczalność (pochodzenia i odbioru) podpisanego dokumentu w długim okresie.	+	+	+	+	+	+
2	Zapewnia integralność, autentyczność podpisanego dokumentu w długim okresie.	+	+	+	+	+	+
3	Zapewnia niezaprzeczalność (pochodzenia i odbioru) każdej z wielu grupy podpisanych dokumentów w określonym momencie czasu.	-	-	+	+	+	+
4	Zapewnia niezaprzeczalność (pochodzenia i odbioru) każdej z wielu grup dokumentów dodawanych przez długi okres.	-	+-	-	+-	+-	+
5	Weryfikacja przez zewnętrznego arbitra.	+	+	+	+	+	+
6	Wymaga współpracy z TSA.	+	-	+	-	-	+
7	Wymaga upubliczniania wartości na koniec rundy.	-	+	-	+	+	-
8	Optymalizacja operacji znakowania czasem.	-	-	+	-	-	+
9	Optymalizacja operacji ponownego znakowania czasem.	-	-	-	-	-	+
10	Uwzględnia strukturę EHR zdefiniowanej w normie ISO/IEC 13606 oraz przechowywanie danych w rejestrach i repozytoriach.	-	-	-	-	-	+

Metoda DPEDZ, tj. pozostałe rozwiązania z Tab. 3.2, pozwala na konserwowanie ważności podpisu cyfrowego dołączonego do pojedynczego dokumentu. Trzecia właściwość, to zapewnienie niezaprzeczalności pochodzenia i odbioru grupy podpisanych dokumentów w określonym momencie czasu, czyli możliwość udowodnienia, że grupa dokumentów dotyczących jednego podmiotu (pacjenta) pochodzi od autorów wymienionych w

dokumentach i dokumenty należące do grupy zostały odebrane przez system w określonym momencie czasu. Poza XADES wszystkie rozwiązania zapewniają taką możliwość. SLW wymaga osobnego zastosowania dla każdej grupy, co powoduje zwiększenie koniecznych wartości do upublicznienia.

Właściwość nr 4, zapewnia niezaprzeczalność pochodzenia i odbioru każdej z wielu grup dokumentów dodawanych przez długi okres. Gdy zbiór dokumentów należących do jednego podmiotu (do jednego pacjenta) jest dodawany przez długi okres (przez wiele rund), to można stwierdzić niezaprzeczalność każdej z grup dokumentów. Zakłada się też, że w każdej rundzie dodawane są dokumenty należące do wielu grup. XADES i ERS nie posiadają funkcjonalności. Za pomocą SLW, SHS, SBM można by osiągnąć taką funkcjonalność, ale wymagałoby to odrębnego obliczania rundy lub przechowywania dodatkowych danych. DPEDZ posiada taką funkcjonalność.

W celu zapewnienia niezaprzeczalności stosowane są dwa podejścia. Pierwsze zakłada stosowanie zaufanych znaczników czasu, a drugie zakłada publikowanie wartości skrótu obliczonego na zakończenie rundy, np. w gazecie codziennej (zakłada się, że nie można sfałszować całego nakładu gazety). DPEDZ tak samo jak XADES i ERS używa TSA. Natomiast pozostałe rozwiązania zakładają publikacje wartości skrótu. SLW nie działa w rundach, więc wymaga publikacji każdego skrótu.

ERS i DPEDZ używają struktur drzewiastych do minimalizacji ilości tworzonych TS. Znaczniki czasu wymagają ponownego znakowania czasem przed upływem daty ich ważności. Jedynie proponowana metoda DPEDZ, w przypadku dodawania dokumentu do grupy minimum raz na okres ważności znacznika czasu, nie wymaga stosowania ponownego znakowania czasem.

3.9. Podsumowanie

Zapewnienie niezaprzeczalności EHR dodaje warstwę bezpieczeństwa, która jest praktycznie niedostępna w przypadku dokumentacji papierowej (jak sprawdzić w wielu miejscach świadczenia usług zdrowotnych, czy cała dokumentacja papierowa jest niezmieniona i dostępna?). W tym celu powyżej zaproponowano metodę DPEDZ. Metoda zapewnia działania konieczne do zapewnienia autentyczności i niezaprzeczalności EHR (pochodzenia i odbioru). System implementujący metodę DPEDZ może być zbudowany w oparciu o aktualne standardy określające model informacyjny EHR.

Niezaprzeczalność pochodzenia jest uzyskiwana przez ciągłe konserwowanie podpisów cyfrowych dołączonych do dokumentów medycznych, tak aby były ważne po dowolnym okresie składowania. A niezaprzeczalność odbioru jest uzyskiwana przez stosowanie znaczników czasu potwierdzających dodanie dokumentu w określonej rundzie.

Systemy EHR projektowane są z użyciem technologii modułowej. Wielu pacjentów będzie posiadało swoje dane w wielu połączonych systemach EHR (np. podczas korzystania z usług opieki zdrowotnej w innych państwach/regionach). Jednakże pomimo, że dla użytkowników struktura systemów jest ukryta, to każdy system EHR tworzy RPR dla części EHR przechowywanej w swoim systemie. W rozdziale zaproponowano dwa warianty tworzenia RPR. Pierwszy, wymagający mniejszej ilości wymiany danych między systemami i obliczeń, który uznaje, że wystarczy zapewnić niezaprzeczalność części EHR przez każdy system EHR. I drugi zapewniający powiązania pomiędzy RPR, a wiec wszystkie dokumenty wchodzące w skład EHR, rozproszone na wiele systemów EHR są ze sobą powiązane.

W porównaniu do znanych metod, metoda DPEDZ zawiera innowacyjne podejście do zabezpieczenia metadanych przechowywanych w rejestrach oraz dokumentów w repozytoriach należących do wielu pacjentów. Nowością jest jednoczesne wiązanie jednostek danych (wpisów do rejestrów zawierającego metadane) należących do jednego pacjenta (wchodzących w skład jednego EHR) w długim okresie przy jednoczesnym podziale czynności aktualizacji RPR na rundy. Działanie takie umożliwia zredukowanie liczby wymaganych znaczników czasu, a także umożliwia udowodnienie autentyczności i niezaprzeczalności dla widoku EHR z dowolnego momentu w przeszłości. Nowe w stosunku do obecnie stosowanych zabezpieczeń w systemach EHR jest również podejście polegające na opracowaniu działań metody DPEDZ i RPR jako słownika uwierzytelnianego, co powoduje, że weryfikacja autentyczności i niezaprzeczalności EHR może odbywać się w pełni automatycznie oraz EHR i RPR nie muszą być przechowywane w strefie zaufanej.

Następny rozdział zawiera badania eksperymentalne zawierające testy wydajności poszczególnych działań składowych metody DPEDZ oraz testy bezpieczeństwa.

4. Badania eksperymentalne

W celu sprawdzenia proponowanej metody DPEDZ wykonano implementacje poszczególnych działań składowych metody. Implementacja została wykorzystana do przeprowadzenia szeregu eksperymentów sprawdzających metodę pod kątem wymagań bezpieczeństwa z Tab. 1.1 i Tab. 1.2.

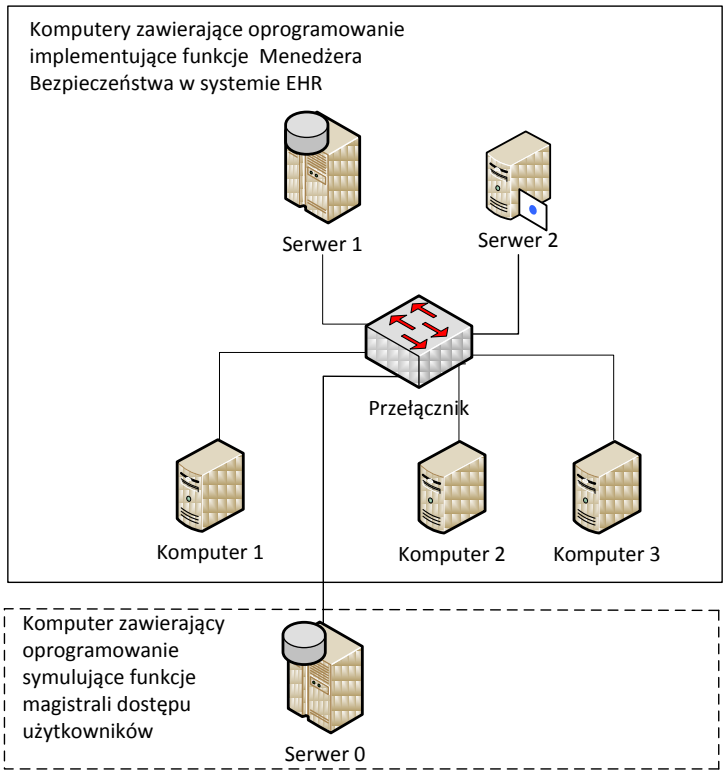
Testy zostały podzielone na dwie grupy. W rozdziale 4.1 zostały umieszczone wyniki testów wydajności, które sprawdzają działania składowe metody DPEDZ pod względem skalowalności lub sprawdzają wydajność dla różnych parametrów lub danych wejściowych. W rozdziale 4.2 umieszczono wyniki testów bezpieczeństwa mających sprawdzić odporność na ataki, których celem jest potwierdzenie spełnienia wymagań bezpieczeństwa z Tab. 1.1 i Tab. 1.2.

4.1. Testy wydajności

4.1.1 Środowisko testowe

Testy zostały przeprowadzone z użyciem środowiska testowego składającego się z trzech serwerów oraz trzech stacji roboczych połączonych przełącznikiem (patrz Rys. 4.1). Serwery 1 i 2 oraz komputery 1 – 3 zawierają oprogramowanie implementujące poszczególne działania składowe metody DPEDZ. Oprogramowanie implementujące funkcje Menedżera Bezpieczeństwa jest w systemie EHR. Dodatkowo, aby zasymulować działanie oprogramowania w przypadku, gdy użytkownicy wysyłają do systemu setki tysięcy dokumentów na godzinę, został użyty serwer 0. W bazie danych znajdującej się na serwerze 0 zostało zapisanych milion wygenerowanych dokumentów. Serwer 0 został wykorzystany do zasymulowania sytuacji, w której w ciągu jednej godziny z systemu korzystają dziesiątki/setki tysięcy użytkowników (specjalistów ds. ochrony zdrowia).

W rzeczywistych zastosowaniach systemy EHR składają się z wielu serwerów przechowywanych w centrach obliczeniowych. Z uwagi na to, że funkcje bezpieczeństwa nie mogą znacząco wpływać na działanie systemu, testy zostały przeprowadzone na środowisku testowym tak skonfigurowanym, aby sprawdzić działanie na minimalnej konfiguracji jaka może zostać wykorzystana w praktyce. Dokładne opisy konfiguracji komputerów i znajdującego się na nich oprogramowania implementującego składowe działania metody DPEDZ zostały umieszczone przy opisach testów. Specyfikacja techniczna komputerów wchodzących w skład środowiska testowego została zawarta w Tab. 4.1.



Rysunek 4.1: Środowisko testowe (źródło: opracowanie własne)

Tabela 4.1: Specyfikacja środowiska testowego (źródło: opracowanie własne)

Nazwa urządzenia	**Specyfikacja techniczna**	**System operacyjny**
Komputer 1 (K1)	Intel Core 2 Duo P9700 @2,80GHz, 6GB RAM	Windows 7 Professional 64bit
Komputer 2 (K2)	Intel Core i7-720QM @1,60GHz, 4GB RAM	Windows 7 Professional 32bit
Komputer 3 (K3)	Intel Xeon W3520 @2,67GHz, 4GB RAM	Windows 7 Professional 64bit
Serwer 0 (S0)	Intel Xeon W3520 @2,67GHz, 4GB RAM	Windows 7 Professional 64bit
Serwer 1 (S1)	2x Intel Xeon E5504 @2,0GHz, 6 GB RAM	Windows Server 2008 R2 Enterprise 64bit
Serwer 2 (S2)	2x Intel Xeon E5504 @2,0GHz, 6 GB RAM	Windows Server 2008 R2 Enterprise 64bit
Przełącznik	HP ProCurve 5412, 1 Gbps Ethernet	CISCO IOS

Używane zestawy danych testowych zostały dobrane w taki sposób, aby sprawdzić działanie programów implementujących protokoły i algorytmy na danych wejściowych w liczbie, która może występować w praktyce dla systemu obejmującego około 50 milionów pacjentów, dla których co roku dodawanych jest średnio 8-10 dokumentów zdrowotnych.

Implementacja została wykonana w języku C# z wykorzystaniem Visual Studio 2008/2010 z NET3.5/4.0 oraz z wykorzystaniem biblioteki kryptograficznej CryptoSys PKI Toolkit. Bazy danych wykorzystują MS SQL Server 2008 Enterprise. Do tworzenia podpisów cyfrowych oraz znaczników czasu zostały wykorzystane algorytmy RSA i SHA512.

4.1.2 Dane testowe

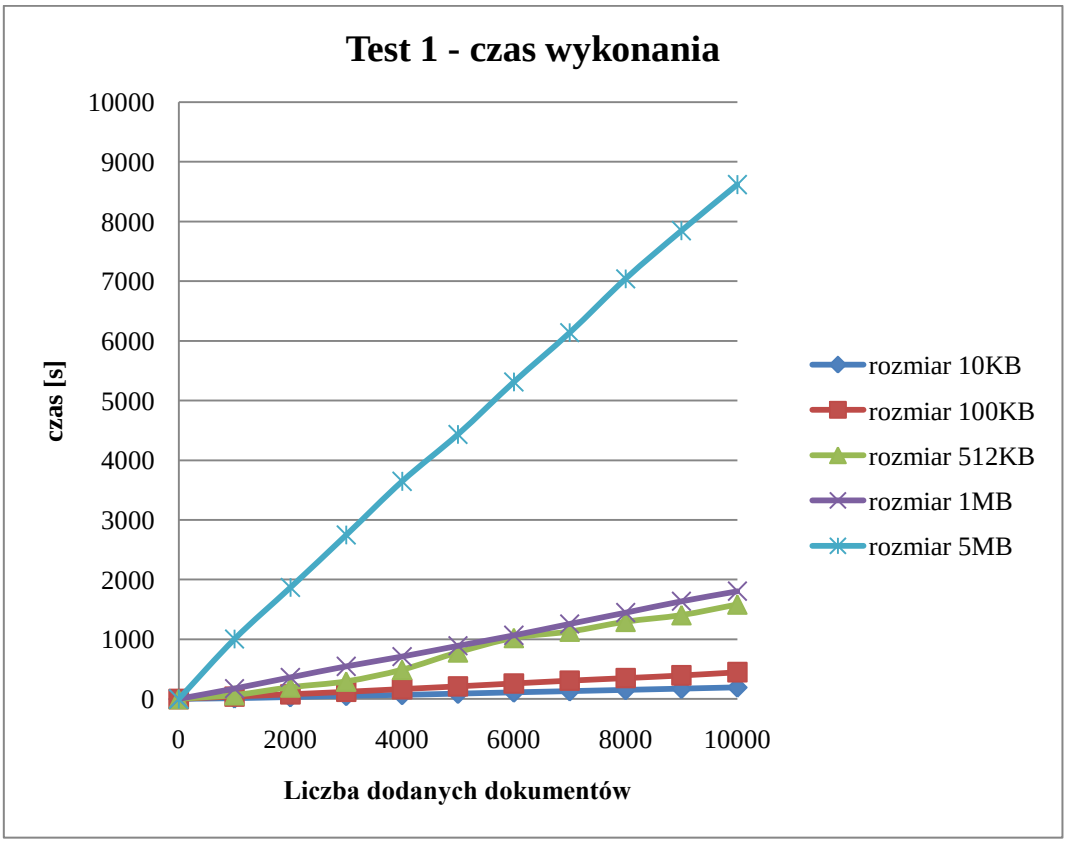
Na potrzeby testów została stworzona aplikacja generująca wejściowe dokumenty testowe. Dokumenty testowe zostały wygenerowane w oparciu o strukturę logiczną dokumentu zawartą w CEN/ISO 13606 (przedstawioną w rozdz. 2.2.2.3). Za pomocą generatora można utworzyć ekstrakty EHR składający się z dowolnej liczby dokumentów medycznych (kompozycji). Dokument może mieć dowolny rozmiar. W nagłówku dokumentu znajdują się metadane m. in.: id pacjenta (id ehr), id lekarza, id archetypu, id systemu pochodzenia. Wszystkie dokumenty są podpisane cyfrowo z użyciem wygenerowanego klucza prywatnego lekarza.

4.1.3 Protokół PDNW

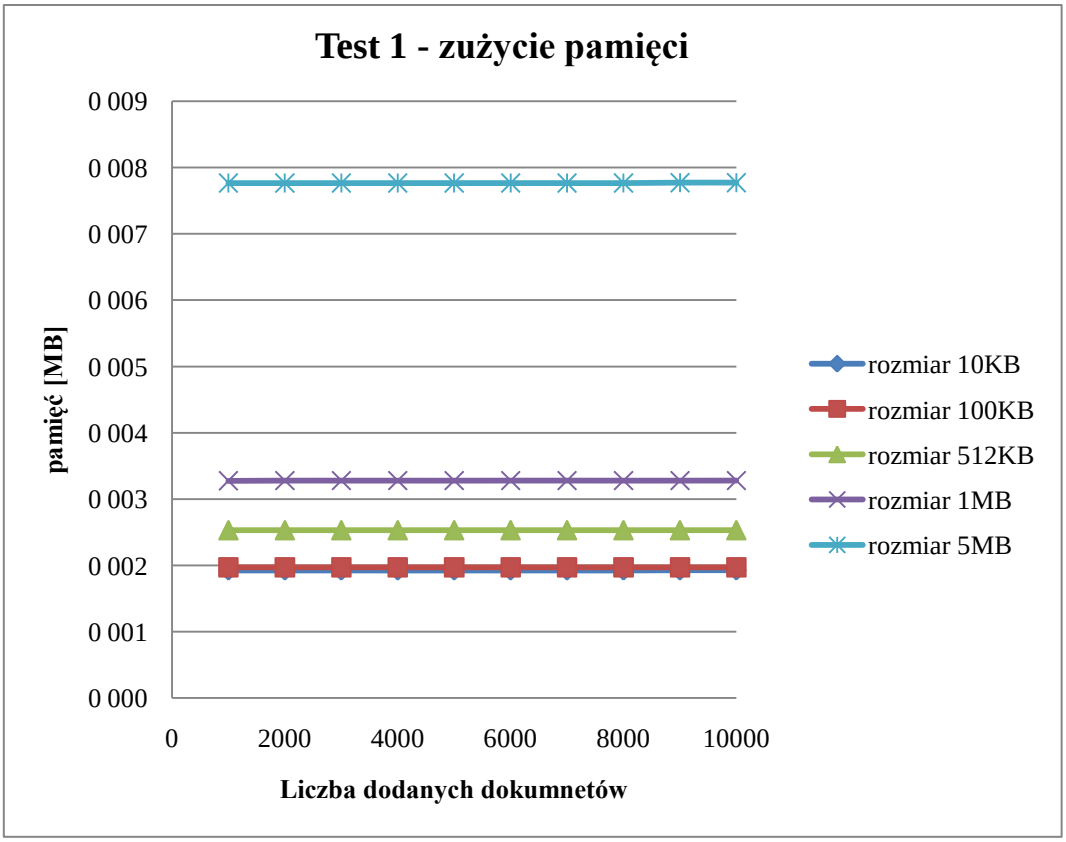
W celu sprawdzenia działania protokołu PDNW zostały przeprowadzone dwa testy. Pierwszy test obejmował dodanie 10000 ekstraktów EHR o różnych rozmiarach (szczegóły – patrz Tab. 4.2), a drugi – działanie protokołu w przypadku dodania miliona ekstraktów EHR (szczegóły patrz Tab. 4.3). Celem było sprawdzenie czasu obliczeń oraz ilości używanej pamięci RAM.

Tabela 4.2: Opis testu nr 1 (źródło: opracowanie własne)

Numer testu	1
Dane wejściowe	5 x 10 000 ekstraktów EHR (każda ekstrakt EHR zawiera 1 dokument 10KB, 100KB, 512KB, 1MB, 5MB – zależnie od serii)
Dane wyjściowe	Dane umieszczone w Bazie RPR na S1, a także dokumenty w repozytoriach i metadane w rejestrach (do symulacji repozytoriów rejestrów wykorzystano bazę danych znajdują się na S1).
Konfiguracja urządzeń testowych	K1 wykorzystany jako UZZ wysyłająca dane do baz danych znajdujących się na S1; dane wejściowe pobierane z S0 symulującego wysyłanie dokumentów przez specjalistów ds. ochrony zdrowia;
Cel testu	Sprawdzenie czasu obliczeń oraz ilości używanej pamięci RAM.
Kod wymagania wg Tab. 1.1 i 1.2	Nie dotyczy
Oczekiwany wynik	Liniowy wzrost czasu obliczeń w związku ze zwiększaniem ilości ekstraktów EHR na wejściu, stałe zapotrzebowanie na pamięć.



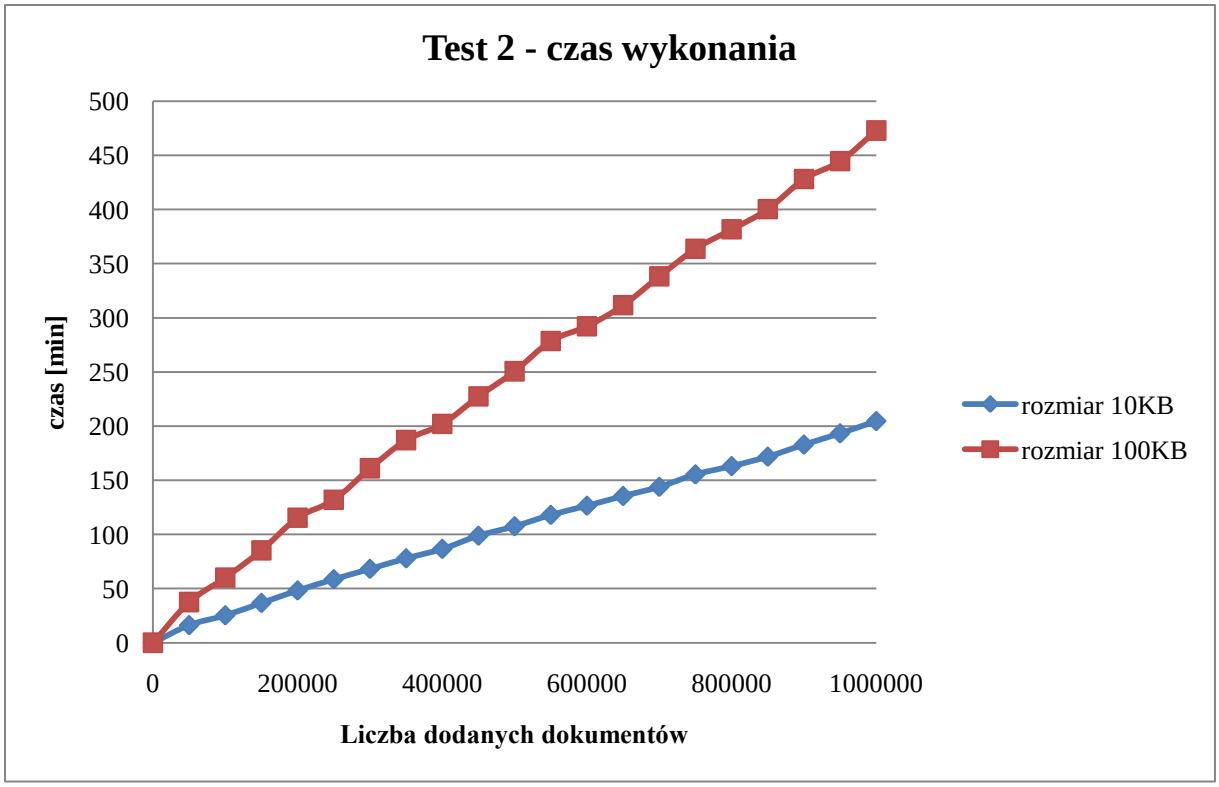
Rysunek 4.2: Test 1 - czas wykonania (źródło: opracowanie własne)



Rysunek 4.3: Test 1 - zużycie pamięci (źródło: opracowanie własne)

Tabela 4.3: Opis testu nr 2 (źródło: opracowanie własne)

Numer testu	2
Dane wejściowe	2 x 1 000 000 ekstraktów EHR (każda ekstrakt EHR zawiera 1 dokument o rozmiarze 10KB lub 100KB – zależnie od serii)
Dane wyjściowe	Dane umieszczone w Bazie RPR na S1, a także dokumenty w repozytoriach i metadane w rejestrach (do symulacji repozytoriów rejestrów wykorzystano bazę danych znajdują się na S1).
Konfiguracja urządzeń testowych	K1 wykorzystany jako UZZ wysyłająca dane do baz danych znajdujących się na S1; dane wejściowe pobierane z S0 symulującego wysyłanie dokumentów przez specjalistów ds. ochrony zdrowia;
Cel testu	Sprawdzenie skalowalności rozwiązania dla systemu obsługującego 50 milionów użytkowników dla których dodawane jest 8-10 dokumentów na rok, co daje średnio 1,2-1,4 miliona dokumentów dziennie.
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Liczba dodawanych ekstraktów EHR nie wpływa na czas przetwarzania pojedynczego ekstraktu EHR. Milion dokumentów zostanie przetworzony poniżej 12h.



Rysunek 4.4: Test 2 - czas obliczeń (źródło: opracowanie własne)

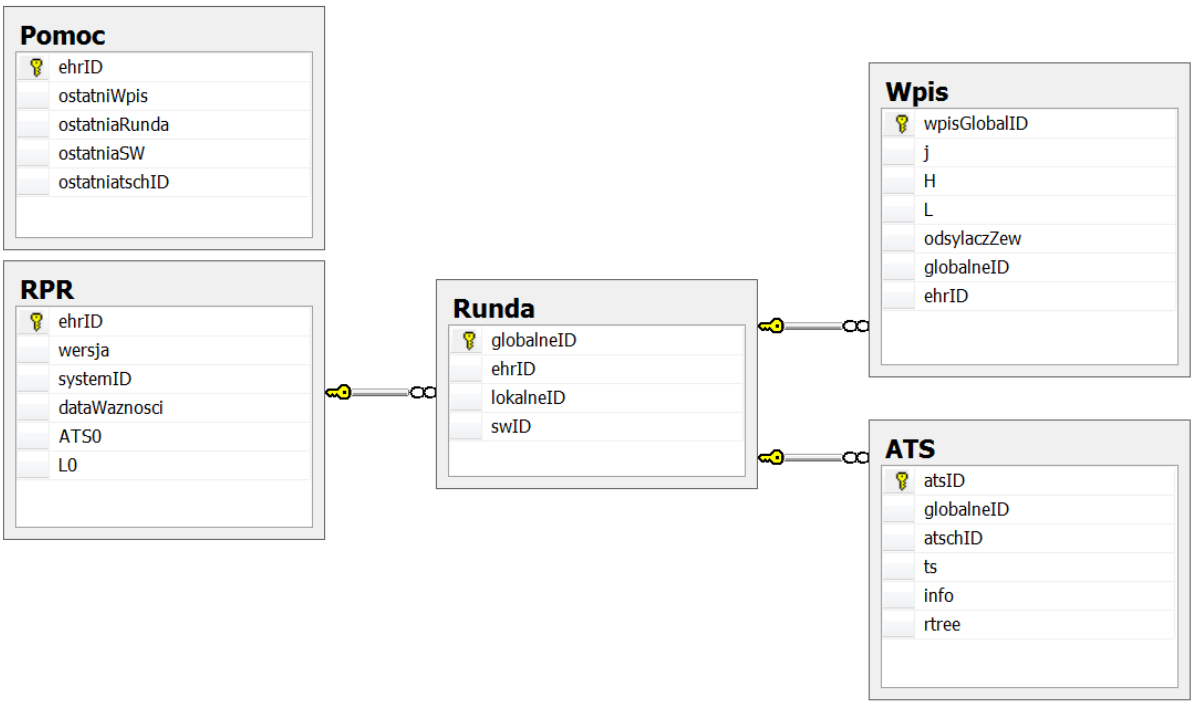
Wynik testów (patrz Rys. 4.2 - 4.4) potwierdzają liniową złożoność obliczeniową programu zawierającego implementację protokołu przy stałym zużyciu pamięci. Czas dodania ekstraktu EHR o określonym rozmiarze jest stały. W czasie drugiego testu w ciągu 8h został dodany milion dokumentów. Uzyskane wyniki pokrywają się z wynikami zakładanymi przed przeprowadzeniem testu.

4.1.4 Algorytmy tworzenia i aktualizacji RPR

4.1.4.1 Algorytm AARPR

Algorytm AARPR jest najbardziej złożonym algorytmem znajdującym się w metodzie DPEDZ. Ponieważ AARPR do swojego działania nie wymaga całych RPR, a jedynie danych z dwóch ostatnich rund, to do celów testowych algorytm został zaimplementowany na dwa sposoby. W pierwszym, RPR są w bazie przechowywane jako plik XML i aby wykonać jakąkolwiek operacje na RPR należy pobrać i później przesłać plik XML. Drugi sposób polega na przechowywaniu poszczególnych elementów RPR w tabelach, tak aby można było pobrać jedynie dane potrzebne przez algorytm (patrz Rys. 4.5). Drugi sposób wymaga przeprowadzania dodatkowych operacji przy weryfikacji, polegających na tworzeniu w locie jednego pliku XML z RPR. Natomiast w pierwszym sposobie, przy wzroście rozmiaru RPR będzie wydłużał się czas potrzebny na pobranie danych z bazy i może zaistnieć problem związany z skalowalnością rozwiązania.

Algorytm został przetestowany pod kątem wpływu na wydajność parametru (rozmiar rundy), rodzaju danych testowych (liczba M_i przypadających średnio na jednego pacjenta w rundzie) oraz skalowalności w przypadku bardzo dużej liczbie rund i dokumentów (symulacja rzeczywistego wykorzystania).

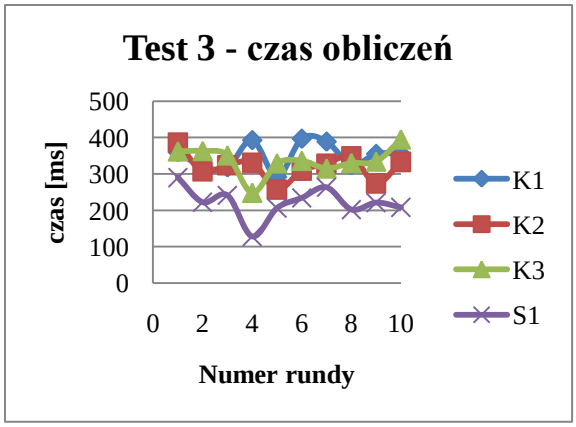


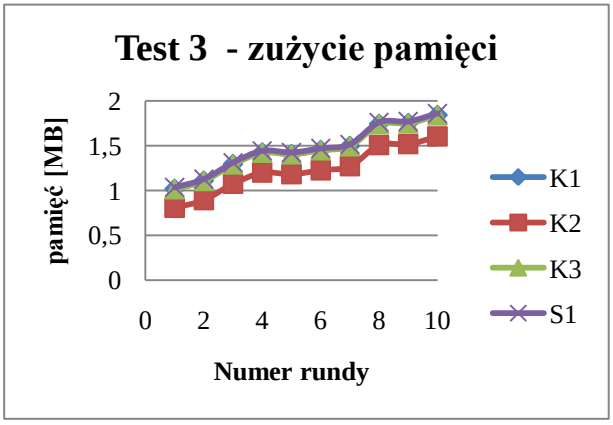
Rysunek 4.5: Schemat przykładowej bazy danych do przechowywania RPR (źródło: opracowanie własne)

Celem testów od 3 do 8 (szczegółowy opis w Tab. 4.4) jest sprawdzenie wymaganego czasu obliczeń i zużycia pamięci przy różnych konfiguracjach danych testowych i parametru algorytmu – rozmiaru rundy. W testach wykorzystano implementacje algorytmu przechowującą RPR w postaci plików w bazie danych.

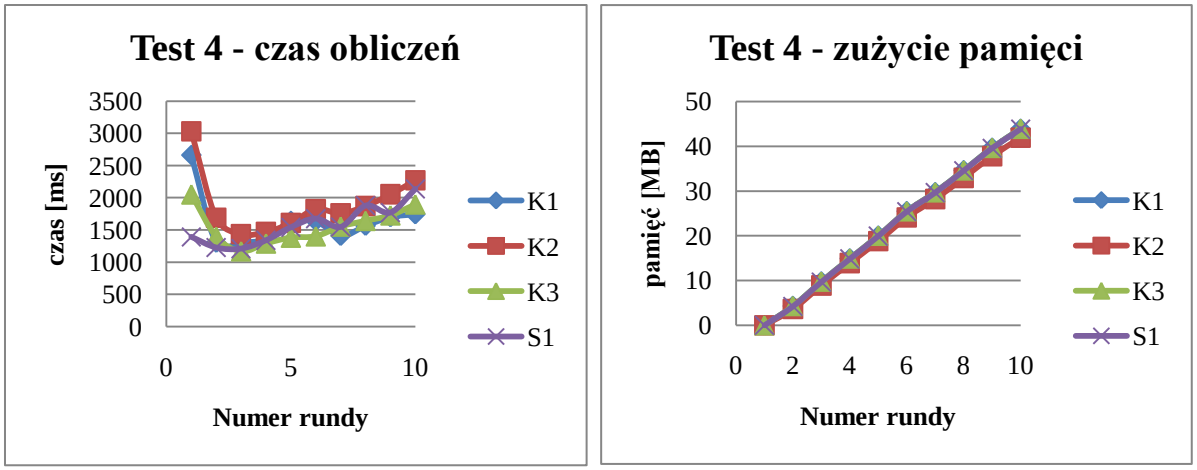
Tabela 4.4: Opis testów nr 3-8 (źródło: opracowanie własne)

Numer testu	3-8
Dane wejściowe – test 3	Zbiór 1000 M_i (średnio 0,1 M_i/P_{id_p} na rundę) w 10 rundach o rozmiarze 100 M_i
Dane wejściowe – test 4	Zbiór 10 000 M_i (średnio 1 M_i/P_{id_p} na rundę) w 10 rundach o rozmiarze 1000 M_i
Dane wejściowe – test 5	Zbiór 100 000 M_i (średnio 10 M_i/P_{id_p} na rundę) w 10 rundach o rozmiarze 10 000 M_i
Dane wejściowe – test 6	Zbiór 1000 M_i (średnio 0,01 M_i/P_{id_p} na rundę) w 10 rundach o rozmiarze 100 M_i
Dane wejściowe – test 7	Zbiór 10 000 M_i (średnio 0,1 M_i/P_{id_p} na rundę) w 10 rundach o rozmiarze 1000 M_i
Dane wejściowe – test 8	Zbiór 100 000 M_i (średnio 1 M_i/P_{id_p} na rundę) w 10 rundach o rozmiarze 10000 M_i
Dane wyjściowe	Zaktualizowane RPR o wejściowe M_i
Konfiguracja urządzeń testowych	K1 lub K2 lub K3 lub S1 używane do uruchomienia algorytmu; S1 używane jak serwer z Bazą RPR; S2 jako serwer z usługą znacznika czasu;
Cel testu	Sprawdzenie wydajności działania dla danych wejściowych o różnym rozmiarze rundy współczynniku i liczby M_i/P_{id_p} na rundę.
Kod wymagania wg Tab. 1.1 i 1.2	Nie dotyczy
Oczekiwany wynik	Wraz ze wzrostem rozmiaru rundy czas obliczeń jak i pamięć będzie wzrastała liniowo; czym większy M_i/P_{id_p} tym czas wykonania algorytmu powinien być większy.

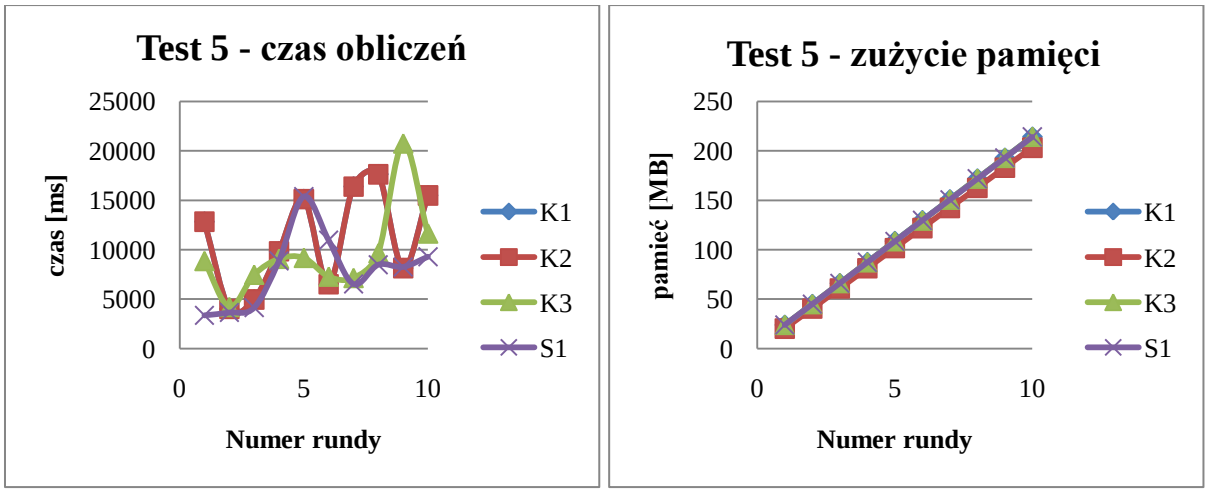




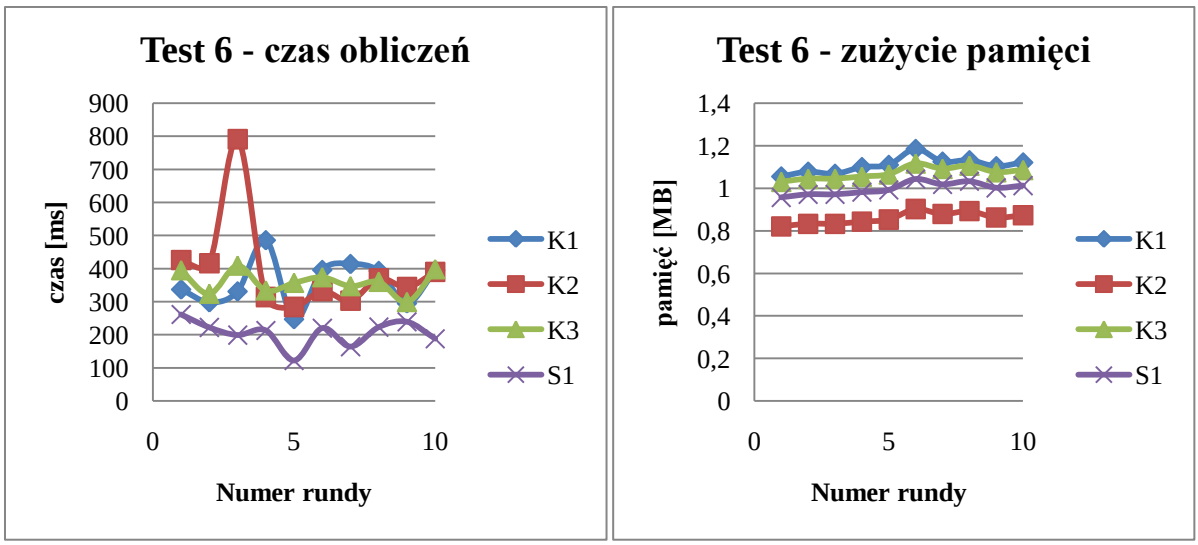
Rysunek 4.6: Wyniki testu nr 3 (źródło: opracowanie własne)



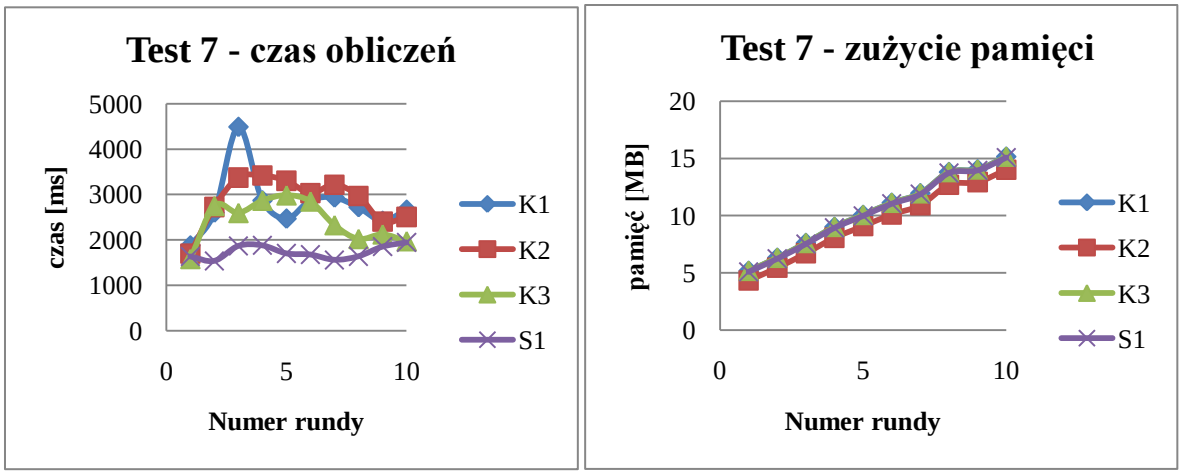
Rysunek 4.7: Wyniki testu nr 4 (źródło: opracowanie własne)



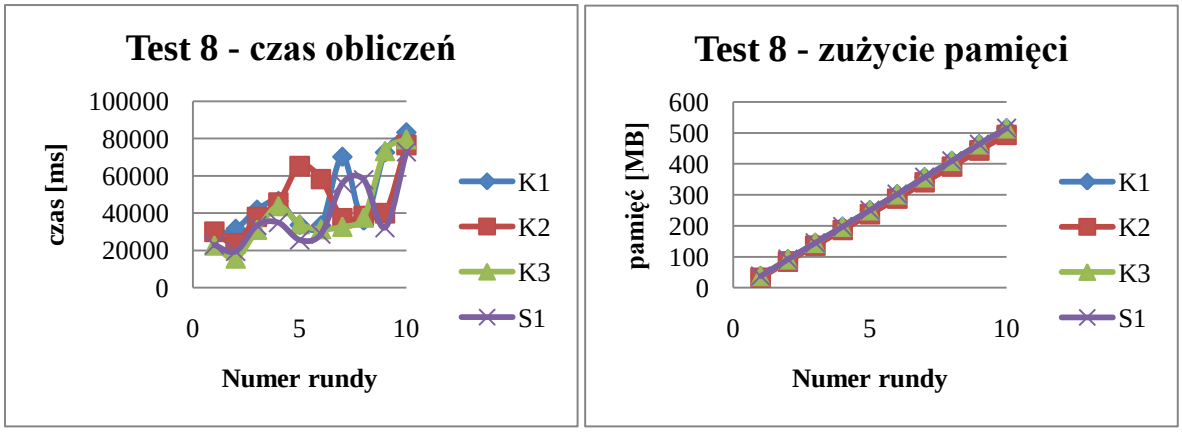
Rysunek 4.8: Wyniki testu nr 5 (źródło: opracowanie własne)



Rysunek 4.9: Wyniki testu nr 6 (źródło: opracowanie własne)



Rysunek 4.10: Wyniki testu nr 7 (źródło: opracowanie własne)



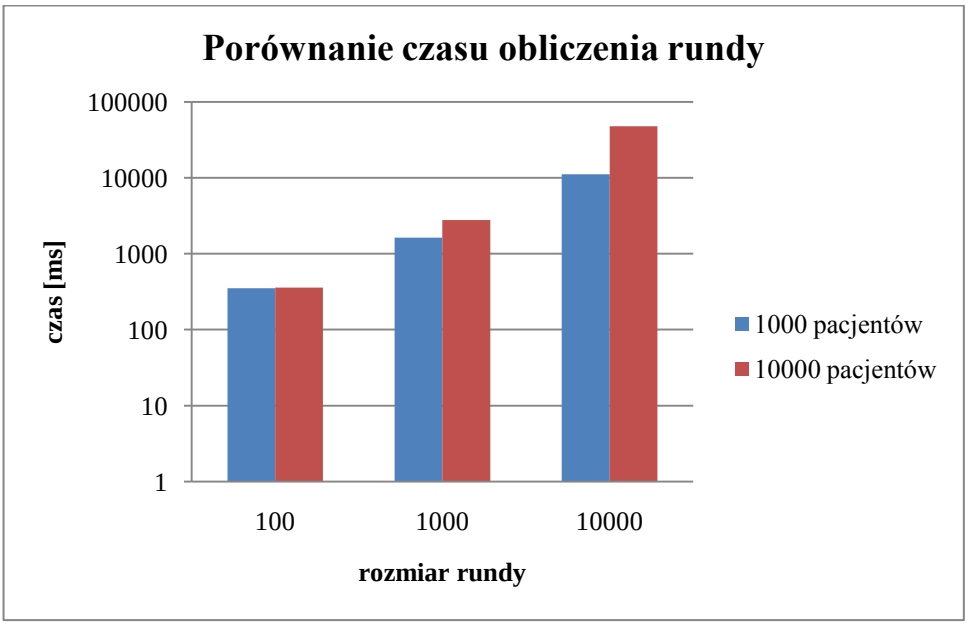
Rysunek 4.11: Wyniki testu nr 8 (źródło: opracowanie własne)

Na początku testów 3-8 każdy RPR był pusty. Wraz z dodawaniem kolejnych wpisów, zwiększa się wykorzystywana pamięć, ponieważ zwiększa się rozmiar RPR pobieranych z bazy. Pobrane pliki XML są podczas wykonania algorytmu przechowywane w pamięci, na którą wzrasta zapotrzebowanie wraz z ilością i rozmiarem RPR. Porównując wyniki testów 4 i 8, w których przypada średnio 1 M_i na pacjenta na rundę, można zauważyć, że rozmiar używanej pamięci jest proporcjonalny do rozmiaru rundy, a tym samym proporcjonalny do wielkości RPR.

Czas wykonania AARPR jest związany z wielkością rundy. Do czasu wykonania rundy jest wliczony czas konieczny do pobrania i wysłania RPR z Bazy RPR. Dla rundy posiadającej 100 M_i na wejściu potrzeba od 100 do 500ms. Dla 1000 M_i – pomiędzy 1 a 4s, a dla 10000 M_i pomiędzy 4 a 80s. Fluktuacje czasu obliczeń powoduje transmisja danych z serwerem zawierającym Bazę RPR (pomimo, że test został przeprowadzony na odseparowanej fizycznie sieci, z wyłączonymi wszystkimi usługami na serwerach poza tymi wykorzystywanymi w testach).

Na Rys. 4.12 zestawiono średni czas wykonania algorytmu z testów 3-8 (skala logarytmiczna). Czas obliczeń jest mniejszy w przypadku, gdy w rundzie więcej dokumentów przypada na jednego pacjenta. Algorytm jest najszybciej wykonywany w teście w którym

M_i / P_{id_p} = 10. Uzyskane wyniki pokrywają się z wynikami oczekiwanymi przed wykonaniem testów.

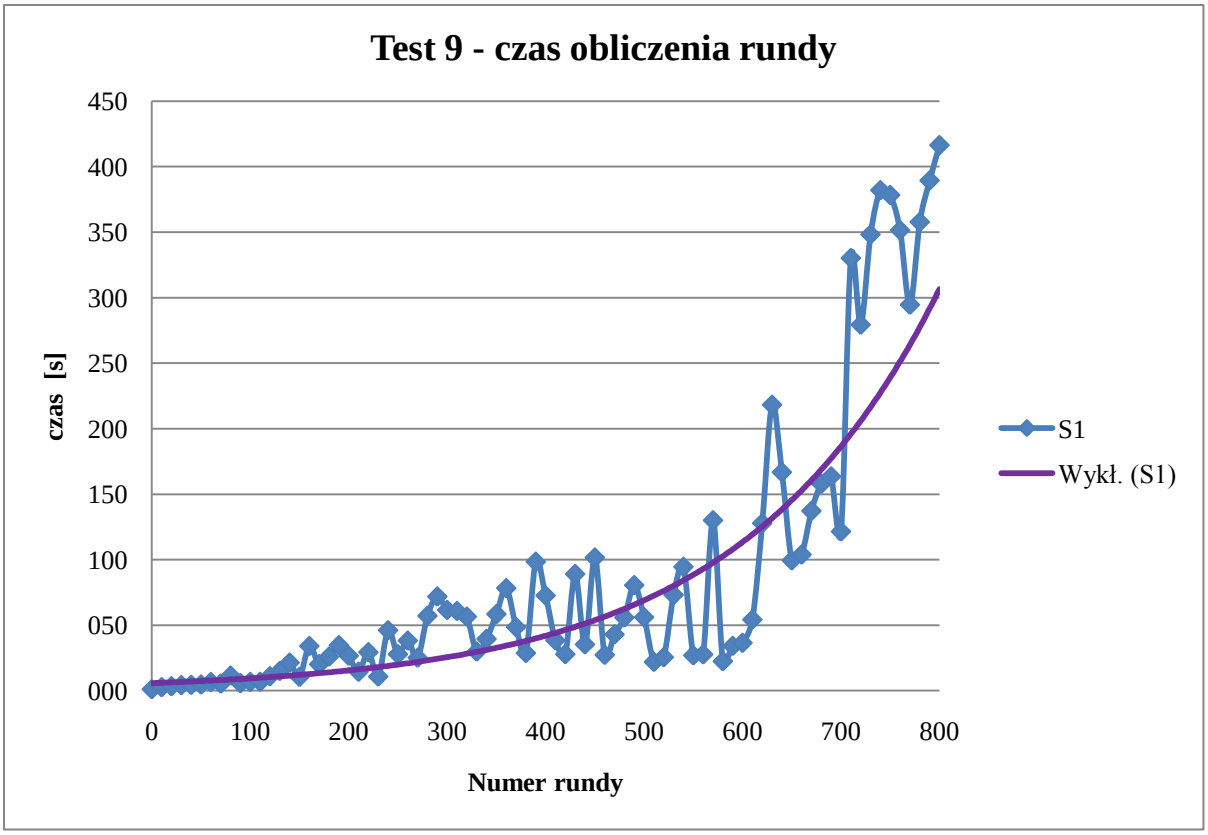


Rysunek 4.12: Porównanie czasu obliczenia rundy (źródło: opracowanie własne)

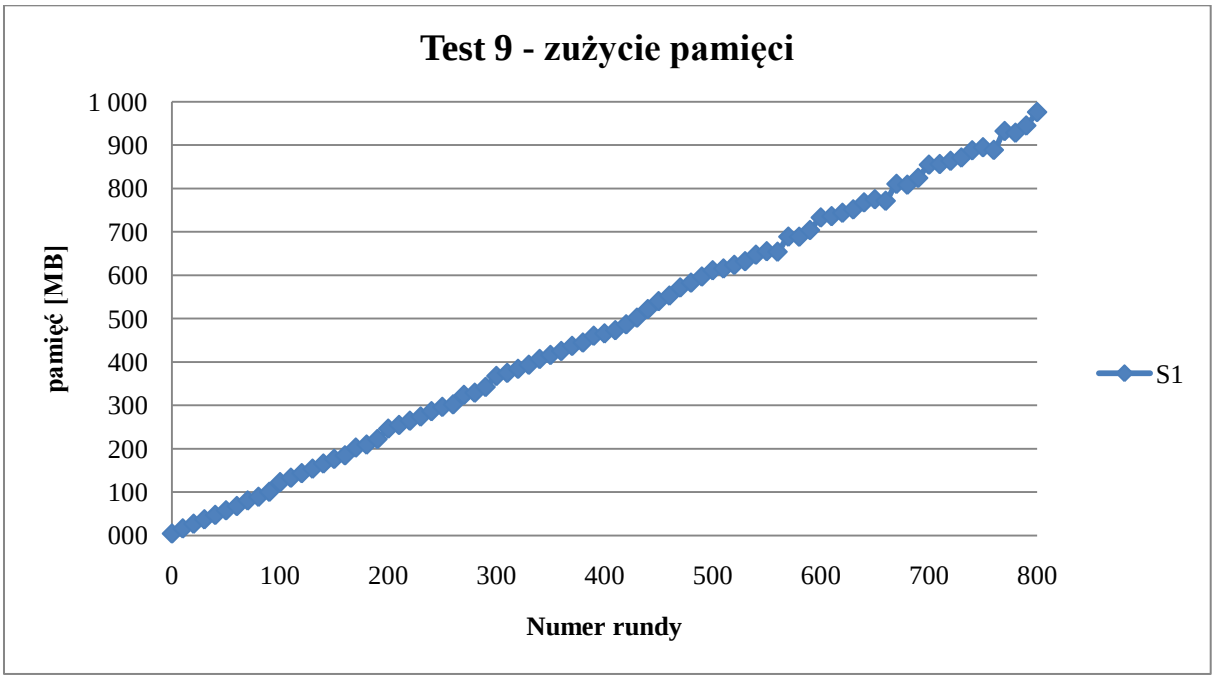
W celu sprawdzenia skalowalności algorytmu dla bardzo dużej ilości danych wejściowych przeprowadzono testy algorytmu używając implementacji algorytmu operującej na całych plikach RPR i na implementacji używającej RPR zapisanego w bazie w postaci tabel.

Tabela 4.5: Opis testu nr 9 (źródło: opracowanie własne)

Numer testu	**9**
Dane wejściowe	Zbiór 800 000 M_i (średnio 0,1 M_i / P_{id_p} na rundach) w 800 rundach o rozmiarze 1000 M_i
Dane wyjściowe	Zaktualizowane RPR'ów o wejściowe M_i
Konfiguracja urządzeń testowych	S1 używany do uruchomienia algorytmu i jako serwer z Bazą RPR, S2 jako serwer z usługą znacznika czasu
Cel testu	Sprawdzenie skalowalności rozwiązania dla dużej ilości danych algorytmu operującego na RPR zapisanych w postaci plików XML w bazie danych.
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania algorytmu i zapotrzebowanie na pamięć dla kolejnej rundy będzie rosło liniowo.



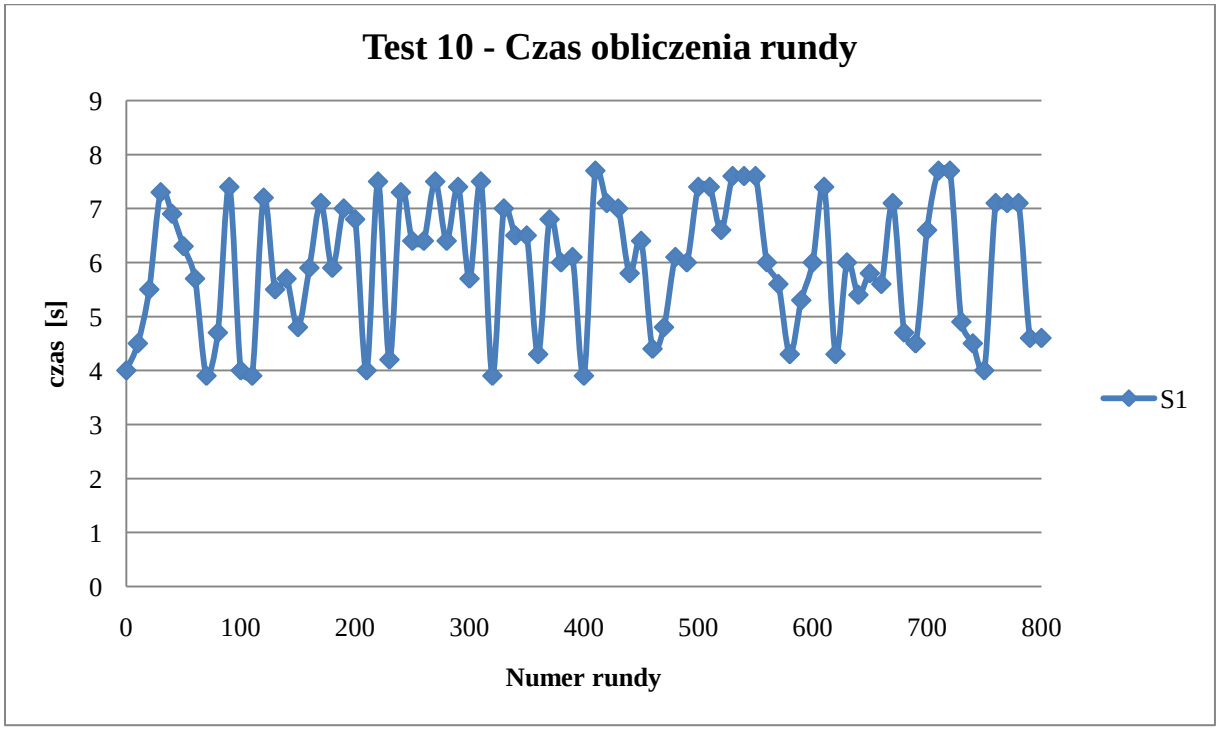
Rysunek 4.13: Wyniki testu nr 9 - czas obliczeń (źródło: opracowanie własne)



Rysunek 4.14: Wyniki testu nr 9 - zapotrzebowanie na pamięć (źródło: opracowanie własne)

Tabela 4.6: Opis testu nr 10 (źródło: opracowanie własne)

Numer testu	**10**
Dane wejściowe	Zbiór 800 000 M_i (średnio 0,1 M_i/ P_{id_p} na rundach) w 800 rundach o rozmiarze 1000 M_i
Dane wyjściowe	Zaktualizowane RPR'ów o wejściowe M_i
Konfiguracja urządzeń testowych	S1 używany do uruchomienia algorytmu i jako serwer z Bazą RPR, S2 jako serwer z usługą znacznika czasu
Cel testu	Sprawdzenie skalowalności rozwiązania dla dużej ilości danych algorytmu operującego na RPR zapisanych w bazie danych w postaci rekordów w tabelach.
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania algorytmu i dla kolejnej rundy będzie stały.



Rysunek 4.15: Wyniki testu 10 – czas obliczeń (źródło: opracowanie własne)

W teście nr 9 (Tab. 4.5, Rys. 4.13, Rys. 4.14) zasymulowano działanie algorytmu AARPR w przypadku, gdy na wejściu jest zbiór 800 000 M_i (dotyczących 10000 różnych P_{id_p}). Łączny rozmiar 10 000 wyjściowych plików XML z RPR wyniósł 301 MB. Wynik oczekiwany zakładał liniowy wzrost, jednak pomiar czasu wykazał wykładniczy wzrost czasu obliczeń, co powoduje, że taka implementacja nie nadaje się do rzeczywistych rozwiązań. Wynik testu nr 10 (Tab. 4.5, Rys. 4.15) potwierdzają, że zapisanie RPR w postaci rekordów w

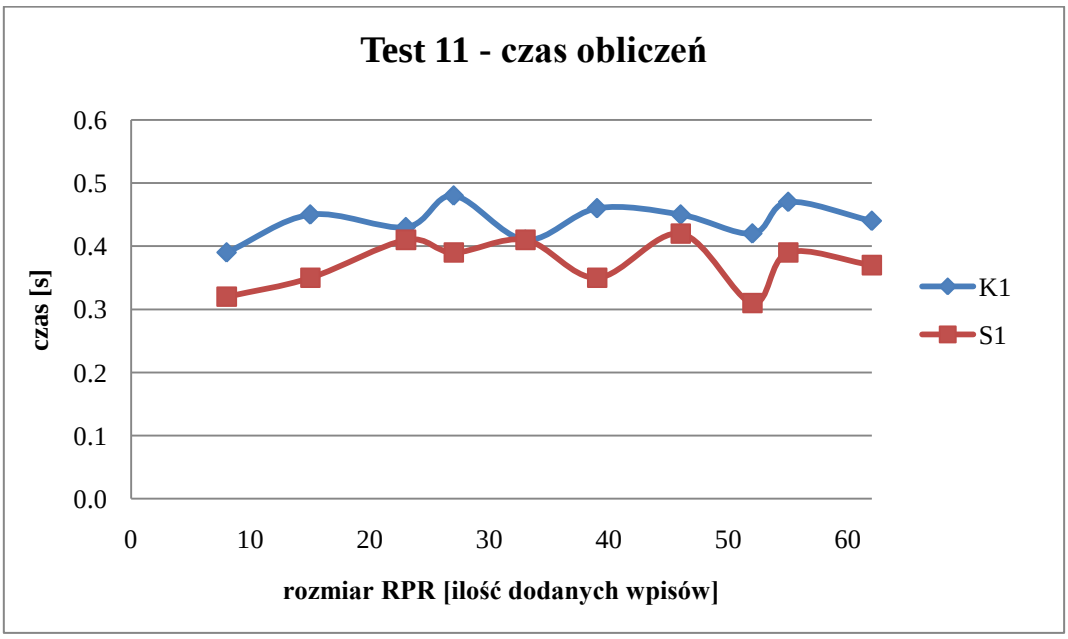
tabelach na poziomie granulacji, który powoduje, że są pobierane tylko konieczne dane, sprawia, że średni czas wykonania kolejnych rund jest stały. Większość czasu wykonania zajmuje transfer danych z/do bazy.

4.1.4.2 Algorytm APWATS

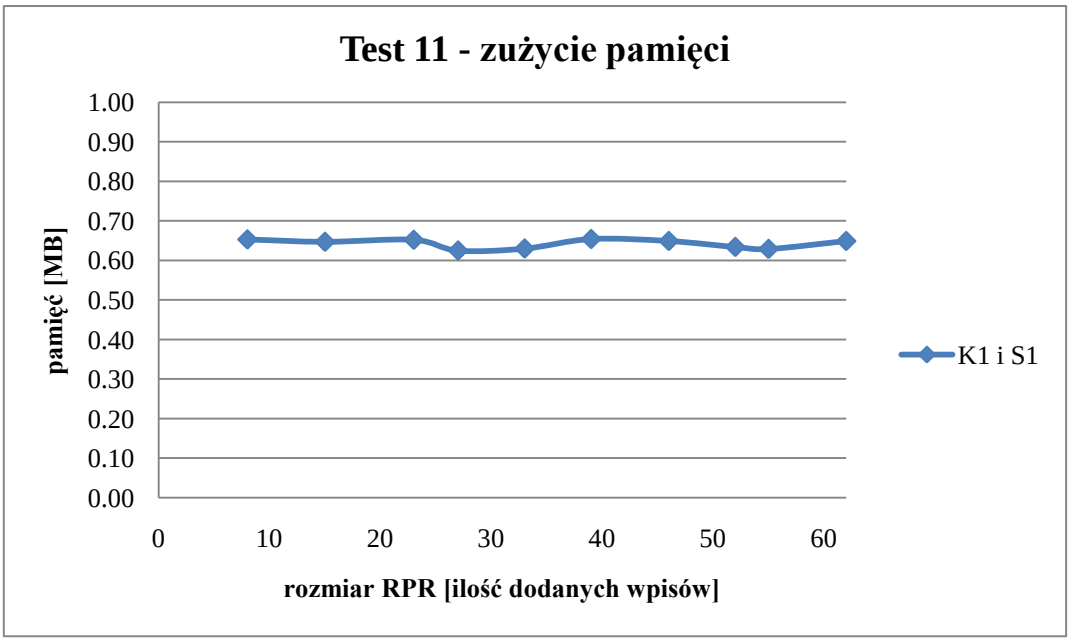
W celu przetestowania algorytmu APWATS został zaprojektowany test nr 11 (szczegóły patrz Tab. 4.7). Na wejściu programu implementującego algorytm znajdują się RPR o różnym rozmiarze tj. zawierające poświadczenia dla różnej ilości wpisów w rejestrze. Spodziewane wyniki wydajności działania powinny być zbliżone do algorytmu AARPR. Program pobiera z bazy danych zawsze tylko poszczególne rekordy, które konieczne są do przeprowadzenia obliczeń.

Tabela 4.7: Opis testu nr 11 (źródło: opracowanie własne)

Numer testu	**11**
Dane wejściowe	1000 RPR z Bazy RPR o rozmiarze od 8 do 62 dodanych wpisów
Dane wyjściowe	Zaktualizowane RPR'ów w bazie RPR
Konfiguracja urządzeń testowych	S1 i K1 używany do uruchomienia algorytmu; S1 jako serwer z Bazą RPR; S2 jako serwer z usługą znacznika czasu;
Cel testu	Sprawdzenie czasu wykonania algorytmu oraz zapotrzebowania na pamięć.
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania algorytmu dla kolejnej rundy będzie stały. Zużycie pamięci będzie stałe. Z uwagi na duże podobieństwo do algorytmu AARPR wyniki szybkości działania powinny być zbliżone.



Rysunek 4.16: Wyniki testu nr 10 – czas obliczeń (źródło: opracowanie własne)



Rysunek 4.17: Wyniki testu nr 10 - zapotrzebowanie na pamięć (źródło: opracowanie własne)

Wyniki testów zgadzają się z wynikami oczekiwanymi przed przeprowadzeniem testu i pokazują, że zapotrzebowanie na pamięć jest stałe oraz średni czas wykonania rundy obliczeń jest stały i niezależny od rozmiaru RPR.

4.1.5 Algorytmy weryfikacji

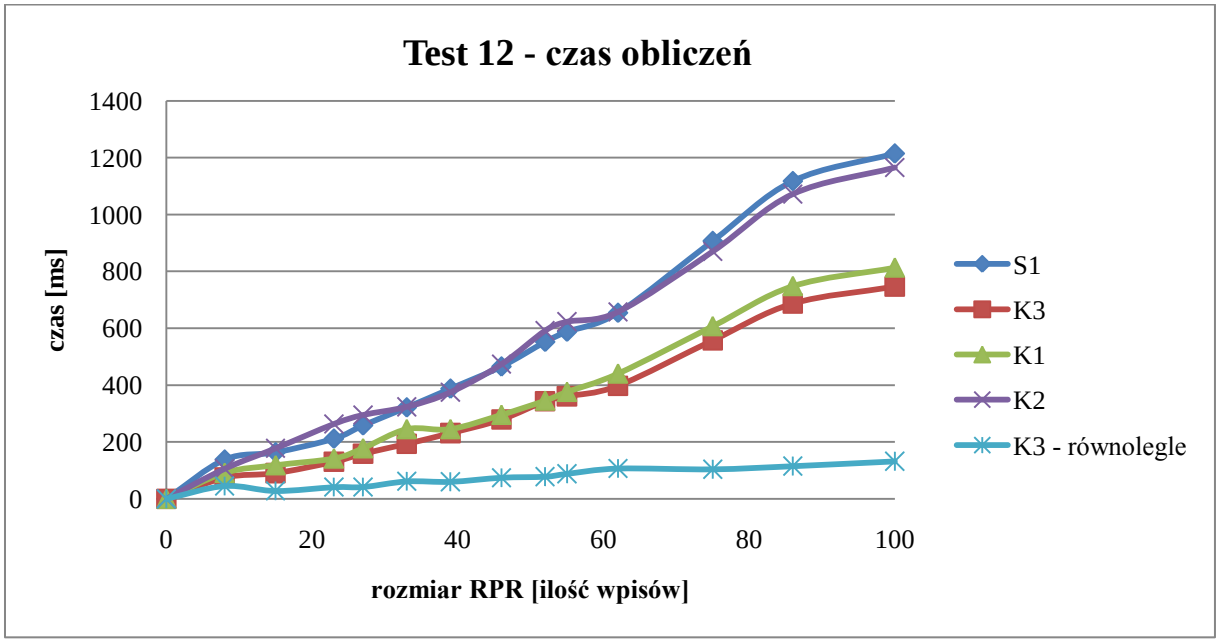
4.1.5.1 Algorytmy AWNR i AWNEHR

W celu sprawdzenia czasu wykonania algorytmu AWAR został przygotowany test nr 12 (Tab. 4.8), w którym zmierzono czas obliczeń dla RPR zawierających różną liczbę wpisów. Wyniki testu zawarte na Rys. 4.18 pokazują, że czas obliczeń dla RPR zawierającego 100 wpisów wynosi, w zależności od komputera, od 700ms do 1200ms, co jest bardzo dobrym czasem świadczącym, że algorytm nadaje się do praktycznego zastosowania. Analiza algorytmu wykazała, że większość czasu zajmuje weryfikacja znaczników czasu (tj. podpisów cyfrowych). Wersja równoległa algorytmu (zrównoleglona weryfikacja znaczników czasu) dla RPR o rozmiarze 100 wpisów wynosi ok. 150ms

Algorytm AWNEHR wymaga wykonania algorytmu AWAR i obliczenia skrótów z dokumentów wchodzących w skład EHR, które następnie należy porównać ze skrótami zawartymi w metadanych znajdujących się w rejestrach. Z uwagi na to, że obliczanie skrótu z dokumentów jest szybką operacją, np. dla pliku 1MB – 7ms (a większość dokumentów wchodzących w skład EHR to dokumenty tekstowe), czas wykonania AWNEHR będzie tylko trochę dłuższy od algorytmu AWAR.

Tabela 4.8: Opis testu nr 12 (źródło: opracowanie własne)

Numer testu	**12**
Dane wejściowe	RPR o rozmiarze od 8 do 100 dodanych wpisów (średnio 1,3 podpisu na rundę)
Dane wyjściowe	Wynik weryfikacji niezaprzeczalności metadanych w rejestrach (prawda/fałsz).
Konfiguracja urządzeń testowych	S1, K1, K2 ,K3 używane do uruchomienia algorytmu; S2 jako serwer z Centrum Informacji Długoterminowej
Cel testu	Sprawdzenie czasu wykonania algorytmu AWAR.
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania algorytmu będzie rósł liniowo wraz ze wzrostem rozmiaru RPR.



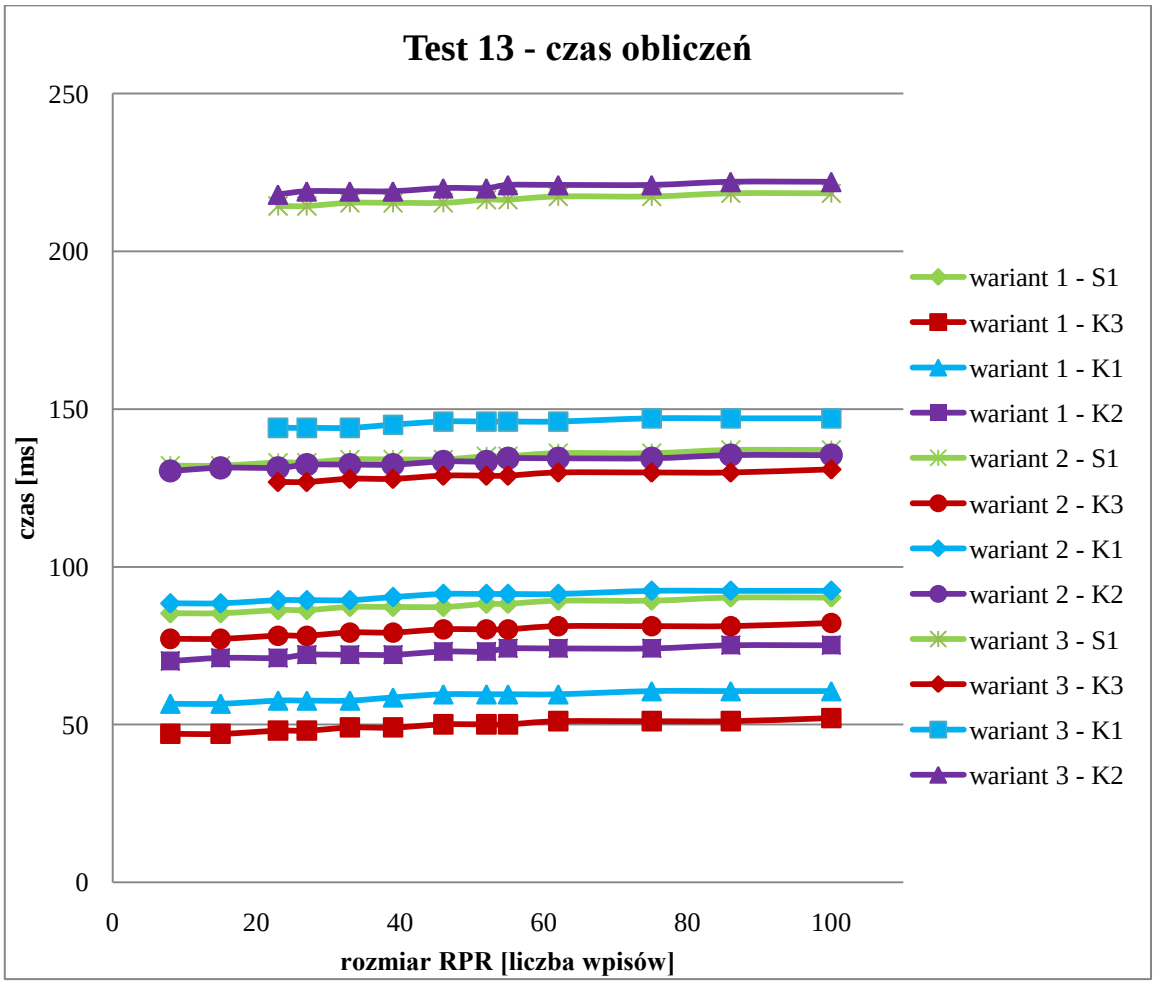
Rysunek 4.18: Wyniki testu nr 12 (źródło: opracowanie własne)

4.1.5.2 Algorytm AWND

Algorytm AWND został przetestowany dla trzech wariantów (dokładny opis Tab. 4.9). Wyniki zawarte na wykresie (Rys. 4.19) pokazują, że czas obliczeń w zależności od wariantu waha się pomiędzy 50ms a 250ms i jest zgodny z wynikami zakładanymi przed wykonaniem testu.

Tabela 4.9: Opis testu nr 13 (źródło: opracowanie własne)

Numer testu	**13**
Dane wejściowe	RPR o rozmiarze od 8 do 100 dodanych wpisów w ciągu 20 lat (średnio 1,3 podpisu na rundę), D_i do weryfikacji którego używany jest W_j z RPR, 3 warianty: 1. Wariant najlepszy – W_j został dodany w ciągu ostatniego roku 2. Wariant średni – W_j został dodany 10 lat temu 3. Wariant najgorszy – W_j został dodany 20 lat temu
Dane wyjściowe	Wynik weryfikacji niezaprzeczalności dokumentu D_i wchodzącego w skład EHR (prawda/fałsz)
Konfiguracja urządzeń testowych	S1, K1, K2 ,K3 używane do uruchomienia algorytmu; S2 jako serwer z Centrum Informacji Długoterminowej;
Cel testu	Sprawdzenie czasu wykonania algorytmu AWND dla weryfikacji dokumentów składowych dodanych do RPR w różnych momentach czasu.
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania algorytmu będzie dłuższy im wcześniej dokument został dodany do EHR.



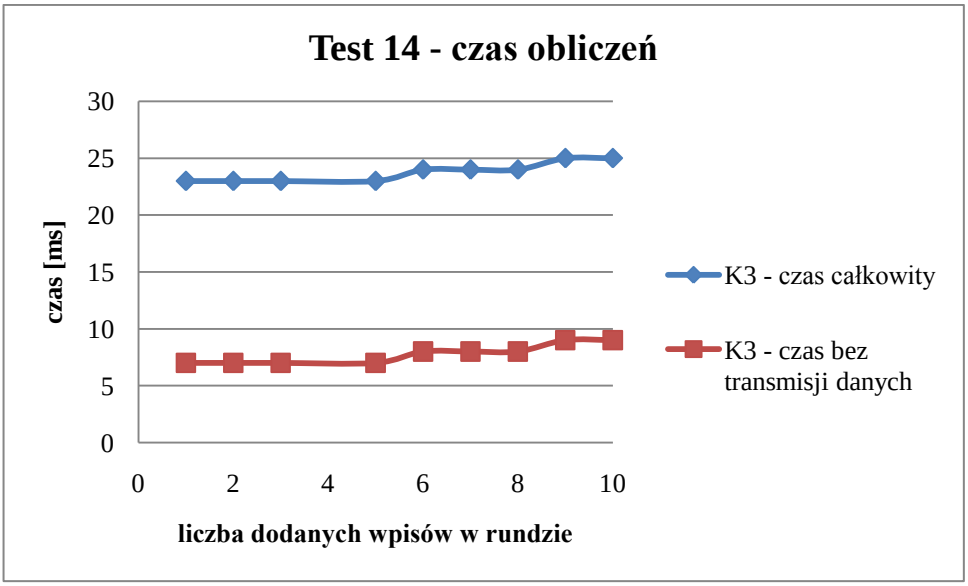
Rysunek 4.19: Wyniki testu nr 13 (źródło: opracowanie własne)

4.1.6 Algorytmy tworzenia i weryfikacji tokenu nadania

Wyniki testów nr 14 i 15 (Tab. 4.10, Tab. 4.11, Rys. 4.20, 4.21) sprawdzające działanie algorytmów tworzenia i weryfikacji tokenów pokazują, że czas ich wykonania wynosi poniżej 50ms co pokazuje, że szybkość działania algorytmów jest zgodna z oczekiwaną.

Tabela 4.10: Opis testu nr 14 (źródło: opracowanie własne)

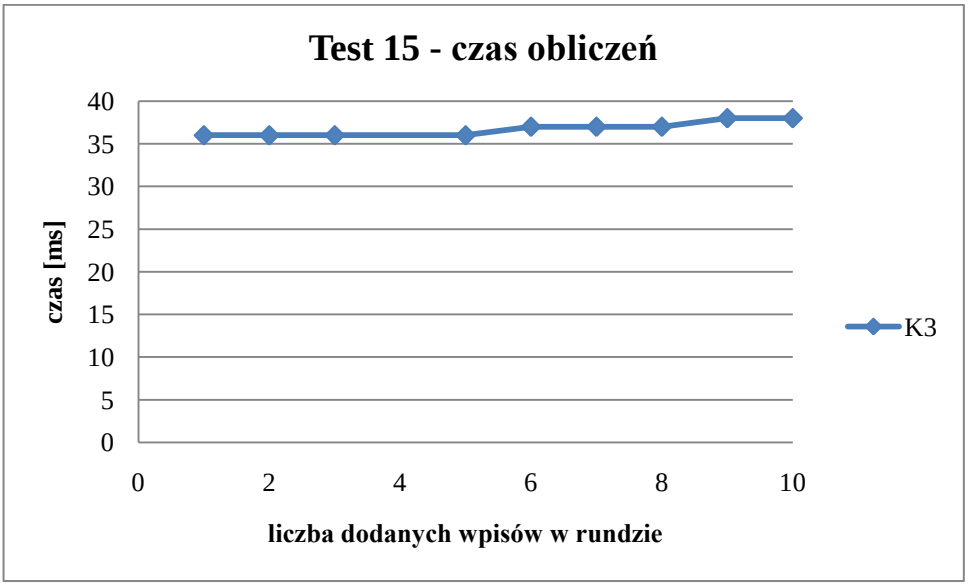
Numer testu	**14**
Dane wejściowe	Od 1 do 10 M_i oraz RPR
Dane wyjściowe	Token
Konfiguracja urządzeń testowych	K3 używany do uruchomienia algorytmu
Cel testu	Sprawdzenie czasu wykonania algorytmu ATTPN
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania będzie liczony w milisekundach i utworzenie tokenu zawierającego potwierdzenie nadania kilku dokumentów naraz będzie tylko nieznacznie wolniejsze niż dla jednego dokumentu.



Rysunek 4.20: Wyniki testu nr 14 (źródło: opracowanie własne)

Tabela 4.11: Opis testu nr 15 (źródło: opracowanie własne)

Numer testu	**15**
Dane wejściowe	Token i RPR
Dane wyjściowe	Wynik weryfikacji (prawda/fałsz)
Konfiguracja urządzeń testowych	K3 używany do uruchomienia algorytmu, S2 jako serwer z Centrum Informacji Długoterminowej
Cel testu	Sprawdzenie czasu wykonania algorytmu AWTPN
Kod wymagania wg Tab. 1.1 i 1.2	PRO2.7: Skalowalność
Oczekiwany wynik	Czas wykonania będzie tylko nieznacznie wolniejszy dla tokenów potwierdzających naraz kilka dokumentów.



Rysunek 4.21: Wyniki testu nr 15 (źródło: opracowanie własne)

4.2. Testy bezpieczeństwa

W Tab. 4.12 zebrano zagrożenia bezpieczeństwa. Każdemu zagrożeniu został przyporządkowany kolejny kod oraz zostały wypisane możliwe ataki. W dalszej części rozdziału zostały zaprezentowane wyniki testów bezpieczeństwa, mające na celu sprawdzenie, czy proponowana metoda będzie odporna na ataki z Tab. 4.12. Testy bezpieczeństwa zostały wykonane z użyciem implementacji poszczególnych działań składowych metody z rozdz. 4.1.1.

Tabela 4.12: Zagrożenia (źródło: opracowanie własne)

Nazwa zagrożenia	Kod zagrożenia	Opis zagrożenia	Ataki
Zniekształcenie dokumentu	ZG1	Przypadkowe lub celowe zniekształcenie dokumentu D_i w repozytorium powodujące przekłamanie dokumentu.	ATK11 – zamiana jednego bajtu w dokumencie; ATK12 – dodanie dodatkowego bajtu do dokumentu; ATK13 – usunięcie bajtu danych z dokumentu;
Usunięcie dokumentu	ZG2	Przypadkowe lub celowe usunięcie dokumentu D_i z repozytorium.	ATK21 – usunięcie dokumentu z repozytorium;
Dodanie dokumentu	ZG3	Celowe dodanie dokumentu D_i bezpośrednio do repozytorium.	ATK31 – dodanie dodatkowego dokumentu do repozytorium;
Zniekształcenie metadanych	ZG4	Przypadkowe lub celowe zniekształcenie metadanych M_i z rejestru.	ATK41 – usunięcie jednej właściwości z metadanych; ATK42 – zamiana jednego bajtu; ATK43 – zamiana URI; ATK44 – zamiana daty dodania; ATK45 – zamiana ID pacjenta; ATK46 – dodanie dodatkowej właściwości do metadanych;
Usunięcie metadanych	ZG5	Przypadkowe lub celowe usunięcie metadanych M_i z rejestru.	ATK51 – usunięcie metadanych z rejestru;

Dodanie metadanych	ZG6	Celowe dodanie fałszywych metadanych M_i bezpośrednio do rejestru.	ATK61 – dodanie fałszywych metadanych do rejestru;
Modyfikacja RPR	ZG7	Przypadkowa lub celowa modyfikacja RPR	ATK71 – usunięcie rekordu z bazy RPR; ATK72 – zmiana w rekordzie w bazie RPR; ATK73 – dodanie dodatkowego rekordu do bazy RPR;
Antydatowanie dokumentu	ZG8	Przypadkowe lub celowe przesłanie do systemu EHR D_i z wsteczną datą.	ATK81 – przesłanie do systemu EHR dokumentu z datą przez 10 lat;
Nieprawidłowy podpis	ZG9	Przypadkowe lub celowe przesłanie do systemu EHR dokumentu nie posiadającego prawidłowego podpisu cyfrowego twórcy	ATK91 – przesłanie do systemu niepodpisanego dokumentu; ATK92 – przesłanie do systemu dokumentu z niepoprawnym podpisem; ATK93 – przesłanie do systemu dokumentu z podpisem cyfrowym wydanym przez niezaufany organ certyfikacji; ATK94 – przesłanie do systemu dokumentu z podpisem cyfrowym utworzonym z wykorzystaniem algorytmów uznawanych za niespełniające wymagań bezpieczeństwa;

W celu wykazania niezaprzeczalności pochodzenia poszczególnych dokumentów składowych należy wykazać, że dokumenty są oryginalne i niezmienione. W tabelach 4.13 do 4.16 zebrano opisy i wyniki testów bezpieczeństwa realizujących ataki na dokumenty składowe znajdujące się w repozytorium.

Tabela 4.13: Test bezpieczeństwa nr 1 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB01
Opis testu	W dokumencie znajdującym się w repozytorium został zmieniony jeden bajt. Następnie, zostały uruchomione programy implementujące algorytmy AWNEHR i AWND.
Realizowany atak	ATK11
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy zmiana zostanie wykryta.
Kod wymagania wg Tab. 1.1 i 1.2	NZP1.1, NZP1.2, NZO1.1, NZO1.2, PRS4.1
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWND zwrócił błąd w linijce kodu odpowiadającej krokowi 2: M_i->$H_{\underline{\underline{D}}}$ =$H(D_i)$; Algorytm AWNEHR zwrócił błąd w linii kodu odpowiadającej krokowi 3.3: *Sprawdź czy* $H_d = H_d'$.

Tabela 4.14: Test bezpieczeństwa nr 2 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB02
Opis testu	Do dokumentu znajdującego się w repozytorium został dodany jeden bajt. Następnie, zostały uruchomione programy implementujące algorytmy AWNEHR i AWND.
Realizowany atak	ATK12
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy dodanie danych do dokumentu zostanie wykryte.
Kod wymagania wg Tab. 1.1 i 1.2	NZP1.1, NZP1.2, NZO1.1, NZO1.2, PRS4.1
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWND zwrócił błąd w linijce kodu odpowiadającej krokowi 2: M_i->$H_{\underline{\underline{D}}}$ =$H(D_i)$; Algorytm AWNEHR zwrócił błąd w linii kodu odpowiadającej krokowi 3.3: *Sprawdź czy* $H_d = H_d'$.

Tabela 4.15: Test bezpieczeństwa nr 3 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB03
Opis testu	Z dokumentu znajdującego się w repozytorium został usunięty jeden bajt. Następnie, zostały uruchomione programy implementujące algorytmy AWNEHR i AWND.
Realizowany atak	ATK13
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy usunięcie danych z dokumentu zostanie wykryte.
Kod wymagania wg Tab. 1.1 i 1.2	NZP1.1, NZP1.2, NZO1.1, NZO1.2, PRS4.1
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWND zwrócił błąd w linijce kodu odpowiadającej krokowi 2: M_i->$H_{\underline{D}}$ =$H(D_i)$; Algorytm AWNEHR zwrócił błąd w linii kodu odpowiadającej krokowi 3.3: *Sprawdź czy* $H_d = H_d'$.

Tabela 4.16: Test bezpieczeństwa nr 4 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB04
Opis testu	Z repozytorium został usunięty dokument.
Realizowany atak	ATK21
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy usunięcie dokumentu zostanie wykryte.
Kod wymagania wg Tab. 1.1 i 1.2	NZP1.1, NZP1.2, NZO1.1, NZO1.2, PRS4.1
Wynik oczekiwany i uzyskany	Pobranie dokumentu składowego z repozytorium Atak jest nieskuteczny: Algorytm AWNEHR zwrócił błąd w linii kodu odpowiadającej krokowi 4, wskazując na brakujący dokument: *Sprawdź czy wszystkie* M_i *z* ZM_{id_p} *zostały wykorzystane, jeżeli nie to zwróć błąd*;

Tabela 4.17: Test bezpieczeństwa nr 5 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB05
Opis testu	Do repozytorium został dodany dodatkowy dokument. Do weryfikacji został przedstawiony EHR wygenerowany z użyciem dodatkowego, sfałszowanego dokumentu składowego.
Realizowany atak	ATK31
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy dokument może zostać dodany bezpośrednio do repozytorium.
Kod wymagania wg Tab. 1.1 i 1.2	NZP1.1, NZP1.2, NZO1.1, NZO1.2, PRS4.1
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWNEHR zwrócił błąd w linii kodu odpowiadającej krokowi 3.2: *Znajdź* $H_d' = ZM_{id_p} \text{->} M_i \text{->} H_d$

Przeprowadzone testy bezpieczeństwa TB01-TB05 wykazały, że ataki ATK11, ATK12, ATK13, ATK21, ATK31 są nieskuteczne.

W celu wykazania autentyczności metadanych w rejestrach należy wykazać, że każda zmiana w metadanych zostanie wykryta. W tabelach 4.18 i 4.19 zebrano opisy i wyniki testów bezpieczeństwa realizujących ataki na metadane znajdujące się w repozytorium.

Tabela 4.18: Test bezpieczeństwa nr 6 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB06
Opis testu	W rejestrze z jednych metadanych M_i, została usunięta jedna właściwość, następnie został zamieniony jeden bajt, URI, data nadania, ID pacjenta, a na końcu została dodana dodatkowa właściwość. Po każdej zmianie został uruchomiony algorytm AWAR i zmiana została cofnięta.
Realizowany atak	ATK41, ATK42, ATK43, ATK44, ATK45, ATK46
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie odporności na zmianę metadanych M_i opisujących dokument składowy w rejestrze.
Kod wymagania wg Tab. 1.1 i 1.2	AUT1.0, NZP1.2, NZO1.1, NZO1.2, PRS4.1, LTA4.4, LTA4.7
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: W każdym przypadku algorytm AWAR zwrócił błąd w linii kodu odpowiadającej krokowi 2.2.1.1.3: *Porównaj obliczone* $Hw_j^{id_p}$ *z* $Hw_j^{id_p}$ *z* R_{rd}*, jeżeli rezultat jest negatywny, zwróć błąd*;

Tabela 4.19: Test bezpieczeństwa nr 7 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB07
Opis testu	Metadane M_i zostały usunięte z rejestru.
Realizowany atak	ATK51;
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy zostanie wykryty brak metadanych.
Kod wymagania wg Tab. 1.1 i 1.2	AUT1.0, NZP1.2, NZO1.1, NZO1.2, PRS4.1, LTA4.4, LTA4.7
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWAR zwrócił błąd braku metadanych w linii kodu odpowiadającej krokowi 2.2.1.1.1: *Oblicz skrót* $Hw_j^{id_p} = H(ZM_{id_p} \text{->} M_i)$*; jeśli* M_i *nie istnieje to zwróć błąd*;

Tabela 4.20: Test bezpieczeństwa nr 8 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB08
Opis testu	Do rejestru zostały dodane fałszywe metadane. Następnie został uruchomiony algorytm AWAR.
Realizowany atak	ATK61
Testowane komponenty	BRPR, SWEHR, CID
Cel testu	Sprawdzenie czy zostanie wykryte dodanie fałszywych metadanych.
Kod wymagania wg Tab. 1.1 i 1.2	AUT1.0, NZP1.2, NZO1.1, NZO1.2, PRS4.1, LTA4.4, LTA4.7
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWNEHR zwrócił błąd w linii kodu odpowiadającej krokowi 2.3: *Sprawdź czy wszystkie* M_i *z* ZM_{id_p} *zostały wykorzystane, jeżeli nie, to zwróć błąd.*

Przeprowadzone testy bezpieczeństwa TB06, TB07, TB08 wykazały, że ataki ATK41-46, ATK51, ATK61 są nieskuteczne.

W tabelach 4.21 do 4.23 zebrano opisy i wyniki testów bezpieczeństwa realizujących ataki na strukturę RPR, mających na celu uniemożliwienie wykrycia próby wstawienia, podmiany lub usunięcia dokumentu składowego.

Tabela 4.21: Test bezpieczeństwa nr 9 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB09
Opis testu	W ramach testu został usunięty rekord z wpisem z RPR symulując próbę modyfikacji RPR w taki sposób, aby nie można było wykazać, że dokument został usunięty.
Realizowany atak	ATK71;
Testowane komponenty	BRPR, MB, SZP, SWEHR
Cel testu	Sprawdzenie odporności na próbę uniemożliwienia wykrycia usunięcia dokumentu.
Kod wymagania wg Tab. 1.1 i 1.2	AUT1.0, NZP1.1, NZP1.2, NZO1.1, NZO1.2, PRS4.1, MEL1.1, MEL2.7, LTA4.4
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWAR zwraca błąd w linii kodu odpowiadającej krokowi 2.2.1.1.10: *Porównaj obliczone* $L_j^{id_p}$ *z* $L_j^{id_p}$ *z Wpisu, jeżeli rezultat jest negatywny, zwróć błąd;*

Tabela 4.22: Test bezpieczeństwa nr 10 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB10
Opis testu	W ramach testu został wstawiony fałszywy rekord z wpisem z RPR symulując próbę modyfikacji RPR w taki sposób, aby potwierdzić wstawienie dokumentu z wsteczną datą.
Realizowany atak	ATK73
Testowane komponenty	BRPR, MB, SZP, SWEHR
Cel testu	Sprawdzenie odporności na próbę uniemożliwienia wykrycia wstawienia fałszywego dokumentu.
Kod wymagania wg Tab. 1.1 i 1.2	AUT1.0, NZP1.2, NZO1.1, NZO1.2, PRS4.1, MEL1.1, MEL2.7, LTA4.4
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWAR zwraca błąd w linii kodu odpowiadającej krokowi 2.2.1.1.10: *Porównaj obliczone* $L_j^{id_p}$ *z* $L_j^{id_p}$ *z Wpisu, jeżeli rezultat jest negatywny, zwróć błąd;*

Tabela 4.23: Test bezpieczeństwa nr 11 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB11
Opis testu	W ramach testu został zmieniony rekord z wpisem z RPR symulując próbę modyfikacji RPR w taki sposób, aby potwierdzić podmianę dokumentu.
Realizowany atak	ATK72
Testowane komponenty	BRPR, MB, SZP, SWEHR
Cel testu	Sprawdzenie odporności na próby uniemożliwienia wykrycia podmiany dokumentu.
Kod wymagania wg Tab. 1.1 i 1.2	AUT1.0, NZP1.2, NZO1.1, NZO1.2, PRS4.1, MEL1.1, MEL2.7, LTA4.4, LTA4.7
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Algorytm AWAR zwraca błąd w linii kodu odpowiadającej krokowi 2.2.1.1.10: *Porównaj obliczone* $L_j^{id_p}$ *z* $L_j^{id_p}$ *z Wpisu, jeżeli rezultat jest negatywny, zwróć błąd;*

Przeprowadzone testy bezpieczeństwa TB09, TB10, TB11 wykazały, że ataki ATK71-43 są nieskuteczne.

W tabelach 4.24 do 4.25 zebrano opisy i wyniki testów bezpieczeństwa realizujących ataki polegające na przesłaniu do systemu EHR dokumentów z wsteczną datą, bez podpisu cyfrowego lub z nieprawidłowym podpisem.

Tabela 4.24: Test bezpieczeństwa nr 12 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB12
Opis testu	Do systemu EHR został przesłany dokument wraz z metadanymi, które zawierają datę przed 10 lat.
Realizowany atak	ATK81;
Testowane komponenty	MB, CID
Cel testu	Sprawdzenie czy metoda wykryje próbę przesłania dokumentu z wsteczną datą.
Kod wymagania wg Tab. 1.1 i 1.2	MEL1.1, MEL2.7
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Protokół PDNW zwrócił błędy w liniach kodu odpowiadających krokom: *2.* UZZ_k *sprawdza poprawność* M_i,

Tabela 4.25: Test bezpieczeństwa nr 13 (źródło: opracowanie własne)

Kod testu bezpieczeństwa	TB13
Opis testu	Do systemu został przesłany: • dokument bez podpisu cyfrowego, • dokument z niepoprawnym matematycznie podpisem, • dokumentu z podpisem cyfrowym wydanym przez niezaufany organ certyfikacji, • dokument z podpisem cyfrowym utworzonym z wykorzystaniem algorytmów uznawanych za niespełniające wymagań bezpieczeństwa.
Realizowany atak	ATK91, ATK92, ATK93, ATK94
Testowane komponenty	MB, CID
Cel testu	Sprawdzenie czy metoda zaakceptuje dokument z niepoprawnym podpisem cyfrowym.
Kod wymagania wg Tab. 1.1 i 1.2	MEL2.7, MEL2.8, MEL2.9
Wynik oczekiwany i uzyskany	Atak jest nieskuteczny: Protokół PDNW zwrócił błędy w liniach kodu odpowiadających krokom: *2.1.: Sprawdź czy podpis cyfrowy jest poprawny pod względem matematycznym* *2.2.: Sprawdź ścieżkę certyfikacji;* *2.3.: Sprawdź listę TSL i LPAK.*

Przeprowadzone testy bezpieczeństwa TB12 i TB13 wykazały, że ataki ATK81 i ATK 91-94 są nieskuteczne. Protokół PDNW wykrył wszystkie próby przesłania dokumentu z nieprawidłowym podpisem lub metadanymi.

W przypadku zaistnienia sporu (przypadek dotyczący niezaprzeczalności odbioru) pomiędzy lekarzem a np. pacjentem, gdy lekarz twierdzi, że przesłał dokument do systemu EHR, a w systemie go nie ma, za pomocą RPR można rozstrzygnąć dany spór. Lekarz nie musi posiadać własnej kopii wysłanego dokumentu. Jeżeli sprawdzenie RPR wykaże, że brakuje dokumentu (jednocześnie pokazując przedział czasowy w którym dokument był dodany), to należy rozstrzygnąć spór na korzyść lekarza i odtworzyć dokument z kopii zapasowej (polityka organizacyjna wymaga replikowanie danych i tworzenie kopii zapasowych). Jeżeli sprawdzenie RPR wykaże, że wszystkie metadane i dokumenty są dostępne i niezmienione (algorytm AWNEHR zwróci pozytywny wynik) to spór należy rozstrzygnąć na korzyść pacjenta.

W przypadku zaistnienia sporu (przypadek niezaprzeczalności pochodzenia) pomiędzy lekarzem a np. pacjentem o zawartość danego dokumentu (np. pacjent twierdzi, że lekarz przepisał mu inną dawkę leku) to, aby rozstrzygnąć spór należy sprawdzić podpis cyfrowy dokumentu. W przypadku, gdy okres ważności certyfikatu powiązanego z podpisem cyfrowym upłynął, należy sprawdzić również znaczniki czasu konserwujące dany podpis, które są zawarte w RPR (algorytm AWND musi zwrócić pozytywny wynik). W przypadku, gdy podpis cyfrowy okaże się poprawny, spór należy rozstrzygnąć na korzyść lekarza, w przeciwnym na korzyść pacjenta.

5. Wnioski i podsumowanie

Głównym celem systemów EHR jest umożliwienie przechowywania i udostępniania uprawnionym podmiotom wszystkich dokumentów zdrowotnych. Duża liczba przetwarzanych dokumentów (liczona w setkach milionów) przekłada się na dużą złożoność systemów EHR. Systemy EHR w porównaniu do systemów przetwarzających inne dokumenty wyróżniają się dużą złożonością, dłuższym zakładanym okresem przechowywania, większą ilością podmiotów mających dostęp do systemu.

W projektowaniu systemów EHR używa się podejścia zorientowanego na pacjenta, czego konsekwencją było stworzenie koncepcji elektronicznego dokumentu zdrowotnego (EHR), który zawiera wszystkie dokumenty zdrowotne danego pacjenta. Do przechowywania dokumentów zdrowotnych używa się repozytoriów, a do ich metadanych rejestrów. Struktura dokumentów medycznych jest opisana w wielu różnych międzynarodowych normach, aby możliwa była interoperacyjność pomiędzy różnymi systemami, czy oprogramowaniem pochodzącym od różnych producentów.

W oparciu o zapytanie wysłane z aplikacji dostępowej lekarza, za pomocą metadanych znajdujących się w rejestrach, wyszukiwane są dokumenty zawarte w repozytoriach i na ich podstawie tworzony jest ekstrakt EHR (zawierający całość lub część EHR), który jest zapisywany w postaci pliku xml o ustandaryzowanej strukturze.

Istnieje dużo standardów dotyczących struktury EHR. Na podstawie struktury systemów EHR w rozprawie zaproponowano architekturę systemu EHR. Przeciwnie do struktury, wymagania bezpieczeństwa są jedynie dokładnie zdefiniowane, a brakuje metod umożliwiających ich zaimplementowanie. Analiza literatury wykazała m. in., że brakuje kompleksowej metody traktującej EHR jako wirtualny kontener oraz brakuje metody sprawdzającej niezaprzeczalność wpisów rejestru/rejestrów zawierających metadane o dokumentach medycznych wchodzących w skład EHR. Proponowana metoda DPEDZ ma na celu wypełnienie tej luki i zagwarantowanie użytkownikowi systemu, że zawartość EHR jest oryginalna i kompletna oraz, że została utworzona we właściwym czasie.

Aby umożliwić weryfikację niezaprzeczalności EHR, autentyczności wpisów (metadanych) w rejestrach oraz niezaprzeczalności pojedynczych dokumentów, została opracowana struktura danych – RPR – służąca do przechowywania poświadczeń. Użytkownik zawsze do weryfikacji otrzymuje plik xml z RPR zawierający dane ze wszystkich stowarzyszonych systemów EHR. Testy wariantów użycia RPR wykazały, że RPR z systemów stowarzyszonych EHR mogą być powiązane z RPR z domowego systemu EHR pacjenta.

Systemy EHR z założenia przechowują elektroniczne dokumenty zdrowotne długoterminowo (dokumenty medyczne pacjenta mogą być skasowane dopiero po jego śmierci). Metoda DPEDZ oraz RPR zostały zaprojektowane tak, aby umożliwić weryfikację niezaprzeczalności i autentyczności EHR po upływie dowolnego okresu czasu. Cel ten został osiągnięty, m. in. przez zastosowanie Centrum Informacji Długoterminowej, które gromadzi informacje o aktualnie zalecanych algorytmach, a także o statusie zaufanych urzędów

znacznika czasu. Z czasem weryfikator może nie mieć informacji o tym, czy poprzednie znaczniki czasu są zaufane. Wtedy może wysłać automatyczne żądanie do Centrum Informacji Długoterminowej będące zaufaną jednostką rządową.

Centrum Informacji Długoterminowej pełni także ważną funkcję związaną z monitorowaniem aktualnego statusu algorytmów i urzędów znacznika czasu. W przypadku, gdy algorytm zostanie przełamany lub jego odporność na ataki typu wyczerpującego (*ang. brute force*) zostania uznana za niewystarczającą lub urząd znacznika czasu zakończy działalność, taka informacja jest wysyłana do Systemu Zarządzania RPR. System Zarządzania RPR może zmienić zestaw używanych algorytmów funkcji skrótu oraz służących do tworzenia podpisu cyfrowego, a następnie uruchomić program implementujący algorytm przedłużania ważności archiwalnych znaczników czasu. Aby zabezpieczyć się przed sytuacją, w której RPR mogą utracić wiarygodność (kompromitacja urzędu znacznika czasu, czy algorytmu) system może tworzyć dwie wersje RPR z różnym zestawem algorytmów i innym wykorzystywanym urzędem znacznika czasu (takie podejście jest również zalecane w specyfikacji ERS).

W badaniach eksperymentalnych został użyty zestaw algorytmów podpisu cyfrowego RSA–SHA512. Ponieważ poszczególne algorytmy wchodzące w skład metody DPEDZ mogą wykorzystywać dowolne (aktualnie uważane za bezpieczne) algorytmy podpisu cyfrowego możliwe jest użycie innych algorytmów np. ECDSA.

System bezpieczeństwa implementujący metodę DPEDZ może być wdrożony przy budowie systemów EHR (np. w Polsce) lub dodany do istniejących systemów jako kolejny komponent zapewniający bezpieczeństwo.

5.1. Odniesienie do tezy

Teza pracy przedstawiona w rozdziale 1 jest następująca: *Opracowanie metody opartej na słownikach uwierzytelnianych i ich wiązaniach umożliwi zapewnienie autentyczności i niezaprzeczalności wirtualnego elektronicznego dokumentu zdrowotnego (EHR) w długim okresie.*

Zgodnie z definicją słownika uwierzytelnianego z rozdz. 2.6.4, słownik uwierzytelniany jest strukturą danych wraz z protokołem do aktualizacji i zapytań, która jest używana przez stronę niezaufaną do udostępniania informacji poświadczonych przez zaufaną stronę. Słownik uwierzytelniany umożliwia umieszczenie informacji w strefie niezaufanej w taki sposób, aby zaufanie do informacji w nim przechowywanych wywodzić jedynie z informacji publicznej dotyczącej zaufanego wystawcy. Struktura RPR została zaprojektowana zgodnie z tym podejściem. Zaufanie do zawartości RPR (a tym samym do zawartości EHR) wywodzi się z zaufania do znaczników czasu wystawianych przez TSA. Działania wchodzące w skład metody DPEDZ umożliwiają aktualizację struktury RPR. Informacje zawarte w RPR umożliwiają natomiast weryfikacje zawartości EHR.

Tabela 5.1: Wymagania bezpieczeństwa w relacji do zagrożeń i testów (źródło: opracowanie własne)

Wymaganie bezpieczeństwa	**Kod komponentu**	**Zagrożenia**	**Testy**
AUT1.0: Autentyczność metadanych	BRPR, MB, SZRPR, SWEHR, CID	ZG4, ZG5, ZG6, ZG7	TB06, TB07, TB08, TB09, TB10, TB11
NZP1.1: Niezaprzeczalność pochodzenia pojedynczego dokumentu	BRPR, MB, SZRPR, SWEHR, CID	ZG1, ZG2, ZG3	TB01, TB02, TB03, TB04, TB05. TB09
NZP1.2: Niezaprzeczalność pochodzenia EHR	BRPR, MB, SZRPR, SWEHR, CID	ZG1, ZG2, ZG3, ZG4, ZG5, ZG6, ZG7	TB01, TB02, TB03, TB04, TB05, TB06, TB07, TB08, TB09, TB10, TB11
NZO1.1: Niezaprzeczalność odbioru pojedynczego dokumentu	BRPR, MB, SZRPR, SWEHR, CID	ZG1, ZG2, ZG3, ZG4, ZG5, ZG6, ZG7	TB01, TB02, TB03, TB04, TB05, TB06, TB07, TB08, TB09, TB10, TB11
NZO1.1: Niezaprzeczalność odbioru EHR	BRPR, MB, SZRPR, SWEHR, CID	ZG1, ZG2, ZG3, ZG4, ZG5, ZG6, ZG7	TB01, TB02, TB03, TB04, TB05, TB06, TB07, TB08, TB09, TB10, TB11
PRO2.7: Skalowalność	BRPR, MB, SZRPR, SWEHR, CID	-	Testy wydajności: 2, 9-15
PRS4.1: Integralność danych	BRPR, MB, SZRPR, SWEHR	ZG1, ZG2, ZG3, ZG4, ZG5, ZG6, ZG7	TB01, TB02, TB03, TB04, TB05, TB06, TB07, TB08, TB09, TB10, TB11
MEL1.1: Wymagania prawne	BRPR, MB, SZRPR, SWEHR, CID	ZG7, ZG8	TB09, TB10, TB11, TB12
MEL2.7: Odpowiedzialność autora I	MB, BRPR, SZRPR, SWEHR, CID	ZG4, ZG5, ZG6, ZG7	TB09, TB10, TB11, TB12, TB13
MEL2.8: Odpowiedzialność autora II	MB	ZG9	TB13
MEL2.9: Atestacja wpisów	MB	ZG9	TB13
LTA4.4 : Poświadczenia	MB, BRPR, SZRPR, SWEHR	ZG4, ZG5, ZG6, ZG7	TB06, TB07, TB08, TB09, TB10, TB11
LTA4.7: Obsługa grup dokumentów	MB, BRPR, SZRPR, SWEHR	ZG4, ZG5, ZG6, ZG7	TB06, TB07, TB08, TB10, TB11

Zaproponowana metoda DPEDZ umożliwia zweryfikowanie w dowolnym momencie wiarygodności wirtualnego, elektronicznego dokumentu zdrowotnego (EHR). W Tab. 5.1 zebrano wymagania bezpieczeństwa postawione w rozdz. 1.2. Każdemu wymaganiu bezpieczeństwa zostały przyporządkowane komponenty systemu EHR implementujące poszczególne działania z metody DPEDZ, które umożliwiają jego realizację oraz możliwe zagrożenia. W celu wykazania odporności na zagrożenia zostały przeprowadzone testy bezpieczeństwa.

Metoda DPEDZ zapewnia niezaprzeczalność EHR, wg definicji z rozdz. 1.2. Niezaprzeczalność EHR jest spełniona, gdy zawartość rejestrów jest autentyczna oraz dokumenty składające się na EHR posiadają właściwość niezaprzeczalności pochodzenia i odbioru. Niezaprzeczalność pochodzenia dokumentów składowych została osiągnięta przez zastosowanie podpisów cyfrowych, które są konserwowane przez zaufane znaczniki czasu. Znacznik czasu zapewniają również niezaprzeczalności odbioru danego dokumentu przez system EHR. Autentyczność rejestrów została osiągnięta przez stworzenie mechanizmu wiązań binarnych pomiędzy wpisami do rejestrów, które wykrywa jakiekolwiek modyfikacje w wpisach w rejestrach oraz dokumentach medycznych składających się na EHR.

5.2. Elementy nowości

Niniejsza rozprawa doktorska zawiera następującą wartość dodaną w stosunku do obecnego stanu wiedzy:

- autorską metodę DPEDZ (rozdz. 3) na którą składają się następujące działania składowe:
    - protokoły PDNW(rozdz. 3.6.1, strona 65) i PSRPR (rozdz. 3.6.6, strona 73);
    - algorytmy tworzenia i aktualizacji RPR – AARPR, APWATS (rozdz. 3.6.3 i 3.6.4, strony 67 i 71);
    - algorytm weryfikacji autentyczności metadanych w rejestrach – AWAR (rozdz. 3.6.7, strona75);
    - algorytm weryfikacji niezaprzeczalności pochodzenia i odbioru EHR – AWNEHR (rozdz. 3.6.8, strona 77);
    - algorytm weryfikacji niezaprzeczalności pochodzenia i odbioru pojedynczego dokumentu wchodzącego w skład EHR – AWND (rozdz. 3.6.9, strona 80);
    - algorytmy tworzenia i weryfikacji tokenów potwierdzenia nadania (rozdz. 3.6.2 i 3.6.5, strony 67 i 73).
- strukturę Rekordów Poświadczeń Rejestrów (RPR) (rozdz. 3.5, strona 61);
- nowy efektywny i odporny na ataki sposób weryfikacji obecności lub braku dokumentu; opracowana metoda pozwala na przechowywanie EHR bez konieczności zaufania do systemu EHR, że zawartość EHR celowo lub przypadkowo nie zostanie zmieniona w nieuprawniony sposób;

- propozycję Centrum Informacji Długoterminowej na potrzeby którego:
    - została opracowana struktura Listy Polecanych Algorytmów Kryptograficznych (LPAK) (rozdz. 3.7.2, strona 83);
    - został opracowany protokół do komunikacji z użytkownikami (rozdz. 3.7.3, strona 84).

W porównaniu do innych rozwiązań metoda DPEDZ wyróżnia się innowacyjną funkcjonalnością, której nie posiadają inne dostępne rozwiązania. Zapewnia niezaprzeczalność każdej z wielu grup dokumentów dotyczących jednego pacjenta dodawanych przez długi okres czasu (szczegóły są przedstawione w rozdz. 3.8). Nowością jest również dostosowanie metody do specyfiki wirtualnego elektronicznego dokumentu zdrowotnego przechowywanego w rejestrach i repozytoriach.

5.3. Dalsze prace

Pacjenci w przypadku wdrażania systemu EHR mogą mieć wiele obaw odnośnie bezpieczeństwa ich danych medycznych. Zapewnienie niezaprzeczalności umożliwia pacjentom zaufać, że ich dokumentacja medyczna jest kompletna i nie zmodyfikowana. Kolejnym ważnym elementem jest stworzenie zaawansowanego systemu zapewniającego poufność EHR. Obecnie poufność w systemach EHR realizuje się poprzez kontrolę dostępu lub poprzez anonimizację (wstawianie anonimowych identyfikatorów i trzymanie mapy identyfikatorów w jedynym bezpiecznym miejscu). Dalsze prace powinny iść w kierunku rozważenia stosowania szyfrowania (co jest metodą dość skomplikowaną ze względu na zarządzania kluczami) oraz informacji biometrycznej. Należy także rozważyć możliwość stosowania przez lekarzy podpisów cyfrowych o zwiększonym bezpieczeństwie wykorzystujących biometrie [91].

6. Odwołania

W pracy znajduje się 51 rysunków, 32 tabel, oraz 108 referencji – w tym 64 do książek i publikacji naukowych (7 do publikacji własnych) oraz 44 do źródeł elektronicznych (m. in. norm, specyfikacji, raportów).

6.1. Spis rysunków

Rysunek 1.1: Wyniki rozprawy doktorskiej na tle systemu EHR ..... - 14 -
Rysunek 2.1: Meta-architektura archetypu ..... - 20 -
Rysunek 2.2: Struktura wysokiego poziomu EHR w openEHR ..... - 21 -
Rysunek 2.3: Hierarchia komponentów modelu referencyjnego EHR_Extract ..... - 23 -
Rysunek 2.4: Diagram hierarchii EHR_Extract ..... - 24 -
Rysunek 2.5: Aktorzy i transakcje w profilu IHE XDS ..... - 30 -
Rysunek 2.6: Tworzenie i weryfikacja podpisu cyfrowego ..... - 37 -
Rysunek 2.7: Tworzenie zaufanego znacznika czasu ..... - 40 -
Rysunek 2.8: Przykład schematu Haber-Stornetta ..... - 41 -
Rysunek 2.9: Ponowne podpisywanie i składanie znacznika czasu dla zbioru dokumentów ..... - 43 -
Rysunek 2.10: Tworzenie podpisów cyfrowych z wykorzystaniem dwóch zestawów algorytmów ..... - 44 -
Rysunek 2.11: Współpracujące TNA i systemy EHR ..... - 45 -
Rysunek 2.12: Kolejne enkapsulacje podpisu i skumulowana notaryzacja ..... - 46 -
Rysunek 2.13: Generowanie znacznika czasu ..... - 47 -
Rysunek 2.14: Struktura obiektu archiwalnego ..... - 48 -
Rysunek 3.1: Ogólna architektura systemu EHR ..... - 55 -
Rysunek 3.2: Środki zabezpieczeń w architekturze systemu EHR ..... - 57 -
Rysunek 3.3: Powiązania pomiędzy oprogramowaniem implementującym algorytmy ..... - 60 -
Rysunek 3.4: Relacje pomiędzy RPR, ZM a dokumentami w repozytoriach ..... - 61 -
Rysunek 3.5: Warianty zastosowania RPR ..... - 62 -
Rysunek 3.6: Struktura Rekordów Poświadczeń Rejestrów ..... - 64 -
Rysunek 3.7: Dodawanie nowych wpisów (dokumentów) do EHR ..... - 66 -
Rysunek 3.8: Przykład działania algorytmu AARPR ..... - 70 -
Rysunek 3.9: Przykład działania algorytmu APWATS ..... - 71 -
Rysunek 3.10: Schemat działania protokołu scalania Rekordów Poświadczeń Rejestrów ..... - 75 -
Rysunek 3.11: Przykład działania algorytmów AWAR i AWNEHR ..... - 79 -
Rysunek 3.12: Przykład działania algorytmu AWND ..... - 81 -
Rysunek 3.13: Schemat Centrum Informacji Długoterminowej ..... - 82 -
Rysunek 3.14: Model logiczny LPAK ..... - 83 -
Rysunek 3.15: Typy wiadomości używanych do komunikacji z CID ..... - 85 -
Rysunek 4.1: Środowisko testowe ..... - 91 -
Rysunek 4.2: Test 1 - czas wykonania ..... - 93 -
Rysunek 4.3: Test 1 - zużycie pamięci ..... - 94 -
Rysunek 4.4: Test 2 - czas obliczeń ..... - 95 -
Rysunek 4.5: Schemat przykładowej bazy danych do przechowywania RPR ..... - 96 -
Rysunek 4.6: Wyniki testu nr 3 ..... - 97 -
Rysunek 4.7: Wyniki testu nr 4 ..... - 98 -
Rysunek 4.8: Wyniki testu nr 5 ..... - 98 -
Rysunek 4.9: Wyniki testu nr 6 ..... - 98 -
Rysunek 4.10: Wyniki testu nr 7 ..... - 99 -
Rysunek 4.11: Wynik testu nr 8 ..... - 99 -

Rysunek 4.12: Porównanie czasu obliczenia rundy ..... - 100 -
Rysunek 4.13: Wyniki testu nr 9 - czas obliczeń ..... - 101 -
Rysunek 4.14: Wyniki testu nr 9 - zapotrzebowanie na pamięć ..... - 101 -
Rysunek 4.15: Wyniki testu 10 – czas obliczeń ..... - 102 -
Rysunek 4.16: Wyniki testu nr 10 – czas obliczeń ..... - 103 -
Rysunek 4.17: Wyniki testu nr 10 - zapotrzebowanie na pamięć ..... - 104 -
Rysunek 4.18: Wyniki testu nr 12 ..... - 105 -
Rysunek 4.19: Wyniki testu nr 13 ..... - 106 -
Rysunek 4.20: Wyniki testu nr 14 ..... - 107 -
Rysunek 4.21: Wyniki testu nr 15 ..... - 108 -

6.2. Spis tabel

Tabela 1.1: Wymagania bezpieczeństwa ..... - 9 -
Tabela 1.2: Wymagania bezpieczeństwa ..... - 10 -
Tabela 2.1: Porównanie norm dotyczących struktury EHR ..... - 27 -
Tabela 2.2: Porównanie dostępnych metod/rozwiązań ..... - 50 -
Tabela 3.1: Implementacja działań metody w komponentach systemu ..... - 58 -
Tabela 3.2: Porównanie metody DPEDZ z innymi rozwiązaniami ..... - 87 -
Tabela 4.1: Specyfikacja środowiska testowego ..... - 91 -
Tabela 4.2: Opis testu nr 1 ..... - 93 -
Tabela 4.3: Opis testu nr 2 ..... - 94 -
Tabela 4.4: Opis testów nr 3-8 ..... - 97 -
Tabela 4.5: Opis testu nr 9 ..... - 100 -
Tabela 4.6: Opis testu nr 10 ..... - 102 -
Tabela 4.7: Opis testu nr 11 ..... - 103 -
Tabela 4.8: Opis testu nr 12 ..... - 105 -
Tabela 4.9: Opis testu nr 13 ..... - 106 -
Tabela 4.10: Opis testu nr 14 ..... - 107 -
Tabela 4.11: Opis testu nr 15 ..... - 108 -
Tabela 4.12: Zagrożenia ..... - 109 -
Tabela 4.13: Test bezpieczeństwa nr 1 ..... - 111 -
Tabela 4.14: Test bezpieczeństwa nr 2 ..... - 111 -
Tabela 4.15: Test bezpieczeństwa nr 3 ..... - 112 -
Tabela 4.16: Test bezpieczeństwa nr 4 ..... - 112 -
Tabela 4.17: Test bezpieczeństwa nr 5 ..... - 113 -
Tabela 4.18: Test bezpieczeństwa nr 6 ..... - 113 -
Tabela 4.19: Test bezpieczeństwa nr 7 ..... - 114 -
Tabela 4.20: Test bezpieczeństwa nr 8 ..... - 114 -
Tabela 4.21: Test bezpieczeństwa nr 9 ..... - 115 -
Tabela 4.22: Test bezpieczeństwa nr 10 ..... - 115 -
Tabela 4.23: Test bezpieczeństwa nr 11 ..... - 116 -
Tabela 4.24: Test bezpieczeństwa nr 12 ..... - 116 -
Tabela 4.25: Test bezpieczeństwa nr 13 ..... - 117 -
Tabela 5.1: Wymagania bezpieczeństwa w relacji do zagrożeń i testów ..... - 121 -

6.3. Bibliografia

(Publikacje własne zostały wyróżnione pogrubioną czcionką)

1. The ACM Computing Classification System, 1998, [online: http://www.acm.org/about/class/ccs98-html].
2. C. Adams, S. Lloyd, *PKI podstawy i zasady działania*, Mikom, 2007.
3. A. Bakker, *Access to EHR and access control at a moment in the past: a discussion of the need and an exploration of the consequences*, International Journal of Medical Informatics 2004, 73, s. 267—270.
4. M. Bartel et. al., *XML Signature Syntax and Processing*, 2008, [Online: http://www.w3.org/TR/xmldsig-core/].
5. D.W. Bates, *Using information technology to reduce rates of medication errors in hospitals*, BMJ, 2000, 320:788–791.
6. D.W. Bates, M. Cohen ,L.L. Leape, J.M. Overhage, M.M. Shabot, T. Sheridan, *Reducing the frequency of errors in medicine using information technology*, J Am Med Inform Assoc, 2001, 8:299–308.
7. D.W. Bates, R.S Evans, H. Murff, P.D. Stetson, L. Pizziferri, G. Hripcsak, Detecting adverse events using information technology, J Am Med Inform Assoc, 2003, 10:115–128.
8. D.W. Bates, L.L. Leape, D.J. Cullen, N. Laird, L.A. Petersen, J.M. Teich, et al, *Effect of computerized physician order entry and a team intervention on prevention of serious medication errors*, JAMA, 1998, 280, s. 1311–1316.
9. D.W. Bates, J.M. Teich, J. Lee, D. Seger, G.J. Kuperman, N. Ma'Luf, et al., *The impact of computerized physician order entry on medication error prevention*, J. Am. Med. Inform. Assoc, 1999, 6, s. 313–321.
10. D. Bayer, S. Haber, W. S. Stornetta, *Improving the efficiency and reliability of digital time-stamping*, Sequences'91: Methods in Communication, Security, and Computer Science, 1992, s. 329-334.
11. T. Beale, *Archetypes: Constraint-based Domain Models for Future-proof Information Systems*, OOPSLA 2002 workshop on behavioural semantics, 2002.
12. T. Beale, S. Heard, *Archetype Definition Language 1.4*, 2007, [Online: http://www.openehr.org/releases/1.0.1/architecture/am/adl.pdf].
13. T. Beale, S. Heard, *openEHR Architecture – Architecture Overview*, 2007, [Online: http://www.openehr.org/svn/specification/TAGS/Release-1.0.1/publishing/architecture/overview.pdf. Release 1.0.1].
14. I. Bedini et al, e*bXML Registry profile for ebXML Core Components v0.1*, OASIS Working Draft, 2005, [online: http://ebxmlrr.sourceforge.net/presentations/regrep-ccts-profile-01.pdf].
15. J. Benaloh, M. de Mare, *Efficient Broadcast time-stamping*, Technical Report 1, Clarkson University Department of Mathematics and Computer Science, 1991.
16. A. J. Blazic, T. Klobucar, B. D. Jerman, *Long-term trusted preservation service using service interaction protocol and evidence records*, Computer Standards & Interfaces, 2007, Tom 29, s. 398-412.
17. J. Blazic, S. Saljic, T. Gondrom, *Extensible Markup Language Evidence Record Syntax*, Internet Draft, 2010.
18. B. Blobel, *Advanced and secure architectural EHR approaches*, International Journal of Medical Informatics, 2006, 75, s. 185—190.
19. B. Blobel, *Authorisation and access control for electronic health record systems*, International Journal of Medical Informatics, 2004, 73, s. 251—257.

20. B. Bobel, *Comparing approaches for advanced e-health security infrastructures,* International Journal of Medical Informatics, 2007, 76 , s. 454–459.
21. N. Boulus, P. Bjorn, *A cross-case analysis of technology-in-use practices: EPR-adaptation in Canada and Norway*, Int. J. Med. Inform., 2008, doi:10.1016/j.ijmedinf.2008.06.008.
22. J.G. Brookshear, *Informatyka w ogólnym zakresie*, WNT, 2003.
23. Z. Bubnicki, *Podstawy informatycznych systemów zarządzania*, Wydawnictwo Politechniki Wrocławskiej ,Wrocław 1993.
24. A. Buldas, P. Laud, H. Lipmaa, J, Villemson, *Time-Stamping with Binary Linking Schemes,* In Advances on Cryptology CRYPTO 1998, s.486-501, Springer-Verlag.
25. S.G. Campbell, L. Gordon, S. Collingwood, The Internet And Electronic Transmission Of Medical Records, Journal of Clinical Monitoring, 1997, 13, s. 325-334.
26. Canada Health Infoway, 2009, [Online: http://www.infoway-inforoute.ca];
27. Canada Health Infoway, *A 'Conceptual' Privacy Impact Assessment (PIA) on Canada's Electronic Health Record Solution (EHRS) Blueprint Version 2*, 2009, [Online: http://www2.infoway-inforoute.ca/Documents/CHI_625_PIA_rj13.pdf].
28. Canada Health Infoway, *Corporate Business Plan 2008/09*, [online: http://www2.infoway-inforoute.ca/Documents/Infoway_Business_Plan_2008-2009_Eng.pdf].
29. CEN, *CEN ENV 13606:2000, Medical Informatics – Electronic healthcare record communication*,European Committee for Standardization, Brussels , 2000.
30. CEN/ISO, *PN-EN 13606-1:2009, Informatyka w ochronie zdrowia. Przesyłanie elektronicznych dokumentów zdrowotnych. Część 1: Model referencyjny,* 2009.
31. G.M. Chertow, J. Lee, G.J. Kuperman, E. Burdick, J. Horsky, D.L. Seger, et al, *Guided medication dosing for inpatients with renal insufficiency*, JAMA, 2001, 286, s. 2839–2844.
32. T. Christensen, A. Faxvaag, H, Lærum, A. Grimsmo, *Norwegians GPs' use of electronic patient record systems*, international journal of medical informatics,2009, 78, s. 808–814.
33. M.A.C. Dekker, S. Etalle, *Audit-Based Access Control for Electronic Health Records,* Electronic Notes in Theoretical Computer Science, 2007, 168, s. 221–236.
34. DICOM**,** *DICOM Homepage,* 2010, [Online http://medical.nema.org/Dicom/].
35. A. Dogac, *ebXML Registry Profile for Web Ontology Language (OWL) v1.5*, OASIS Committee Draft, 2006, [online: http://xml.coverpages.org/OASIS-regrepOWL-Profile-22611.pdf].
36. R. H. Dolin, L. Alschuler, S. Boyer, C. Beebe, F. M. Behlen, P. V. Biron, A. Shabo, *HL7 Clinical Document Architecture*, Release 2, Journal of the American Medical Informatics Association, 2006, Vol. 13, 1.
37. ebXML Registry Information Model Version 3, [online: http://www.oasis-open.org/committees/regrep/documents/3.0/specs/regrep-rim-3.0-cs-01.pdf].
38. ebXML Technical Architecture Project Team, *ebXML Technical Architecture Specification*, v1.0.4, 2001, [online: http://xml.coverpages.org/ebXML_TA_v102.pdf].
39. M. Eichelberg, T. Aden, J. Riesmeier, A. Dogac, G. Laleci, *A Survey and Analysis of Electronic Healthcare Record Standards*, *ACM Computing Surveys*, 2005, Tom 37, 4.
40. M. Eichelberg, T. Namlý**,** *Electronic Health Records - a Tutorial*, 2006,[Online: http://www.srdc.metu.edu.tr/webpage/projects/ride/publicDocuments/icict06_ehr_tutorial_update.ppt].
41. ETSI, *ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES), v1.4.*, czerwiec 2009.

42. ETSI, *ETSI TS 102 176-1, Electronic Signatures and Infrastructures (ESI); Algorithms and Parameter for Secure Electronic Signatures; Part1: Hash functions and asymmetric algorithms,* v2.0.0, 2007.
43. ETSI, *ETSI TS 102 231, Electronic Signatures and Infrastructures (ESI); Provision of harmonized Trust-service status information,* v2.1.1, 2006.
44. EU Commision**,** *An Information Society for All. An Action Plan,* EU Commision Communication, COM, vol. 263, 2002.
45. EU Commision**,** *Making Healthcare Better for European Citizens,* An Action Plan for a European eHealth area, EU Commision Communication, COM vol. 356, 2004.
46. EU Commision, IDA Programme, *Model Requirments For The Management Of Electronic Records,* CECA-CEE-CEEA, 2001.
47. A. D. Fernandes, *Risking "trust" in a public key infrastructure: old techniques of managing risk applied to new technology,* Decision Support Systems, 2001, 31, s. 303 – 322.
48. L. Gallagher, L. Carnahan, *A general purpose registry/repository information mode,* Information Technology Laboratory National Institute of Standards and Technology, 2nd Draft, 2001, [online: ftp://xsun.sdct.itl.nist.gov/regrep/GPregrepModel.pdf].
49. Gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte, 2009, [online: http://www.gematik.de].
50. T. Gondrom, R. Brandner, U. Pordesch, *RFC 4998 Evidence Record Syntax (ERS),* sierpień 2007.
51. M. T. Goodrich, R. Tamassia, A. Schewerin, *Implementation of an Authenticated Dictionary with Skip Lists and Commutative Hashing,DARPA Information Survivability Conference & Exposition II, 2001. DISCEX '01. Proceedings, s.* 68 - 82 vol.2.
52. D. Gritzalis, C. Lambrinoudakis, *A security architecture for interconnecting health information systems,* International Journal of Medical Informatics, 2004, 73, s. 305—309.
53. S. Haber, W. S. Stornetta, *How to Time-Stamp a Digital Document,* Journal of Cryptology, 1991, 3(2), s. 99-111.
54. K. Hayrinen, K. Saranto, P. Nykanen, *Definition, structure, content, use and impacts of electronic health records: A review of the research literature,* International Journal of Medical Informatics, 2008, Tom 77, s. 291–304.
55. HL7, *HL7 Reference Information Model*, 2010, [omline: http://www.hl7.org/Library/data-model/RIM/modelpage_mem.htm].
56. House of Commons Health Committee, T*he Electronic Patient Record Sixth Report of Session 2006–07*, 2009, [online:*http://www.publications.parliament.uk/pa/cm200607/cmselect/cmhealth/422/422.pdf*].
57. R. Hussein, U. Engelmann, A. Schroeter, U. Engelmann, A. Schroeter, *DICOM Structured Reporting,* RadioGraphics, 2004, 24:891–896.
58. **T. Hyla,** ***Automatyczne sprawdzanie i weryfikacja statusu algorytmów kryptograficznych wykorzystywanych w infrastrukturze klucza publicznego,*** Metody Informatyki Stosowanej, 2009, nr 2 (19), s. 31-40.
59. **T. Hyla,** ***Infrastruktura zabezpieczeń elektronicznych dokumentów zdrowotnych,*** Rozdział w książce Inwestycja w Wiedzę pod redakcją R. Błasiak-Grudzień, Wojewódzki Urząd Pracy, Szczecin 2010, s. 31-36, ISBN 978-83-61985-02-0.
60. **T. Hyla, W. Bielecki, J. Pejaś,** ***Non-repudiation of Electronic Health Records in distributed healthcare systems,*** Pomiary Automatyka Kontrolna, 2010, nr 08, s. 1170-1173.
61. **T. Hyla, J. Pejaś,** ***A method for long-term EHR metadata preservation in healthcare systems,*** Metody Informatyki Stosowanej, 2008, nr 3, s. 125-134 .

62. **T. Hyla, J. Pejaś, *A security architecture of an inter-jurisdiction EHR system,*** Pomiary Automatyka Kontrola, 2009 nr 10, s. 823-826.
63. **T. Hyla, J. Pejaś, *Long–term secure EHR data storage in an electronic registry,*** Polish Journal of Environmental Studies, 2008, Vol. 17 No. 4C, s. 347-353.
64. L. Iacovino M. Todd, *The long-term preservation of identifiable personal data: a comparative archival perspective on privacy regulatory models in the European Union, Australia, Canada and the United States,* Arch Sci, 2007, 7:107–127.
65. A. K. Jha, D. Doolan, D. Grandt, T. Scott, D. W. Bates, *The use of health information technology in seven nations,* Int. J. Med. Inform, 2008, 77, s. 848–854.
66. IHE International, *IT Infrastructure Technical Framework, Volume 1 (ITI TF-1) Integration Profile,* August 10, 2009, Revision 6.0 – Final Text.
67. International Health Terminology Standards Development Organisation (IHTSDO), *SNOMED CT (Systematized Nomenclature of Medicine-Clinical Terms),* 2010, [Online: http://www.ihtsdo.org/our-standards/snomed-ct/].
68. ISO/IEC, *PN-ISO/IEC 13888-1:1999, Technika informatyczna -- Techniki zabezpieczeń -- Niezaprzeczalność -- Model ogólny,* ISBN: 83-236-4122-6.
69. ISO, *ISO TS 18308 - Health Informatics - Requirments for an Electronic Health Record Architecture.* 2003.
70. ISO, *ISO/TR 20514:2005, Health informatics — Electronic health record — Definition, scope, and context,*Geneva.
71. ISO, *ISO 14721:2003 - Space Data and Information Transfer system - Open Archival Information System - Refernce Model,* 2003.
72. ISO, *ISO 7498-2, Information processing systems -- Open Systems Interconnection -- Basic Reference Model -- Part 2: Security Architecture,* 1989.
73. W. Kluge, Eike-Henner, *Secure e-Health: Managing risks to patient health data. international journal of medical informatics,* 2007, 76, s. 402–406.
74. İ. Köse, N. Akpinar, M. Gürel, Y. Arslan, H. Özer, N.Yurt, Y. Kabak, A. Dogac, Turkey's *National Health Information System (NHIS),* 2009,[online: http://www.srdc.metu.edu.tr/webpage/publications/2008/9.pdf].
75. T. Kotarbiński, *Elementy teorii poznania, logiki formalnej i metodologii nauk,* Ossolineum, Wrocław 1961.
76. S. Lancaster, D. C. Yen, S.-M. Huang, *Public key infrastructure: a micro and macro analysis,* Computer Standards & Interfaces, 2003, 25, s. 437-446.
77. D. Lekkas, D. Gritzalis, *Long-term verifiability of the electronic healthcare records' authenticity,* International Journal of Medical Informatics, 2007, Tom 76, s. 442-448.
78. H. van der Linden, D. Kalra, A. Hasman, J. Talmon, *Inter-organizational future proof EHR systems: A review of the security and privacy related issues,* Internationa Journal of Medical Informatics, 2009, Tom 78, s. 141-160.
79. D.F. Lobach, D.E. Detmer, *Research Challenges for Electronic Health Records,* Am J Prev Med, 2007, 32(5S).
80. D.A. Ludwick, J. Doucette, *Adopting electronic medical records in primary care: Lessons learned from health information systems implementation experience in seven countries,* Int. J. Med. Inform, 2008, doi:10.1016/j.ijmedinf.2008.06.005.
81. W. Maćków, *Linked authenticated dictionaries for certificate ststus verification,* Enhanced Methods in Computer Security, Biometric and Artificial Intelligence Systems, 2005, s. 35-46.
82. A. Menezes, P. Oorschot, S. Vanstone, *Handbook of Applied Cryptography,* CRC Press, 1996.
83. R. C. Merkle, *Method of providing digital signatures,* US Patent number: 4309569, Issue date: Jan 5, 1982.

84. M. L. Muller, F. Uckert, T. Burkle, *Cross-institutional data exchange using the clinical document architecture (CDA),* International Journal of Medical Informatics, 2005, 74, s. 245—256.
85. F. Najmi, et al, *ebXML Registry profile for Web Services v1.0*, draft OASIS Profile, 2005, [online: http://www.oasis-open.org/committees/download.php/14756/regrep-ws-profile-1.0-draft3.pdf].
86. R. Neame, Communications and EHR: authenticating who's who is vital, *International Journal of Medical Informatics*, 2000, 60, s. 85–190.
87. openEHR Foundation, *openEHR*, [Online: http://www.openehr.org].
88. openEHR Foundation, *The openEHR Reference Model – Support Information Model*, 2007, [Online: http://www.openehr.org/svn/specification/TAGS/Release-1.0.1/publishing/architecture/rm/ehr_im.pdf], Release 1.0.1.
89. J.M. Overhage, W.M. Tierney, X.A. Zhou, C.J. McDonald, *A randomized trial of corollary orders to prevent errors of omission,* J Am Med Inform Assoc, 1997, 4, s. 364–365.
90. J. Parre, *Electronic Health Record Project of Estonia - Nation-wide Integrated eHealth Services,*2009, [online: http://www.riigikantselei.ee/3qc/docs/ehealth/E_tervishoid_J_Parre_020904.ppt].
91. **J. Pejaś, T. Hyla, *Trójczynnikowy Schemat silnego podpisu cyfrowego oparty na odwzorowaniu biliniowym i skrócie z odcisku palca,*** Rozdział w Monografii: Metody biometryczne i kryptograficzne w zintegrowanych systemach bezpieczeństwa pod redakcją J. Pomykała, B. Hołyst, Oficyna Wydawnicza WSM (w druku) .
92. J. Pejaś, W. Maćków, *Long Term Archive System for Electronic Documents Preservation with Authenticity,* Polish Journal of Environmental Studies, Vol. 16, No. 5B, s. 300-305, 2007.
93. P. Pharow, B. Blobel, *Electronic signatures for long-lasting storage purposes in electronic archives*, International Journal of Medical Informatics, 2005, 74, s. 279-287.
94. PKN, *PN-I-02000:2002, Technika informatyczna -- Zabezpieczenia w systemach informatycznych -- Terminologia,* ISBN: 83-236-7759-X.
95. D. Protti, et al., *Comparing the application of Health Information Technology in primary care in Denmark and Andalucía, Spain*, Int. J. Med. Inform, 2008, doi:10.1016/j.ijmedinf.2008.08.002.
96. K. Rebane, eHealth in Estonia, 2009, [online: *http://www.epist.org/documents/balticIT&T/eHealth%20in%20Estonia.pdf*].
97. Regenstrief Institute, LOINC, 2010, [Online: http://loinc.org/].
98. Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty, oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*, Dz.U. 2002 nr 128 poz. 1094.
99. P. Ruotsalainen, *A cross-platform model for secure Electronic Health Record communication,* International Journal of Medical Informatics, 2004, 73, s. 291—295.
100. P. Routsalainen, B. Manning, *A notary archive model for secure preservation and distribution of electrically signed patinet documents*, International Journal of Medical Informatics, 2007, 76, s. 449-453.
101. R. E. Scott, P. Jennett, M. Yeo, *Access and authorisation in a Glocal e-Health Policy context,* International Journal of Medical Informatics, 2004, 73, s. 259—266.
102. W. Susilo, K. Than Win, *Security and Access of Health Research Data,* J Med Syst, 2007, 31, s.103–107.

103. Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym, Dz.U. 2001 nr 130 poz. 1450.
104. R. Veryard, *Information modelling : practical guidance*, New York, Prentice Hall, 1992.
105. C. Wallace et. al., *RFC 4810, Long-Term Archive Service Requirements,* Marzec 2007.
106. A. Westerinen, et al., *Terminology for Policy-Based Management,* The Internet Society, RFC 3198, 2001.
107. K. T. Win, J. A. Fulcher, *Consent Mechanisms for Electronic Health Record Systems: A Simple Yet Unresolved Issue,* J Med Syst, 2007, 31, s. 91–96.
108. J.I. Wolfstadt, J.H. Gurwitz, T.S. Field, M. Lee, S. Kalkar, Wu, et al. *The effect of computerized physician order entry with clinical decision support on the rates of adverse drug events: a systematic review*, J. Gen. Intern. Med, 2008, Tom 23, s. 451–458.

Załączniki

Do niniejszej rozprawy została dołączona płyta CD zawierające następujące załączniki w wersji elektronicznej:

1. Normy, Specyfikacje
    a. Specyfikacja IHE zawierające profil IHE XDS;
    b. RFC 4810 *Long-Term Archive Service Requirements;*
    c. RFC 4998 *Evidence Record Syntax*;
    d. ETSI TS 101 903, *XML Advanced Electronic Signatures (XAdES);*
2. Biblioteka CryptoSys PKI Toolkit;
3. Oprogramowanie implementujące działania składowe metody DPEDZ używane do przeprowadzenia testów;
4. XML Schema
    a. Rekordy Poświadczeń Rejestrów (*RPR.xsd*);
    b. Typy wiadomość służące do komunikacji z CID (*S.xsd*).