

Część 3 — Struktura techniczna CHF

Spis treści

Część 3 — Struktura techniczna CHF	1
Struktura techniczna CHF	4
Uwzględnienie powszechnych problemów dotyczących architektury	4
Wielorakość	4
Zapewnienie dostępu do stale rozszerzającego się zakresu funkcji	4
Różnorodność kanałów dostępu	5
Szerokie wsparcie różnorodnych platform klienckich	5
Obsługa wielu języków i wszechstronny dostęp	5
Obsługa wielu różnych poświadczeń tożsamości	6
Udostępnienie każdej z usług e-zdrowia w spójny i bezpieczny sposób	6
Zarządzanie tożsamością	7
Pojedyncze poświadczenia we wszystkich usługach systemu e-zdrowia	7
Spójne logowanie a pojedyncze logowanie	7
Odwzorowywanie tożsamości	8
Trudne przypadki	9
Początkowa identyfikacja użytkownika	9
Problemy integracji	10
Różne możliwości integracji	11
Integracja natywna	11
Adaptory w hubie	11
Adaptory w systemach zdalnych	12
Rozdzielenie integracji ogólnej i specyficznej	13
Wspólne rozwiązanie integracyjne	14
Elastyczność i sprawność	15
Dlaczego elastyczność i sprawność są tak ważne	15
Tworzenie architektury z myślą o elastyczności	15
Zabezpieczanie rozwiązania	16
Dlaczego bezpieczeństwo jest tak ważne?	16
Projektowanie bezpiecznych rozwiązań	17
Skalowalność, wydajność, dostępność	17
Dostępność i odporność	18
Odtwarzanie po awariach	18
Konstrukcja wspólnego huba	19
Potrzeba ustalenia właściciela lub finansującego	19
Początkowa inwestycja z odroczonymi korzyściami	19
Typowe konflikty z projektami indywidualnymi	19
Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia	21
Reguły rządzące architekturą	22
Orientacja na usługi	22
Interfejsy i standardy	22
Wyszukiwanie usług	22
Stowarzyszone funkcje zabezpieczeń	22
Elastyczność	23
Bezpieczeństwo	23
Skalowalność i wydajność	23
Hub usług e-zdrowia	24
Kontekst i interakcje zewnętrzne huba	24
Interakcje z klientami	24
Interakcje z usługami zewnętrznymi	25
Usługi świadczone przez hub	26

Usługi zarządzania tożsamością.....	29
Podstawowy model tożsamości i zasady	29
Podstawowe encje modelu tożsamości	29
Model tożsamości	30
Separacja tożsamości od poświadczeń uwierzytelniania	31
Obsługa uwierzytelniania stowarzyszonego	31
Usługi Web Services.....	31
Wzorzec ogólny — wymienni dostawcy	32
Początkowe zgłaszanie użytkowników.....	33
Początkowe uwierzytelnianie oparte na wiedzy	33
Wybór odpowiedniego zestawu informacji dla KBA.....	34
Logika weryfikująca i dane referencyjne	35
Pozyskiwanie informacji do celów uwierzytelniania opartego na wiedzy	37
Skoncentrowane na usługach podejście do zgłaszania użytkowników	37
Rejestracja w usługach i odwzorowywanie tożsamości	38
Aktywacja zgłoszenia i rejestracji	38
Ogólny dostawca poświadczeń i uwierzytelniania.....	40
Zarządzanie użytkownikami i rejestracjami.....	41
Dodawanie i usuwanie użytkowników	41
Tworzenie, aktywacja i usuwanie rejestracji.....	42
Przypisywanie (delegowanie) uprawnień — agenci	42
Pomoc techniczna i odzyskiwanie kont użytkowników	43
Aktualizowanie identyfikatorów specyficznych dla usługi	43
Usługi poufności danych i bezpieczeństwa.....	45
Ogólne sposoby podejścia do problemu bezpiecznej architektury rozwiązania	45
Wzorce i dobre praktyki dotyczące bezpieczeństwa	46
Najlepsze praktyki dotyczące bezpieczeństwa.....	47
Zabezpieczanie usług Web Services.....	47
Zagadnienie bezpieczeństwa specyficzne dla architektury systemów e-zdrowia.....	48
Ochrona i poufność danych	48
Infrastruktura techniczna i sieci komputerowe.....	48
Zabezpieczanie hostów	49
Ataki typu DoS (Denial of Service)	50
Zabezpieczenie przed zgłaszaniem fałszywych użytkowników	50
Zabezpieczenie przed nieudanymi próbami logowania	51
Zabezpieczenie przed żądaniami wymagającymi dużej mocy obliczeniowej	51
Usługi uwierzytelniania i autoryzacji	53
Uwierzytelnianie	53
Poziomy uwierzytelniania	53
Przedstawianie poświadczeń i stwierdzeń	54
Uwierzytelnianie stowarzyszone.....	55
Autoryzacja.....	57
Sprawdzanie rejestracji w usługach	58
Odwzorowanie tożsamości na identyfikatory specyficzne dla usług	58
Delegowanie zaufania	58
Szczegółowość autoryzacji.....	59
Usługa tokenów zabezpieczeń.....	59
Tokeny bezpieczeństwa	60
Wydawanie tokenów bezpieczeństwa	60
Możliwe scenariusze zastosowań	60
Udostępnianie usług uwierzytelniania i autoryzacji.....	63
Usługa zarządzania zgodami	64
Usługa anonimizacji	65
Usługi prezentacji i punktu dostępu	66
Usługi publikacji i wyszukiwania usług.....	67
Usługa katalogu usług	67

UDDI	68
Metadane usług	68
Publikacja usługi	68
Wyszukiwanie usługi	69
Replikacja	70
Usługi elektronicznej dokumentacji medycznej	72
Usługi domeny zdrowia	73
Usługi rejestru medycznego	74
Usługi integracyjne	76
Usługa rejestracji dokumentów	76
Rola usługi rejestracji dokumentów	76
Podstawowa architektura usługi rejestracji dokumentów	77
Interfejs publiczny	77
Komunikacja asynchroniczna	78
Komunikacja synchroniczna	79
Implementacja prywatna	79
Format komunikatów	81
Koperty, nagłówki i zawartości komunikatów	81
Załączniki komunikatów	83
Bezpieczeństwo komunikatów	84
Dlaczego zabezpieczenie tylko warstwy transportowej może nie być wystarczające? ..	84
Przyszłość to zabezpieczenia na poziomie komunikatu	84
Poufność	85
Integralność	85
Autoryzacja	86
Walidacja komunikatu	87
Magazyn komunikatów	87
Usługa trasowania komunikatów	88
Adresowanie usług Web Services	89

Struktura techniczna CHF

Uwzględnienie powszechnych problemów dotyczących architektury

W tej sekcji dokumentu zajmiemy się najważniejszymi problemami związanymi z architekturą techniczną rozwiązań e-zdrowia, obszarami, które wymagają szczególnego potraktowania — a często, przynajmniej na początkowych etapach projektu, umykają uwadze — i możliwymi wariantami rozwiązań oraz opiszemy zalecany sposób rozwiązywania tych problemów. Oprócz omówienia problemów zwykle spotykanych w wielkoskalowych projektach informatycznych i integracyjnych, szczególny nacisk położymy na najważniejsze problemy charakterystyczne dla rozwiązań e-zdrowia.

Chcąc uświadomić architektom złożoność projektu, potencjalne problemy i dostępne opcje, zamieściliśmy tu ogólny opis zagadnień związanych z architekturą techniczną, niezależny od specyficznych technologii czy implementacji. Bardziej szczegółowe zalecenia dotyczące rozwiązywania tych problemów zamieszczono w sekcjach *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* oraz *Building Blocks* w dalszej części tego dokumentu.

W witrynie MSDN dostępne są szczegółowe wskazówki firmy Microsoft, dotyczące architektur i wzorców projektowych dla korporacyjnych rozwiązań integracyjnych (patrz dział *Integration Patterns* pod adresem <http://msdn.microsoft.com/library/en-us/dnpag/html/intpatt.asp>). Pomimo że wzorce te opisywane są w kontekście integracji korporacyjnej, to niektóre z nich (na przykład Gateway, Message Broker) nadają się do bezpośredniego zastosowania w rozwiązaniach integracyjnych e-zdrowia.

Comment [JB1]: nie ma takiej sekcji w otrzymanym do tłumaczenia zestawie dokumentów

Wielorakość

Wiele zagadnień związanych z usługami e-zdrowia dotyczy problemu wielorakości, w związku z czym konsolidacja i uproszczenie wynikające z unifikacji wspólnej infrastruktury, wspierającej te usługi, mogą okazać się bardzo korzystne.

Zapewnienie dostępu do stale rozszerzającego się zakresu funkcji

Inicjatywy w zakresie e-zdrowia zwykle powstają jako niewielkie projekty z ograniczonym zestawem funkcji, a następnie są stopniowo rozwijane i obejmują coraz szerszą funkcjonalność. Związanych jest z tym kilka specyficznych problemów, wynikających z różnorodności typów systemów i z rosnącej liczby tych systemów.

Systemy zaplecza (back-end) świadczące usługi zdrowotne pracują na wielu różnych platformach i korzystają z różnych technologii. Stopniowe wdrażanie różnorodnych usług jest scenariuszem typowym ze względu na stały rozwój i ewolucję inicjatyw e-zdrowia. Zaprojektowanie i wdrożenie wspólnej infrastruktury, zdolnej do efektywnej obsługi rosnącej funkcjonalności systemu, jest dużym wyzwaniem, wykraczającym znacznie poza problemy spotykane w tradycyjnych systemach komercyjnych.

Efektywna platforma e-zdrowia — wdrożona i działająca w warunkach produkcyjnych — powinna być dostatecznie elastyczna, by można było w łatwy sposób wprowadzać nowe usługi, nowe transakcje i dostosowywać platformę do zmieniających się wymagań — i to bez zmian w kodzie podstawowego rozwiązania, a najlepiej bez powodowania przestoju innych usług. Wdrażanie nowych usług powinno być standardową funkcją systemu, odpowiednio uwzględnioną w projekcie rozwiązania, a nie rzadkim, wymagającym specjalnego traktowania przypadkiem.

Różnorodność kanałów dostępu

Istnieje wysokie prawdopodobieństwo, że nawet jeśli kanały dostępu do pierwotnego zestawu usług zostaną dobrze zdefiniowane w początkowym etapie projektu i właściwie przygotowane w pierwszej implementacji, to po pewnym czasie i tak pojawi się potrzeba obsługi nowych kanałów dostępu, takich jak kioski multimedialne, interaktywna telewizja czy urządzenia przenośne.

Dobrze zaprojektowana platforma integracyjna, zapewniająca spójny sposób świadczenia usług, powinna umożliwiać dodawanie nowych kanałów dostępu poprzez jednorazowe zmodyfikowanie centralnego huba bez konieczności modyfikowania poszczególnych usług.

Szerokie wsparcie różnorodnych platform klienckich

Projekty dla opieki zdrowotnej są często przedmiotem znacznie bardziej ścisłych regulacji i ograniczeń niż typowe systemy komercyjne. Zapewnienie niedyskryminującego dostępu do usług opieki zdrowotnej z szerokiej gamy platform klienckich jest często wymaganiem jasno sprecyzowanym w przepisach prawnych, a przynajmniej pożądanym z politycznego punktu widzenia. Może się to wiązać z obsługą różnych typów i wersji sprzętu, systemów operacyjnych i oprogramowania przeglądarkowego.

Właściciel systemu komercyjnego może podjąć uzasadnioną ekonomicznie decyzję wykluczenia niewielkiej części potencjalnych klientów poprzez ograniczenie zakresu obsługiwanych platform. Takie postępowanie — niewiele zmniejszając potencjalny przychód — pozwala uzyskać znaczne oszczędności, wynikające z mniejszego zakresu prac projektowych i programistycznych nad systemem i mniejszej liczby niezbędnych do wykonania testów.

Dostawcy usług zdrowotnych są w tym zakresie znacznie bardziej ograniczeni i często muszą ponosić znaczne koszty związane z uwzględnieniem różnych platform, by nie wykluczyć i nie dyskryminować nawet niewielkich grup społecznych.

Jest niezwykle istotne, by ograniczenia i wymagania związane z obsługą szerokiego spektrum platform klienckich zostały uwzględnione już na etapie projektowania architektury platformy integracyjnej dla e-zdrowia — uwzględnienie tych warunków na dalszych etapach projektu może być bardzo kosztowne, a nawet niemożliwe.

Obsługa wielu języków i wszechstronny dostęp

W wielu krajach zapewnienie wielojęzycznego dostępu do usług opieki zdrowotnej jest wymaganiem prawnym, a przynajmniej należy do dobrych zwyczajów. Uwzględnienie tego warunku już na początku realizacji projektu jest istotne, ponieważ wymaganie to ma duży wpływ na architekturę rozwiązania. Należy też mieć na uwadze:

- Zapewnienie różnych poziomów obsługi wielojęzyczności, w tym akceptowanie danych wielojęzycznych, zróżnicowanie skryptów i stron (na przykład do obsługi języków zapisywanych od prawej do lewej czy języków zapisywanych za pomocą innych alfabetów).
- Problemy dotyczące przetwarzania i przechowywania danych, które mają wpływ na stosowany model danych i wymagają szczególnej uwagi podczas pisania kodu aplikacji.
- Wymagania zaprojektowania w pełni wielojęzycznego interfejsu użytkownika, w którym wszystkie łańcuchy tekstowe i komunikaty są odseparowane od kodu. W takim wypadku do pełnej obsługi języków pisanych od prawej do lewej i innych języków znakowych niezbędne jest przygotowanie alternatywnych plików graficznych i innych treści. Należy także wziąć pod uwagę, że ten sam tekst w różnych językach może mieć różną długość.

Witryny i usługi opieki zdrowotnej są często objęte bardzo rygorystycznymi wymaganiami dotyczącymi przystępności dla osób o ograniczonej sprawności (accessibility) — znacznie większymi niż w przypadku zwykłych witryn komercyjnych, gdzie przystępność jest pożądana w celu poszerzenia grupy odbiorców, ale jej brak ma jedynie niewielki wpływ na komercyjny efekt przedsięwzięcia. Dla witryn i usług opieki zdrowotnej przystępność jest zwykle wymagana prawem, a na dodatek jest ważnym problemem politycznym. Zająć się problemem przystępności już po zaprojektowaniu systemu jest trudne, drogie, a często niewykonalne. Przystępność już od samego początku powinna być podstawowym założeniem projektu.

W części *Odsyłacze, listy kontrolne i dalsze informacje* tego opracowania zamieszczono listy kontrolne dotyczące tworzenia aplikacji łatwych w lokalizacji oraz listę odsyłaczy do bieżących regulacji prawnych dotyczących przystępności, do inicjatyw (w tym także do wytycznych w zakresie przystępności, opracowanych przez organizację World Wide Web Consortium — W3C), do programów syntezy mowy odczytujących teksty z ekranu komputera oraz do specjalnych przeglądark, narzędzi do testowania przystępności aplikacji oraz do innych przydatnych zasobów.

Obsługa wielu różnych poświadczeń tożsamości

Korzystanie z różnych usług opieki zdrowotnej zwykle wymaga podania specyficznego dla danej usługi identyfikatora użytkownika — na przykład numeru pacjenta, identyfikatora specjalisty opieki zdrowotnej, identyfikatora dostawcy usług zdrowotnych itp. Gdy kontrola dostępu jest implementowana niezależnie dla każdej z usług, umożliwienie elektronicznego dostępu do wielu usług oznacza utworzenie odrębnych, niezależnych dla każdej usługi poświadczeń tożsamości. Użytkownicy muszą wtedy pamiętać wiele identyfikatorów i zarządzać wieloma hasłami.

Stanowi to problem nawet w przypadku często wykorzystywanych usług, takich jak bankowość elektroniczna. W przypadku usług opieki zdrowotnej, z których pacjenci korzystają dość rzadko i nieregularnie (np. w razie nagłej potrzeby), próba przypomnienia sobie hasła czy identyfikatora do każdej z usług może sprawić jeszcze większe trudności. Wprowadzenie platformy e-zdrowia zapewniającej dostęp do wielu usług na podstawie pojedynczego zestawu poświadczeń tożsamości jest niezwykle istotne dla upowszechnienia się usług e-zdrowia.

Udostępnienie każdej z usług e-zdrowia w spójny i bezpieczny sposób

Udostępnienie dowolnej usługi e-zdrowia za pomocą kanałów elektronicznych wymaga znacznych nakładów i wysiłków — konieczne jest spełnienie wszystkich wymagań w zakresie bezpieczeństwa, dostępności i niezawodności. W niektórych krajach obowiązują rygorystyczne uregulowania prawne i każdy system opieki zdrowotnej przed podłączeniem do Internetu musi przejść obowiązkowy proces certyfikacji. Tworzenie dostępu elektronicznego dla każdej usługi z osobna prowadzi do powielenia tych wysiłków. Oznacza to stratę czasu, zasobów i niepotrzebne angażowanie specjalistów, którzy nie zawsze są dostępni w agencjach świadczących te usługi.

Problem staje się szczególnie istotny, gdy usługi elektroniczne zaczynają być tak popularne, że muszą być świadczone nie tylko przez początkową grupę dużych agencji opieki zdrowotnej, które mają odpowiednią wielkość, widoczność i wpływy polityczne potrzebne do zabezpieczenia sobie niezbędnych zasobów. Mniejsze organizacje, takie jak regionalne zarządy opieki zdrowotnej, nie są w stanie samodzielnie pokryć początkowych kosztów świadczenia usług w sposób elektroniczny.

Zidentyfikowanie najbardziej problematycznych elementów systemu opieki zdrowotnej i jednokrotne zaimplementowanie ich w powszechnej platformie e-zdrowia,

współdzielonej przez wszystkie usługi, pozwala zapewnić wysoką jakość, spójność i bezpieczeństwo tworzonych rozwiązań i pozwala uzyskać znaczące oszczędności.

Zarządzanie tożsamością

Zaprojektowanie i wdrożenie efektywnego i bezpiecznego systemu zarządzania tożsamością dla usług e-zdrowia nie jest zadaniem trywialnym, zważywszy że liczba potencjalnych użytkowników może sięgać setek tysięcy specjalistów opieki zdrowotnej lub milionów pacjentów. Ze względu na koszty i złożoność problemu, jest oczywiste, że zarządzanie tożsamością powinno zostać zaimplementowane w postaci pojedynczego systemu, współdzielonego przez wszystkie usługi.

Pojedyncze poświadczenia we wszystkich usługach systemu e-zdrowia

Wprowadzenie możliwości wykorzystania pojedynczego poświadczenia tożsamości do dostępu do wielu usług e-zdrowia (jak zostało to opisane wcześniej w rozdziale *Obsługa wielu różnych poświadczeń tożsamości*) wymaga zbudowania powszechnej infrastruktury uwierzytelniania użytkowników, wspólnej dla wszystkich usług wchodzących w skład systemu.

Warto w tym miejscu zauważyć, że stosowanie jednego zestawu poświadczeń tożsamości do dostępu do **wielu** usług wcale nie oznacza, że jeden i ten sam zestaw poświadczeń musi być stosowany do dostępu do **wszystkich** usług. Mimo oczywistych zalet dostępu do wielu usług z wykorzystaniem jednego zestawu poświadczeń, platforma powinna pozostawiać użytkownikom swobodę wyboru usług, do których chcą uzyskiwać dostęp na podstawie określonego zestawu poświadczeń, i umożliwiać korzystanie z wielu niezależnych zestawów poświadczeń. Jest to zgodne z zasadami przedstawionymi w artykule *The Laws of Identity*, dostępnym pod adresem <http://msdn.microsoft.com/library/en-us/dnwebsrv/html/lawsidentity.asp>.

Spójne logowanie a pojedyncze logowanie

Gdy użytkownicy uzyskali już możliwość logowania się do rosnącej liczby usług za pomocą jednego zestawu poświadczeń, to zarówno dla użytkowników, jak i dostawców usług istotne staje się, by koszty i nakłady pracy, związane z umożliwieniem dostępu do każdej kolejnej usługi, utrzymać na jak najniższym poziomie.

Dostęp do poszczególnych usług na podstawie jednego zestawu poświadczeń może być realizowany na różnych poziomach — między innymi poprzez *spójne logowanie* lub *pojedyncze logowanie*. Spójne logowanie to forma najprostsza — dostęp do poszczególnych usług realizowany jest na podstawie pojedynczego zestawu poświadczeń, ale użytkownik nadal musi meldować się do każdej usługi z osobna. Co prawda użytkownicy muszą pamiętać tylko jeden zestaw poświadczeń, ale za każdym razem, gdy chcą korzystać z innej usługi, muszą się ponownie zameldować (jednak w niektórych przypadkach taki dodatkowy etap logowania może okazać się pożądanym).

Jednym ze sposobów implementacji spójnego logowania jest utrzymywanie przez każdą niezależną usługę własnej bazy danych uwierzytelniających. Bazy danych wzajemnie synchronizują swoją zawartość, dzięki czemu poszczególne kopie poświadczeń logowania są identyczne. Poszczególne usługi — zamiast implementować własne mechanizmy uwierzytelniania — mogą korzystać z pojedynczej, wspólnej usługi uwierzytelniania. Zakładana spójność uzyskiwana jest automatycznie, ponieważ poświadczenia użytkowników przechowywane są tylko w jednej lokalizacji.

Bardziej zaawansowane rozwiązanie umożliwia użytkownikom przezroczysty dostęp do wielu usług po jednokrotnym zalogowaniu. Oznacza to prostotę korzystania z systemu

przez użytkowników i pozwala na agregowanie usług. Dobrymi przykładami takich rozwiązań są portale, które komunikując się w tle z różnymi usługami zapewniają użytkownikom możliwość korzystania z wielu usług jednocześnie.

Odwzorowywanie tożsamości

Zastosowanie pojedynczego zestawu poświadczeń do dostępu do wielu usług jest niewątpliwie użyteczne, ale rozwiązuje tylko jedną część problemu — ułatwia użytkownikowi korzystanie z systemu. Systemy docelowe nadal korzystają z własnych, specyficznych identyfikatorów, wyróżniających użytkownika w kontekście danego systemu. Przykładami takich identyfikatorów są: numer pacjenta w przypadku elektronicznej dokumentacji medycznej, identyfikator specjalisty w przypadku zlecania badań laboratoryjnych czy identyfikator administratora w przypadku systemu planowania zadań i zarządzania wydajnością. Identyfikatory te są niezbędne do prawidłowego rozpoznania użytkownika i poprawnej pracy systemu i zwykle nie mają żadnego znaczenia poza kontekstem określonej usługi. Większość obecnie wykorzystywanych systemów korzysta z takich specyficznych identyfikatorów, w związku z tym udostępnianie przez wspólną platformę e-zdrowia funkcji odwzorowania pojedynczego zestawu poświadczeń na odpowiednie identyfikatory, specyficzne dla poszczególnych usług, jest niezwykle istotne dla zapewnienia efektywnego dostępu do rosnącej liczby usług.

W wielu krajach nie wprowadzono uniwersalnego krajowego identyfikatora dla obywateli, w związku z czym każda usługa wykorzystuje własne, specyficzne identyfikatory. Pewne ograniczenia istnieją nawet w krajach, w których wszyscy obywatele posiadają unikatowe identyfikatory i systemy opieki zdrowotnej mogą w oparciu o nie identyfikować użytkownika (przykłady takich krajów to Irlandia, Belgia, Francja i Bułgaria). Na przykład w sytuacji, gdy jedna osoba może mieć wiele relacji z daną usługą (np. kontakt z wieloma szpitalami), identyfikator obywatela nie pozwala na rozróżnienie poszczególnych relacji, w związku z czym potrzebny jest identyfikator specyficzny dla danej usługi.

W przypadku bardziej złożonych relacji (na przykład takich jak opisane w następnym rozdziale *Trudne przypadki*) konieczność odwzorowania pojedynczego zestawu poświadczeń na odpowiedni, właściwy w danym kontekście identyfikator, jest jeszcze bardziej oczywista.

Nawet jeśli bezpośrednie zastosowanie numeru identyfikacyjnego obywatela czy narodowego numeru pacjenta jest technicznie możliwe, mogą pojawić się wątpliwości dotyczące poufności danych (patrz przypadek USA opisany w części 1. opracowania) i może to złamać podstawowe zasady zarządzania tożsamością. Chodzi głównie o zasady *minimalnego zakresu ujawniania niezbędnych informacji* oraz *tożsamości ukierunkowanej*, opisane w dokumencie *The Laws of Identity* pod adresem <http://msdn.microsoft.com/library/en-us/dnwebsrv/html/lawsidentity.asp>.

W czasie obsługi interakcji użytkownika z usługą należy uwierzytelnić użytkownika (jeśli to możliwe — na podstawie pojedynczego zestawu poświadczeń), a następnie przekazać usłudze jedynie specyficzne dla niej identyfikatory dotyczące tej interakcji. Nie należy ujawniać głównego identyfikatora użytkownika, który mógłby zostać użyty do skorelowania tożsamości użytkownika w poszczególnych usługach. W przypadkach, gdy taka korelacja jest korzystna i potrzebna (na przykład w celu zapewnienia lepszej obsługi użytkowników i agregacji usług), musi ona zostać przeprowadzona jawnie i za zgodą użytkownika. Korelowanie informacji o użytkowniku bez uzyskania zgody tego użytkownika jest niedozwolone — raz ze względu na dobre praktyki, dwa — na uwarunkowania prawne. W niektórych krajach, takich jak Francja, Portugalia czy Wielka Brytania, tworzenie takich korelacji jest zabronione prawem.

Zapewnienie niezawodnego, bezpiecznego, jednokierunkowego odwzorowania tożsamości użytkownika na specyficzne dla usług i właściwe dla kontekstu interakcji identyfikatory to podstawowe zadanie, realizowane przez powszechną infrastrukturę e-zdrowia, współdzieloną przez wszystkie wchodzące w skład systemu usługi.

Trudne przypadki

W przypadku usług e-zdrowia dość powszechne są sytuacje, których nie da się obsłużyć prostymi, tradycyjnymi metodami zarządzania dostępem. O ile zasada „jeden użytkownik, jeden zestaw poświadczeń, dostęp do wielu usług” to dobra podstawa, istnieją jednak sytuacje, w których potrzebne są bardziej złożone relacje pomiędzy użytkownikami a usługami docelowymi (np. jeden do wielu lub wielu do wielu):

- Wiele osób, z których każda posiada własny zestaw poświadczeń, uzyskuje dostęp do tej samej usługi docelowej w tym samym kontekście (innymi słowy, każda z tych osób korzysta z tego samego identyfikatora specyficznego dla usługi). Sytuacja taka ma miejsce w przypadku urzędników określonej organizacji czy pracowników przedsiębiorstwa lub korporacji.
- Odpowiednio umocowany reprezentant, korzystający z pojedynczego zestawu poświadczeń, uzyskuje dostęp do jednej usługi docelowej, działając w imieniu wielu klientów w różnych kontekstach, a więc używa różnych identyfikatorów specyficznych dla usługi.

Ten typ uwierzytelniania dostępu można uzyskać poprzez powiązanie poświadczeń tożsamości określonej osoby z usługą docelową. Każdorazowe uzyskanie dostępu będzie wymagało podania informacji na temat kontekstu. Istotne jest także zapewnienie niezaprzeczalności i możliwości śledzenia realizowanych transakcji, a także inspekcji wykorzystywanych poświadczeń.

Utrzymywanie takich powiązań, a także śledzenie ich wykorzystania (o ile nie zmieniają się bardzo często) można realizować w ramach wspólnej infrastruktury e-zdrowia, współdzielonej przez wszystkie usługi, zamiast w każdej usłudze z osobna. Rozwiązanie takie ma dwie zalety. Po pierwsze, implementowane jest tylko jednokrotnie, po drugie — nie wymaga modyfikowania istniejących systemów, których dostosowanie do nowych potrzeb może być utrudnione.

Początkowa identyfikacja użytkownika

Bezpieczne udostępnianie usług uzależnione jest od rozwiązania problemu identyfikacji początkowej, to jest od przydzielania poświadczeń tożsamości konkretnym osobom. Prawidłowa identyfikacja początkowa jest niezwykle istotna dla ogólnego bezpieczeństwa i udanego wdrożenia rozwiązania. W przypadku platformy e-zdrowia, gdzie liczba użytkowników może sięgać wielu milionów, a każdy z użytkowników korzysta z rosnącej liczby usług, niezwykle istotne jest przeprowadzenie tej identyfikacji w sposób efektywny, skalowalny i wystarczająco elastyczny, by uwzględnić szeroki zakres wymagań.

Istnieje kilka sposobów początkowej identyfikacji użytkownika:

- **Scentralizowany** — pojedynczy, zunifikowany mechanizm początkowej identyfikacji użytkowników. Po początkowym zidentyfikowaniu użytkownika i przydzieleniu mu poświadczeń tożsamości, wszystkie kolejne relacje z różnymi usługami inicjowane są na podstawie tej jednokrotnej identyfikacji początkowej, co implikuje, że wszystkie usługi opierają się na zunifikowanej procedurze identyfikacji początkowej i ufają jej.
- **Zdecentralizowany** (związany z usługami) — relacje pomiędzy użytkownikiem a poszczególnymi usługami nawiązywane są indywidualnie i są niezależne od relacji z innymi usługami. W takim wypadku nie występują związki zaufania ani

zależności pomiędzy usługami. Poszczególne usługi mogą definiować własne, odpowiednie i różne reguły i procedury identyfikacji początkowej.

- **Zaufanie ukierunkowane** — poszczególne usługi mogą opierać się na procedurach identyfikacyjnych innych usług. Inaczej mówiąc, mogą ufać tym usługom. Model ten jest podobny do modelu scentralizowanego, pozwala jednak na tworzenie wielu różnych związków zaufania.

Model scentralizowany może wydawać się atrakcyjny, prostszy i bardziej efektywny, istnieje jednak kilka przeszkód utrudniających udaną implementację tego modelu w rozwiązaniach e-zdrowia:

- Model ten wymaga istnienia nadrzędnego organu opieki zdrowotnej, któremu ufają i będą ufać wszystkie inne usługi i który będzie prowadził scentralizowany proces identyfikacji. Nawet jeśli dostawcy początkowego zestawu usług uzgodnią odpowiadający im wspólny proces identyfikacji początkowej, to nie ma gwarancji, że powstające w przyszłości usługi będą pasowały do tego modelu.
- Wymagany poziom szczegółowości i niezawodności identyfikacji początkowej jest różny dla różnych kategorii usług, dlatego pojedyncza uniwersalna procedura identyfikacji musi gwarantować najwyższy poziom pewności, jaki może być wymagany przez dowolną z usług. Może to być zbyt uciążliwe dla użytkowników, którzy korzystają wyłącznie z usług o niższych wymaganiach co do identyfikacji początkowej.

Model zdecentralizowany (związany z usługami) daje większą elastyczność i pozwala na uwzględnienie szerszego zakresu wymagań, włącznie z wymaganiami zmiennymi w czasie i nieznanymi podczas pierwotnej implementacji systemu. Jeśli identyfikacja początkowa zostanie oparta na podstawowej, wspólnej strukturze, pozwalającej na stosowanie „wymyślnych” reguł, definiowanych przez poszczególne usługi, rozwiązanie może łatwo ewoluować — można w nim wprowadzać dodatkowe wymagania dla nowych usług bez wpływu na działanie usług już istniejących. Jeśli liczba oferowanych przez system usług jest znaczna, taki zdecentralizowany, związany z usługami model jest jedynym realnym rozwiązaniem.

Szczegółowe praktyczne wskazówki dotyczące implementacji efektywnego, zdecentralizowanego modelu identyfikacji początkowej można znaleźć w rozdziałach poświęconych zarządzaniu tożsamością w sekcjach *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* oraz *Building Blocks* niniejszego opracowania.

Model zdecentralizowany, opisany w sekcji *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* — dzięki elastyczności wymiennych modułów uwierzytelniania początkowego — pozwala także na implementację modelu zaufania ukierunkowanego, który może obejmować sprawdzenie, czy dany użytkownik został wcześniej zidentyfikowany przez inną usługę.

Problemy integracji

W przypadku inicjatyw e-zdrowia prawdopodobnie największym wyzwaniem jest efektywna integracja huba pośredniczącego w kontaktach z klientami ze stale rosnącą liczbą specjalizowanych systemów, specyficznych dla poszczególnych usług. Podczas gdy nawet najbardziej złożone systemy komercyjne muszą zapewnić integrację ze skończonym zestawem systemów, dobrze znanym już na początkowych etapach projektu, przed rozwiązaniami z zakresu e-zdrowia stoi zwykle znacznie trudniejsze zadanie. Muszą one zapewnić platformę umożliwiającą integrację większych i w pewnym zakresie nieznanych zestawów usług, które są dostępne obecnie albo będą dostępne dopiero w przyszłości. Ułatwienie zadań integracji oraz zapobieganie przerwom

Comment [JB2]: nie ma takiej sekcji w otrzymanym do tłumaczenia zestawie dokumentów

w dostępności istniejących usług to ważny warunek udanego wdrożenia rozwiązania e-zdrowia.

Różne możliwości integracji

W kolejnych sekcjach tego dokumentu opisano różne możliwe sposoby integrowania odrębnych systemów (działających na różnych platformach z różnymi zestawami oprogramowania). Wybór najlepszego wariantu zależy od różnych ograniczeń, wymaganego typu integracji i współpracy oraz od innych czynników.

Uwaga — szczegółowe wytyczne Microsoft, dotyczące tego zagadnienia, można znaleźć w dokumencie *Integration Patterns* pod adresem <http://msdn.microsoft.com/library/en-us/dnpag/html/intpatt.asp>.

Integracja natywna

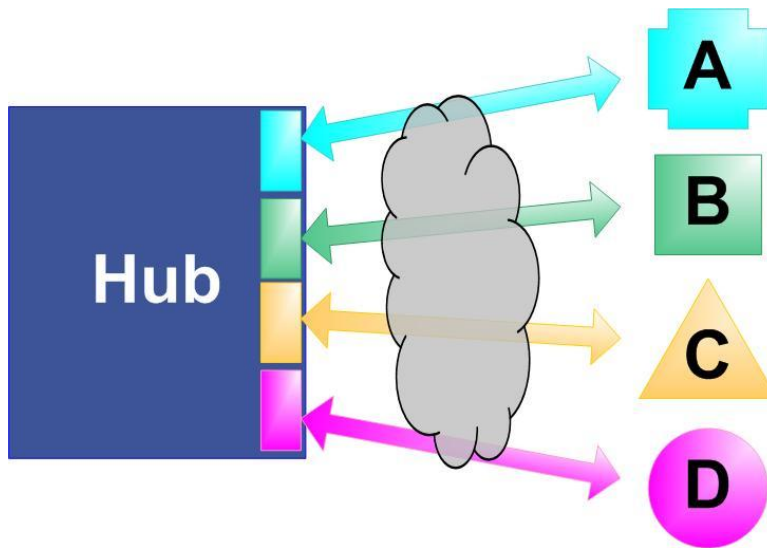
Warunkiem natywnej integracji dwóch systemów jest ich kompatybilność na odpowiednio wysokim poziomie (patrz *sześć poziomów podstawowego modelu interoperacyjności* wymienionych na początku tego opracowania). Innymi słowy, infrastruktura i systemy sieciowe, funkcje dostępu do danych, model usługowy i komponentowy, sposoby integracji procesów, implementacja systemu zabezpieczeń i zarządzania tożsamością oraz sposoby zarządzania systemem muszą być wzajemnie kompatybilne w obu integrowanych rozwiązaniach. Jeśli obydwa systemy mogą współpracować ze sobą, to do ich integracji być może potrzebny będzie tylko minimalny nakład pracy.

Do niedawna taka integracja była możliwa tylko wtedy, gdy obydwa systemy pracowały na tej samej platformie i oparte były na kompatybilnym oprogramowaniu, modelu obiektowym i narzędziach programistycznych. Obecnie — dzięki architekturze zorientowanej na usługi (SOA) — taką interoperacyjność można uzyskać pomiędzy znacznie bardziej zróżnicowanymi platformami, o ile tylko są one zgodne z ogólnie przyjętymi standardami.

Natywna integracja to idealne rozwiązanie dla systemów e-zdrowia, do którego należy dążyć zawsze, gdy jest to możliwe, ponieważ pozwala na zminimalizowanie nakładów pracy niezbędnych do pełnej integracji. Architektura powinna jednak uwzględniać także przypadki, w których ograniczenia istniejących lub przyszłych systemów, niewspierających lub nie mogących wspierać standardowych interfejsów SOA (takich jak usługi Web Services), mogłyby uniemożliwić integrację.

Adaptory w hubie

Jedną z typowych metod integrowania różnorodnych systemów, które być może pracują na różnorodnych platformach, jest wbudowanie odpowiednich adapterów w system centralny, czyli hub. Każdy z adapterów zapewnia dostęp do innego typu systemu zdalnego. Podejście to przedstawiono na *ilustracji 1*. — hub zawiera cztery adaptory, które z wykorzystaniem czterech technologii integracyjnych zapewniają dostęp do czterech usług.



Ilustracja 1. Integracja różnych systemów poprzez zastosowanie adapterów wewnątrz huba

Zaletą tego rozwiązania jest to, że nie trzeba wprowadzać zmian w systemach zdalnych — to hub wykonuje wszystkie dodatkowe prace, takie jak tłumaczenie protokołów sieciowych, transformowanie danych, dopasowywanie semantyki, zarządzanie przepływem wymienianych komunikatów. Rozwiązanie to ma jednak pewne wady:

- komunikacja pomiędzy hubem, wewnątrz którego znajdują się adaptery, a systemami zdalnymi odbywa się za pomocą natywnych protokołów tych systemów; stosowanie tych protokołów poza granicami systemów macierzystych może być kłopotliwe lub niemożliwe, jeżeli komunikacja ma odbywać się poprzez sieć WAN lub poprzez Internet,
- rozszerzenie integracji na systemy nowego typu wymaga wprowadzenia zmian w hubie — konieczne jest dodanie nowego adaptera, co może mieć wpływ na pracę innych usług,
- rozwiązanie to charakteryzuje się ograniczoną skalowalnością, co może mieć duże znaczenie z tego względu, że liczba i zróżnicowanie zintegrowanych systemów stale wzrastają.

Realizacja rozwiązania polegającego na umieszczeniu adapterów w centralnym hubie nie jest zwykle realna. Wyjątkiem może tu być system składający się z kilku adapterów wspierających powszechnie stosowane i dobrze znane standardy.

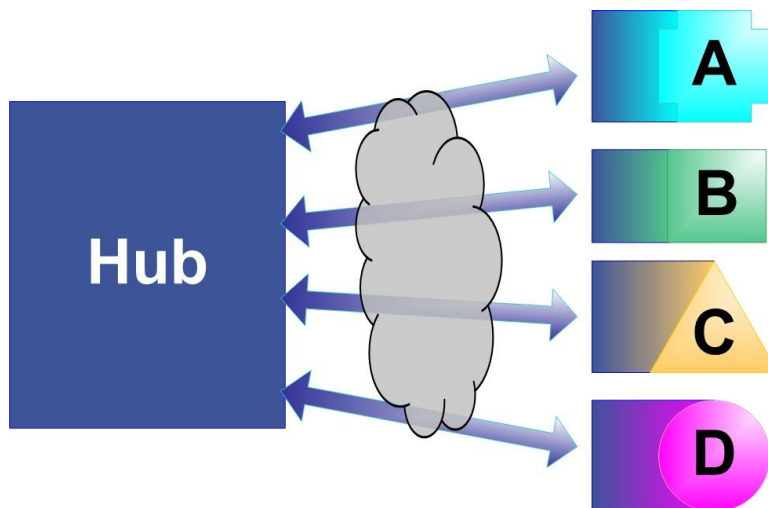
Adaptery w systemach zdalnych

Alternatywą powyższej metody jest stosowanie adapterów zdalnych. W takim wypadku adaptacja cech charakterystycznych danego systemu zdalnego — łączności i protokołów sieciowych, formatów danych i semantyki komunikatów — realizowana jest wewnątrz tego systemu. Każdy system jest sam odpowiedzialny za zapewnienie sposobu komunikacji zgodnego z ogólnie przyjętym standardem.

Obecnie powszechnie przyjętym i rekomendowanym standardem, stosowanym do tego celu, są usługi Web Services. System zdalny, wyposażony w odpowiedni adapter, może zostać w sposób natywny zintegrowany z hubem. Zakres niezbędnych prac integracyjnych zależy od tego, na ile system zdalny różni się od przyjętego standardu

komunikacji. Zwykle jednak jest porównywalny z zakresem prac wymaganych do przygotowania rozwiązania „adapter w hubie” — jedynie umiejscowienie adaptera jest inne.

Adapter może zostać utworzony jako nowa część pierwotnego systemu zdalnego lub zaimplementowany osobno z wykorzystaniem platformy pośredniczącej. Ta druga metoda może być przydatna w przypadku, gdy nie jest możliwe wprowadzenie zmian w istniejących systemach. Zarys architektury, której adaptery umieszczone są w systemach zdalnych, ale nie są ich częścią, przedstawiono na *ilustracji 2*.



Ilustracja 2. Integracja różnych systemów poprzez zastosowanie adapterów w systemach zdalnych

Cechy charakterystyczne takiego rozwiązania to:

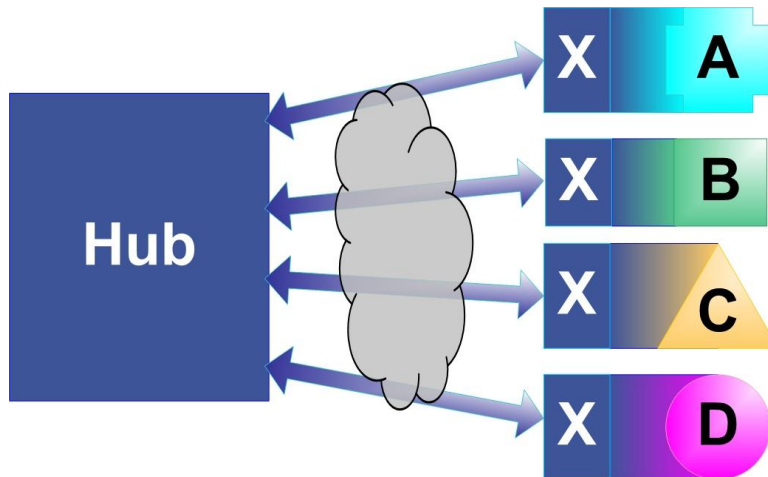
- każdy system jest odpowiedzialny za zapewnienie standardowego sposobu komunikacji; implementacja integracji realizowana jest lokalnie w systemie docelowym, dlatego potencjalnie jest łatwiejsza,
- zestandaryzowany sposób komunikacji ze zdalnymi systemami za pośrednictwem wydzielonej sieci WAN lub innych sieci, takich jak Internet,
- nowe usługi mogą być łatwo dodawane, ponieważ nie ma potrzeby wprowadzania modyfikacji w hubie centralnym; do huba nie trzeba dodawać nowych adapterów, a integracja ze wszystkimi zdalnymi usługami realizowana jest w ten sam zestandaryzowany sposób,
- pomimo że pomiędzy adapterami dla poszczególnych usług może istnieć pewne podobieństwo, nakłady pracy poświęcanej na integrację zależą od liczby integrowanych systemów, a często to samo zadanie realizowane jest wielokrotnie.

Rozdzielenie integracji ogólnej i specyficznej

Adaptery integracyjne są specyficzne, dostosowane i unikatowe dla każdego systemu docelowego, charakteryzują się jednak pewną wspólną funkcjonalnością, niezbędną do

integracji obsługiwanych przez nie systemów zdalnych z hubem centralnym. Wydzielenie takiej ogólnej funkcjonalności (na przykład bezpieczeństwo, niezawodność komunikacji, zarządzanie przepływem komunikatów) z adaptera integracyjnego niesie pewne korzyści. Daje to możliwość wielokrotnego wykorzystywania ogólnej podstawy integracyjnej, co eliminuje powtarzanie realizacji niektórych zadań — integrując nową usługę z systemem wystarczy zaimplementować funkcjonalność specyficzną dla tej usługi.

Na *ilustracji 3.* przedstawiono wielokrotne wykorzystanie określonych elementów (na ilustracji oznaczono je literą X) rozwiązania integracyjnego w więcej niż jednym adapterze, co skraca czas i zmniejsza nakłady pracy związane z implementacją integracji.



Ilustracja 3. Wielokrotne wykorzystanie ogólnych składników integracyjnych w wielu adapterach systemów zdalnych

Wspólne rozwiązanie integracyjne

Następnym logicznym krokiem jest utworzenie wspólnej implementacji ogólnej funkcjonalności integracyjnej, co jest korzystne dla wszystkich usług zdalnych. Jednokrotne zainwestowanie w zaprojektowanie, utworzenie i przetestowanie takiego rozwiązania integracyjnego i udostępnienie go dostawcom usług jako podstawy dla ich własnych rozwiązań integracyjnych pozwala uzyskać znaczne oszczędności przy jednoczesnym zachowaniu wysokiej jakości rozwiązania podstawowego. Wspólne rozwiązanie integracyjne może efektywnie obsłużyć większość trudnych zagadnień, dotyczących niezawodnej komunikacji, bezpieczeństwa i innych wymagań, do których realizacji niezbędne może być zatrudnienie wysoko wykwalifikowanych specjalistów, na co nie każda agencja opieki zdrowotnej może sobie pozwolić — zwłaszcza że usługi e-zdrowia zaczynają być świadczone przez mniejsze, regionalne jednostki. Zrealizowanie lokalnie, w systemie docelowym, jedynie integracji specyficznej dla danej usługi może być znacznie łatwiejsze niż utworzenie pełnego rozwiązania integracyjnego do komunikacji z hubem.

Połączenie takiego podejścia do projektowania struktury z odpowiednim nadzorem i działaniami handlowymi (na przykład udostępnienie kompletnego, bazowego rozwiązania integracyjnego, obejmującego sprzęt, oprogramowanie, instalację i wsparcie techniczne) może w znaczący sposób wpłynąć na upowszechnienie się elektronicznego

dostarczania usług e-zdrowia. Zalety takiego właśnie podejścia do problemu integracji zostały potwierdzone pozytywnymi doświadczeniami w wielu krajach. Jest to znacznie lepsze rozwiązanie niż udostępnienie potencjalnym dostawcom usług jedynie specyfikacji sposobu komunikacji z hubem i pozostawienie ich samym sobie.

Elastyczność i sprawność

Dla większości systemów możliwość efektywnego radzenia sobie ze zmianami oraz adaptacji do nowych wymagań to konieczność. W przypadku rozwiązań integracyjnych e-zdrowia cechy te są jeszcze ważniejsze — szybkość wzrostu i liczba niewiadomych na początku projektu sprawiają, że częstotliwość zmian w tych systemach jest zwykle dużo wyższa. Również potrzeba zapewnienia kompatybilności wstecznej z wdrożonymi wcześniej systemami i wcześniejszymi wersjami oprogramowania jest szczególnie silna.

Dlaczego elastyczność i sprawność są tak ważne

Rozwiązanie integracyjne e-zdrowia to platforma, która musi wspierać stale rosnącą liczbę usług. W odróżnieniu od wielu systemów komercyjnych, gdzie liczba i zróżnicowanie obecnych i przyszłych usług i kanałów dostępu są zwykle dobrze znane, w przypadku platformy integracyjnej e-zdrowia musi istnieć możliwość dostosowania jej do zmieniających się wymagań (niezależnie od tego, czy zmiany te można było przewidzieć, czy nie) — i to najlepiej bez konieczności przeprojektowywania czy zakłócania pracy istniejących usług.

W wielu krajach można spotkać się z następującym schematem: rozwiązanie e-zdrowia powstaje jako projekt pilotowy albo „dla sprawdzenia koncepcji” i obejmuje kilka precyzyjnie wybranych usług (dobrych na podstawie widoczności tych usług, pilności ich udostępnienia i łatwości dostarczenia w postaci elektronicznej). Po udanej fazie wstępnej bardzo szybko rosną ambicje i chęć udostępnienia większej liczby usług. Równocześnie pojawiają się oczekiwania, że dopiero co wdrożona platforma powinna bez trudu poradzić sobie z tym zadaniem.

Zmiany takie jak udostępnienie nowych usług, wdrożenie nowych mechanizmów uwierzytelniania czy nowych kanałów dostępu nie mogą być traktowane jako rzadkie przypadki, wymagające okresowego wdrażania nowych wersji platformy integracyjnej e-zdrowia. Wdrażanie nowych usług powinno być standardową funkcją systemu. Warunek ten musi zostać we właściwy sposób uwzględniony w projekcie architektury systemu, muszą też powstać odpowiednie narzędzia i procedury. Idealne rozwiązanie powinno pozwalać na wprowadzanie takich zmian w działającym systemie bez potrzeby wstrzymywania jego pracy. Udana wdrożenia w kilku krajach potwierdziły, że opracowanie takiego systemu jest możliwe.

Tworzenie architektury z myślą o elastyczności

Uzyskanie tak wysokiej elastyczności to główny wyznacznik docelowej architektury systemu. Umożliwienie wprowadzania w systemie tak dużych zmian (dodawanie nowych usług, nowych typów transakcji, modyfikowanie reguł walidacji danych, rekonfigurowanie reguł przepływu informacji) — i to bez modyfikowania kodu rozwiązania — wymaga, by rozwiązaniem można było zarządzać za pomocą parametrów konfiguracyjnych i danych modyfikowanych zgodnie z potrzebami wtedy, gdy potrzeby te występują.

Architektura, która z założenia wspiera modułowość na każdym poziomie (mechanizmy autoryzacji, modele identyfikacji, reguły specyficzne dla usług), to warunek konieczny. Jeśli założymy, że wymagania i reguły związane z poszczególnymi usługami ulegają zmianom (jeśli nie już na pierwszych etapach projektu, to na pewno w przyszłości), to architektura rozwiązania musi wspierać klasyfikację. Pozwala to zminimalizować liczbę powszechnych reguł i przepływów komunikatów, które będą musieli obsługiwać dostawcy

w celu uwzględnienia ich usług w systemie. Gdy rozwiązanie musi wspierać stale rosnącą liczbę usług, unikanie zakładania z góry określonego sposobu komunikacji, konfiguracji zabezpieczeń czy narzucania innych ograniczeń logistycznych to konieczność.

Zabezpieczanie rozwiązania

Ze wszystkich problemów, jakie architekci oprogramowania i programiści muszą rozwiązać, tworząc platformę integracyjną e-zdrowia, bezpieczeństwo — jeśli nie zostanie we właściwy sposób zaimplementowane na wszystkich poziomach, w całym zakresie aplikacji — może sprawić największe kłopoty. Zabezpieczenia często traktowane są jako funkcje dodatkowe, o które można zacząć się martwić już po zaprojektowaniu i wdrożeniu rozwiązania. Takie podejście to proszenie się o kłopoty. Bezpieczeństwo musi zostać uwzględnione w architekturze aplikacji już na początku projektu.

Dlaczego bezpieczeństwo jest tak ważne?

Wszystkie witryny internetowe, usługi i aplikacje muszą stale bronić się przed utratą danych i atakami powodowanymi przez użytkowników działających w złych zamiarach, automatyczne programy (takie jak wirusy i robaki internetowe) oraz przed przestojami powodowanymi przez ataki DoS (Denial of Service — zablokowanie usługi). Projekty w zakresie e-zdrowia niosą ze sobą szczególne ryzyko — większe niż w przypadku nawet instytucji finansowych takich jak banki internetowe. Jest tak, ponieważ systemy takie są ważnym celem dla:

- osób próbujących dokonać kradzieży tożsamości — na przykład pobrać szczegółowe informacje dotyczące zeznań podatkowych, prawa jazdy, paszportu, dokumentacji medycznej i innych szczegółowych informacji umożliwiających kradzież tożsamości użytkownika,
- anarchistów i politycznie zaangażowanych włamywaczy, mających na celu włamanie się do systemu opieki zdrowotnej i spowodowanie jak największych zniszczeń,
- ataków na indywidualnych użytkowników, podyktowanych celami pozapolitycznymi, na przykład prób podważenia bezpieczeństwa systemu w oczach użytkownika lub uniemożliwienia mu dostępu do usług, z których ma prawo korzystać,
- nadużyć lub prób nadużyć poprzez nieautoryzowaną modyfikację danych, na przykład w celu uniknięcia płatności podatku dochodowego, obrotowego lub od wartości dodanej. Do ataków tego typu można również zaliczyć próby zatarcia śladów wykonania działań, co przez opinię publiczną nie zawsze jest uznawane za nadużycie.

Niektóre organizacje i instytucje starają się ukryć rezultaty naruszeń ich systemów bezpieczeństwa. Aplikacje e-zdrowia charakteryzują się jednak dobrą widocznością dla społeczeństwa, a więc każdy udany atak z pewnością nie zostanie przeoczony przez użytkowników. Wydarzenia takie stawiają organizację w kłopotliwej sytuacji — zarówno pod względem politycznym, jak i w zakresie public relations — wobec dostawców i użytkowników. Efektem nawet najmniejszych problemów z bezpieczeństwem mogą być nieprzewidziane koszty oraz utrata zaufania użytkowników i innych organizacji opieki zdrowotnej, a więc — na dłuższą metę — utrudnienie upowszechnienia elektronicznych usług medycznych.

Projektowanie bezpiecznych rozwiązań

Szczegółowe wskazówki dotyczące projektowania i tworzenia bezpiecznych rozwiązań zawarto w sekcji *Bezpieczeństwo* w rozdziale *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* niniejszego przewodnika. Wskazówki obejmują między innymi sposób zastosowania wielu warstw zabezpieczeń do realizacji trzech głównych celów (poufność, integralność danych, niezawodne uwierzytelnianie). Opisano także zagadnienia związane z modelowaniem zagrożeń oraz dostępne środki zaradcze.

Bezpieczeństwo to jednak coś więcej niż sama implementacja techniczna. Aby rozwiązanie mogło być na bieżąco przystosowywane do stale zmieniających się wymagań w zakresie bezpieczeństwa, podczas projektowania należy wziąć pod uwagę dodatkowe uwarunkowania:

- możliwość stopniowego rozbudowywania i wprowadzania nowych usług i funkcji,
- zapewnienie bezpiecznych sposobów przechowywania istotnych danych, wykorzystanie kluczy cyfrowych i certyfikatów,
- zarządzanie zespołem programistycznym i metodologią implementacji w celu zagwarantowania przestrzegania najlepszych praktyk,
- przetestowanie zabezpieczeń aplikacji we wszystkich możliwych sytuacjach w celu upewnienia się, że projekt architektury jest poprawny i spełnia założone wymagania odnośnie bezpieczeństwa,
- wprowadzenie odpowiednich zabezpieczeń w trakcie oraz po wdrożeniu środowiska; upewnienie się, że konfiguracja i bezpieczeństwo instalacji spełniają założone wymagania,
- monitorowanie wydajności aplikacji i usług, inspekcja procesów, tworzenie planów awaryjnych na wypadek włamania lub uszkodzenia danych,
- stałe działania mające na celu analizowanie nowo odkrytych zagrożeń bezpieczeństwa, regularne aktualizowanie sprzętu i oprogramowania z wykorzystaniem dodatków service pack.

Firma Microsoft stara się ułatwić projektowanie, tworzenie i wdrażanie bezpiecznych rozwiązań, zapewniając przewodniki, wzorce i przykłady, szczegółową dokumentację dla programistów oraz udokumentowane najlepsze praktyki. Materiały te można znaleźć w witrynie Microsoft Security Developer Center pod adresem <http://msdn.microsoft.com/security>.

Skalowalność, wydajność, dostępność

Rozwiązania e-zdrowia muszą zwykle spełniać rygorystyczne wymagania pod względem wydajności i skalowalności. Ze względu na swą naturę, wiele interakcji z usługami opieki zdrowotnej jest realizowane dość rzadko — raz na rok lub raz na kwartał — z charakterystycznymi szczytami aktywności przypadającymi na terminy takie jak koniec roku podatkowego. Wydajność tworzonego systemu powinna pozwalać na obsługę takich szczytowych aktywności bez znacznych spadków wydajności. Jest to szczególnie istotne dla powszechnej popularyzacji świadczenia usług opieki zdrowotnej drogą elektroniczną. Wszelkie awarie, opóźnienia czy brak dostępności usług w takich krytycznych okresach są kłopotliwe, podważają publiczne zaufanie co do pewności świadczonych usług i mają negatywny wpływ na jeden z najważniejszych czynników istotnych dla popularyzacji elektronicznego dostępu do usług — przewagę szybkości interakcji elektronicznych nad tymi obsługiwanymi za pomocą tradycyjnych kanałów dostępu.

Rozwiązania e-zdrowia, zwykle rozpoczynające swój żywot jako niewielkie projekty, stopniowo rosną i rozbudowują się w miarę wzrostu popularności usług elektronicznych

oraz liczby użytkowników korzystających z takich usług. Gdy usługi udostępniane są za pośrednictwem współdzielonej infrastruktury, to poza wzrostem intensywności korzystania z każdej z usług, mamy też wzrost liczby usług. Warto więc dwukrotnie przemyśleć i zweryfikować szacowane i przewidywane współczynniki wzrostu. Zbyt często nasze założenia są za bardzo optymistyczne.

Podstawowym wyznacznikiem jest ocena takich czynników poprzez porównanie ich z dostępnymi, znanymi metrykami (obecna liczba interakcji w ramach tradycyjnych kanałów dostępu, rozpowszechnienie usług elektronicznych w podobnych obszarach zastosowań) oraz ograniczeniami (przepustowość sieci, możliwości wykorzystywanych systemów zaplecza). W kilku przypadkach proste oszacowanie na podstawie liczby interakcji pomnożonej przez średni ruch generowany przez taką interakcję dało wyniki znacznie przekraczające przepustowość wykorzystywanej sieci, jasno pokazując, że przyjęte wcześniej założenia były nierealne i niemożliwe do osiągnięcia z powodu innych ograniczeń. Ślepe akceptowanie takich „przewidywanych” wymagań w zakresie wydajności, a także próby spełnienia tak postawionych założeń mogą niepotrzebnie skomplikować projekt i implementację platformy e-zdrowia.

Wskazówki na temat projektowania wydajnych i skalowalnych rozwiązań e-zdrowia można znaleźć w sekcji *Skalowalność i wydajność* rozdziału *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* tego opracowania.

Dostępność i odporność

Z zagadnieniami skalowalności i wydajności aplikacji związane są także inne problemy. Ograniczona wydajność w oczywisty sposób wpływa na dostępność rozwiązania, powodując chwilowe lub nawet długotrwałe utrudnienia dla użytkowników próbujących uzyskać dostęp do aplikacji i korzystać z niej. Zapewnienie wysokiej dostępności oznacza zagwarantowanie, że wszystkie składniki infrastruktury, takie jak sprzęt, oprogramowanie czy sieć, są odporne na awarie. Innymi słowy, żadna pojedyncza awaria nie powinna zatrzymać pracy całego systemu.

Zagadnienia dostępności i odporności dotyczą wielu problemów związanych z architekturą rozwiązania. W sekcji *Skalowalność i wydajność* rozdziału *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* opisano, jak skalowanie sprzętu — dzięki wykorzystaniu wielu komponentów lub zastosowaniu komponentów redundantnych — pozwala na ochronę systemu przed przestojami, powodowanymi przez pojedynczą awarię sprzętu lub oprogramowania, poprzez przejmowanie pracy uszkodzonych komponentów.

Odtwarzanie po awariach

Oczywiście nie można zagwarantować, że awaria nigdy się nie wydarzy. Awaria może zostać spowodowana błędem w oprogramowaniu, uszkodzonym komponentem sprzętowym, a nawet być skutkiem uszkodzenia łącza internetowego przez ekipę wykonującą w okolicy roboty drogowe. W przypadku poważniejszych wydarzeń, takich jak pożar lub katastrofa budowlana budynku, w którym zainstalowane są serwery, awaria aplikacji jest prawie że gwarantowana. Innymi przyczynami awarii mogą być złośliwe działania operatorów systemu, nieumyślne pomyłki personelu czy błędy logiczne danych, które mogą spowodować utratę zawartości całych macierzy dyskowych.

Aby móc poradzić sobie z takimi problemami, niezbędne jest opracowanie szczegółowego, ścisłego, w pełni przetestowanego planu postępowania na wypadek takiej awarii. Plan powinien obejmować wszystkie możliwości — od ponownego wczytania danych z dysków lub taśm zapasowych po przeniesienie działalności do innej lokalizacji, wyposażonej w sprzęt i oprogramowanie gotowe do natychmiastowego podjęcia pracy. Istnieją na rynku firmy świadczące usługi planowania i utrzymywania

takich systemów, co może pozwolić na znaczne zredukowanie czasu przestoju aplikacji, których stała dostępność — jak w przypadku rozwiązań e-zdrowia — może być kwestią życia lub śmierci.

Konstrukcja wspólnego huba

Powszechne rozwiązanie integracyjne e-zdrowia, współdzielone przez wiele usług, pozwala w efektywny sposób rozwiązać wiele z przedstawionych dotychczas problemów. Bardziej szczegółowe informacje na ten temat zamieszczono w sekcji *Hub usług e-zdrowia* rozdziału *Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia* w tym przewodniku. Chociaż rozwiązanie to charakteryzuje się niewątpliwymi zaletami, jego wdrożenie może wiązać się koniecznością pokonania wielu przeszkód natury politycznej lub komercyjnej oraz innych utrudnień. Najważniejsze z tych zagadnień omówiono w kolejnych sekcjach dokumentu.

Potrzeba ustalenia właściciela lub finansującego

W wielu krajach agencje opieki zdrowotnej wdrażają własne, oddzielne, nieskoordynowane ze sobą rozwiązania e-zdrowia, będące często rozszerzeniami systemów i projektów prowadzonych już przez te agencje. Nawet jeśli istnieje jakiś centralny organ opieki zdrowotnej, odpowiedzialny za inicjatywy e-zdrowia, może on mieć zbyt małe możliwości, by wspierać i koordynować implementację wspólnej infrastruktury e-zdrowia oraz zbyt małe fundusze, by zaprojektować, opracować i wdrożyć taką infrastrukturę. W efekcie — nawet jeśli większość uczestników rynku usług medycznych uzna zalety stosowania wspólnej platformy integracyjnej i przekona się o możliwych oszczędnościach — bez jasnego wskazania właściciela i finansującego rozwiązanie takie ma nikłe szanse na praktyczną realizację.

Najlepsze rezultaty można osiągnąć, gdy istnieje centralna agencja opieki zdrowotnej, posiadająca niezbędną władzę i zasoby finansowe umożliwiające popularyzację usług e-zdrowia, która może pokierować pracami nad tworzeniem wspólnej platformy integracyjnej.

Początkowa inwestycja z odroczonymi korzyściami

Inwestycja w opracowanie architektury, zaprojektowanie, utworzenie i wdrożenie wspólnej platformy to pierwszy krok w kierunku udostępnienia efektywnych usług e-zdrowia. W początkowych fazach tworzona jest jednak tylko podstawowa infrastruktura. Infrastruktura ta nie jest widoczna dla użytkownika końcowego i bezpośrednio nie przynosi żadnych korzyści. Jest jedynie gwarancją sukcesu usług e-zdrowia, które są stopniowo udostępniane.

Aby móc zademonstrować zalety nowej platformy, potrzebne jest szybkie wdrożenie początkowego zestawu usług. Dzięki temu dostawcy usług i konsumenci usług szybciej zobaczą bardziej namacalne korzyści. Co więcej, jeśli platforma została poprawnie zaprojektowana i zaimplementowana, ogólne korzyści będą coraz lepiej widoczne wraz z każdą nową usługą dodaną do platformy.

Typowe konflikty z projektami indywidualnymi

Podczas jednoczesnych prac projektowania i implementowania platformy integracyjnej e-zdrowia oraz początkowego zestawu usług, które będą udostępniane w oparciu o tę platformę, pojawiają się napięcia powodowane różnicami pomiędzy ogólnym charakterem platformy a specyficznymi wymaganiami każdej z usług. O ile napięcia takie sprzyjają kreatywności i mają pozytywny wydźwięk, stanowiąc dobry sposób walidacji styku pomiędzy platformą a dostawcami usług na wczesnych stadiach projektu, mogą

także wywierać negatywny wpływ na projekt platformy powodując, że zostanie w niej zaimplementowana funkcjonalność, która nie powinna się tam w ogóle znaleźć.

Pod silną presją ciasnych ram czasowych i ograniczonych środków finansowych, wśród wykonawców odpowiedzialnych za poszczególne części projektu szczególnie wyraźnie widoczna staje naturalna tendencja przesuwania granicy pomiędzy usługami i przekazywania części zadań komuś innemu. W powiązaniu z faktem, że projekty e-zdrowia często prowadzone są przez jedną lub kilka silnych agencji opieki zdrowotnej, które zwykle zakres i budżet projektu wspólnej infrastruktury ustalają samodzielnie, naciski na przesunięcie części funkcjonalności — szczególnie tej, która nie jest całkowicie ogólna, ale zaimplementowanie jej w platformie przyniosłoby oszczędności czasu i kosztów — mogą być bardzo duże. Działania takie z pewnością naruszają integralność architektury i będą miały wpływ na pozostałe usługi, które trzeba będzie dostosować do zmian wprowadzonych dla wygody zaledwie kilku osób.

Architektura referencyjna ogólnego rozwiązania integracyjnego e-zdrowia

W tej sekcji przedstawiamy typową referencyjną architekturę rozwiązania integracyjnego e-zdrowia, opartą na połączonej platformie opieki zdrowotnej Microsoft Connected Health Framework (CHF). Na rozdział ten składają się następujące sekcje:

- **Reguły rządzące architekturą** — omówienie ogólnych zasad projektowania oraz architektury zorientowanej na usługi (Service Oriented Architecture — SOA), na której oparta jest cała platforma.
- **Hub usług e-zdrowia** — jak zapewnić wspólną infrastrukturę, z której może korzystać wielu dostawców usług e-zdrowia.
- **Usługi huba e-zdrowia** — opis poszczególnych usług zapewnianych przez hub usług e-zdrowia. Usługi te to między innymi:
 - usługi zarządzania tożsamością,
 - usługi zachowania poufności i bezpieczeństwa,
 - usługi prezentacji i punktu dostępu,
 - usługi publikacji i wyszukiwania usług,
 - usługi elektronicznej dokumentacji medycznej (Electronic Health Record — EHR),
 - usługi domeny zdrowotnej,
 - usługi rejestru medycznego,
 - usługi integracyjne,
 - usługi operowania danymi,
 - **usługi zarządzania systemem,**
 - **usługi komunikacyjne.**
- **Opcje wdrożeniowe** — opis różnych metod wdrażania usług, jakie warto rozważyć podczas implementacji referencyjnej architektury e-zdrowia, uwzględniając przy tym zmienne uwarunkowania prawne i inne ograniczenia.
- **Wydajność i skalowalność** — omówienie zagadnień związanych ze spełnieniem kryteriów dostępności, niezawodności i wydajności. Opisano między innymi sposoby planowania wydajności systemu oraz implementacji skalowalnej architektury sprzętowej i programistycznej.
- **Zarządzanie i eksploatacja** — zagadnienia związane z eksploatacją i zarządzaniem rozwiązaniem (w sensie biznesowym), zapewnieniem pomocy i wsparcia technicznego oraz świadczeniem usług.

Reguły rządzące architekturą

Aby pomyślnie rozwiązać problemy opisane w rozdziale *Uwzględnienie powszechnych problemów dotyczących architektury* wyżej w tym dokumencie, opisywana tu architektura referencyjna została przygotowana w oparciu o następujące zasady:

Orientacja na usługi

Zastosowanie architektury zorientowanej na usługi (Service Oriented Architecture — SOA) w implementacji dużych i złożonych systemów informatycznych, jakimi są rozwiązania integracyjne e-zdrowia, pozwala na spełnienie warunku podstawowego — sprawienie, by systemy te były łatwe w adaptacji, elastyczne i niezawodne.

Architektura zorientowana na usługi to struktura oraz zestaw zasad i praktyk pozwalających na implementowanie funkcjonalności aplikacji w usługach dostępnych z zewnątrz. Szczegółowość dekompozycji na usługi zależy wyłącznie od wymagań strony korzystającej z tych usług — usługi pozwalają na wyodrębnienie implementacji części funkcjonalności aplikacji z wykorzystaniem pojedynczego, opartego na standardach, typu interfejsu.

Funkcjonalność platformy integracyjnej e-zdrowia powinna być dostępna w postaci zestawu ogólnych usług, z których można korzystać niezależnie od innych usług i wtedy, gdy jest to potrzebne.

Interfejsy i standardy

Dominującą metodą udostępniania usług w sposób zgodny z przyjętymi standardami i niezależny od implementacji oraz wykorzystywanej platformy stają się usługi sieciowe Web Services. Standardy związane z usługami Web Services wdrażane są przez wszystkich wiodących producentów oprogramowania i coraz więcej produktów programistycznych wspiera te standardy. Pozwoli to na stopniowe zmniejszenie ilości pracy poświęcanej na tworzenie kodu pisanego „na miarę” na rzecz korzystania — tam, gdzie jest to możliwe — z produktów komercyjnych. Oparcie implementacji podstawowych funkcji oprogramowania, takich jak bezpieczeństwo czy niezawodna komunikacja, na gotowych narzędziach i produktach pozwoli zmniejszyć koszty i nakłady pracy niezbędne do uzyskania wymaganej funkcjonalności.

Szczegółowe informacje oraz łącza do pełnej specyfikacji standardów usług Web Service można znaleźć pod adresem <http://msdn.microsoft.com/library/en-us/dnglobspec/html/wsspecover.asp> oraz w sekcji *Odsyłacze, listy kontrolne i dalsze informacje* w ostatniej części tego opracowania.

Wyszukiwanie usług

Architektura referencyjna zapewnia infrastrukturę pozwalającą na rejestrowanie i wyszukiwanie dostępnych usług (w czasie projektowania lub w czasie pracy aplikacji) oraz repozytorium do przechowywania metadanych opisujących usługi — schematów, interfejsów, zasad. Format metadanych odpowiada powszechnie przyjętym standardom branżowym.

Stowarzyszone funkcje zabezpieczeń

Architektura musi obsługiwać wiele różnych mechanizmów uwierzytelniania, typów poświadczeń, dostawców tożsamości, metod autoryzacji i modeli zaufania. Co więcej, niektóre z nich nie są znane nawet na etapie projektowania architektury. Architektura powinna zatem zapewnić ogólną strukturę, umożliwiającą stopniowe dodawanie nowych

dostawców i mechanizmów oraz konstruowanie systemów o różnych topologiach, uwzględniających specyficzne wymagania i ograniczenia.

Nie należy zakładać, że możliwe jest centralne uwierzytelnianie i zarządzanie wszystkimi potencjalnymi użytkownikami systemu przez jednego dostawcę usług.

Wprowadzenie standardów usług Web Service także w tej przestrzeni pozwoli na uzyskanie interoperacyjności pomiędzy różnymi implementacjami i efektywne wykorzystywanie — gdy tylko staną się dostępne — produktów komercyjnych o takich możliwościach.

Elastyczność

Kluczem do sukcesu rozwiązań e-zdrowia jest elastyczność — zapewniana przez architekturę i uwzględniona już na pierwszym etapie projektu. Rozszerzanie i adaptowanie podstawowej infrastruktury w odpowiedzi na zmieniające się wymagania (na przykład dodawanie nowych usług lub dostawców uwierzytelniania) to standardowy — możliwy do realizacji każdego dnia — przypadek użycia, który powinien być poprawnie obsługiwany przez platformę, procesy i narzędzia, a nie proces realizowany okresowo przy okazji wdrażania nowej wersji platformy.

Bezpieczeństwo

Aby umożliwić budowanie rozwiązań gwarantujących odpowiedni poziom bezpieczeństwa dostępu do usług e-zdrowia, już w pierwszych fazach projektowania architektury należy pomyśleć o wielowarstwowych zabezpieczeniach i innych aspektach związanych z bezpieczeństwem systemu. Sam model zabezpieczeń powinien być elastyczny i pozwalać na adaptację w celu uwzględnienia różnych — dostępnych obecnie i w przyszłości — technik zabezpieczeń bez potrzeby projektowania systemu od początku.

Skalowalność i wydajność

Architektura powinna zapewniać adekwatną wydajność i pozwalać na rozbudowę systemu wraz ze wzrostem zapotrzebowania na dostęp do coraz szerszego zakresu oferowanych usług.

Hub usług e-zdrowia

Wspólna infrastruktura, współdzielona przez wielu dostawców usług e-zdrowia, jest rozwiązaniem wielu z problemów naświetlonych w rozdziale *Uwzględnienie powszechnych problemów dotyczących architektury*. Infrastrukturę tę będziemy dalej nazywali **hubem usług e-zdrowia** (lub w skrócie — hubem).

Chociaż zalety stosowania takiego huba są tym większe, im więcej usług z niego korzysta (zamiast niezależnie implementować podobną funkcjonalność), nie oznacza to wcale, że wszystkie usługi e-zdrowia muszą być obsługiwane za pomocą tylko jednego huba. Możliwa jest współpraca wielu hubów, z których każdy implementuje tylko część z pełnej funkcjonalności i współpracuje z pozostałymi hubami w różnych topologiach w stowarzyszonym modelu. Celem jest uzyskanie elastyczności umożliwiającej dostosowanie systemu do różnych wymagań, topologii i potrzebnej skali implementacji przy zachowaniu tych samych metod projektowania poszczególnych węzłów.

Kontekst i interakcje zewnętrzne huba

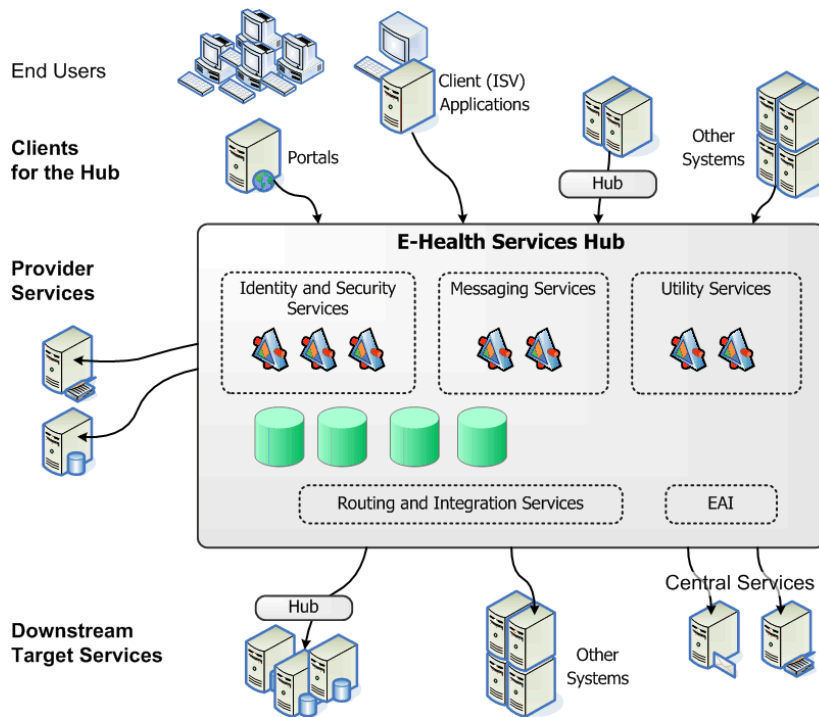
Hub usług e-zdrowia implementuje zestaw usług udostępnianych klientom różnego typu. Sam hub także jest klientem — korzysta z innych systemów (usług) zewnętrznych (patrz *ilustracja 4*).

Interakcje z klientami

Z punktu widzenia architektury, klientem jest wszystko, co korzysta z usług udostępnianych przez hub usług e-zdrowia. Klientami mogą być witryny internetowe i portale obsługujące własnych użytkowników końcowych w oparciu o usługi świadczone przez hub, aplikacje uruchamiane w systemach klienckich lub inne systemy korzystające z usług huba.

Typowe kategorie klientów huba to:

- **portale** — mogą korzystać z udostępnianych przez hub usług zarządzania tożsamością i bezpieczeństwem w celu uwierzytelniania użytkowników, wykonywania zadań konserwacyjnych, przekazywania dokumentów w imieniu użytkownika poprzez usługi komunikacyjne huba lub wykorzystywać usługi narzędziowe,
- **aplikacje klienckie** — na przykład aplikacje kliniczne uruchamiane na stacjach roboczych i serwerach klientów, kontaktujące się z hubem w celu przekazywania dokumentów i dostępu do innej funkcjonalności,
- **inne systemy** (albo inne huby) — mogą działać i korzystać z funkcjonalności huba jako klienty. Mogą to być systemy utrzymywane przez niezależne organizacje, systemy zaplecza (agencje opieki zdrowotnej) lub inne huby.



Ilustracja 4. Kontekst i interakcje zewnętrzne huba usług e-zdrowia

Wszystkie interakcje z klientami odbywają się za pośrednictwem opublikowanych interfejsów, opartych na branżowych standardach usług Web Services. Podejście takie zapewnia niezbędną otwartość, kompatybilność z szeroką gamą produktów komercyjnych oraz możliwość współpracy z oprogramowaniem działającym na innych platformach. Interakcje klientów z hubem usług e-zdrowia są niezależne od sposobu implementacji aplikacji klienckich i platform, na których aplikacje te są uruchamiane.

Uwaga — warto pomyśleć przyszłościowo i udostępnić pełną funkcjonalność huba za pośrednictwem interfejsów programistycznych. W niektórych wczesnych implementacjach takich systemów częścią huba był przeglądarkowy interfejs użytkownika i część funkcjonalności dostępna była wyłącznie za pośrednictwem przeglądarki. Po pewnym czasie okazało się, że wiele agencji opieki zdrowotnej wolałoby korzystać z funkcjonalności huba za pośrednictwem własnych portali ze względu na łatwiejszą obsługę. Dodanie interfejsów programistycznych do działającego systemu jest zwykle dużo trudniejsze niż uwzględnienie ich w projekcie już na samym początku.

Interakcje z usługami zewnętrznymi

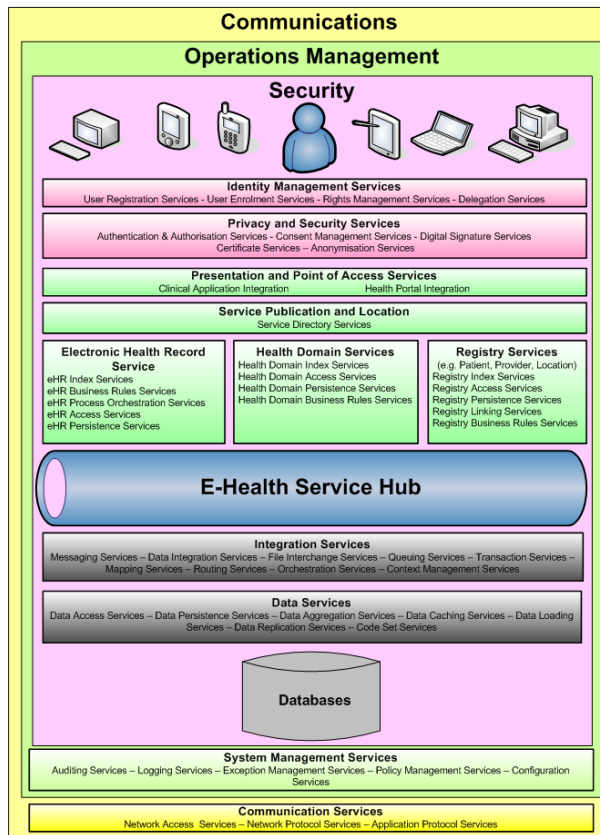
Hub działa także jako klient, uzyskując dostęp do innych usług (wewnętrznych lub zewnętrznych). Z architektonicznego punktu widzenia interakcje te nie różnią się od siebie, choć można wyróżnić wśród nich następujące typy:

- **Usługi, na których opiera się podstawowa funkcjonalność huba** — zewnętrzni dostawcy mechanizmów uwierzytelniania wywoływani przez hub w celu weryfikacji poświadczeń tożsamości.
- **Specjalizowane usługi docelowe**, otrzymujące żądania od klientów za pośrednictwem huba. Hub działa jako pośrednik i może pełnić dodatkowe funkcje na drodze przekazywania komunikatów — na przykład zapewnić walidację. Usługi docelowe mogą być świadczone przez agencje opieki zdrowotnej, inne systemy lub inne huby integracyjne działające w takich systemach.
- **Usługi centralne**, z których korzystają klienci. Pomimo że hub może dostarczać usługi ogólnego przeznaczenia, pod względem architektury systemu usługi te znajdują się na zewnątrz huba. Usługi takie często są hostowane i zarządzane w oparciu o infrastrukturę techniczną huba centralnego, a dostęp do nich realizowany jest za pośrednictwem huba.

Usługi świadczone przez hub

Pełny zakres usług zapewnianych przez hub można podzielić na następujące główne kategorie (patrz *ilustracja 4*):

- usługi zarządzania tożsamością,
- usługi zachowania poufności i bezpieczeństwa,
- usługi prezentacji i punktu dostępu,
- usługi publikacji i wyszukiwania usług,
- usługi elektronicznej dokumentacji medycznej (Electronic Health Record — EHR),
- usługi domeny zdrowotnej,
- usługi rejestru medycznego,
- usługi integracyjne,
- usługi operowania danymi,
- usługi zarządzania systemem,
- usługi komunikacyjne.



<rysunek>

komunikacja
zarządzanie eksploatacją
bezpieczeństwo

usługi zarządzania tożsamością

usługi zgłoszenia użytkownika — usługi rejestracji użytkownika — usługi zarządzania prawami dostępu — usługi delegowania

usługi zachowania poufności i bezpieczeństwa

usługi uwierzytelniania i autoryzacji — usługi zarządzania zgodami — usługi podpisu cyfrowego – usługi certyfikatów – usługi anonimizacji

usługi prezentacji i punktu dostępu

integracja aplikacji klinicznych — integracja portali zdrowotnych

publikacja i wyszukiwanie usług

usługi katalogu usług

usługi elektronicznej dokumentacji medycznej

usługi indeksu EHR

usługi reguł biznesowych EHR

usługi orkiestracji procesów EHR

usługi dostępu do EHR

usługi składowania danych RHR

usługi domeny zdrowia

usługi indeksu danych domeny zdrowia
usługi dostępu do danych domeny zdrowia
usługi składowania danych domeny zdrowia
usługi reguł biznesowych domeny zdrowia

usługi rejestru medycznego

(np. pacjentów, dostawców, placówek)

usługi indeksu rejestru medycznego
usługi dostępu do rejestru medycznego
usługi składowania danych rejestru medycznego
usługi łączenia danych rejestru medycznego
usługi reguł biznesowych rejestru medycznego

hub Connected Health Framework

usługi integracyjne

usługi komunikacji — usługi integracji danych — usługi wymiany plików — usługi kolejowania —
usługi obsługi transakcji — usługi odwzorowywania tożsamości — usługi przekazywania
komunikatów — usługi orkiestracji — usługi zarządzania kontekstem

usługi operowania danymi

usługi dostępu do danych — usługi składowania danych — usługi agregacji danych — usługi
buforowania danych — usługi ładowania danych — usługi replikacji danych — usługi zestawów
kodu

bazy danych

usługi zarządzania systemem

usługi inspekcji — usługi dzienników zdarzeń — usługi zarządzania wyjątkami — usługi
zarządzania zasadami — usługi konfiguracji

usługi komunikacyjne

usługi dostępu sieciowego — usługi protokołów sieciowych — usługi protokołów aplikacyjnych
</rysunek>

Każda z tych grup została omówiona w kolejnych sekcjach niniejszego dokumentu.

Usługi zarządzania tożsamością

Usługi zarządzania tożsamością, udostępniane przez hub usług e-zdrowia, można podzielić na następujące kategorie:

- usługi zgłaszania użytkowników — początkowa identyfikacja użytkowników oraz utworzenie cyfrowej tożsamości dla każdego z użytkowników;
- usługi rejestracji użytkowników — rejestracja cyfrowej tożsamości użytkownika w usługach, z których użytkownik będzie korzystał;
- usługi zarządzania prawami dostępu — stały nadzór nad rejestracją użytkowników oraz rejestrowaniem się do usług;
- usługi delegowania — przydzielanie praw do działania w imieniu wybranej jednostki w kontekście określonej usługi.

Podstawowy model tożsamości i zasady

Sekcja ta zawiera definicję podstawowych encji modelu tożsamości, relacji pomiędzy nimi oraz opis reguł określających wszystkie aspekty zarządzania tożsamością w architekturze. Ogólny model zarządzania tożsamością powinien być na tyle otwarty i elastyczny, by można go było dostosować do różnych (obecnych i przyszłych) wymagań dotyczących różnych typów uwierzytelniania, odwzorowywania poświadczeń na identyfikatory użytkowników stosowane w poszczególnych usługach, delegowania uprawnień itp.

Podstawowe encje modelu tożsamości

Poniżej zestawiono opis encji składających się na podstawowy model tożsamości:

- **użytkownik** (petent, wyborca) — osoba, która musi zostać zidentyfikowana, uwierzytelniona i otrzymać autoryzację do korzystania z określonych usług. W ramach modelu użytkownicy reprezentowani są przez poświadczenia i tożsamość;
- **tożsamość** — reprezentuje i identyfikuje użytkownika w systemie zarządzania tożsamością. Pojedynczy użytkownik może posiadać kilka niezależnych tożsamości, odpowiadających różnym pełnionym przez niego rolaom w systemie lub grupom wydzielonych usług;
- **poświadczenie** — informacje lub inne obiekty, których weryfikacja pozwala na ustalenie tożsamości przedstawiającego się nimi użytkownika. Z pojedynczą tożsamością może być powiązane wiele różnych poświadczeń. Typowe przykłady poświadczeń to nazwa użytkownika wraz z hasłem, certyfikat cyfrowy itp.;
- **usługa** — logiczny zbiór funkcjonalności biznesowej udostępniany przez dostawcę usług, charakteryzujący się spójnymi regułami dotyczącymi autoryzacji i dostępu do usługi przez użytkowników. Agencja opieki zdrowotnej może oferować wiele niezależnych usług, różniących się regułami dostępu i wymaganymi poziomami uwierzytelnienia. Jedna usługa może także udostępniać zbiór funkcjonalności biznesowej oferowanej przez różne agencje — warunkiem jest jasne ustalenie zakresu własności i odpowiedzialności za każdą usługę zagregowaną w ramach tej jednej usługi;
- **rejestracja** — powiązanie tożsamości z określoną usługą, realizowane za pośrednictwem odpowiednich, specyficznych dla danej usługi atrybutów kontekstu (identyfikatorów). Prawidłowa i aktywna rejestracja uprawnia jej posiadacza (lub dobrze umocowanego reprezentanta) do dostępu do usługi w kontekście określonym przez identyfikatory;
- **identyfikatory** — atrybuty informacyjne towarzyszące rejestracji, które jednoznacznie identyfikują i stanowią kontekst relacji tożsamości z daną usługą.

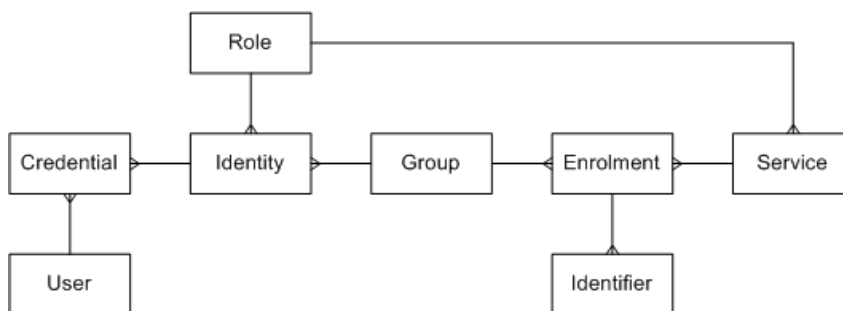
Przykładami takich identyfikatorów mogą być: numer identyfikacji podatkowej, krajowy numer ubezpieczenia, numer ubezpieczenia społecznego, numer rejestrowy przedsiębiorstwa, identyfikator płatnika podatku VAT, identyfikator płatnika podatku od nieruchomości, identyfikator dostawcy czy numer konta;

- **grupa** — reprezentuje zbiór użytkowników współdzielących takie same rejestracje. Użytkownicy tacy często pełnią rolę reprezentantów organizacji;
- **rola** — szeroka kategoria tożsamości stosowana do określenia lub ograniczenia dostępu do odpowiednich usług dla wszystkich użytkowników w ramach tej tożsamości. Typowe przykłady ról to między innymi:
 - osoba (obywatel) — reprezentuje klientów usług opieki zdrowotnej;
 - organizacja (grupa) — reprezentuje organizacje (firmy), w których wiele osób należących do jednej grupy może współdzielić tę samą rejestrację i działać w imieniu organizacji;
 - pośrednik (agent, delegat) — stały lub wyznaczony tymczasowo reprezentant osoby lub organizacji, uprawniony do działania w ich imieniu w kontekście określonej usługi;
 - opieka zdrowotna — osoby i systemy reprezentujące agencje opieki zdrowotnej, uprawnione do dostępu do określonych usług.

Model tożsamości

Na ilustracji REF ilustracja5 Vh 5 przedstawiono relacje pomiędzy wymienionymi powyżej encjami modelu tożsamości. Warto zauważyć, że:

- pojedynczy użytkownik może posiadać wiele poświadczeń;
- każdy zestaw poświadczeń odpowiada pewnej tożsamości, a jedna tożsamość może być identyfikowana wieloma zestawami poświadczeń;
- każda tożsamość jest powiązana z jedną rolą, która określa zbiór usług dostępnych dla osoby posługującej się tą tożsamością;
- z jedną grupą może być związane wiele tożsamości;
- grupa może posiadać wiele rejestracji w poszczególnych usługach;
- jedna rejestracja dotyczy tylko jednej usługi;
- każda rejestracja w usłudze ma przypisane określone identyfikatory określające kontekst relacji pomiędzy posiadaczem rejestracji a usługą.



Ilustracja 5. Model tożsamości

Separacja tożsamości od poświadczeń uwierzytelniania

Oddzielenie tożsamości od poświadczeń uwierzytelniania to ważna zasada, od której zależy elastyczność modelu. Uwierzytelnienie określonej tożsamości może być związane z niezależną weryfikacją wielu poświadczeń tożsamości. Pozwala to na wygodne uwierzytelnianie użytkownika korzystającego z usług za pośrednictwem wielu kanałów dostępu — dostępne technologie i schematy korzystania z poszczególnych kanałów dostępu mogą ograniczać możliwość przedstawiania niektórych typów poświadczeń (na przykład brak czytników kart elektronicznych, możliwość wprowadzania wyłącznie danych numerycznych itp.).

Obsługa wielu typów poświadczeń pozwala na rozwój i rozszerzanie istniejącego zestawu relacji (rejestracji) poprzez stopniową migrację do wyższych poziomów uwierzytelniania, zapewniających dostęp do szerszego zestawu usług. Migrację taką można zrealizować minimalnymi nakładami pracy bez zakłócania działania istniejących usług. Odseparowanie poświadczeń od tożsamości pozwala także na uwierzytelnianie na podstawie poświadczeń zewnętrznych, obsługiwane na zewnątrz huba usług e-zdrowia. Daje to podstawę do obsługi uwierzytelniania stowarzyszonego i innych zaawansowanych scenariuszy zastosowań.

Usługi uwierzytelniania mogą być zapewniane przez różnych dostawców (w zależności od rodzaju uwierzytelniania i jego wystawcy) przy jednoczesnym zachowaniu ogólności funkcji autoryzacji i odwzorowywania tożsamości na identyfikatory wykorzystywane przez różne usługi. Jest to możliwe dzięki przypisaniu wielu poświadczeń do jednej tożsamości.

Obsługa uwierzytelniania stowarzyszonego

Tworząc rozwiązanie perspektywiczne, które bez większych modernizacji powinno funkcjonować przez wiele lat, warto już na początku prac projektowych zastanowić się nad wdrożeniem modelu uwierzytelniania stowarzyszonego. Innymi słowy — warto założyć, że system będzie korzystał z wielu dostawców poświadczeń i tożsamości. Aby to osiągnąć, dobrze jest oddzielić samo uwierzytelnianie (implementowane natywnie w istniejących i przyszłych produktach i technologiach) od specyficznej funkcjonalności, takiej jak odwzorowywanie tożsamości użytkowników na identyfikatory użytkowników stosowane przez usługi (odwzorowanie z pewnością jest specyficzną relacją, wymagającą obsługi za pomocą specjalnie zaprojektowanego do tego celu procesu).

Uwierzytelnianie stowarzyszone powinno być oparte na istniejących obecnie standardach branżowych, takich jak WS-Federation, WS-Trust itd. (więcej informacji na temat tych standardów można znaleźć w zasobach wymienionych w części *Odsyłacze, listy kontrolne i dalsze informacje*, będącej ostatnią częścią tego opracowania). Takie podejście pozwoli zagwarantować interoperacyjność pomiędzy różnymi platformami i dostawcami oraz umożliwi wykorzystanie produktów komercyjnych wspierających te standardy. Więcej informacji na temat proponowanej przez Microsoft interoperacyjnej architektury zarządzania cyfrową tożsamością, opartej na założeniu, że każda osoba może posługiwać się wieloma cyfrowymi tożsamościami opartymi na różnych technologiach, implementacjach i przyznawanymi przez różnych dostawców, można znaleźć w artykule pod adresem <http://msdn.microsoft.com/library/en-us/dnwebsrv/html/iidentitymetasystem.asp>.

Usługi Web Services

Funkcjonalność podsystemu zarządzania tożsamościami w hubie usług e-zdrowia udostępniania jest w postaci zestawu usług Web Service, które można podzielić na następujące kategorie:

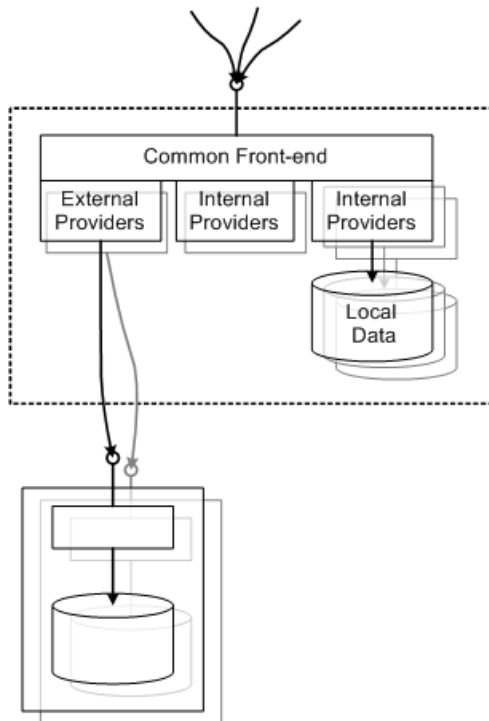
- identyfikacja początkowa i rejestracja;
- uwierzytelnianie;

- autoryzacja i odwzorowywanie tożsamości;
- zarządzanie użytkownikami i rejestracjami.

Wzorzec ogólny — wymienni dostawcy

Implementacja usług tożsamości oparta jest na jednym, ogólnym wzorcu, który przedstawiono na *ilustracji 6*. Na implementację tę składa się wspólna, zunifikowana czołowa usługa Web Service oraz pewna liczba wymiennych dostawców, będących implementacjami dowolnych z następujących sposobów obsługi:

- **interfejs** łączący z zewnętrznym dostawcą usług, który może korzystać ze zdalnych danych referencyjnych,
- **przetwarzanie wewnętrzne** przez reguły znajdujące się w kodzie programu, bez potrzeby sięgania do danych referencyjnych,
- **wewnętrzny dostawca** usługi, który lokalnie przechowuje niezbędne dane referencyjne.



Ilustracja 6. Ogólny wzorzec wymiennych dostawców

Możliwe jest stosowanie wielu instancji dostawcy tego typu, na przykład w celu realizacji różnych typów walidacji lub dostępu do różnych dostawców zewnętrznych. Zakłada się oparcie wszystkich interakcji zewnętrznych na standardowych usługach Web Service,

jednak tam, gdzie nie jest to możliwe, można przygotować komponent-interfejs, który tłumaczy wywołania na protokół zrozumiały przez dostawcę.

Początkowe zgłaszanie użytkowników

Jak wspomnieliśmy w sekcji *Początkowa identyfikacja użytkownika* rozdziału *Uwzględnienie powszechnych problemów dotyczących architektury* tego opracowania, z tworzeniem rozwiązań e-zdrowia na wielką skalę związane są liczne problemy. Proces początkowego zgłaszania (identyfikacji i rejestracji) użytkowników musi być efektywny, bezpieczny, a jednocześnie powinien wymagać jak najmniejszego nakładu pracy ludzkiej po stronie dostawcy usług. Idealnym rozwiązaniem byłoby zgłaszanie samoobsługowe, realizowane w całości przez samych użytkowników. Aby system pozwalał na dopasowanie do ewoluujących i coraz bardziej zróżnicowanych wymagań, musi zapewniać elastyczność definiowania specyficznych reguł i procesów dla każdej z usług z osobna.

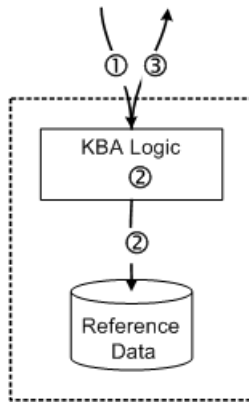
Początkowe uwierzytelnianie oparte na wiedzy

Zważywszy na specyficzne dla rozwiązań e-zdrowia wymagania, takie jak duża liczba potencjalnych użytkowników, brak wcześniejszych doświadczeń z systemami elektronicznymi i mała częstotliwość interakcji, coraz większą popularność zyskuje pomysł nazywany **uwierzytelnianiem opartym na wiedzy** (Knowledge Based Authentication — KBA).

Mówiąc krótko, w modelu KBA do weryfikacji tożsamości użytkownika wykorzystywane są dostarczone przez niego informacje. Mogą to być ogólne informacje związane z użytkownikiem (identyfikujące użytkownika) albo z kontekstem określonej usługi (identyfikacja płatnika podatku od nieruchomości na podstawie posiadanych przez niego nieruchomości).

Na *ilustracji 7*. przedstawiono ogólną architekturę systemu uwierzytelniania na podstawie wiedzy. Obieg informacji, oznaczony na ilustracji kolejnymi liczbami, przebiega następująco:

1. Użytkownik przedstawia zestaw informacji (faza ta poprzedzona jest zadaniem użytkownikowi zestawu pytań).
2. Reguły KBA porównują przedstawione informacje (odpowiedzi na zadane pytania) z danymi referencyjnymi. Dane te mogą być przechowywane lokalnie lub zdalnie.
3. Odpowiedź systemu zawiera informację na temat wyniku uwierzytelnienia (pozytywny lub negatywny) oraz dane dodatkowe — na przykład unikalny identyfikator użytkownika, ustalony w procesie porównywania danych przedstawionych przez użytkownika. Identyfikator nie musi być elementem tych informacji.



Ilustracja 7. Ogólna architektura usługi uwierzytelniania opartego na wiedzy

Uwaga — szczegółowe informacje na temat uwierzytelniania opartego na wiedzy można znaleźć w prezentacji *KBA Applicability to e-Health*, której autorami są Mindy Rudell, Dick Stewart, Robin Medlock i Angel Rivera. Prezentacja dostępna jest pod adresem <http://csrc.nist.gov/kba/Presentations/Day%202/Rudell%20-%20KBA%20Applicability%20to%20e-Gov.pdf>

Wybór odpowiedniego zestawu informacji dla KBA

Wiarygodność uwierzytelniania KBA zależy od rodzaju wybranego zestawu informacji uwierzytelniających oraz od sposobu realizacji procesu walidacji. Typowe wymagania dotyczące doboru tych informacji to:

- Informacje są bezpośrednio związane z użytkownikiem i jednoznacznie go identyfikują. Informacją taką nie jest na przykład kod pocztowy, ale numer PESEL lub numer ubezpieczenia społecznego — jest.
- Informacje są dobrze znane użytkownikowi, ale nie są łatwo dostępne dla innych osób. Informacją taką nie jest na przykład numer rejestrowy firmy (umieszczany na papierze firmowym i wizytówkach, dostępny praktycznie dla każdego). Informacjami takimi mogą być na przykład specyficzne dane z ostatniej faktury — numer referencyjny lub ilość zamówionego towaru (dane takie znane są zwykle wyłącznie stronie zainteresowanej).
- Możliwość odgadnięcia poprawnej odpowiedzi jest ograniczona — zakres wartości jest na tyle szeroki, że wypróbowanie wszystkich możliwych wartości jest niewykonalne, a odgadnięcie poprawnej wartości na podstawie innych, znanych danych jest niemożliwe (należy na przykład unikać stosowania numerowania kolejnymi numerami).
- Wykorzystanie do uwierzytelniania informacji podlegających okresowym zmianom (na przykład kwota ostatniej płatności) dodatkowo zmniejsza prawdopodobieństwo odgadnięcia, a więc dane takie stanowią lepsze zabezpieczenie niż dane niezmiennie.

Warto podkreślić, że powyższe wymagania dotyczą zbioru informacji jako całości. Innymi słowy, różne informacje, z których każda oddzielnie nie zapewnia dostatecznego poziomu wiarygodności identyfikacji, połączone razem mogą dać wysoką pewność i bezpieczeństwo uwierzytelnienia.

Logika weryfikująca i dane referencyjne

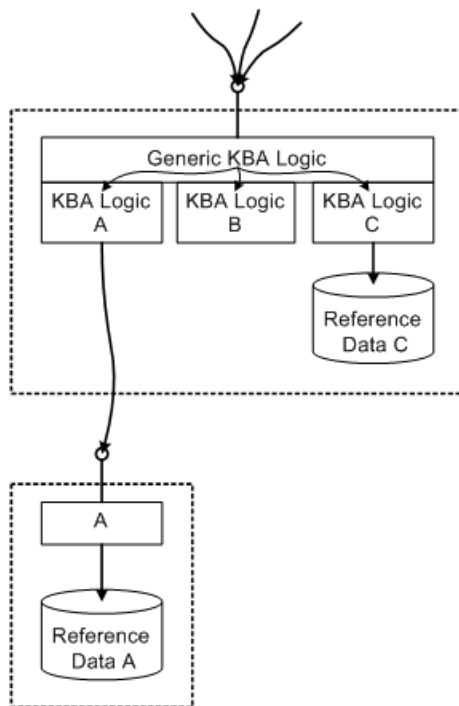
Gdy użytkownik przedstawi informacje uwierzytelniające, trzeba je zweryfikować. Weryfikacja zwykle odbywa się na podstawie pewnych danych referencyjnych z wykorzystaniem odpowiednich reguł porównujących. Można stosować różne transformacje pozwalające na porównywanie przybliżone — na przykład nie uwzględniać wielkości liter, ignorować znaki niedrukowane (np. spacje), dokonywać częściowego porównywania danych takich jak kod pocztowy i inne dane adresowe czy dopuszczać stosowanie skrótów i różnych wariantów pisowni. Ogólnie rzecz biorąc, trudno jest jednak opracować zadowalające metody porównywania danych, które mogą występować w wielu różnych formatach (tak jak na przykład dane adresowe), zatem zalecane jest wykorzystywanie danych o bardziej przewidywalnych formatach.

Reguły porównujące mogą także sprawdzać zależności pomiędzy wprowadzonymi informacjami. Można na przykład uznać, że wystarczające jest udzielenie poprawnej odpowiedzi na 3 z 4 pytań. Ponieważ reguły porównujące mogą być dostosowywane do potrzeb, i — jeśli jest zachodzi taka konieczność — można stosować różne reguły dla różnych rodzajów uwierzytelniania i różnych usług, pozwalają na dopasowanie systemu do wielu różnych wymagań — zarówno obecnych, jak i tych, które dopiero zostaną zdefiniowane. Jest to istotne dla elastyczności rozwiązania i stanowi jedno z podstawowych założeń architektury platformy (zgodnie z opisem w sekcji *Elastyczność i sprawność* rozdziału *Uwzględnienie powszechnych problemów dotyczących architektury* wcześniej w tym dokumencie).

Dane referencyjne wykorzystane do walidacji mogą być albo lokalne (dostarczone przez właściciela i przechowywane w hubie), albo zdalne (hub w celu weryfikacji informacji przedstawionych przez użytkownika odwołuje się do właściciela danych, a same dane pozostają u właściciela). Możliwe jest także skonstruowanie reguł sprawdzających, opierających się wyłącznie na informacjach przedstawionych przez użytkownika — bez potrzeby korzystania z danych referencyjnych. W takim wypadku wynik uwierzytelnienia zależy od spójności całego zestawu danych. Jedna z przedstawianych informacji może być na przykład wynikiem jakiejś transformacji pozostałych danych, podobnie jak w przypadku cyfr kontrolnych na kartach kredytowych — jednak wykorzystana transformacja musi być bardziej bezpieczna. W przypadku weryfikacji bez wykorzystania danych referencyjnych, w skład zestawu informacji przedstawianych przez użytkownika musi także wchodzić unikalny identyfikator użytkownika lub informacje te muszą wystarczać do ustalenia (np. obliczenia) identyfikatora użytkownika.

Na *ilustracji 8*. przedstawiono trzy różne sposoby walidacji, możliwe do przeprowadzenia z wykorzystaniem wymiennego dostawcy, takiego jak usługa KBA.

- A — dane referencyjne przechowywane są zdalnie, reguły KBA w celu walidacji użytkownika odwołują się do dostawcy danych,
- B — logika walidacyjna jest niezależna od jakichkolwiek danych referencyjnych,
- C — dane referencyjne przechowywane są wewnątrz huba, reguły walidacyjne odwołują się do nich lokalnie.



Ilustracja 8. Różne rodzaje walidacji, korzystające z lokalnych i zdalnych danych referencyjnych

Ogólna architektura huba obsługuje wymienne moduły walidacji dowolnego typu. Decyzja co do tego, który moduł należy zastosować, zależy od wielu czynników. Najważniejsze z nich to:

- **czas odpowiedzi operacji walidacji** — przechowywanie danych referencyjnych wewnątrz huba pozwala na przyspieszenie walidacji. Odwołania z huba do zdalnego magazynu danych mogą wprowadzać znaczne opóźnienia, co może mieć negatywny wpływ na wydajność i ocenę systemu przez użytkownika;
- **dostępność** — przechowanie danych referencyjnych wewnątrz huba zapewnia niezależność procesu weryfikacji od innych systemów, dzięki czemu dostępność procesu walidacji jest równa dostępności huba. Oparcie walidacji na zdalnych danych referencyjnych uzależnia dostępność całego rozwiązania od dostępności systemu zdalnego;
- **objętość danych** — rozmiar danych referencyjnych może być znaczny — powinno być to uwzględnione podczas planowania wydajności systemu. Jeśli z usługi korzystać będzie tylko niewielka część użytkowników, przechowywanie wewnątrz huba kopii danych referencyjnych całej społeczności może być zbyt drogie i zbyt kłopotliwe;
- **uaktualnianie danych referencyjnych** — dane referencyjne przechowywane wewnątrz huba muszą być stale uaktualniane na podstawie ich źródła. W zależności od szybkości zmian zachodzących w tych danych, objętość zmian danych dotyczących wszystkich potencjalnych użytkowników usługi może być dość duża.

Korzystanie z danych zdalnych, pozostających u ich właściciela, eliminuje potrzebę aktualizowania danych w hubie;

- **problemy dotyczące poufności danych** — prawodawstwo niektórych krajów (na przykład Portugalii) zabrania przechowywania danych specyficznych dla usługi poza agencją opieki zdrowotnej udostępniającą tę usługę. Przechowywanie danych referencyjnych w hubie centralnym jest tam niemożliwe — niezależnie od wszelkich innych czynników czy możliwości technicznych.

Wybór najlepszego mechanizmu walidacji i miejsca przechowywania danych referencyjnych może być różny dla różnych dostawców usług.

Pozyskiwanie informacji do celów uwierzytelniania opartego na wiedzy

Informacje przedstawiane przez użytkowników do celów uwierzytelniania opartego na wiedzy mogą być danymi znanymi przez tych użytkowników lub danymi, które uzyskali oni w wyniku innych interakcji z dostawcą usług (na przykład w korespondencji lub wraz z rachunkiem). Mogą to być również informacje przekazane specjalnie do celu pierwszego uwierzytelnienia elektronicznego. Możliwe jest także powiązanie procesu pozyskania niezbędnych informacji z jakąś procedurą, akredytacją lub weryfikacją dokumentów (przedstawianych zdalnie za pośrednictwem poczty elektronicznej lub osobiście). Uwierzytelnianie oparte na wiedzy to ogólny mechanizm, niezależny od dokładnego sposobu pozyskania niezbędnych danych. Realizacja procesów uwierzytelniania odbywa się poza samym hubem, może być różna dla różnych usług i może być łączona z innym, zewnętrznym procesem.

Skoncentrowane na usługach podejście do zgłaszania użytkowników

Jak wspomnieliśmy w sekcji *Początkowa identyfikacja użytkownika* we wcześniejszym rozdziale *Uwzględnienie powszechnych problemów dotyczących architektury*, opracowanie metody początkowej identyfikacji użytkowników o wiarygodności na poziomie akceptowalnym przez wszystkie usługi jest często bardzo trudne. Aby zapewnić niezbędną elastyczność i możliwość adaptacji do zróżnicowanych wymagań, stawianych przez obecnych i przyszłych dostawców usług, preferowane jest przeprowadzanie początkowej identyfikacji użytkowników niezależnie dla każdej usługi. Pozwala to na definiowanie informacji uwierzytelniających, reguł walidacji i danych referencyjnych osobno dla każdej usługi i zupełnie niezależnie od innych usług.

Takie specyficzne dla poszczególnych usług uwierzytelnianie początkowe może być dodatkiem do jakiejś procedury wstępnej walidacji użytkownika jako osoby w sensie bardziej ogólnym (w oderwaniu od usług). Można też całkowicie zrezygnować ogólnej identyfikacji użytkownika — każda usługa będzie identyfikowała użytkowników niezależnie, bez relacji zaufania do innych usług. W tym drugim wypadku rejestracja użytkownika w systemie zależy od pomyślnej początkowej identyfikacji użytkownika przez co najmniej jedną usługę. Takie rozwiązanie jest przydatne w krajach, w których nie ustalono ogólnego identyfikatora obywateli i identyfikacja początkowa musi być oparta na danych referencyjnych i procedurach walidacji zdefiniowanych przez dostawców usług.

Uwaga — chociaż możliwe jest rejestrowanie użytkowników z pominięciem walidacji początkowej i późniejsze wiązanie tożsamości z usługami, należy unikać takich rozwiązań. Gdy nie ma wiarygodnego sposobu identyfikacji początkowej, trudno uchronić hub przed atakami typu DoS (Denial of Service) polegającymi na rejestrowaniu dużych ilości fałszywych użytkowników (bez walidacji przez jakiegokolwiek usługi) — nie istnieje wtedy żaden mechanizm, który pozwoliłby na odróżnienie rejestracji fałszywej od rejestracji prawdziwego użytkownika. Działania takie mogą ograniczyć objętość dostępnej przestrzeni przechowywania danych i moc

obliczeniową, co może negatywnie wpłynąć na dostępność systemu i znacznie podnieść koszty bieżące. Podejście skoncentrowane na usługach wymaga przeprowadzania walidacji przed rejestracją użytkownika, przez co zapewnia lepsze bezpieczeństwo. Pozwala także na wdrożenie dodatkowych procedur aktywacji, zależnych od danych udostępnionych przez usługi (na przykład dane adresowe), co w przeciwnym wypadku może nie być możliwe. Szczegółowe rozważania na temat możliwych rozwiązań aktywacji przedstawiono w sekcji *Aktywacja zgłoszenia i rejestracji* w dalszej części tego opracowania.

Rejestracja w usługach i odwzorowywanie tożsamości

Po udanej identyfikacji początkowej użytkownika w kontekście określonej usługi, dostępny zestaw unikalnych i specyficznych dla tej usługi identyfikatorów użytkownika pozwala na zarejestrowanie użytkownika w usłudze. Tożsamość ogólna pozostaje przezroczysta i nie jest widoczna dla dostawcy usług — jest ona odwzorowywana na identyfikatory zrozumiałe dla danej usługi. Obiekt rejestracji może na przykład powiązać tożsamość Jana Kowalskiego z usługami opieki zdrowotnej za pośrednictwem identyfikatora przydzielonego przez fundusz zdrowia i z usługą podatkową za pośrednictwem numeru identyfikacji podatkowej i innych danych. Dzięki zapamiętaniu odpowiedniego zbioru unikalnych identyfikatorów, specyficznych dla danej usługi jako atrybutów rejestracji w tej usłudze, możliwe jest w czasie wszystkich późniejszych uwierzytelnień i autoryzacji użytkownika odwzorowanie tożsamości ogólnej na tożsamość specyficzną dla usługi.

Odwzorowywanie tożsamości to jedna z unikatowych, dodatkowych funkcji zapewnianych przez hub usług e-zdrowia. Nawet jeśli mechanizmy uwierzytelniania zostaną przeniesione całkowicie na zewnątrz huba (innymi słowy, informacje na temat tożsamości użytkowników nie będą w żaden sposób przechowywane wewnątrz huba, a hub będzie całkowicie opierał się na zewnętrznych dostawcach uwierzytelniania), odwzorowywanie zweryfikowanej tożsamości ogólnej na odpowiadające jej identyfikatory specyficzne dla usług gwarantuje, że usługa docelowa otrzyma zrozumiałe dla siebie identyfikatory użytkownika. Podejście to jest zgodne z regułami zarządzania tożsamością (*zasady minimalnego zakresu ujawniania niezbędnych informacji i tożsamości ukierunkowanej*), opisanymi wcześniej w tym opracowaniu w rozdziale *Uwzględnienie powszechnych problemów dotyczących architektury*.

Aktywacja zgłoszenia i rejestracji

Początkowa identyfikacja oparta na wiedzy może zostać uzupełniona dodatkowymi procedurami, podnoszącymi poziom bezpieczeństwa zapewniany przez identyfikowanie użytkowników na podstawie wprowadzonych przez nich informacji (i niskie prawdopodobieństwo, że jakiś użytkownik także może znać te informacje i wykorzystać je do podszywania się pod innego użytkownika). Dodatkowe procedury mogą być uruchamiane po udanej walidacji początkowej opartej na wiedzy i mogą obejmować wysłanie do użytkownika dodatkowych informacji, które ten musi wprowadzić do systemu w celu ukończenia procesu weryfikacji.

Typowa implementacja (zastosowano ją w Wielkiej Brytanii i innych krajach) polega na pobraniu od dostawcy usług adresu korespondencyjnego użytkownika i wysłaniu na ten adres jednorazowego kodu aktywacyjnego. Rejestracja w usłudze (utworzona w stanie „oczekiwania na aktywację”) zostaje aktywowana, dając pełny dostęp do funkcjonalności dopiero po przedstawieniu hubowi otrzymanego kodu aktywacyjnego. Dzięki dodatkowej weryfikacji opartej na sprawdzeniu, czy użytkownik otrzymał kod aktywacyjny, procedura ta charakteryzuje się wyższym poziomem bezpieczeństwa.

Udany atak przez osobę podszywającą się pod użytkownika wymagałby nie tylko pozyskania i przedstawienia poprawnych informacji do celów uwierzytelnienia w oparciu

o wiedzę, ale także przechwycenia przesyłki pocztowej lub ingerencji w proces jej dostarczenia. Ze względu na wysoką wiarygodność przedsiębiorstw pocztowych i różne regulacje prawne (w USA na przykład wszelkie próby zakłócenia dostarczania poczty są przestępstwami federalnymi o wysokim wymiarze kary), dodatkowy etap weryfikacji znacząco podnosi ogólne bezpieczeństwo rozwiązania.

Do przesłania kodu aktywacyjnego można też stosować inne kanały komunikacyjne, takie jak poczta elektroniczna, telefon, wiadomość SMS itp. Pojawia się tu jednak problem wiarygodności adresu docelowego. O ile większość dostawców usług przechowuje adresy korespondencyjne swoich klientów, to inne dane kontaktowe mogą być albo niedostępne, albo nieaktualne. Wybierając metodę komunikacji należy dokładnie rozważyć potencjalne zagrożenia i ograniczyć możliwości wykorzystania danego kanału do podszycia się pod użytkownika. Jednym ze sposobów podniesienia wiarygodności adresu poczty elektronicznej jest korzystanie z adresów, które zostały już wcześniej zweryfikowane — na przykład adresów poczty elektronicznej podanych w certyfikatach cyfrowych użytkowników.

Dodatkowy etap aktywacji może pomóc w podniesieniu bezpieczeństwa, jednak ma też pewne wady:

- Dostawca usługi musi dysponować wiarygodnymi danymi adresowymi użytkowników. Rozpoczęcie dodatkowego etapu weryfikacji wymaga przesłania tych danych do huba (masowo lub pojedynczo — w zależności od sposobu prowadzenia rejestracji).
- Konieczne jest zakupienie i wdrożenie — lokalnie lub u zewnętrznego dostawcy — urządzeń do bezpiecznego drukowania i rozsyłania kodów aktywacyjnych (w sposób podobny do stosowanego przez banki podczas rozsyłania PIN-ów do kart płatniczych). Nie wszystkie agencje opieki zdrowotnej, które będą korzystały z huba, mogą pozwolić sobie na zakup takich urządzeń — konieczne jest udostępnienie tych urządzeń w ramach centralnej, współdzielonej infrastruktury e-zdrowia.
- Bezpieczne sposoby przekazywania kodów aktywacyjnych i danych adresowych do jednostki zajmującej się drukowaniem i rozsyłką — dane te są ściśle poufne i powinny być chronione odpowiednimi środkami technicznymi i procedurami operacyjnymi.
- Wprowadzenie opóźnienia — druk kodów aktywacyjnych i rozsyłka ich drogą pocztową wydłuża okres pomiędzy identyfikacją początkową a aktywacją rejestracji w usłudze nawet o kilka dni. Może to być niewygodne dla potencjalnych użytkowników — szczególnie wtedy, gdy rejestrują się do usług e-zdrowia tuż przed jakimś wyznaczonym terminem i dowiadują się, że z powodu oczekiwania na aktywację nie będą mogli ukończyć określonej operacji na czas (na przykład nie złożą formularza podatkowego).

Istnieje możliwość wyeliminowania opóźnień przy jednoczesnym zachowaniu zalet dodatkowej fazy aktywacji. W urzędzie podatkowym Wielkiej Brytanii i kilku innych instytucjach z powodzeniem udało się wdrożyć zmodyfikowany model aktywacji, zwany *aktywacją natychmiastową*. Polega on na wygenerowaniu kodów aktywacyjnych i przekazaniu ich potencjalnym użytkownikom jeszcze zanim zdecydują się zarejestrować w usłudze.

Można połączyć obydwie fazy początkowej identyfikacji użytkowników w oparciu o wiedzę i żądać podania kodu aktywacyjnego wraz z pozostałymi informacjami podczas rejestracji. Przesłany użytkownikowi kod aktywacyjny przechowywany jest wtedy wraz z danymi referencyjnymi, a procedura weryfikacyjna, oprócz sprawdzenia informacji przedstawionych przez użytkownika, sprawdza także podany przez niego kod. Jeżeli użytkownik poda prawidłowy kod, system może od razu aktywować rejestrację

i odpowiednie usługi natychmiast stają się dostępne dla użytkownika. Zmiana kolejności procedur weryfikacyjnych (rozsyłka kodów aktywacyjnych nadal ma miejsce, ale odbywa się przed rejestracją użytkownika w usłudze) pozwala na uzyskanie tak samo wysokiego poziomu bezpieczeństwa i uniknięcie opóźnień. Rozsyłka kodów aktywacyjnych z wyprzedzeniem działa także jako swoiste zaproszenie do skorzystania z usług i przyczynia się do podniesienia świadomości społecznej dostępności usług e-zdrowia, zwiększając także popyt na te usługi.

Ogólny dostawca poświadczeń i uwierzytelniania

Funkcjonalność zarządzania tożsamością w hubie usług e-zdrowia oparta jest na usługach świadczonych przez jednego lub kilku dostawców tożsamości. Niektórzy z dostawców mogą być dostawcami zewnętrznymi. W takich wypadkach hub w celu weryfikacji poświadczeń przedstawionych przez użytkownika musi odwołać się do dostawcy zewnętrznego. Hub może całkowicie opierać się na zewnętrznych dostawcach uwierzytelniania i nie utrzymywać własnej wewnętrznej bazy poświadczeń, ale może też korzystać z wewnętrznego dostawcy poświadczeń i uwierzytelniania. Dzięki temu użytkownicy, którzy nie ustalili relacji z żadnym z dostawców zewnętrznych, mogą zarejestrować się w systemie i uzyskać poświadczenia wygenerowane przez hub.

Aby system mógł być dostosowywany do stale zmieniających się wymogów związanych z różnymi typami poświadczeń, ogólny dostawca poświadczeń w hubie musi zapewniać elastyczną obsługę wydawania takich poświadczeń. Reguły mogą być konfigurowane albo statycznie — w czasie instalacji dostawy, albo dynamicznie — poprzez zmianę parametrów podczas pracy. Oto przykładowe typy poświadczeń:

- **identyfikator użytkownika wraz z hasłem** — dostawca poświadczeń generuje identyfikator użytkownika, który jest unikalny w obrębie huba. Format i długość identyfikatora są z góry ustalone. Hasło jest albo wybierane przez użytkownika, albo generowane przez dostawcę. Tu także mają zastosowanie reguły narzucające format i odpowiednią złożoność hasła. Do poprawnego uwierzytelnienia użytkownika niezbędne jest podanie pełnej i poprawnej kombinacji identyfikatora i hasła;
- **zapamiętywane słowa** (z podpowiedzią lub bez podpowiedzi) — mechanizm ten można połączyć z nazwą i hasłem użytkownika w celu zapewnienia wyższego poziomu bezpieczeństwa. Podanie słów może być wymagane tylko podczas przeprowadzania określonych operacji (na przykład zresetowanie hasła użytkownika) albo zawsze. Często stosuje się pytania o fragment zapamiętanego słowa — na przykład o losowo wybrane znaki (trzecia i piąta litera, numery liter losowane są za każdym razem) lub wiele par pytań i odpowiedzi i zadanie tylko jednego, losowanego za każdym razem pytania;
- **certyfikaty** — ogólny dostawca poświadczeń w hubie może wydawać cyfrowe certyfikaty dla użytkowników. O ile realizacja techniczna takiego systemu jest możliwa, to logistyka i zarządzanie nim wymagają głębokiego namysłu. Obsługa certyfikatów bez odpowiedniego doświadczenia i zaplecza technicznego może być nie lada wyzwaniem. W większości krajów, w których wdrożono huby e-zdrowia, procedury wydawania i obsługi certyfikatów postanowiono oprzeć na usługach świadczonych przez akredytowanych i sprawdzonych dostawców zewnętrznych.

Wybierając rodzaj poświadczeń i reguły zarządzania poświadczeniami warto rozważyć następujące kwestie:

- **wcześniejsze ograniczenia i wymagania**, takie jak zalecenie wykorzystania jako identyfikatorów użytkownika — zamiast identyfikatorów generowanych losowo — ustalonych wcześniej unikalnych identyfikatorów (na przykład numer PESEL);

- **skala** — zakres i rodzaj użytych identyfikatorów powinny pozwalać na wydanie unikalnych identyfikatorów w liczbie wystarczającej do obsłużenia potencjalnej liczby użytkowników;
- **bezpieczeństwo** — długość i złożoność identyfikatora oraz hasła powinny być na tyle duże, by nieopłacalne były ataki metodą przeglądu zupełnego (ang. brute force, próba odgadnięcia identyfikatora i hasła poprzez wypróbowanie wszystkich możliwych kombinacji);
- **wygoda** — posługiwanie się identyfikatorami, hasłami i innymi informacjami powinno być łatwe dla użytkowników (w idealnej sytuacji powinny dać się łatwo zapamiętać). Im dłuższe i bardziej złożone identyfikatory i hasła, tym większe prawdopodobieństwo, że użytkownicy będą musieli je zapisywać, co przyniesie skutek odwrotny od tego, który miał zostać osiągnięty poprzez podniesienie złożoności haseł. W tym obszarze niezbędny jest kompromis między wygodą a bezpieczeństwem;
- **kanały dostępu** — sposób doboru identyfikatorów i haseł może ograniczyć stosowanie niektórych kanałów dostępu. Na przykład automatyczne systemy obsługi klienta (IVR), systemy telefoniczne, telefony komórkowe oraz telewizja interaktywna (IPTV) pozwalają na wprowadzanie wyłącznie liczb. Tu także uzyskany poziom bezpieczeństwa zależy od kompromisu pomiędzy zakładanym przeznaczeniem systemu a wygodą użytkownika. Być może warto zastanowić się nad wprowadzeniem różnych zestawów poświadczeń dla różnych kanałów dostępu oraz zróżnicowaniem zestawów usług udostępnianych za pośrednictwem różnych kanałów w zależności od poziomu bezpieczeństwa zapewnianego przez dany kanał.

Zarządzanie użytkownikami i rejestracjami

W tej sekcji omówiono funkcje zarządzania użytkownikami i ich rejestracjami oraz zagadnienia bieżącego utrzymywania kont użytkowników, rejestracji w usługach, umowy, delegacje uprawnień itp.

Dodawanie i usuwanie użytkowników

Oprócz procesu pełnego początkowego uwierzytelniania i zgłaszania użytkowników, opisanego w sekcji *Początkowe zgłaszanie użytkowników* wcześniej w tym rozdziale, system może także obsługiwać inne sposoby zgłaszania użytkowników. Na przykład zarejestrowani użytkownicy mogą działać w roli mentorów i zgłaszać nowych użytkowników według procedury uproszczonej. Aby odróżnić ten proces od pełnego uwierzytelnienia początkowego, procedurę uproszczoną będziemy nazywać procesem dodawania lub wprowadzania nowych użytkowników. Użytkownicy wprowadzani w ten sposób do systemu współdzielą to samo zgłoszenie i nie muszą ustanawiać odrębnych, niezależnych zgłoszeń. Funkcjonalność ta jest najbardziej użyteczna w organizacjach, w których wielu użytkowników działa jednocześnie w imieniu całej organizacji oraz w przypadku, gdy wielu użytkowników korzysta z tego samego kontekstu usługi (posiada takie same identyfikatory specyficzne dla usługi).

W wielu dotychczasowych implementacjach hubów usług e-zdrowia zastosowanie takiej funkcjonalności ograniczono jedynie do ról organizacji. Jednakże w przypadku zastosowania szerszego i bardziej wszechstronnego modelu, funkcjonalność taką można udostępnić także dla innych ról i na przykład pozwolić osobom na wprowadzanie innych użytkowników i tworzenie grupy osób współdzielących to samo zgłoszenie.

Tożsamość nowo wprowadzonego użytkownika (potwierdzana na podstawie istniejących lub nowo utworzonych poświadczeń) jest powiązana z tożsamością użytkownika, który wprowadził tę nową tożsamość. W momencie wprowadzenia pierwszego użytkownika tworzona jest grupa użytkowników. Kolejni wprowadzani użytkownicy dołączani są do

istniejącej grupy, a ich tożsamości łączone są z tożsamościami wszystkich pozostałych użytkowników. Pozwala to na pominięcie całego procesu uwierzytelnienia opartego na wiedzy w relacji do jednej lub kilku usług oraz upraszcza i znacznie przyspiesza całą procedurę.

W czasie wprowadzania nowego użytkownika, mentor może określić poziom jego uprawnień:

- **użytkownik pełnoprawny** — nowy użytkownik dołącza do grupy użytkowników równorzędnych, posiadających takie same uprawnienia jak mentor — włącznie z możliwością wprowadzania nowych użytkowników — i współdzielących wszystkie obecne i przyszłe rejestracje w usługach, utworzone przez dowolnego członka grupy;
- **użytkownik-asystent** (konto ograniczone albo podrzędne) — nowy użytkownik posiada bardzo ograniczone uprawnienia, które są kontrolowane przez mentora. Użytkownik taki musi zostać jawnie przypisany do wszystkich zgłoszeń, do których ma mieć dostęp.

Użytkownicy należący do grupy mogą przeglądać listę użytkowników tej grupy i usuwać z niej innych użytkowników. Użytkownicy o ograniczonych uprawnieniach widoczni są wyłącznie dla ich mentora i tylko on może nimi zarządzać. W przypadku usunięcia konta mentora, użytkownicy ograniczeni stają się widoczni dla wszystkich użytkowników należących do grupy. Dowolny z tych użytkowników może przypisać ich do nowego mentora. Mechanizm taki jest bardzo wygodny w dużych organizacjach, liczących wielu użytkowników i asystentów — pozwala uniknąć powtarzania procesu wprowadzania asystentów, gdy ich sponsor odchodzi z organizacji lub zmienia pełnioną rolę. Użytkownicy mogą także samodzielnie usuwać (wyrejestrowywać) swoje konta — niezależnie od tego, czy należą do grupy, czy nie.

Tworzenie, aktywacja i usuwanie rejestracji

Rejestracja w nowych usługach odbywa się zgodnie z procesem uwierzytelniania opartym na wiedzy, opisanym w sekcji *Początkowe zgłaszanie użytkowników* wcześniej w tym rozdziale. Rejestracja w każdej usłudze rządzi się własnymi zasadami i jest całkowicie niezależna od rejestracji w pozostałych usługach.

Uwaga — rejestracje w usługach tworzone przez niezależnych użytkowników zawsze pozostają niezależne od siebie, nawet jeśli dotyczą tego samego kontekstu usługi (korzystają z tych samych identyfikatorów specyficznych dla usługi). Nie istnieje żadna wiarygodna metoda wykrywania współdzielenia określonych rejestracji czy przyłączenia takiego użytkownika do grupy. Fakt, że dwaj użytkownicy uzyskują dostęp do jednej usługi na podstawie tego samego identyfikatora, nie oznacza wcale, że użytkownicy ci chcą współdzielić pozostałe rejestracje w ramach grupy.

W przypadkach, gdy współdzielenie rejestracji jest pożądane, nowi użytkownicy — zamiast niezależnie rejestrować się w systemie i w poszczególnych usługach — powinni być wprowadzani za pomocą funkcji dodawania użytkownika. Dzięki temu cała grupa będzie mogła współdzielić wszystkie rejestracje.

Aktywacja rejestracji w nowej usłudze odbywa się w taki sam sposób — poprzez jawną opóźnioną aktywację z wykorzystaniem kodu aktywacyjnego lub natychmiastowo — o ile usługa pozwala na aktywację natychmiastową, a użytkownik przedstawił prawidłowy kod aktywacyjny. Użytkownicy, którzy utworzyli własne rejestracje, mogą nimi zarządzać i usuwać je, podobnie jak każdy użytkownik należący do ich grupy.

Przypisywanie (delegowanie) uprawnień — agenci

Użytkownicy mogą przypisywać (delegować) swoje uprawnienia innym użytkownikom w odniesieniu do określonych rejestracji w usługach. Ustanowieni w ten sposób agenci mogą działać w imieniu użytkownika, który przypisał im prawa. Jednym z przykładów

zastosowania tej techniki jest autoryzacja księgowych i agentów podatkowych do przesyłania dokumentów w imieniu ich mocodawcy, którym może być osoba lub organizacja. W zależności od usługi docelowej można wymusić stosowanie określonych reguł, na przykład:

- przypisanie (delegacja) uprawnień może odbywać się na zasadzie wyłączności — po przydzieleniu agentowi rejestracji do usługi, mocodawca traci prawo do działania w kontekście tej samej rejestracji do momentu usunięcia agenta (wycofania przypisania);
- aby móc działać jako agent, użytkownik musi zarejestrować się w określonej usłudze agenta. Jest tak najczęściej w przypadkach, w których wymagane jest zweryfikowanie określonych kwalifikacji zawodowych lub akredytacji. Reguły i procedury uwierzytelniania początkowego mogą w takim przypadku obejmować niezbędną weryfikację — przedstawienie dokumentów, uzyskanie kodu aktywacyjnego itp.

Relacje przypisania agentów są przechowywane wewnątrz huba i wykorzystywane do realizacji odpowiedniego odwzorowania tożsamości agenta na identyfikatory wykorzystywane w rejestracjach przypisanych mu przez mocodawców. W złożonych przypadkach mocodawcy mogą wyznaczać na agentów całe organizacje — organizacja ma wtedy możliwość wyznaczenia agentów-asystentów opiekujących się określonymi klientami.

Uwaga — wyznaczenie agenta to delikatny proces o poważnych implikacjach prawnych. Fakt wyznaczenia agenta powinien podlegać inspekcji i być łatwo weryfikowalny. Dowód delegacji uprawnień powinien być przechowywany w sposób nie budzący zastrzeżeń (najlepiej w postaci zapisu u dostawcy usługi docelowej) i gwarantować niepodważalność działań agenta podjętych w imieniu użytkownika.

Poza możliwością wyznaczenia stałego agenta, możliwa jest także czasowa delegacja uprawnień (na ograniczony okres i wyłącznie w kontekście określonej transakcji).

W takich wypadkach potwierdzeniem delegacji są odpowiednie tokeny zabezpieczeń, przesyłane wraz z komunikatami w systemie. Tokeny te są niezależnie weryfikowane przez hub podczas przetwarzania żądania.

Pomoc techniczna i odzyskiwanie kont użytkowników

System musi zapewniać funkcje niezbędne do świadczenia pomocy dla użytkowników i realizacji działań biura obsługi Klientów, takich jak resetowanie zapomnianych haseł, odszukiwanie utraconych poświadczeń itp.

Aktualizowanie identyfikatorów specyficznych dla usługi

W hubie przechowywany jest dla każdej rejestracji zestaw identyfikatorów specyficznych dla usługi, której dotyczy rejestracja. Kolejne interakcje z hubem (uwierzytelnienie, autoryzacja, przesłanie dokumentu) odwzorowują zweryfikowaną ogólną tożsamość użytkownika na identyfikatory specyficzne dla usługi. Wszelkie zmiany tych identyfikatorów, na przykład ze względu na modyfikacje wprowadzane w systemach informatycznych dostawców usług lub reorganizację agencji, wymagają komunikacji z hubem w celu uaktualnienia odpowiednich identyfikatorów zapisanych wraz z rejestracjami użytkowników.

Aktualizacje mogą być realizowane na poziomie pojedynczej rejestracji (odnalezienie konkretnego zestawu identyfikatorów i wymienienie go na nowy zestaw) lub jako grupowe modyfikacje wybranych identyfikatorów (na przykład odnalezienie wszystkich zestawów identyfikatorów, w którym pole „identyfikator urzędu skarbowego” ma wartość 015, 018 lub 022 i zmiana wartości tego pola na 088).

Uwaga — dobierając zestawy identyfikatorów dla poszczególnych usług warto wziąć pod uwagę nakłady pracy, jakie będzie pochłaniało utrzymanie ich aktualności. O ile przechowywanie atrybutów dodatkowych (wykraczających poza minimalny zestaw niezbędny do jednoznacznej identyfikacji użytkownika i kontekstu) i otrzymywanie ich w wyniku odwzorowania tożsamości może być bardzo wygodnym rozwiązaniem, nakład prac na utrzymanie aktualności tych identyfikatorów może przeważać korzyści wynikające z ich przechowywania.

Usługi poufności danych i bezpieczeństwa

Usługi utrzymania poufności i bezpieczeństwa, zapewniane przez hub usług e-zdrowia, można przypisać do następujących kategorii:

- usługi uwierzytelniania i autoryzacji,
- usługi tokenów bezpieczeństwa,
- usługi zarządzania zgodami,
- usługi anonimizacji.

Jednym z najważniejszych aspektów, dotyczących każdej aplikacji, jest zabezpieczenie tej aplikacji przed działaniami złośliwych użytkowników, automatyzowanymi atakami z wykorzystaniem wirusów i robaków internetowych, atakami typu DoS (Denial of Service — zablokowanie usługi) czy wyciekami informacji poufnych. W przypadku projektów integracyjnych e-zdrowia wymagania te mają szczególne znaczenie — charakter przechowywanych danych sprawia, że aplikacje te są narażone na częste ataki mające na celu kradzież tożsamości, zniszczenie danych lub zablokowanie dostępu do usług. Architektura bezpiecznego rozwiązania musi uwzględniać zarówno ogólne zagadnienia związane z bezpieczeństwem, jak i zagadnienia specyficzne dla rozwiązań integracyjnych e-zdrowia.

Ogólne sposoby podejścia do problemu bezpiecznej architektury rozwiązania

Trzy najważniejsze związane z bezpieczeństwem cele, o których należy pamiętać projektując dowolną aplikację, to:

- **poufność** — aplikacja musi dawać gwarancję, że dostęp do danych oraz do wszystkich funkcji modyfikujących dane mają wyłącznie uprawnieni użytkownicy. Żaden inny użytkownik nie powinien mieć możliwości wyświetlenia, usunięcia lub zmodyfikowania jakichkolwiek danych;
- **integralność** — wszystkie realizowane na danych operacje muszą chronić te dane przed uszkodzeniem. Każda operacja powinna albo zakończyć się pomyślnie i pozostawić dane w nowym, poprawnym stanie, albo zakończyć się niepowodzeniem, pozostawić dane w stanie niezmienionym i poinformować użytkownika lub inną uprawnioną osobę o niepowodzeniu. Wszelkie modyfikacje danych muszą być odnotowywane (na przykład w dzienniku inspekcji) z możliwością odtworzenia danych oryginalnych i bieżącego monitorowania wprowadzanych zmian;
- **uwierzytelnianie** — każdy użytkownik musi zostać odpowiednio zidentyfikowany na początku pracy z aplikacją, oraz — jeśli zachodzi taka potrzeba — także w trakcie pracy, przed wykonaniem określonej operacji. Dotyczy to przede wszystkim przeglądania, usuwania i modyfikowania danych.

Realizacja tych celów wymaga podziału architektury na warstwy logiczne i zaimplementowania bezpieczeństwa w poszczególnych warstwach. Każda warstwa, odwołując się do innej warstwy albo do usługi zewnętrznej, wraz z wywołaniem przesyła informacje uwierzytelniające, oparte na uwierzytelnieniu użytkownika, który spowodował wywołanie danej usługi. Jeśli warstwa lub usługa odbierająca wywołanie wymaga dodatkowych informacji, powinna zażądać ich przed przejściem do dalszych etapów procesu.

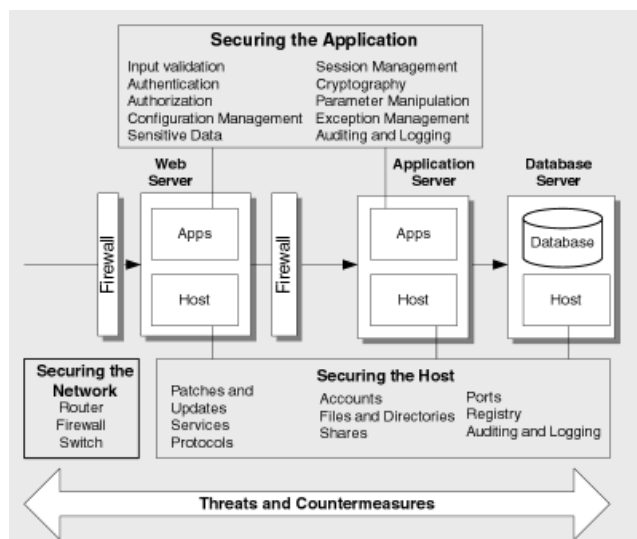
Wskazówki dotyczące projektowania architektury bezpiecznych rozwiązań opartych na .NET Framework i usługach Web Services oraz implementowania takich rozwiązań

można znaleźć w witrynie Microsoft Security Developer Center. Witryna, znajdująca się pod adresem <http://msdn.microsoft.com/security/default.aspx>, zawiera ogólne informacje dotyczące bezpieczeństwa oraz łączy do witryny Microsoft Patterns and Practices Center, w której zgromadzono zalecenia dotyczące określonych przykładów zastosowań.

Wzorce i dobre praktyki dotyczące bezpieczeństwa

Koncepcję wzorców i najlepszych praktyk opisano na stronie katalogowej witryny Microsoft Patterns and Practices Center pod adresem <http://msdn.microsoft.com/practices/GetStarted/>. Lista dostępnych wzorców i praktyk znajduje się pod adresem <http://msdn.microsoft.com/practices/>.

Pierwszy etap tworzenia bezpiecznej architektury polega na rozpoznaniu zagrożeń dla danej aplikacji oraz analizie dostępnych technik zabezpieczenia aplikacji przed tymi zagrożeniami. Najczęstsze zagrożenia przedstawia *ilustracja 9*, zaczerpnięta z opracowanego przez dział Microsoft Patterns & Practices dokumentu *Improving Web Application Security: Threats and Countermeasures*. Dokument ten dostępny jest pod adresem <http://msdn.microsoft.com/library/en-us/dnnetsec/html/ThreatCounter.asp>.



Ilustracja 9. Zakres ulepszeń bezpieczeństwa aplikacji internetowych — zagrożenia i środki zaradcze (ilustracja zaczerpnięta z dokumentu „Improving Web Application Security: Threats and Countermeasures”, opracowanego przez dział Patterns and Practices)

Dokument zawiera opisy zagadnień takich jak modelowanie zagrożeń, zabezpieczanie poszczególnych warstw aplikacji, zabezpieczanie hostów oraz zabezpieczanie samej aplikacji. W dokumencie zamieszczono także listy kontrolne, pomocne w praktycznym wykorzystaniu zgromadzonych informacji, oraz serię artykułów „jak to zrobić”, opisujących poszczególne zadania w systematyczny sposób.

Najlepsze praktyki dotyczące bezpieczeństwa

Szczegółowe informacje na temat projektowania bezpiecznych architektur rozwiązań dostępne są w witrynie Security Best Practices pod adresem <http://msdn.microsoft.com/security/securecode/bestpractices/default.aspx>. Można tam znaleźć serie artykułów poświęcone najlepszym praktykom stosowanym w określonych sytuacjach, w tym między innymi:

- wskazówki dotyczące pisania bezpiecznego kodu dla platformy .NET Framework,
- najlepsze praktyki stosowania zabezpieczeń opartych na uprawnieniach kodu (Code Access Security),
- minimalizacja ilości kodu dostępnego dla niezauważanych użytkowników,
- projektowanie zarządzanych przez aplikację mechanizmów autoryzacji,
- budowa i konfiguracja bezpiecznych witryn internetowych.

Zabezpieczanie usług Web Services

Bezpieczeństwo aplikacji opartych na architekturze zorientowanej na usługi (SOA), czyli większości aplikacji integracji usług — w tym także projektów integracyjnych e-zdrowia, w znacznym stopniu zależy od bezpieczeństwa i niezawodności protokołów wykorzystanych do przekazywania komunikatów pomiędzy użytkownikami a usługami docelowymi. Aby zapewnić odpowiedni poziom bezpieczeństwa, usługi Web Services muszą być wyposażone w niezawodne mechanizmy uwierzytelniania, zapewniać poufność danych na wszystkich etapach przetwarzania i wspierać mechanizmy gwarantowanego jednorazowego dostarczania komunikatów z niezaprzeczalnością jego odbioru.

Przekazywaniem komunikatów zwykle zajmują się usługi i oprogramowanie orkiestracyjne — na przykład Microsoft BizTalk Server. BizTalk Server zapewnia funkcjonalność niezawodnego dostarczania komunikatów. Ochrona zawartości i zachowanie poufności komunikatów wymagają utrzymania bezpiecznych połączeń sieciowych pomiędzy użytkownikiem, hubem i usługami docelowymi. Odpowiednie bezpieczeństwo połączeń zapewniają protokoły SSL (Secure Sockets Layer) oraz HTTPS. Gwarancja niepodważalności i ochrona przed manipulowaniem zawartością komunikatów zapewniana jest przez certyfikaty cyfrowe.

Uwierzytelnianie dostępu do usług Web Services najlepiej jest rozwiązać poprzez wykorzystanie rozszerzeń „WS*” standardów usług Web Services. Jedną z implementacji tych rozszerzeń jest pakiet Microsoft Web Service Enhancements (WSE). Szczegółowe informacje na temat pakietu można znaleźć pod adresem

<http://msdn.microsoft.com/webservices/building/wse/>. Dostępny jest także artykuł opisujący całą serię rozszerzeń oraz uzasadniający konieczność stosowania ich w aplikacjach Web Services. Artykuł ten znajduje się pod adresem <http://msdn.microsoft.com/library/en-us/dnwse/html/whywse.asp>.

Uwaga — warto w tym miejscu podkreślić, że WSE to pakiet zbiorczy, obejmujący obsługę wielu rozszerzeń standardów Web Services. Z punktu widzenia bezpieczeństwa, najważniejszymi rozszerzeniami są:

- WS-Security — pozwala na łatwe przekazywanie zabezpieczonych komunikatów z wykorzystaniem istniejących mechanizmów transportowych. Bezpieczeństwo realizowane jest na poziomie pojedynczego komunikatu, a nie warstwy transportowej.
- WS-Trust — zapewnia funkcje bezpiecznego przesyłania poświadczeń tożsamości za pośrednictwem usług Web Service.

- WS-Policy — definicja składni XML do celów walidacji odbieranych komunikatów SOAP w oparciu o opis cech takich jak podpisy cyfrowe i szyfrowanie. Cechy te nie są obsługiwane przez standardowe dokumenty WSDL.
- WS-Addressing — zapewnia lepszą kontrolę nad przekazywaniem komunikatów Web Services pomiędzy serwerami i usługami.

Jednym ze sposobów uproszczenia uwierzytelniania i autoryzacji w rozwiązaniu integracyjnym, obejmującym wiele zdalnych usług, jest zaimplementowanie do tego celu centralnej usługi opartej na tokenach, której będą ufały wszystkie pozostałe usługi. Usługa centralna — zaimplementowana wewnątrz huba — wydaje użytkownikom tokeny, które ci następnie przedstawiają każdej usłudze, do której uzyskują dostęp. Usługi zdalne mogą zweryfikować token, odwołując się do usługi centralnej. Uzyskujemy w ten sposób proste rozwiązanie problemów zwielokrotnienia, charakterystycznych dla wszystkich rozwiązań integracyjnych. Podejście takie na dodatek ułatwia tworzenie niestandardowych mechanizmów uwierzytelniania dla każdego użytkownika i każdej usługi. System uwierzytelniania wykorzystany w architekturze referencyjnej opisano w sekcji na temat uwierzytelniania i autoryzacji.

Zagadnienie bezpieczeństwa specyficzne dla architektury systemów e-zdrowia

Projekty integracyjne e-zdrowia mają wiele cech wspólnych z innymi systemami usług elektronicznych powszechnego użytku (na przykład z usługami bankowymi czy sklepami internetowymi). Wszystkie wymienione w poprzednim rozdziale ogólne zagrożenia oraz wskazówki dotyczą także systemów e-zdrowia. Istnieją jednak pewne związane z bezpieczeństwem zagadnienia specyficzne dla architektury systemów e-zdrowia. Opisujemy je w tym rozdziale.

Ochrona i poufność danych

W zależności od wybranej topologii i sposobu implementacji, hub usług e-zdrowia może przechowywać dane osobowe bardzo wielu użytkowników — nawet wszystkich obywateli kraju. Na kształt architektury systemu mogą mieć wpływ różne uwarunkowania prawne, co może ograniczyć wybór dostępnych rozwiązań technicznych.

Jeśli na przykład lokalne regulacje prawne zabraniają jakiegokolwiek współdzielenia informacji (nawet samych identyfikatorów) przez agencje opieki zdrowotnej, początkowa identyfikacja użytkowników podczas rejestracji do usług będzie musiała być realizowana zdalnie. Centralny hub w celu zweryfikowania informacji przedstawionych przez użytkownika, zamiast skorzystać z przechowywanych zwykle lokalnie danych referencyjnych, będzie musiał odwołać się do dostawcy usługi (szczegółowy opis możliwych rozwiązań identyfikacji początkowej znajduje się w sekcji *Logika weryfikująca i dane referencyjne* rozdziału *Usługi zarządzania tożsamością* wcześniej w tym dokumencie).

Gdy dane referencyjne poszczególnych usług przechowywane są w hubie centralnym, niezbędne jest zastosowanie odpowiednich środków kontroli dostępu do tych danych. Na przykład przechowywanie danych referencyjnych różnych usług w niezależnych bazach danych pozwala na zróżnicowanie praw dostępu do tych danych dla poszczególnych administratorów.

Infrastruktura techniczna i sieci komputerowe

W niektórych krajach istnieje dedykowana infrastruktura techniczna (w tym sieci komputerowe) przeznaczona do obsługi agencji opieki zdrowotnej. Ze względu na określone reguły dostępu i procedury akredytacyjne, określające kto i w jaki sposób może korzystać z infrastruktury, infrastruktura ta zwykle może być uważana za bardziej

bezpieczną. Samo uzyskanie dostępu do infrastruktury zwykle zapewnia wystarczająco wysoki poziom bezpieczeństwa i niezawodności komunikacji z innymi agencjami opieki zdrowotnej, co ułatwia proces integracji całego rozwiązania.

W przypadkach, gdy taka infrastruktura jest dostępna i łączy już dostawców usług e-zdrowia, łatwiejsze jest bezpieczne udostępnienie usług tych dostawców dla społeczeństwa za pośrednictwem wspólnego huba usług e-zdrowia. Hub może pracować jako most łączący bezpieczną infrastrukturę opieki zdrowotnej z siecią publiczną. Poszczególni dostawcy usług nie muszą niezależnie spełniać wymagań bezpieczeństwa przed podłączeniem ich systemów do sieci publicznej. Praca ta (i wszelkie potrzebne akredytacje) może zostać wykonana jednokrotnie — podczas budowy centralnego huba. Jedyne, co muszą zrobić dostawcy usług, to uzyskać połączenie z hubem.

Nawet jeśli taka bezpieczna infrastruktura istnieje, a dostawcy usług mogą z niej korzystać, trzeba zadbać o to, by architektura systemu nie stała się zbyt uproszczona. Nie należy zakładać, że połączenia ze wszystkimi dostawcami usług — obecnymi i przyszłymi — zawsze będą realizowane za pośrednictwem bezpiecznej sieci. Architektura powinna zapewniać funkcje niezbędne do obsługi bezpiecznej komunikacji za pośrednictwem sieci publicznych, najlepiej w postaci prostej opcji, skonfigurowanej niezależnie dla poszczególnych usług lub węzłów sieci. Pozwoli to w przyszłości dostosować się do nowych wymagań, takich jak na przykład obsługa dostawców usług e-zdrowia działających poza agencjami opieki zdrowotnej posiadającymi dostęp do bezpiecznej sieci komputerowej. Z doświadczeń, zebranych w ramach licznych projektów integracyjnych e-zdrowia w wielu krajach, wynika, że potrzeba takiej elastyczności zwykle pojawia się znacznie szybciej niż się spodziewano, a koszt późniejszego dostosowania ograniczonej, opracowanej na podstawie z góry przyjętych założeń architektury, może być wysoki.

Zabezpieczanie hostów

Systemy e-zdrowia mają często postać skomplikowanej pajęczyny, łączącej różne węzły oparte na różnych platformach. Poszczególne węzły należą do różnych właścicieli i zarządzane są w różny sposób. Czasami brak jest jednostki nadrzędnej, która mogłaby efektywnie zobligować wszystkich członków do stosowania dobrych praktyk w zakresie bezpieczeństwa. W niektórych krajach wszystkie elementy infrastruktury opieki zdrowotnej muszą spełniać odpowiednie standardy bezpieczeństwa (na przykład ISO 17799) z obowiązkową akredytacją przed dopuszczeniem do użytku produkcyjnego, ale nie jest tak w każdym kraju. Odpowiednie zabezpieczenie hostów pracujących w takim środowisku jest zadaniem znacznie trudniejszym niż w przypadku środowisk komercyjnych. Należy więc założyć, że niektóre hosty mogą być celem udanego ataku, w związku z czym niezbędne jest wdrożenie odpowiednich, dodatkowych warstw ochrony, umożliwiających efektywne działanie w przypadku włamania.

Błędne założenia co do fizycznego bezpieczeństwa systemów uczestniczących w wymianie komunikatów i nadmierna ufność w skuteczność takich zabezpieczeń mogą być zagrożeniem dla systemów pracujących w bezpiecznych centrach danych (na przykład w szpitalu). Przykładem może być założenie, że wzajemne uwierzytelnianie TLS/SSL punktów końcowych połączenia daje wystarczającą gwarancję, że żądania pochodzą z zaufanego źródła i nie ma potrzeby wprowadzania zabezpieczeń na poziomie pojedynczego komunikatu.

Jednak gdy ta sama usługa zostanie udostępniona szerszej rzeszy klientów, ryzyko komunikacji ze skompromitowanym hostem jest dużo wyższe. Na przykład udostępnienie usługi zdalnym aptekom, których komputery nie są fizycznie bezpieczne, a pracownicy nie są specjalistami IT, wymaga wprowadzenia dodatkowych zabezpieczeń — konkretnie szyfrowania przesyłanych komunikatów. Zalecanym rozwiązaniem jest więc zaprojektowanie odpowiednich warstw zabezpieczeń już w pierwszej fazie projektu

architektury, z możliwością włączania i wyłączania tych zabezpieczeń w razie potrzeby. Pozwoli to na uzyskanie lepszej elastyczności i szybsze dostosowywanie się do różnych obecnych i przyszłych, znanych i nieznanymi wymagań.

Zabezpieczanie hostów to ważny element ogólnej polityki bezpieczeństwa. Zaleca się, by poziom bezpieczeństwa hostów był tak wysoki, jak to tylko możliwe. W zależności od wykorzystywanej platformy i wersji systemów operacyjnych, dostępna jest cała gama możliwości — od narzędzi przeznaczonych dla środowisk zarządzanych (SMS, WSUS) po usługi zorientowane na konsumenta (na przykład automatyzacja aktualizacji Windows Update) — ułatwiających instalowanie najnowszych uaktualnień i rozszerzeń zabezpieczeń.

Ataki typu DoS (Denial of Service)

Ataki typu DoS (Denial of Service — zablokowanie usługi) są dość często kierowane przeciwko systemom komercyjnym i istnieje duże prawdopodobieństwo wykorzystania ich przeciwko systemom e-zdrowia (co może mieć znacznie poważniejsze skutki) — po pierwsze systemy e-zdrowia są atrakcyjnym i dobrze widocznym celem, a po drugie liczba użytkowników dotkniętych takim atakiem jest znacznie wyższa. Należy więc dołożyć wszelkich starań, aby do minimum ograniczyć możliwości przeprowadzenia ataków DoS przeciwko hubom usług e-zdrowia. Objawy takich ataków to między innymi:

- zgłaszanie dużych ilości fałszywych użytkowników — gdy testy wiarygodności zgłoszenia nowego użytkownika są nieefektywne, osoba atakująca może zgłosić do systemu bardzo wielu użytkowników z nieprawdziwymi danymi osobowymi. Zgłoszenie dużej liczby użytkowników może przeciążyć dostępne zasoby obliczeniowe i zablokować magazyny danych, czego wynikiem zwykle jest zablokowanie dostępu do systemu dla rzeczywistych użytkowników;
- powtarzające się nieudane próby logowania — brak efektywnej kontroli logowań (na przykład zliczania nieudanych prób logowania i blokowania konta po przekroczeniu limitu) może zostać wykorzystany przez osobę atakującą do obciążenia systemu dużą liczbą żądań uwierzytelnienia, co w konsekwencji prowadzi do zablokowania zasobów systemowych. Jeśli natomiast kontrola logowań została zaimplementowana, a atakujący zna prawidłowe identyfikatory użytkowników, atak może doprowadzić do zablokowania kont użytkowników;
- powtarzające się żądania, których obsłużenie wymaga dużej mocy obliczeniowej — powtarzające się żądania innego niż wymienione wyżej typu, których obsługa zajmuje zasoby systemowe. Może to być na przykład przesyłanie poprawnych, ale dużych dokumentów za pośrednictwem systemu rejestracji dokumentów.

Zapewnienie ochrony przed takimi atakami może wymagać odpowiedniego przygotowania architektury systemu. Poniżej podano przykładowe techniki minimalizujące prawdopodobieństwo przeprowadzenia udanego ataku.

Zabezpieczenie przed zgłaszaniem fałszywych użytkowników

Jeśli nie istnieje wiarygodna metoda weryfikacji, czy próba zgłoszenia dotyczy prawdziwego użytkownika, zgłoszenie można uzależnić od innego, weryfikowalnego procesu — na przykład od prawidłowej rejestracji w usłudze. Nie należy przyjmować zgłoszeń użytkowników wyłącznie na podstawie wybranej nazwy lub identyfikatora oraz hasła, ponieważ proces taki nie pozwala na efektywne rozróżnienie prawdziwych i fałszywych danych osobowych. Dobrym rozwiązaniem jest uzależnienie utworzenia konta użytkownika od prawidłowej rejestracji w co najmniej jednej usłudze, co wymaga zweryfikowania informacji podanych przez użytkownika z informacjami referencyjnymi. Praktycznie eliminuje to ryzyko przyjęcia zgłoszenia dużej liczby fałszywych użytkowników. Szczegółowe informacje na temat rejestrowania użytkowników

w usługach znajdują się w podsekcji *Początkowa identyfikacja użytkownika* w sekcji *Zarządzanie tożsamością* wcześniej w tym dokumencie.

Zabezpieczenie przed nieudanymi próbami logowania

Zabezpieczenie systemu przed powtarzającymi się nieudanymi próbami logowania może być trudne, zwłaszcza w przypadku ataków na losowe identyfikatory użytkowników. Licznik nieudanych prób logowania zawsze musi być związany z jakimś unikalnym identyfikatorem — najczęściej z identyfikatorem użytkownika. Rozproszenie ataku na różne, losowe identyfikatory użytkowników sprawia, że standardowe metody zliczania nieudanych prób logowania na poziomie systemu lub aplikacji stają się nieskuteczne. Ataki takie mają jednak jedną cechę charakterystyczną — dużą liczbę nieudanych prób logowania z jednego lub kilku źródeł w sieci — możliwa jest więc obrona na poziomie infrastruktury sieciowej w oparciu o lokalizację, z której nadchodzą żądania (na przykład adres IP atakującego komputera).

Istnieje jednak prawdopodobieństwo nieprawidłowego zidentyfikowania jako atak działań dużej liczby użytkowników pracujących w środowisku widocznym w sieci jako pojedyncza lokalizacja (tak jest na przykład, gdy użytkownicy korzystają z serwera pośredniczącego — proxy). Zakres stosowania opisanych wyżej środków zaradczych musi zostać bardzo precyzyjnie dobrany. Aby zminimalizować prawdopodobieństwo zablokowania dostępu prawidłowym użytkownikom, można wdrożyć mechanizm samonaprawczy — założenie blokady na pewien okres i automatyczne odblokowanie dostępu po upływie tego okresu. Dzięki temu, jeśli atak spowoduje zablokowanie dostępu dla dużej liczby użytkowników, po pewnym czasie dostęp zostanie przywrócony. Bez mechanizmu samonaprawczego, udany atak nie tylko zablokowałby dostęp, ale także dołożyłby pracy służbom pomocy technicznej, które musiałyby ręcznie przywracać dostęp poszczególnym użytkownikom.

Zabezpieczenie przed żądaniami wymagającymi dużej mocy obliczeniowej

Dobrym przykładem, ilustrującym konieczność zabezpieczenia się przed atakami polegającymi na przesyłaniu żądań, których obsługa wymaga dużej mocy obliczeniowej, jest odnawianie certyfikatów cyfrowych. Certyfikaty cyfrowe mogą służyć do weryfikowania tożsamości użytkownika i wiązania jej z rejestracjami w poszczególnych usługach e-zdrowia. Uwierzytelnienie użytkownika na podstawie certyfikatu zwykle polega na sprawdzeniu pochodzenia certyfikatu (jego wystawcy), poprawności (nie wygasł i nie został odwołany) oraz odwzorowania unikalnego identyfikatora certyfikatu na tożsamość użytkownika. Kolejnym etapem jest odszukanie odwzorowań łączących tożsamość użytkownika z rejestracjami w usługach.

Gdy system korzysta z zewnętrznych wystawców certyfikatów, okresowe odnawianie certyfikatów może odbywać się bez wiedzy huba. Na przykład gdy certyfikat jest odnawiany (u niektórych wystawców proces odnowienia certyfikatu jest przezroczysty dla użytkownika), wystawiany jest nowy certyfikat z takimi samymi danymi osobowymi — nowe są tylko numer seryjny i data wygaśnięcia. Pierwsza próba uwierzytelnienia w hubie za pomocą nowego certyfikatu i standardowej procedury porównującej nie powiedzie się, ponieważ hub nie wie nic o odnowieniu certyfikatu, a w bazie nadal zapisany jest poprzedni numer seryjny. Aby poprawnie obsłużyć uwierzytelnienie, hub musi skorzystać z bardziej złożonej procedury porównania, uwzględniającej także inne dane osobowe z certyfikatu. Jeśli wynik porównania będzie pozytywny, hub aktualizuje swoje dane — uaktualnia zapisany numer seryjny, utrzymując jednocześnie wszystkie pozostałe rejestracje i powiązania.

Aby móc obsłużyć taką procedurę odnawiania certyfikatów, hub musi przechowywać więcej informacji niż sam numer seryjny (na przykład nazwę wyróżniającą lub inne

atrybuty). Dane te potrzebne są do rozpoznania i porównania starego i nowego certyfikatu. Poszukiwanie polega na porównywaniu długich łańcuchów znaków — jeśli populacja użytkowników jest duża, poszukiwanie może być dość kosztowe pod względem zapotrzebowania na zasoby systemowe. Poszukiwanie takie realizowane jest za każdym razem, gdy numer seryjny certyfikatu nie zostanie znaleziony w lokalnym magazynie danych referencyjnych — także w przypadku przedstawienia dowolnego (nie związanego z systemem e-zdrowia) certyfikatu wystawionego przez zaufanego wystawcę. Niektóre techniki, powszechnie używane do obrony przed takimi atakami, to:

- Poprzedzenie wyszukiwania i porównywania długiego identyfikującego łańcucha znaków (nazwy wyróżniającej) wyszukaniem wartości skrótu (ang. hash) tego łańcucha znaków. Długość wartości skrótu łańcucha jest dużo mniejsza niż długość tego łańcucha, co pozwala na zwiększenie wydajności operacji wyszukiwania. Wymaga to jednak wcześniejszego obliczenia i zapisania wartości skrótów nazw wyróżniających wszystkich certyfikatów w bazie danych oraz odpowiedniego poindeksowania tych danych. W czasie uwierzytelniania należy obliczyć wartość skrótu nazwy wyróżniającej z przedstawionego certyfikatu i poszukać jej w bazie. Prawdopodobieństwo wystąpienia kolizji (dwie różne nazwy wyróżniające mają taką samą wartość skrótu) jest bardzo niskie, należy jednak po udanym wyszukiwaniu według wartości skrótu porównać także nazwy wyróżniające.
- Zastosowanie rejestru identyfikatorów certyfikatów wykorzystywanych do uwierzytelniania. Do inicjacji uwierzytelniania wymagane jest posiadanie prawidłowego certyfikatu wystawionego przez zaufanego wystawcę (w innym wypadku certyfikat zostanie odrzucony na etapie walidacji, przed rozpoczęciem procesu poszukiwania starego certyfikatu). Można więc przypuszczać, że do ataku zostanie wykorzystane tylko kilka certyfikatów. Ochrona przed atakiem polega na prowadzeniu rejestru podejrzanych, kilkakrotnie odrzuconych już certyfikatów i sprawdzaniu takiej „czarnej listy” przed rozpoczęciem poszukiwań wymagających dużej mocy obliczeniowej.

Przedstawiono tu zaledwie kilka wybranych przykładów, ilustrujących dodatkowe problemy i zagadnienia mające wpływ na architekturę rozwiązań e-zdrowia.

Usługi uwierzytelniania i autoryzacji

Uwierzytelnianie i autoryzacja to główna część funkcjonalności usług zabezpieczeń udostępnianych przez hub usług e-zdrowia. Funkcje uwierzytelniania i autoryzacji zapewniane przez hub usług e-zdrowia są funkcjami ogólnymi, dotyczącymi wszystkich typów tożsamości, reprezentujących poszczególnych użytkowników (bezpośrednio lub przez przedstawicieli), organizacje, systemy i inne jednostki. Funkcjonalność ta może być wykorzystywana bezpośrednio — na przykład przez portale do celów weryfikacji tożsamości użytkowników. W takim wypadku hub działa jako dostawca tożsamości i usługa wydawania tokenów zabezpieczeń. Możliwe jest także pośrednie korzystanie z funkcjonalności, na przykład przez usługi komunikacyjne, do celu weryfikacji tożsamości jednostki, która podpisała dokument lub do celu autoryzacji dostępu do usług docelowych.

Uwierzytelnianie

Funkcje uwierzytelniania weryfikują poświadczenia tożsamości przedstawione przez użytkownika i odwzorowują je na konkretną tożsamość.

Poziomy uwierzytelniania

Do każdego uwierzytelnienia można przypisać poziom określający wiarygodność tego uwierzytelnienia i związane z nim procedury.

Jedną z takich klasyfikacji jest używana w Wielkiej Brytanii klasyfikacja tScheme, której poszczególne poziomy — 0, 1, 2 oraz 3 — odpowiadają kolejnym wyższym poziomom wiarygodności uwierzytelnienia, uprawniającym do określonych typów działań.

- poziom 0 — brak uwierzytelnienia. Rzeczywista tożsamość osoby nie jest weryfikowana. Poziom ten dotyczy dostępu anonimowego lub sytuacji, w których użytkownicy podają pewne informacje, takie jak imię czy adres poczty elektronicznej, które są wykorzystywane w procesie i zapisywane, ale nie są weryfikowane;
- poziom 1 — tożsamość użytkownika jest z **dużym prawdopodobieństwem** prawdziwa (na przykład internetowe zamówienie książki z użyciem karty kredytowej z dostawą na adres posiadacza rachunku);
- poziom 2 — istnieje **wysoka pewność**, że tożsamość użytkownika jest prawdziwa (na przykład złożenie zeznania podatkowego dotyczącego podatku od towarów i usług lub podatku obrotowego, które jest wiążące prawnie);
- poziom 3 — prawdziwość tożsamości użytkownika pozostaje **poza wszelką wątpliwością** (złożenie elektronicznego podania o wydanie paszportu).

Im wyższy poziom, tym wyższa wymagana pewność weryfikacji tożsamości użytkownika. Poszczególne poziomy wiarygodności weryfikacji uzyskuje się, stosując odpowiednie, zatwierdzone i akredytowane przez tScheme procedury i metody techniczne.

Niewątpliwą zaletą stosowania systemu tScheme lub podobnego jest jednolitość wymagań oraz powszechna akceptacja (i kompatybilność) akredytowanych przez tScheme dostawców przez wszystkie agencje opieki zdrowotnej. W krajach, w których struktura taka jeszcze nie istnieje, wdrożenie podobnego systemu może mieć wpływ na przyspieszenie popularyzacji usług e-zdrowia.

Związanie z każdym uwierzytelnieniem informacji o poziomie jego wiarygodności oraz określenie minimalnego poziomu, wymaganego do przeprowadzanie poszczególnych operacji, sprawia, że kontrola uprawnień dostępu na różnych etapach przetwarzania staje się łatwa i bardzo efektywna. Na przykład odpowiedź na pytanie „które usługi można udostępnić danemu użytkownikowi?” brzmi „te, których minimalny wymagany poziom

wiarygodności jest równy lub niższy niż poziom uwierzytelnienia tego użytkownika”. „Czy ten użytkownik może przesłać żądanie tego typu?” — „tak, pod warunkiem, że minimalny poziom wiarygodności, wymagany do przesłania tego żądania, jest równy lub niższy niż poziom uwierzytelnienia tego użytkownika oraz spełnione są pozostałe warunki autoryzacji”.

Gdy szczegółowość tScheme nie jest wystarczająca do zaspokojenia jakichś specyficznych wymagań, możliwe jest rozszerzenie i uogólnienie tej struktury na dwa sposoby:

- Dodanie poziomów pośrednich — na przykład 1,5; 2,1; 2,3 — przy jednoczesnym utrzymaniu prostoty reguły podstawowej (poziom uwierzytelnienia musi być większy lub równy minimalnemu wymaganemu poziomowi wiarygodności). Różne rodzaje uwierzytelniania nadal porównywane są wyłącznie na podstawie zapewnianego przez nie poziomu, a więc poziom 2,2 zawsze będzie wyższy niż 2, niezależnie od dostawcy wybranego do celu uwierzytelnienia. Klasyfikacja ta jest powszechnie akceptowana przez wszystkich uczestników projektu i dostawców usług docelowych.
- Rozróżnianie dostawców uwierzytelniania (nawet jeśli oferują takie same poziomy wiarygodności) i stosowanie bardziej złożonych reguł — na przykład uzależniających prawa dostępu zarówno od poziomu uwierzytelnienia, jak i od dostawcy. Chociaż takie podejście jest elastyczne i pozwala na definiowanie specyficznych wymagań (takich jak „wymagaj uwierzytelnienia na poziomie 3 za pomocą karty inteligentnej wbudowanej w prawo jazdy, ale nie akceptuj uwierzytelnienia na poziomie 3 od innego dostawcy, na przykład na podstawie karty kredytowej”), ogranicza jednak spójność oraz możliwości wielokrotnego wykorzystywania dostawców uwierzytelniania we wszystkich usługach e-zdrowia. Model „każda usługa z własnym dostawcą uwierzytelniania” nie jest zbyt wygodny, a jego zakres zastosowań jest ograniczony do spełnienia określonych wymagań.

Zgodnie z zasadą elastyczności (patrz wcześniejsza sekcja *Reguły rządzące architekturą*), aby hub usług e-zdrowia mógł zaspokoić wszystkie wymagania, jakie mogą pojawić się w okresie jego eksploatacji, usługa uwierzytelniania i autoryzacji powinna zapewniać pełną elastyczność według powyższego opisu (większa szczegółowość poziomów oraz możliwość definiowania bardziej skomplikowanych reguł).

Przedstawianie poświadczeń i stwierdzeń

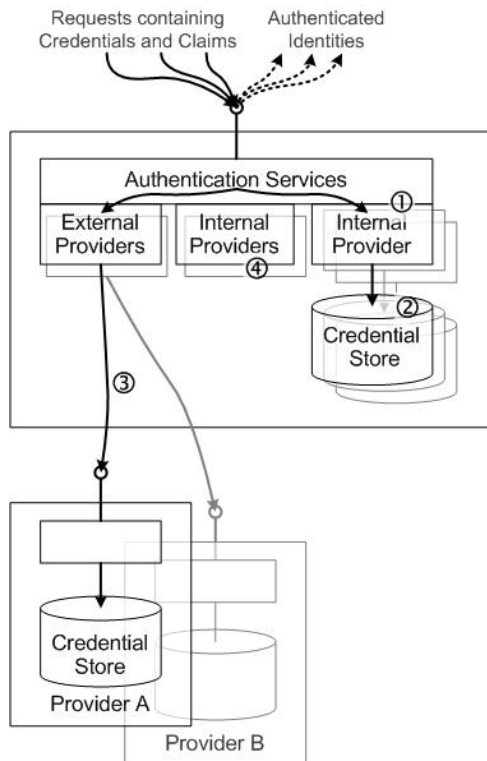
Uwierzytelnienie polega na zweryfikowaniu poświadczeń lub stwierdzeń przedstawionych przez użytkownika. Jeśli weryfikacja zakończy się pozytywnie, z użytkownikiem można powiązać odpowiednią tożsamość, co pozwala na utworzenie nowych związanych z tą tożsamością. Model ogólnego dostawcy pozwala na stosowanie wielu dostawców obsługujących różne rodzaje poświadczeń tożsamości.

Na *ilustracji 10*, przedstawiono kilka możliwych przebiegów procesu uwierzytelniania w oparciu o różnych dostawców uwierzytelniania. Numerami oznaczono różne sposoby weryfikacji tożsamości użytkownika w oparciu o przesłane wraz z żądaniem poświadczenia, ich rodzaj oraz miejsce, z którego je wysłano:

- bezpośrednio przez wewnętrznego (lokalnego) dostawcę (1), który weryfikuje dane użytkownika w oparciu o lokalny magazyn poświadczeń (2),
- poprzez odwołanie się do zaufanego dostawcy zewnętrznego (3), który przeprowadza własną procedurę weryfikacji poświadczeń.

Gdy żądanie uwierzytelnienia zawiera token bezpieczeństwa, jest on zwykle weryfikowany lokalnie (4). Może to być token wystawiony przez zaufaną przez hub usługę tokenów zabezpieczeń (Security Token Service — STS) lub token wystawiony

przez sam hub w wyniku wcześniejszego uwierzytelnienia według jednego z opisanych wcześniej sposobów.



Ilustracja 10. Wywoływanie różnych dostawców uwierzytelniania

Niezależnie od konkretnego typu weryfikacji i dostawcy wykorzystywanego w procesie uwierzytelniania (dostawca wewnętrzny lub zewnętrzny), pomyślna weryfikacja odwzorowuje poświadczenia lub stwierdzenia na tożsamość użytkownika. Daje to podstawę do dalszego odwzorowania tożsamości na identyfikatory użytkownika wykorzystywane przez poszczególne usługi (patrz sekcja *Odwzorowanie tożsamości na identyfikatory specyficzne dla usług* w dalszej części tego dokumentu) oraz wydawania tokenów zabezpieczeń (patrz sekcja *Usługa tokenów zabezpieczeń* w dalszej części tego dokumentu).

Uwierzytelnianie stowarzyszone

Tradycyjne modele uwierzytelniania, w których weryfikację poświadczeń realizuje jeden dostawca tożsamości, uniemożliwiają stosowanie wielu istniejących lub przyszłych dostawców tożsamości i ograniczają dostęp różnych grup użytkowników do wspólnego podstawowego zestawu usług e-zdrowia.

Uwierzytelnianie stowarzyszone zapewnia lepszą elastyczność i pozwala użytkownikom należącym do różnych (niezależnych i oddzielnych) domen zaufania uwierzytelniać się na podstawie poświadczeń charakterystycznych dla ich domen i uzyskiwać dostęp do

zasobów w innych domenach — w oparciu o relacje zaufania pomiędzy domenami. Usługi docelowe nie muszą znać lokalnych identyfikatorów użytkowników, w związku z czym tożsamość i inne atrybuty mogą pozostawać niejawne. Pozostaje to w zgodzie z zasadami zarządzania tożsamością — zasadą minimalnego zakresu ujawniania niezbędnych informacji oraz zasadą tożsamości ukierunkowanej — opisanymi wcześniej w rozdziale *Uwzględnienie powszechnych problemów dotyczących architektury* oraz w artykule <http://msdn.microsoft.com/library/en-us/dnwebsrv/html/lawsidentity.asp>.

Model uwierzytelniania stowarzyszonego oparty jest na zestawie specyfikacji i standardów usług Web Services, dzięki czemu jest niezależny od platform systemowych i implementacji. Pozwala to na łatwą integrację systemu oraz na stosowanie gotowego, komercyjnego oprogramowania. Więcej informacji na temat standardów takich jak WS-Security, WS-Trust i WS-Federation można znaleźć w ostatniej części tego opracowania, zatytułowanej *Odsyłacze, listy kontrolne i dalsze informacje*.

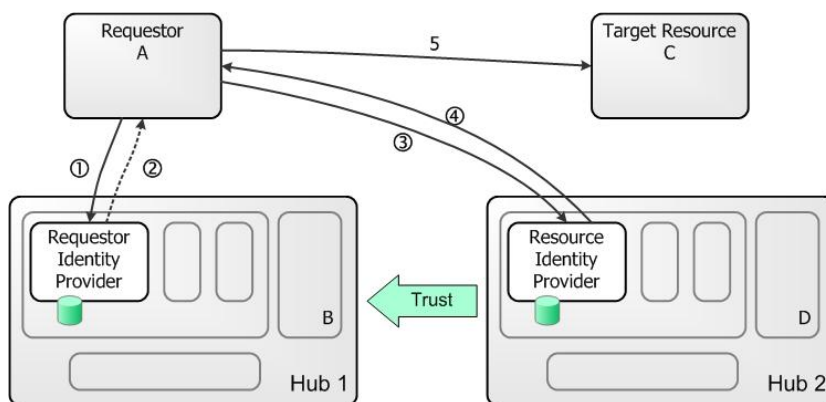
Hub usług e-zdrowia może pełnić wiele różnych ról i być elementem różnych topologii relacji zaufania w modelu uwierzytelniania stowarzyszonego. Jak opisano w sekcji *Możliwe topologie* w rozdziale *Hub usług e-zdrowia* wcześniej w tym przewodniku, pojedyncza topologia może obejmować wiele hubów. Hub może działać jako:

- **żądający dostawca tożsamości** — w procesie uwierzytelniania użytkownika hub generuje token bezpieczeństwa, który następnie — w celu uzyskania autoryzowanego dostępu do usługi docelowej — może zostać przedstawiony tej usłudze,
- **docelowy dostawca tożsamości** — weryfikuje tokeny bezpieczeństwa przedstawiane przez użytkowników i wystawia tokeny uprawniające do dostępu do usługi docelowej,
- **broker relacji zaufania** pomiędzy dwiema lub więcej stronami (patrz ilustracja w temacie *Huby równorzędne* w podsekcji *Możliwe topologie* w sekcji *Hub usług e-zdrowia* wcześniej w tym opracowaniu) — relacje zaufania każdej ze stron z brokerem zaufania pozwalają na utworzenie pośredniej relacji zaufania pomiędzy stronami.

Comment [JB3]: nie ma takiej sekcji

Na *ilustracji 11* przedstawiono przykład typowych przepływów danych pomiędzy stronami. Numerami oznaczono kolejne kroki:

1. Żądający A przedstawia niezbędne poświadczenia swojemu dostawcy tożsamości w hubie 1.
2. Dostawca tożsamości żądającego w hubie 1 weryfikuje poświadczenia i zwraca **token tożsamości** żądającemu A.
3. Żądający A przedstawia token tożsamości docelowemu dostawcy tożsamości w hubie 2.
4. Docelowy dostawca tożsamości w hubie 2 sprawdza poprawność i pochodzenie tokenu tożsamości i zwraca **token dostępu** uprawniający do dostępu do zasobu docelowego. Docelowy dostawca tożsamości nie musi znać żądającego A ani jego tożsamości — ufa dostawcy tożsamości żądającego w hubie 1 i wydanemu przez niego tokenowi tożsamości.
5. Żądający A w celu uzyskania dostępu do zasobu docelowego C, którego zabezpieczenia zarządzane są przez hub 2, przedstawia mu token dostępu.



Ilustracja 11. Uwierzytelnianie stowarzyszone

W przykładzie tym specjalnie rozdzielono poszczególne strony, by móc jasno przedstawić wszystkie interakcje. Żądający A może być portalem lub innym systemem, hub 1 — centralnym hubem usług e-zdrowia, zasób docelowy może być jakimś dostawcą usług e-zdrowia korzystającym z usług uwierzytelniania i autoryzacji świadczonych przez hub 2. Oczywiście możliwe są także inne warianty implementacji takiego samego ogólnego przepływu danych. Na przykład podsystem komunikacyjny (B), znajdujący się wewnątrz huba 1, także może pełnić rolę żądającego, który w celu komunikacji z podsystemem komunikacyjnym (D), działającym wewnątrz huba 2, musi uzyskać niezbędne tokeny tożsamości i dostępu.

Autoryzacja

Po poprawnym uwierzytelnieniu się i ustaleniu tożsamości użytkownika zwykle następuje proces autoryzacji o szczegółowości odpowiadającej poziomowi kontekstu. Połączenie procesu uwierzytelnienia z procesem autoryzacji pozwala podnieść wydajność — cały proces może zamknąć się w jednym odwołaniu do podsystemu uwierzytelniania i autoryzacji.

Żądania autoryzacji można realizować na dwa podstawowe sposoby:

- **pobierz wszystko** — podaj listę wszystkich zasobów, do których dana tożsamość posiada uprawnienia (i do których żądający może uzyskać autoryzowany dostęp — patrz komentarze poniżej),
- **proces jawny** — żądanie autoryzacji zawiera jawne określenie zasobu docelowego, którego dotyczy.

O ile metoda „pobierz wszystko” może wydawać się prostsza i łatwiejsza, przed podjęciem decyzji o jej wykorzystaniu warto wziąć pod uwagę kilka istotnych w kontekście usług e-zdrowia zagadnień. Stosując tę metodę można niepotrzebnie udostępnić żądającemu informacje, co do których nie mamy pewności, czy żądający może mieć do nich dostęp. Ogólnie rzecz biorąc, zastosowanie tej metody może doprowadzić do złamania niektórych podstawowych zasad zarządzania tożsamością.

Weźmy na przykład użytkownika, który posiada pojedyncze poświadczenie uprawniające go do dostępu do kilku usług e-zdrowia. Użytkownik może nie życzyć sobie, by w czasie, gdy używa portalu systemu emerytalnego, portal ten mógł pobrać identyfikatory związane ze sprawami podatkowymi czy choćby uzyskać informacje, że użytkownik jest

zarejestrowany w takich usługach, skoro informacje te nie mają żadnego związku z usługą, z której korzysta użytkownik. Jeśli portal może przeprowadzić operację autoryzacji „pobierz wszystko”, to może uzyskać informacje o wszystkich relacjach pomiędzy tym użytkownikiem a innymi użytkownikami, co nie jest pożądane.

Zalecanym rozwiązaniem w takich przypadkach jest autoryzacja jawna. Żądający definiuje, jakiego obiektu dotyczy żądanie, a dostawca usług autoryzacji zwraca odpowiednią odpowiedź. Żądanie autoryzacji nie musi dotyczyć pojedynczego celu — może zawierać całą listę usług docelowych. Można też uwzględniać dodatkowe warunki, na przykład w oparciu o tożsamość żądającego (w przypadku pośrednika można na przykład sprawdzić, do jakich zasobów żądający ma prawo sprawdzać autoryzację) lub w oparciu o jawną zgodę użytkownika, dołączoną do samego żądania.

W uzasadnionych wypadkach (i gdy użytkownik wyraził na to zgodę) można odstąpić od tego ogólnego zalecenia i uzyskać autoryzację do wszystkich usług, do których użytkownik posiada prawa dostępu. Przykładem takiej sytuacji jest przedstawienie pełnej listy dostępnych usług w celach konserwacyjnych (zarządzanie rejestracjami, przypisywanie praw itp.).

Sprawdzanie rejestracji w usługach

Jednostką autoryzacji w przyjętym ogólnym modelu tożsamości (opisanym w części *Podstawowy model tożsamości i zasady* w sekcji *Zarządzanie tożsamością* wcześniej w tym dokumencie) jest pojedyncza usługa docelowa — można sprawdzić tylko to, czy użytkownik „może, czy nie może uzyskać dostęp do usługi X”. Ma to wpływ na definicję usługi docelowej — każda usługa musi być grupą akcji (żądań lub operacji przedłożenia dokumentu) o odrębnych regułach dostępu.

Żądanie autoryzacji odwzorowuje uwierzytelnioną wcześniej tożsamość na poprawne, istniejące i aktywne rejestracje w usługach. W przypadku żądań typu „pobierz wszystko” operacja autoryzacji zwraca listę wszystkich rejestracji związanych z daną tożsamością. Autoryzacja jawna porównuje żądanie zawierające listę usług, do których żądający chce uzyskać dostęp, z ważnymi rejestracjami dla danej tożsamości i zwraca jedynie podzbiór tej listy (to jest listę usług, w których tożsamość posiada prawidłową rejestrację).

Odwzorowanie tożsamości na identyfikatory specyficzne dla usług

Ważnym aspektem autoryzacji jest odwzorowanie ogólnej (i potencjalnie takiej samej dla wielu usług) tożsamości na identyfikatory specyficzne dla danych usług, związane z aktywnymi rejestracjami, odnalezionymi w procesie autoryzacji. Odwzorowanie pozwala na ukrycie ogólnej tożsamości i określa kontekst relacji z daną usługą. Usługi docelowe mogą niezależnie ustalać wykorzystywane przez nie identyfikatory i nie ma potrzeby modyfikowania istniejących już systemów w celu wprowadzenia jakiegoś nowego identyfikatora (chyba że właściciel sam zdecyduje się na taki krok). Gdy ogólna tożsamość zostanie związana z usługą poprzez proces rejestracji ustalający kontekst relacji i zbiór identyfikatorów specyficznych dla usługi, kolejne żądania autoryzacji dla tej tożsamości będą zwracały te identyfikatory. Szczegółowe zasady działania opisano w temacie *Rejestracja w usługach i odwzorowywanie tożsamości* w sekcji *Zarządzanie tożsamością* wcześniej w tym dokumencie.

Delegowanie zaufania

W przypadku delegowania uprawnień, które polega na upoważnieniu innego użytkownika do działania w imieniu określonej osoby lub organizacji w kontekście określonej usługi (patrz temat *Przypisywanie (delegowanie) uprawnień — agenci* w sekcji *Zarządzanie użytkownikami i rejestracjami* wcześniej w tym dokumencie), proces odwzorowania jest bardziej skomplikowany. Polega on na odszukaniu prawidłowego łańcucha odwzorowań łączącego tożsamość z usługą docelową. Użytkownik z jednej organizacji może na

przykład uprawnień inną organizację-agenta do działania w jego imieniu, a następnie użytkownik z organizacji-agenta może ustanowić asystenta, którego zadaniem jest opiekowanie się określonymi klientami. Wynik operacji autoryzacji ma jednak nadal tę samą postać — „tożsamość A może uzyskać dostęp do usługi S w kontekście wyznaczanym przez specyficzne dla tej usługi identyfikatory X, Y i Z”. Taka delegacja uprawnień jest relatywnie wygodna w przypadku stałej, długotrwałej delegacji, która może zostać unieważniona przez jawne jej wypowiedzenie.

W przypadku delegacji krótkotrwałych (takich jak delegacje ustanowione jedynie na potrzeby określonej interakcji — na przykład przedłożenia dokumentu), prawo delegacji może zostać przesłane wraz z samym żądaniem autoryzacji. W takim wypadku proces odwzorowania tożsamości na rejestrację w usłudze bierze pod uwagę delegację (i daje wynik taki sam, jak w przypadku delegacji stałej, jedynie o krótszym okresie ważności i z innymi ograniczeniami). Taki proces nie oznacza trwałego zapisania relacji delegacji. Zrealizowana delegacja krótkotrwała nie ma wpływu na nowe żądania, chyba że żądania te same dotyczą delegacji.

Szczegółowość autoryzacji

Testy autoryzacji, realizowane przez hub w oparciu o aktywne rejestracje i ewentualne delegacje uprawnień, są ograniczone do poziomu usługi docelowej. Dalsze decyzje autoryzacji na niższych poziomach mogą być realizowane gdzie indziej (na przykład w innym hubie) w oparciu o dostarczone przez hub identyfikatory specyficzne dla danej usługi. Ustalenie odpowiedniej szczegółowości usług oraz poziomu szczegółowości identyfikatorów to bardzo ważne zagadnienie. Niezbędne jest zachowanie równowagi pomiędzy wygodą otrzymywania wszystkich informacji w ramach identyfikatorów zwracanych w procesie autoryzacji (identyfikatory te mogą obejmować także rolę i inne atrybuty) a koniecznością utrzymania aktualności kopii tych identyfikatorów, przechowywanej w hubie.

Przykładem autoryzacji „kaskadowej” może być przypadek prawnika działającego w imieniu swojego klienta w kontekście procesu sądowego. Prawnik, zarejestrowany w odpowiednich „usługach prawniczych” (przy czym rejestracja wymaga przedstawienia dokumentów potwierdzających prawo do wykonywania zawodu), może uzyskać dostęp do centralnego huba usług e-zdrowia, korzystając z poświadczeń wystawionych przez ten hub lub uzyskanych od innego zaufanego lub stowarzyszonego dostawcy tożsamości. Gdy prawnik korzysta z „portalu prawnego” lub innej usługi, hub e-zdrowia uwierzytelnia go i autoryzuje jego dostęp do „usług prawniczych”. Proces autoryzacji zwraca odpowiednie identyfikatory wykorzystywane przez „usługi prawnicze”.

Z punktu widzenia huba, uwierzytelniona tożsamość prawnika ma prawa dostępu do „usług prawniczych” w kontekście określanym przez odpowiednie, specyficzne dla tej usługi identyfikatory. W oparciu o te identyfikatory portal (lub inny system, z którego ten portal korzysta) może podejmować dalsze decyzje dotyczące autoryzacji. Może na przykład sprawdzić powiązania z określoną sprawą lub pełnioną rolę i na tej podstawie udzielić dostępu do pewnych dokumentów. Usługa docelowa utrzymuje szczegółowe informacje autoryzacyjne, dotyczące powiązań prawników ze sprawami, i nie udostępnia tych informacji hubowi — zadaniem huba jest tylko uwierzytelnienie użytkownika i sprawdzenie autoryzacji dostępu do określonej usługi jako całości.

Usługa tokenów zabezpieczeń

Hub usług e-zdrowia może pełnić rolę usługi tokenów zabezpieczeń (Security Token Service — STS), zdefiniowanej w standardach WS-Trust, WS-Federation i WS-Security (łączy do tych standardów znajdują się w sekcji *Odsyłacze, listy kontrolne i dalsze informacje*). Hub może zatem być częścią stowarzyszonej sieci usług Web Services,

zapewniających funkcje uwierzytelniania, autoryzacji i inną funkcjonalność ułatwiającą integrowanie systemu w oparciu o sprawdzone standardy i specyfikacje.

Usługa tokenów zabezpieczeń wydaje, weryfikuje i wymienia tokeny zabezpieczeń. Żądający przesyła żądanie, a usługa — jeśli pozwalają na to wymagania adresata oraz obowiązujące zasady — wydaje mu token bezpieczeństwa.

Tokeny bezpieczeństwa

Tokeny bezpieczeństwa zawierają zbiory stwierdzeń, których wiarygodność gwarantowana jest przez wydawcę tokenu. Wydawca może podpisywać tokeny z wykorzystaniem metod kryptograficznych, co gwarantuje ich integralność (brak możliwości wprowadzenia zmian po podpisaniu) i pozwala na weryfikację ich pochodzenia. Pomyślne przeprowadzenie przez hub usług e-zdrowia procesu uwierzytelniania i autoryzacji skutkuje zwykle wydaniem żądającemu tokenu bezpieczeństwa.

Wydawanie tokenów bezpieczeństwa

Token bezpieczeństwa jest wynikiem przeprowadzonego przez hub procesu uwierzytelniania i autoryzacji. Token może zawierać następujące informacje:

- uzyskane w wyniku uwierzytelnienia informacje na temat tożsamości wraz z odpowiednimi atrybutami, takimi jak sposób uwierzytelnienia i poziom wiarygodności,
- informacje na temat autoryzacji dostępu, na przykład w postaci listy dostępnych usług docelowych,
- specyficzne dla poszczególnych usług identyfikatory i atrybuty.

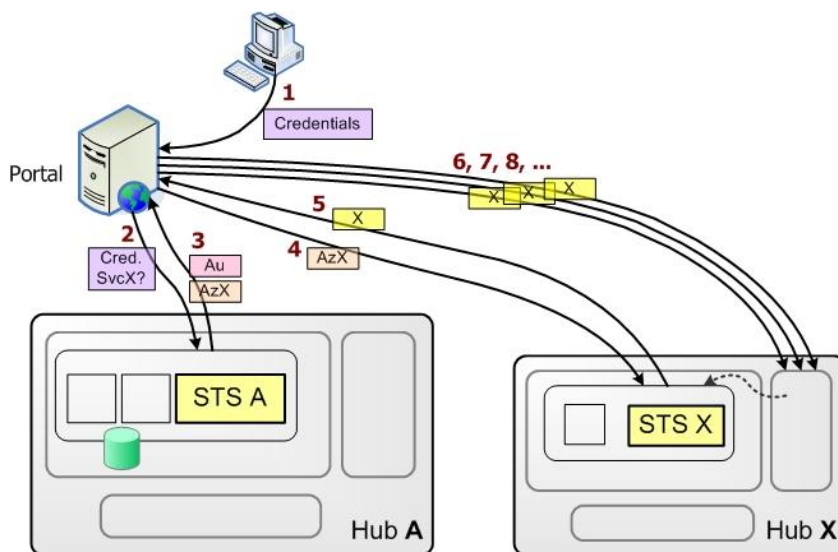
Rodzaj stwierdzeń zawartych w tokenie może się różnić w zależności od roli pełnionej przez hub i jego lokalizacji w topologii całego systemu. Możliwe jest także wydawanie wielu tokenów uprawniających do dostępu do różnych usług docelowych. W następnej sekcji przewodnika opisano kilka przykładowych scenariuszy zastosowań.

Możliwe scenariusze zastosowań

Interakcje pomiędzy poszczególnymi hubami oraz role pełnione przez odpowiadające im usługi tokenów bezpieczeństwa mogą być różne, w zależności od wybranej topologii systemu i przyjętego modelu zabezpieczeń. Na *ilustracji 12.* przedstawiono kilka możliwych scenariuszy. Kolejne etapy procesu oznaczono numerami:

1. Użytkownik kontaktuje się z portalem i przedstawia mu swoje poświadczenia tożsamości dla systemu e-zdrowia.
2. Portal wysyła żądanie do huba A (który może być centralnym hubem e-zdrowia), przedstawiając poświadczenia tożsamości użytkownika i wskazując usługę docelową X.
3. Po pomyślnym uwierzytelnieniu użytkownika i sprawdzeniu autoryzacji dostępu do usługi X, hub A zwraca dwa tokeny wystawione przez usługę STS A:
 - a. token uwierzytelnienia (**Au**) potwierdzający pomyślne uwierzytelnienie użytkownika. Token ten może zostać później wykorzystany do uzyskania dodatkowych autoryzacji bez potrzeby ponownego pełnego uwierzytelnienia użytkownika na podstawie poświadczeń tożsamości,
 - b. token autoryzacji dostępu użytkownika do usługi X (**AzX**), zawierający odpowiednie identyfikatory specyficzne dla usługi X, definiujące kontekst relacji użytkownika z tą usługą (na przykład numer identyfikacji podatkowej, identyfikator systemu zdrowotnego, identyfikator usług socjalnych).

4. Portal w imieniu użytkownika kontaktuje się z usługą STS X i przedstawia jej token uwierzytelnienia **AzX** wystawiony przez usługę STS A.
5. Usługa STS X sprawdza prawidłowość tokenu **AzX** i wystawia nowy token **X** (token specyficzny dla tej usługi STS), zawierający stwierdzenia potrzebne do dostępu do usługi X. Usługa może na przykład przetłumaczyć lub dokonać odwzorowania znajdujących się w tokenie **AzX** identyfikatorów specyficznych dla usługi na informację na temat roli danego użytkownika i na inne atrybuty w kontekście interakcji z usługą X.
- 6,7,8... Obsługując kolejne wywołania usługi X przez użytkownika końcowego, portal przedstawia token **X**, którego walidacja może być bardzo efektywna — o wiele bardziej wydajna niż wcześniejsza walidacja tokenu **AzX** z translacją lub odwzorowywaniem atrybutów. Umieszczenie w kontekście wywołania odpowiednich identyfikatorów, specyficznych dla usług X, zawartych w tokenie **X**, pozwala także na podejmowanie dalszych decyzji dotyczących autoryzacji wewnątrz usługi.

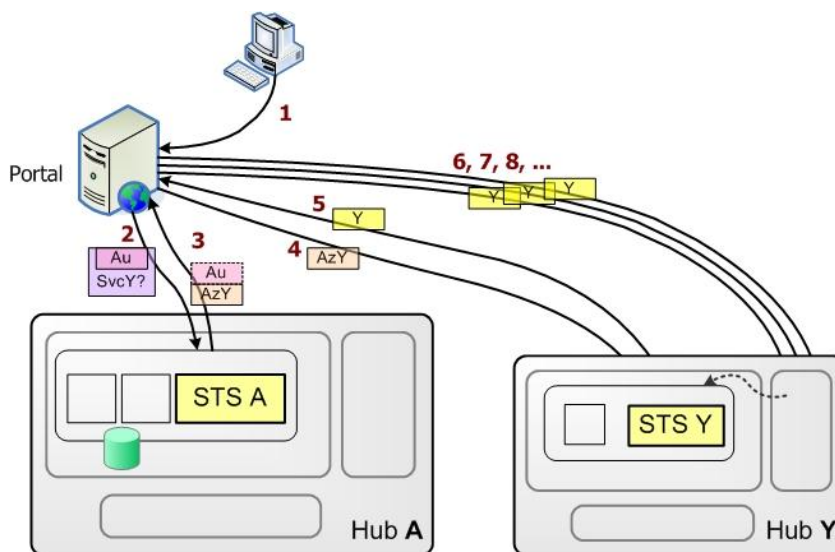


Ilustracja 12. Role usług STS i wymiana tokenów

Kontynuujemy nasz przykład. Po zakończeniu interakcji z usługą X, użytkownik (lub portal w imieniu użytkownika) chce uzyskać dostęp do usługi Y. Proces autoryzacji przedstawiono na ilustracji 13. Proces przebiega nieco inaczej niż w poprzednim przykładzie.

Jeśli token uwierzytelnienia (**Au**), wystawiony w poprzednim przykładzie przez usługę STS A, jest nadal ważny i został w odpowiedni, bezpieczny i wiarygodny sposób przechowany przez pośrednika (portal) lub użytkownika końcowego, uzyskanie autoryzacji dostępu do usługi Y jest prostsze i nie wymaga ponownego podania poświadczeń przez użytkownika. W ten sposób użytkownik raz zameldowany do systemu może uzyskać dostęp do wielu usług. Proces autoryzacji przebiega następująco:

1. Użytkownik żąda dostępu do usługi Y.
2. Portal wysyła żądanie do huba A, przedstawiając token uwierzytelniania (**Au**), uzyskany wcześniej od usługi STS A, i wskazuje usługę docelową Y.
3. Po zweryfikowaniu poprawności tokenu uwierzytelniania **Au** i autoryzacji dostępu użytkownika do usługi Y, hub A zwraca dwa tokeny wystawione przez usługę STS A:
 - a. opcjonalnie — odświeżony lub odnowiony token uwierzytelniania (**Au**) o przedłużonym okresie ważności, co pozwala na przedłużenie pierwszego uwierzytelnienia i dalsze korzystanie z „usług dostępu z jednokrotnym logowaniem” (wystawienie takiego tokenu podlega odpowiednim zasadom — konieczne jest utrzymanie równowagi między wygodą użytkownika a bezpieczeństwem),
 - b. token autoryzacji dostępu użytkownika do usługi Y (**AzY**), zawierający odpowiednie identyfikatory specyficzne dla usługi Y, definiujące kontekst relacji użytkownika z tą usługą.
4. Portal w imieniu użytkownika kontaktuje się z usługą Y i przedstawia jej token autoryzacji **AzY** wystawiony przez usługę STS A.
5. Usługa STS Y sprawdza prawidłowość tokenu **AzY** i wystawia nowy token Y (token specyficzny dla tej usługi STS), zawierający stwierdzenia potrzebne do dostępu do usługi Y.
- 6,7,8... W kolejnych wywołaniach usługi Y użytkownik końcowy lub portal przedstawia usłudze token Y, którego walidacja może być bardzo efektywna — o wiele więcej wydajna, niż początkowa walidacja tokenu **AzY** z translacją lub odwzorowywaniem atrybutów. Umieszczenie w kontekście wywołania odpowiednich identyfikatorów specyficznych dla usług Y, zawartych w tokenie Y, pozwala także na podjęcie dalszych decyzji dotyczących autoryzacji wewnątrz usługi.



Ilustracja 13. Role STS i wymiana tokenów — kolejna usługa

Możliwość pełnienia przez hub usług e-zdrowia roli usługi tokenów bezpieczeństwa STS pozwala na obsługę także wielu innych scenariuszy i umożliwia stosowanie różnych topologii odpowiadających określonym wymaganiom i ograniczeniom.

Udostępnianie usług uwierzytelniania i autoryzacji

Funkcjonalność uwierzytelniania i autoryzacji udostępniania jest w postaci zbioru usług Web Services, dzięki czemu jest ogólnie dostępna dla klientów wszystkich typów — innych systemów, portali i pakietów oprogramowania uruchamianych na komputerach klienckich. Bezpieczeństwo wywołań usług Web Services może zostać zapewnione na różnych poziomach:

- **bezpieczeństwo na poziomie transportowym**, na przykład wykorzystanie protokołów TLS/SSL, które pozwalają na szyfrowanie wszystkich przesyłanych informacji i chronią przed podsłuchami. Protokoły te pozwalają także na zapewnienie dostępu tylko tym jednostkom, które posiadają odpowiedni certyfikat klienta,
- **bezpieczeństwo na poziomie komunikatu (Web Services)** — żądanie samo zawiera elementy zabezpieczeń niezbędne do zidentyfikowania nadawcy i zaszyfrowania określonych części komunikatu.

Zważywszy na poufność wywołań dotyczących uwierzytelniania i autoryzacji, warto rozważyć ograniczenie dostępu do różnych części tej funkcjonalności poprzez identyfikowanie klientów i wprowadzenie ochrony przed potencjalnymi atakami. Na przykład: „Czy ten portal (usługa) jest akredytowany i ma prawo przeprowadzać operacje uwierzytelniania i autoryzacji?” oraz „Czy ten klient ma prawo pytać o autoryzację dostępu do usługi X?”.

W przypadkach, gdy hub usług e-zdrowia zapewnia zarówno funkcjonalność komunikacyjną, jak i funkcjonalność uwierzytelniania i autoryzacji, warto rozważyć udostępnienie funkcjonalności uwierzytelniania i autoryzacji niezależnie od interfejsów Web Services — wewnętrznie, dla zaufanych podsystemów, takich jak usługi komunikacji. Pozwoli to uniknąć dodatkowych nakładów zasobów obliczeniowych na wywoływanie publicznie dostępnych usług Web Services i podnieść wydajność. Podejmując decyzję o takiej modyfikacji, należy wziąć pod uwagę także inne interfejsy publiczne i prywatne.

Usługa zarządzania zgodami

Usługa zarządzania zgodami służy do zarządzania zapisami na temat zgód pacjentów w kontekście usług i rozwiązań e-zdrowia. Zasady zachowania poufności danych — a co za tym idzie, także zasady zarządzania zgodami pacjentów — są bardzo zróżnicowane w różnych krajach i obszarach podlegających różnym władzom ustawodawczym i sądowiczym. Z tego powodu usługa zarządzania zgodami musi charakteryzować się najwyższą elastycznością i szerokimi możliwościami konfiguracji. Ze względu na duże zróżnicowanie zasad zachowania poufności danych i zarządzania zgodami pacjentów w różnych krajach i obszarach podległych różnej jurysdykcji, usługa zarządzania zgodami musi być skonfigurowana zgodnie z obowiązującymi zasadami i zapisami prawnymi dotyczącymi rozwiązań e-zdrowia.

Zgody pacjentów mogą być:

- o domniemane lub jawne,
- o zapisywane w lokalnej lub centralnej bazie danych albo w wielu lokalizacjach,
- o stosowane do danych i usług począwszy od ujęcia ogólnego, a skończywszy na pojedynczych elementach danych z domeny zdrowotnej,
- o pomijane w razie potrzeby (np. w nagłych wypadkach).

Usługa zarządzania zgodami rejestruje, zarządza i waliduje informacje na temat zgód pacjentów i gwarantuje, że żądania dostępu do danych na temat pacjenta obsługiwane są zgodnie z zarejestrowanymi wytycznymi, określonymi przez pacjenta. Wytyczne te mogą być uzupełniane innymi ograniczeniami dotyczącymi poufności danych, na przykład przepisami prawnymi czy specyficznymi regułami biznesowymi, obowiązującymi w danej domenie danych.

Usługa zarządzania zgodami dostępna jest w formie zbioru usług Web Services, zapewniającego następujące funkcje:

- o rejestracja i odwoływanie zgód pacjentów,
- o walidacja zgód pacjentów,
- o pominięcie zgody pacjenta,
- o zapewnienie kontroli dostępu do danych pacjentów w oparciu o zarejestrowane zgody (oraz opcjonalnie inne, zarządzane reguły biznesowe),
- o rejestracja i inspekcja wszystkich działań związanych ze zgodami pacjentów.

Usługa anonimizacji
do zrobienia

Usługi prezentacji i punktu dostępu

Usługi publikacji i wyszukiwania usług

Usługa katalogu usług

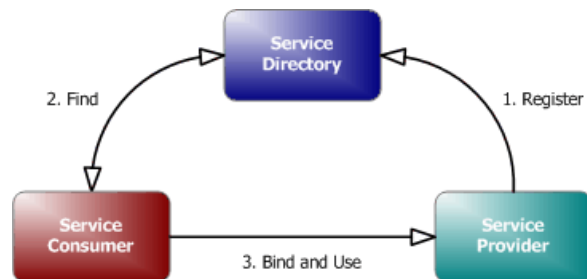
Jedną z głównych cech architektury zorientowanej na usługi (Service Oriented Architecture — SOA) jest przezroczystość (niezależność) lokalizacji usług udostępnianych konsumentom. Fizyczna lokalizacja usługi może ulec zmianie z wielu powodów — jedna usługa, udostępniana w ramach jednego kontraktu usługowego, może być świadczona jednocześnie z wielu rozproszonych geograficznie lokalizacji; udostępnienie usługi w innej lokalizacji może też być spowodowane awarią w podstawowej lokalizacji świadczenia tej usługi.

Fizyczny adres usługi może zostać odnaleziony ręcznie i zapisany w aplikacji w czasie jej tworzenia, ale także może być przechowywany w danych konfiguracyjnych. Przeniesienie lub wycofanie usługi sprawi jednak, że aplikacja ta przestanie poprawnie funkcjonować. Co więcej, konsumenta nie interesuje fizyczne miejsce świadczenia usług. Konsument jest zainteresowany tym, co dana usługa może mu zaoferować.

W związku z tym konsument musi mieć możliwość ustalenia fizycznego adresu świadczenia usługi w czasie pracy aplikacji (zatem należy unikać zapisywania tego adresu w kodzie aplikacji). W tym zakresie można polegać na katalogu usług. Katalog umożliwi konsumentom wyszukiwanie usług na podstawie pewnego zbioru kryteriów w czasie pracy aplikacji, wtedy, gdy zachodzi taka potrzeba.

Ze względu na brak wiedzy na temat wzajemnego położenia aplikacji i usługi przed skorzystaniem z tej usługi, dostawca usługi powinien udostępnić prosty interfejs wywołania usługi. Interfejs zbyt „drobnoziarnisty” lub „gadatliwy” może powodować kłopoty z wydajnością w przypadku, gdy aplikację i usługę będą dzieliły tysiące kilometrów. Usługi powinny przyjmować komunikaty zawierające wszystkie dane niezbędne do realizacji całej operacji, bez konieczności prowadzenia długiej i kosztownej wymiany komunikatów pomiędzy konsumentem a dostawcą, typowej dla protokołów typu RPC z rozproszonym modelem obiektowym.

Usługa katalogu usług powinna utrzymywać rejestr wszystkich usług huba e-zdrowia (dokumentacja medyczna EHR, dane rejestrowe, bezpieczeństwo, integracja itd.), pozwalając konsumentom na wyszukiwanie określonych usług — na przykład usługi rejestracji dokumentów dla określonego regionu lub lokalnej usługi zabezpieczeń oferującej funkcje uwierzytelniania. Interakcje pomiędzy konsumentem a dostawcą z wykorzystaniem katalogu usług przedstawiono na *ilustracji 14*.



{wstaw ilustrację: figure.gif}

Ilustracja 14. Interakcje pomiędzy konsumentem usługi, dostawcą usługi i katalogiem usług

Dostawca usługi rejestruje się w katalogu usług, umożliwiając konsumentom odnalezienie potrzebnych im usług. Konsument może przeszukać katalog usług na podstawie metadanych opisujących zarejestrowane usługi. Po odnalezieniu odpowiedniej usługi konsument nawiązuje połączenie z jej dostawcą i może rozpocząć korzystanie z usługi.

UDDI

UDDI to zaakceptowany przez branżę standard, definiujący strukturę katalogu usług i odpowiednie protokoły do obsługi tego katalogu.

Uwaga — UDDI to akronim od *Universal Description, Discovery and Integration* (uniwersalne opisywanie, wyszukiwanie i integrowanie usług). Niedawno opublikowana została wersja 3 tego standardu, natomiast standard WS-I Basic Profile 1.1 (stanowiący podstawy interoperacyjności pomiędzy usługami Web Services) obecnie oparty jest na wersji 2 tego standardu. Tworzeniem specyfikacji UDDI zajmuje się organizacja OASIS; specyfikacja dostępna jest pod adresem <http://www.uddi.org>.

UDDI umożliwia dostawcom rejestrowanie udostępnianych usług Web Services i publikowanie opisów usług dla konsumentów. Katalog może zatem służyć do ogłaszania dostępności usług i wyszukiwania potrzebnych usług.

Usługi UDDI oferują zwykle trzy kategorie usług: tzw. „białe strony”, „żółte strony” i „zielone strony”. Białe strony zawierają dane kontaktowe, adresy i inne informacje na temat przedsiębiorstw udostępniających usługi Web Services. Żółte strony kategoryzują usługi Web Services zgodnie ze standardową taksonomią. Zielone strony obejmują specyfikacje techniczne zarejestrowanych usług, takie jak informacje niezbędne do nawiązania połączenia czy szczegóły na temat implementacji.

Uwaga — ze względu na potencjalnie dużą złożoność relacji tworzonych w rejestrze UDDI, możliwość rozszerzania modelu danych o nowe schematy kategoryzacyjne oraz konieczność stosowania spójnych standardów nazewnicznych, przed implementacją katalogu konieczne jest zaplanowanie odpowiedniej struktury rejestru UDDI. Planowanie i projektowanie struktury zwykle odbywa się na zasadach podobnych do tych stosowanych podczas implementowania katalogu Active Directory.

Metadane usług

Każda usługa może posiadać w katalogu UDDI zestaw metadanych, który konsumenci mogą wykorzystywać w poszukiwaniu usług umożliwiających wykonanie określonej operacji lub funkcji. Te metadane to tModel wykorzystywany do wymiany informacji takich jak opis usługi (który może być zapisany w WSDL) lub wskaźników do innych metadanych związanych z usługą. tModel nie jest ograniczony do poszczególnych rejestracji usług w UDDI — może posłużyć do wyszukiwania kompatybilnych usług Web Services. Wiele usług może zawierać wskaźniki do tego samego obiektu tModel. Każda usługa może także zawierać wskaźniki do wielu różnych obiektów tModel, odpowiadających różnym implementowanym przez nią interfejsom.

Publikacja usługi

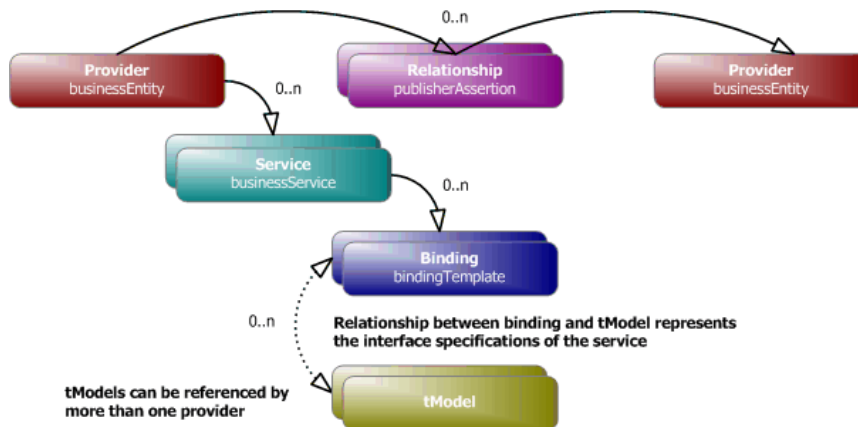
Katalog UDDI udostępnia interfejsy SOAP API do publikowania i pobierania informacji z katalogu UDDI. Dostawcy usług korzystają z publikacyjnego interfejsu API do wprowadzania do katalogu UDDI informacji kontaktowych na temat przedsiębiorstwa, nowych usług, tModeli i klasyfikacji. Wszystkie żądania wykonania operacji przesyłane są do operatora katalogu UDDI z wykorzystaniem protokołu HTTPS, co zapewnia zachowanie poufności przekazywanych informacji.

Dostawca usług, aby móc korzystać z publikacyjnego interfejsu API, musi najpierw zarejestrować się u operatora katalogu UDDI (właściciela katalogu usług) i uzyskać poświadczenia niezbędne do nawiązania połączenia z katalogiem. Na podstawie tych poświadczeń dostawca usługi może za każdym razem, gdy chce skorzystać z interfejsu publikacyjnego do wprowadzenia danych o udostępnianych przez siebie usługach, uzyskać token uwierzytelniający. Wystawienie tokenu realizowane jest z wykorzystaniem operacji `get_authToken`.

Model danych UDDI obejmuje wymienione poniżej encje. Encje te modyfikowane są przez publikacyjny interfejs API podczas wprowadzania informacji o dostawcy usług oraz oferowanych przez niego usługach.

- `businessEntity` — opis dostawcy usługi. Z tą strukturą związane są wszystkie poniższe struktury oraz dane kontaktowe, takie jak nazwa i adres dostawcy. Dostawcy mogą być organizacjami, oddziałami przedsiębiorstw itp. Wzajemne relacje pomiędzy elementami `businessEntity` reprezentowane są przez encję `publisherAssertion`;
- `businessService` — opis zbioru jednej lub więcej usług biznesowych udostępnianych przez dostawcę. Opis może zawierać kategoryzację usługi na postawie schematu i obejmować lokalizację geograficzną, typ usługi, parametry zapewnienia jakości obsługi (QoS — Quality of Service) itd.,
- `bindingTemplate` — opis sposobu połączenia z usługą Web Service reprezentującą określoną usługę biznesową. W przypadku usług Web Services udostępnianych za pośrednictwem protokołu SOAP, którego komunikaty przekazywane są za pomocą protokołu HTTP, encja ta zawiera adres URL, pod którym dostępna jest usługa,
- `tModel` — „odcisk palca” — zbiór informacji na temat specyfikacji usługi Web Service. Zwykle jest to określenie lokalizacji przechowywania zapisanej w języku WSDL specyfikacji interfejsów usługi, jednak mogą to być także inne dane opisowe.

Relacje pomiędzy tymi encjami przedstawiono na *ilustracji 15*.



Ilustracja 15. Relacje pomiędzy encjami UDDI

Wyszukiwanie usługi

Interfejs API wyszukiwania usług umożliwia konsumentowi usług odszukanie i nawiązanie połączenia z usługą Web Service w czasie wykonywania aplikacji. Kryteriami wyszukiwania mogą być dane organizacji udostępniającej usługę, atrybuty usługi lub obiekty tModel (interfejsy usług). W wyniku operacji wyszukiwania konsument otrzymuje zbiór wyników, który może następnie przejrzeć i wybrać najbardziej odpowiednią usługę.

Zawieranie kontraktu (tzn. ustalanie warunków dostarczania usług przez dostawcę) w czasie pracy aplikacji nie jest działaniem typowym — to zadanie zwykle realizowane jest na etapie opracowywania aplikacji. Programista, aby móc wykorzystać daną usługę w swojej aplikacji, musi zrozumieć jej interfejs. Nie da się tego zrobić dynamicznie. Dynamiczne łączenie z usługą w czasie wykonywania aplikacji dotyczy wyłącznie fizycznej lokalizacji usługi (adres lub łańcuch URL) oferującej znany interfejs.

API umożliwia realizację kilku podstawowych operacji związanych z wyszukiwaniem zbioru powiązanych ze sobą usług:

- `find_business` — wyszukanie informacji o jednej lub większej liczbie organizacji charakteryzowanych przez określone kategorie lub identyfikatory. Można także wyszukiwać według nazwy lub referencji do obiektu Model;
- `find_service` — operacja zwraca listę usług spełniających podane kryteria wyszukiwania, na przykład typ usługi;
- `find_tModel` — operacja zwraca struktury Model, umożliwiając konsumentowi przeszukanie katalogu pod kątem usług implementujących interfejsy odpowiadające wyszukanej strukturze tModel.

Istnieje możliwość wdrożenia prostej metody równoważenia obciążenia — przy każdym wywołaniu usługi aplikacja powinna nawiązywać połączenie z kolejną usługą z listy odnalezionych usług implementujących ten sam interfejs (tak zwane wybieranie round-robin). Co więcej, jeśli w przypadku niepowodzenia wywołania usługi Web Service aplikacja ponowi żądanie, wysyłając je do tej samej usługi lub do usługi następnej na liście, uzyskamy ochronę przed skutkami awarii pojedynczego dostawcy usług.

Replikacja

Rejestr UDDI pozwala na replikację danych z innymi rejestrami w sposób podobny do systemu DNS (Domain Name System). Do obsługi replikacji służy specjalny interfejs API, umożliwiający operatorom rejestru synchronizację rejestrów UDDI. Synchronizacja powoduje, że pomiędzy bazami danych przesyłane są informacje na temat zmian wprowadzonych do tych baz (na przykład zmienione adresy usług), jednak dostawca usług powinien aktualizować własne informacje zawsze u tego operatora, u którego zarejestrował je po raz pierwszy.

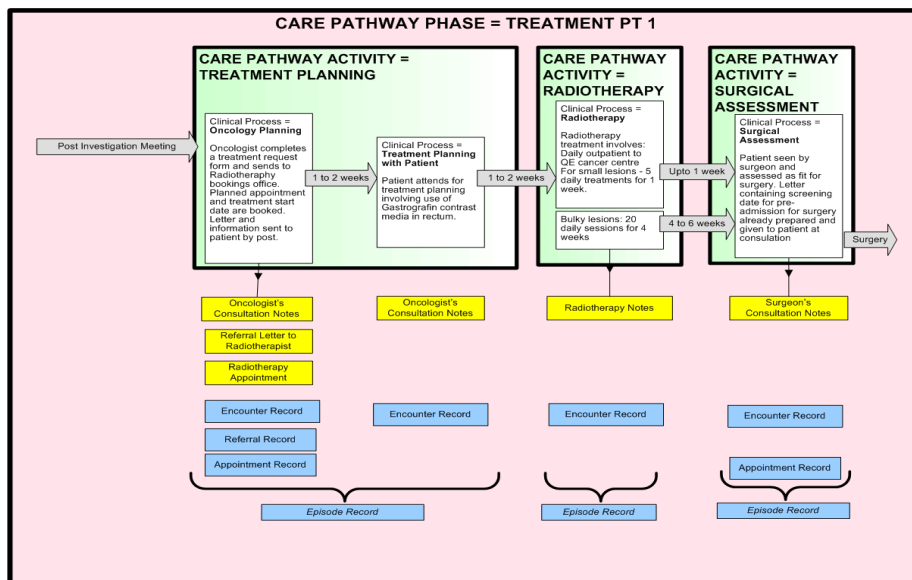
Replikacja rejestrów usług sprawia, że konsument może w lokalnym katalogu usług wyszukiwać usługi, których dostawcy zarejestrowani są w innych katalogach. Jedyną niezbędną konfiguracją to podanie lokalizacji odpowiedniego katalogu usług. Gdyby nie było replikacji, konsument, chcąc odszukać fizyczną lokalizację potrzebnej usługi, musiałby jeszcze przed rozpoczęciem poszukiwań wiedzieć, w którym katalogu zarejestrowany jest dostawca poszukiwanej usługi.

Usługi biznesowe e-zdrowia

Usługi opisane w tej sekcji dokumentu to usługi biznesowe e-zdrowia, które w rozwiązaniu e-zdrowia zapewniają bezpośrednie wsparcie dla działań z zakresu domeny medycznej. Usługi e-zdrowia i związane z nimi komponenty biznesowe są w całości zależne od specyficznych wymagań, które ma spełniać dane rozwiązanie.

Struktura biznesowa e-zdrowia, opisana w drugiej części tego opracowania, obejmuje definicje pojęć takich jak rejestr medyczny pacjenta, ścieżka leczenia, przebieg terapii czy dostawy usług medycznych. Wszystkie te pojęcia stanowią układ odniesienia i umożliwiają opisanie konkretnego rozwiązania dla opieki zdrowotnej.

Na poniższej ilustracji przedstawiono przykładowy fragment ogólnej ścieżki leczenia raka jelita grubego. Schemat pełnej ścieżki leczenia jest obszerny i znajduje się w załączniku w części 5. tego opracowania. Znajdują się tam także diagramy pomocnicze, prezentujące poszczególne fazy ścieżki leczenia. Prezentowany fragment ścieżki leczenia w przypadku raka jelita grubego ilustruje przebieg leczenia i opiera się na wskazówkach uzyskanych od specjalistów. Strukturę ścieżki można przedstawić w postaci zorientowanego poziomo schematu, którego bloki odpowiadają poszczególnym etapom procesu terapeutycznego. W całym procesie wyróżniono cztery fazy (zaznaczone kolorem różowym) — wywiad, leczenie, leczenie pooperacyjne oraz kontynuacja leczenia. Każda z podanych faz obejmuje szereg przedsięwzięć (kolor zielony), a każde z nich implikuje pewien proces kliniczny; z kolei każdy proces (kolor biały) składa się z szeregu działań.



Opisane w tej sekcji usługi e-zdrowia zapewniają funkcje niezbędne do obsługi ścieżek leczenia i przebiegów terapii, spełniające wymagania rozwiązań e-zdrowia. Usługi te zgrupowano w trzy kategorie odpowiadające określonym zbiorom wymagań biznesowych e-zdrowia, które — zebrane razem — odpowiadają pełnym wymaganiom stawianym rozwiązaniom e-zdrowia. Grupy te to usługi elektronicznego rejestru zdrowia (Electronic Health Record — EHR), usługi domeny zdrowotnej oraz usługi rejestru medycznego. Z tego opisu w oczywisty sposób wynika, że usługi e-zdrowia — w znacznie wyższym stopniu niż pozostałe usługi zawarte w opisywanej tu architekturze referencyjnej — są specyficzne i zależne od konkretnych wymagań, jakie musi spełnić określone rozwiązanie e-zdrowia.

Usługi elektronicznej dokumentacji medycznej

Usługi elektronicznej dokumentacji medycznej (Electronic Health Record — EHR) to podzbiór usług e-zdrowia odpowiedzialny za zbieranie i przechowywanie danych dotyczących pełnej dokumentacji medycznej pacjentów. Usługi te odpowiedzialne są także za tworzenie zestawień danych oraz zapewnianie dostępu do zgromadzonych informacji zarówno w formie skróconej, jak i szczegółowej. Usługi EHR są podstawowymi usługami każdego rozwiązania e-zdrowia i stanowią centralny komponent huba usług e-zdrowia. Wszystkie specyficzne dla danej domeny opieki zdrowotnej rozwiązania e-zdrowia (np. systemy laboratoryjne lub systemy informacji o lekach) wymagają dostępu do usług e-zdrowia w celu uzyskania niezbędnych podstawowych informacji o pacjencie, a także zlokalizowania źródłowego systemu opieki zdrowotnej, w którym przechowywana jest kompletna dokumentacja medyczna tego pacjenta. Usługi EHR są odpowiedzialne za przyjmowanie i przekazywanie żądań pobrania, utworzenia lub uaktualnienia danych na temat pacjenta i na temat kontaktu z pacjentem (np. wizyty). Usługi te działają jako pośrednik w dostępie do usług i repozytoriów danych specyficznych dla różnych domen opieki zdrowotnej. Same także są źródłem danych zapewniającym dostęp do skróconego rejestru zdrowia pacjenta.

Usługi EHR wspierane są przez repozytorium skróconych danych klinicznych (Summary Clinical Data Repository — SCDR), zawierające podstawowy zbiór danych na temat pacjenta oraz kontaktów z pacjentem, wystarczający do obsłużenia na poziomie podstawowym większości zapytań o informacje na temat zdrowia pacjenta. Repozytorium SCDR zawiera także wskaźniki do wszystkich rejestrów danych pacjenta i zapisów dotyczących kontaktów z pacjentem, na podstawie których opracowano przechowywane dane zbiorcze. Zaleca się, by model danych, na którym oparte jest repozytorium SCDR, był zgodny z referencyjnym modelem HL7 v3 Reference Information Model (RIM). Zgodność pozwoli zagwarantować, że udostępniane usługi EHR będą w pełni wspierały infrastrukturę komunikatów HL7 v3, co zapewni wysoki poziom zgodności pomiędzy dostępnymi usługami a SCDR.

Poniżej wymieniono usługi EHR udostępniane za pośrednictwem huba usług e-zdrowia. Usługi te powinny być oparte na komunikatach HL7 v3 przekazywanych z wykorzystaniem usług Web Services.

- usługi dostępu do EHR
Usługi dostępu do EHR pozwalają na wyszukiwanie i pobieranie z SCDR skróconych danych dotyczących pacjenta i kontaktów z pacjentem. Parametry zapytań oparte są na zunifikowanych identyfikatorach pacjentów i dostawców. Skrócone i zagregowane dane dotyczące pacjentów i kontaktów z pacjentami udostępniane są na podstawie parametrów zapytania. Zwracane przez te usługi skrócone dane pacjentów i kontaktów z pacjentami zawierają także wskazanie lokalizacji usługi źródłowej (adres usługi), z której pochodzą informacje o poszczególnych kontaktach z pacjentem.

- usługi aktualizacji EHR
Usługi aktualizacji EHR umożliwiają uczestniczącym w projekcie systemom i usługom klinicznym aktualizowanie repozytorium SCDR nowymi informacjami na temat pacjentów i kontaktów z pacjentami. Głównymi klientami usług aktualizacji EHR są usługi domeny zdrowotnej (opisane poniżej). Za każdym razem, gdy w jednej z domen zdrowotnych realizowane jest jakieś działanie, odpowiedzialna za nie usługa aktualizuje odpowiednie dane na temat kontaktu z pacjentem, korzystając z usług aktualizacji EHR.
- usługi orkiestracji procesów EHR
Usługi orkiestracji procesów EHR utrzymują i realizują inicjowane przez usługi EHR przepływy zadań (zwane też orkiestracjami) kontrolujące interakcje pomiędzy usługami magistrali usług e-zdrowia. Może to dotyczyć orkiestracji usług integracyjnych, usług bezpieczeństwa, usług domeny zdrowotnej itp.
- usługi reguł biznesowych EHR
Usługi reguł biznesowych EHR utrzymują i wykonują reguły biznesowe związane z działaniem usług EHR. Reguły biznesowe mogą realizować bardzo różne funkcje — od prostych walidacji po złożoną logikę biznesową.

Usługi domeny zdrowia

Usługi domeny zdrowia to podzbiór usług e-zdrowia odpowiedzialny za zbieranie, przechowywanie i zapewnianie dostępu do informacji związanych ze specyficznymi domenami zdrowia (na przykład dane dla systemów laboratoryjnych, systemów informacji o lekach, systemów obrazowania diagnostycznego itp.) zarówno w formie uproszczonej, jak i o pełnej szczegółowości. Usługi domeny zdrowia znajdują zastosowanie we wszystkich rozwiązaniach e-zdrowia, zapewniając obsługę działań związanych z kontaktami z pacjentem. Usługi domeny zdrowia utrzymują aktualność skróconego elektronicznego rejestru zdrowia (EHR), wykorzystując opisane wcześniej usługi EHR. Analogicznie, usługi EHR korzystają z usług domeny zdrowia w celach pobrania szczegółowych danych na temat kontaktów klinicznych z pacjentem i późniejszego ich streszczenia. Zakres implementacji i wdrożenia usług domeny zdrowia będzie różny w różnych rozwiązaniach e-zdrowia i będzie zależał od specyficznych wymagań, jakie dane rozwiązanie będzie musiało spełniać. Usługi domeny zdrowia mogą być wykorzystywane w ramach pojedynczej domeny lub w celu agregacji informacji z wielu domen zdrowia.

Poniżej wymieniono usługi domeny zdrowia wymagane dla każdej domeny zdrowia obsługiwanej w ramach rozwiązania opieki zdrowotnej (np. laboratorium, apteka itd.). Usługi te publikowane są poprzez hub usług e-zdrowia, a komunikacja z nimi powinna być oparta na komunikatach HL7 v3.

- usługi dostępu do danych domeny zdrowia
Usługi dostępu do danych domeny zdrowia obsługują wyszukiwanie i pobieranie informacji specyficznych dla danej domeny zdrowia ze źródłowych systemów tej domeny (np. z systemu laboratoryjnego lub repozytorium danych). Usługi te zwykle służą do pobierania informacji szczegółowych w celu uzupełnienia informacji skróconych uzyskanych za pośrednictwem usług EHR.
- usługi aktualizacji danych domeny zdrowia
Usługi aktualizacji danych domeny zdrowia umożliwiają systemom klinicznym i usługom aktualizowanie źródłowego repozytorium SCDR domeny świeżymi informacjami na temat pacjentów i kontaktów z pacjentami. Usługi aktualizacji danych domeny zdrowia są głównymi klientami usług aktualizacji EHR (opis powyżej) — każde działanie w zakresie danej domeny zdrowia wymaga

uaktualniania przechowywanych w EHR informacji na temat kontaktu z pacjentem. Uaktualnienie odbywa się za pośrednictwem usług aktualizacji EHR.

- usługi orkiestracji procesów domeny zdrowia
Usługi orkiestracji procesów domeny zdrowia utrzymują i realizują przepływy zadań (zwane też orkiestracjami) kontrolujące interakcje pomiędzy usługami magistrali usług e-zdrowia na potrzeby usług domeny zdrowia. Może to dotyczyć orkiestracji usług integracyjnych, usług bezpieczeństwa, usług EHR itp.
- usługi reguł biznesowych domeny zdrowia
Usługi reguł biznesowych domeny zdrowia utrzymują i wykonują reguły biznesowe związane z działaniem wszystkich usług domeny zdrowia. Reguły biznesowe mogą realizować bardzo różne funkcje — od prostych walidacji po złożoną logikę biznesową.

Usługi rejestru medycznego

Usługi rejestru medycznego to podzbiór usług e-zdrowia odpowiedzialny za utrzymywanie centralnego indeksu rejestrów zdrowotnych. Rejestry nadzorowane przez ten zbiór usług obejmują rejestry pacjentów, rejestry dostawców usług zdrowotnych czy rejestry placówek opieki medycznej. Funkcje świadczone przez te usługi to zapewnianie dostępu, indeksowanie, aktualizowanie oraz łączenie zawartości poszczególnych rejestrów.

Poniżej wymieniono usługi rejestru medycznego publikowane poprzez hub usług e-zdrowia. Usługi te powinny być oparte na komunikatach HL7 v3, przekazywanych z wykorzystaniem usług Web Services.

- usługi dostępu do rejestru medycznego
Usługi dostępu do rejestru obsługują wyszukiwanie i pobieranie informacji z rejestrów medycznych (rejestrów pacjentów, dostawców usług opieki zdrowotnej, placówek). Usługi, kompletując informacje do przekazania żądającemu, stosują algorytmy wyszukiwania bezpośredniego i łączenia probabilistycznego. W procesie tworzenia i konserwacji indeksu rejestru, usługi dostępu do rejestru medycznego zwykle korzystają z rozwiązań typu EMPI (Enterprise Master Patient Index).
- usługi aktualizacji danych w rejestrze medycznym
Usługi aktualizacji rejestru medycznego umożliwiają systemom klinicznym i usługom aktualizowanie rejestrów medycznych (pacjentów, dostawców usług opieki zdrowotnej, placówek) i wprowadzanie nowych informacji. Usługi aktualizacji z reguły wywoływane są wraz z usługami domeny zdrowotnej lub usługami EHR (na przykład gdy pacjent wywołuje określone zdarzenie w połączonym systemie klinicznym) albo w odpowiedzi na wywołania tych usług.
- usługi orkiestracji procesów rejestru medycznego
Usługi orkiestracji procesów rejestru medycznego utrzymują i realizują przepływy zadań (zwane też orkiestracjami), kontrolujące interakcje pomiędzy usługami magistrali usług e-zdrowia na potrzeby usług rejestru medycznego. Może to dotyczyć orkiestracji usług integracyjnych, usług bezpieczeństwa, usług domeny zdrowotnej itp.
- usługi reguł biznesowych rejestru medycznego
Usługi reguł biznesowych rejestru medycznego utrzymują i wykonują reguły biznesowe związane z działaniem wszystkim usług rejestru medycznego.

Reguły biznesowe mogą realizować bardzo różne funkcje — od prostych walidacji po złożoną logikę biznesową.

Usługi integracyjne

Usługi biznesowe e-zdrowia, opisane w poprzedniej sekcji dokumentu, są bezpośrednio wspierane przez bogaty zestaw usług integracyjnych, odpowiedzialnych za zapewnienie łączności pomiędzy wszystkimi składającymi się na rozwiązanie systemami opieki zdrowotnej. Usługi integracyjne zapewniają interoperacyjność łączonych systemów i usług opieki zdrowotnej, realizując niezbędne translacje protokołów sieciowych i aplikacyjnych, syntaktyczne i semantyczne transformacje komunikatów, trasowanie komunikatów, orkiestrację procesów i funkcjonalność zarządzania transakcjami. Usługi te oferowane są na bazie bezpiecznej, niezawodnej i wysoko dostępnej architektury.

Usługa rejestracji dokumentów

Opisana w tym przewodniku architektura referencyjna pozwala na elektroniczną interakcję z hubem usług e-zdrowia za pośrednictwem wielu różnych kanałów dostępu. Najważniejszym etapem interakcji z dowolną agencją opieki zdrowotnej jest etap przedłożenia dokumentu. Zamawianie testów laboratoryjnych, przeglądanie skróconego rejestru zdrowia pacjenta czy aktualizacja adresu pacjenta — wszystkie te operacje wymagają przedłożenia dokumentu określonego rodzaju (czasem wraz z załącznikami takimi jak zdjęcia).

Rola usługi rejestracji dokumentów

Usługa rejestracji dokumentów w hubie usług e-zdrowia jest odpowiedzialna za przyjmowanie dokumentów i przetwarzanie ich w imieniu usługi rejestracji dokumentów kanału lub innej równorzędnej usługi rejestracji dokumentów, która zainicjowała dostarczenie dokumentu.

Koperta dokumentu to komunikat, który zawiera nie tylko sam dokument, ale także metadane opisujące ten dokument, takie jak tożsamość nadawcy, aplikacja użyta do utworzenia dokumentu, data przedłożenia dokumentu oraz typ dokumentu dołączonego do komunikatu. Metadane komunikatu mogą być przydatne dla usług, które muszą analizować pewne ogólne cechy zawartości komunikatu (dokumentu) w celu podjęcia decyzji na temat dalszego przetwarzania lub dalszej drogi przesyłu komunikatu. Przykładem podstawowych metadanych, jakie mogą być przydatne podczas podejmowania decyzji o przekazaniu komunikatu do właściwej agencji, mogą być agencja docelowa i typ dokumentu.

Usługa rejestracji dokumentów jest także odpowiedzialna za sprawdzanie bezpieczeństwa komunikatu i ochronę przed manipulowaniem jego zawartością. Oprócz sprawdzenia poprawności komunikatu, obowiązkiem usługi może także być odszyfrowanie zawartości komunikatu w celu przekazania jej usłudze agencji, która nie ma dostępu do technologii umożliwiającej poznanie treści komunikatu.

Po sprawdzeniu poprawności komunikatu, usługa rejestracji dokumentu powinna zweryfikować autentyczność jego nadawcy poprzez sprawdzenie, czy dołączony do komunikatu token bezpieczeństwa jest poprawny. Następnie musi przeprowadzić autoryzację dokumentu w oparciu o wymagania docelowej usługi zdrowotnej i porównanie poziomu uwierzytelnienia nadawcy z minimalnym poziomem określonym dla tej usługi. Innymi słowy, usługa opieki zdrowotnej może wymagać weryfikacji tożsamości nadawcy w oparciu o nazwę użytkownika i odpowiednio silne hasło. Jeśli uwierzytelnienie odbędzie się za pośrednictwem nazwy użytkownika i słabego hasła, usługa może odrzucić komunikat. Poziom uwierzytelnienia powinien być właściwością komunikatu (zabezpieczoną podpisem cyfrowym przed ewentualnymi nadużyciami).

Po zweryfikowaniu nadawcy i potwierdzeniu odpowiedniego poziomu uwierzytelnienia dla docelowej usługi zdrowotnej, może nastąpić ogólna autoryzacja operacji. Przez operację

rozumiemy tu przedłożenie dokumentu określonego typu w określonej usłudze opieki zdrowotnej albo przekazanie dokumentu do innej, równorzędnej usługi rejestracji dokumentów. Przed takim przekazaniem może jednak nastąpić autoryzacja wstępna. Autoryzacja polega na sprawdzeniu zestawu stwierdzeń w oparciu o usługę autoryzacji. Jako stwierdzenia można przyjąć prawo nadawcy do przedkładania dokumentów typu X, jego przynależność do grupy Y lub dowolną kombinację takich stwierdzeń.

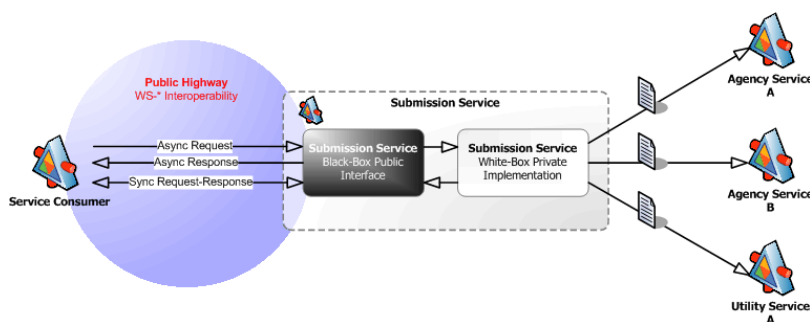
Przekazanie dokumentu do usługi docelowej następuje po pozytywnym przejściu komunikatu przez wszystkie testy bezpieczeństwa. Jeśli dokument przekazywany jest do równorzędnej usługi rejestracji dokumentów, testy bezpieczeństwa mogą nie być przeprowadzane — zależy to tylko od wymagań stawianych nadawcy. Wymagania mogą być określone w taki sposób, że komunikat zostanie sprawdzony tylko po przesłaniu go do właściwego odbiorcy lub przez dowolną usługę pośredniczącą w przekazywaniu tego dokumentu.

Podstawowa architektura usługi rejestracji dokumentów

Podstawową architekturę usługi rejestracji dokumentów można podzielić na dwa obszary:

- stronę publiczną, wykorzystywaną przez konsumentów przedkładających dokumenty,
- stronę prywatną, wykorzystywaną przez dostawcę usługi (centralną jednostkę opieki zdrowotnej, władzę, lokalny organ zarządzający opieką zdrowotną lub pojedynczą agencję udostępniającą usługę rejestracji dokumentów) i umożliwiającą integrację usługi z systemami informatycznymi agencji.

Dwa obszary podstawowej architektury usługi rejestracji dokumentów przedstawiono na ilustracji 16.



Ilustracja 16. Podstawowa architektura usługi rejestracji dokumentów

Interfejs publiczny

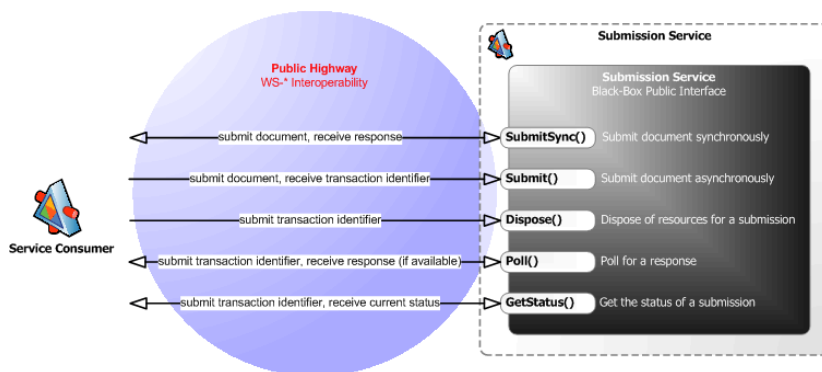
Publiczny interfejs usługi rejestracji dokumentów wyznacza sposób interakcji konsumentów z tą usługą, określa obsługiwane operacje, protokoły i formaty komunikatów oraz inne nakładane przez usługę na konsumenta niefunkcjonalne wymagania, takie jak wymagany poziom szyfrowania i podpisywania zawartości. Określa sposób, w jaki usługa ta jest widoczna dla konsumenta.

Zewnętrzny konsument usługi, którym może być portal, aplikacja niezależnego producenta, inna usługa lub partner, komunikuje się z usługą rejestracji dokumentów za pośrednictwem interfejsu publicznego. Dostawca usługi udostępnia interfejs, który

umożliwia konsumentom przedkładanie dokumentów zarówno w sposób synchroniczny, jak i asynchroniczny. Interfejs obsługuje także operacje pomocnicze, takie jak sprawdzenie stanu dokumentu, a w przypadku komunikacji asynchronicznej — pobranie i usunięcie odpowiedzi itp.

W większości przypadków interfejs publiczny usługi rejestracji dokumentów będzie opakowany zestawem interfejsów specyficznych dla poszczególnych dostawców opieki zdrowotnej, publikowanych za pośrednictwem usług katalogu usług.

Ogólną strukturę publicznego interfejsu usługi rejestracji dokumentów przedstawiono na ilustracji 17.



Ilustracja 17. Wysokopoziomowe usługi świadczone przez interfejs publiczny usługi rejestracji dokumentów

Komunikacja asynchroniczna

Usługa rejestracji, aby zapewnić wsparcie dla jak największej liczby aplikacji klienckich, implementuje podstawowe mechanizmy komunikacyjne (synchroniczne i asynchroniczne). Gdy konsument korzysta z interfejsu synchronicznego, usługa musi przyjąć dokument, przetworzyć go i zwrócić odpowiedź w ramach tego samego połączenia. Oznacza to dłuższe blokowanie zasobów niż w przypadku połączeń asynchronicznych oraz ograniczenie skalowalności usługi.

Preferowanym interfejsem, wykorzystywanym do przedkładania dokumentów, jest interfejs asynchroniczny, który zapewnia lepszą skalowalność — konsument nie jest blokowany w oczekiwaniu na odpowiedź. Co więcej, technologia zastosowana do implementacji usługi rejestracji dokumentów nie musi gwarantować przetworzenia dokumentu i zwrócenia odpowiedzi w najkrótszym możliwym czasie.

Konsument podaje usłudze adres, na który ta ma przekazać swoją odpowiedź po przetworzeniu tego dokumentu, niezależnie od sesji, w której zostało przekazane żądanie. Jeśli konsument nie może podać takiego adresu, może co jakiś czas sprawdzać, czy odpowiedź jest już gotowa i czy można ją pobrać (tzw. polling). Z tego względu niezbędne jest, by usługa przechowywała informacje o stanie wszystkich odpowiedzi otrzymanych asynchronicznie z usług agencji, usług pomocniczych czy równorzędnych usług rejestracji dokumentów. Rodzi się także pytanie — po jakim okresie można usunąć odpowiedzi nieodebrane przez konsumentów?

Najprostszym wyjściem jest wprowadzenie w usłudze rejestracji dokumentów funkcji „oczyszczania” — konsument po zakończeniu przetwarzania odpowiedzi może uprzątnąć (zwołać) zajmowane zasoby. Poza tym usługa rejestracji dokumentów może sama zwalniać zasoby po odebraniu odpowiedzi przez konsumenta, a w przypadku odpowiedzi nieodebranych — po ustalonym okresie zwłoki. W istocie jest to implementacja mechanizmu Garbage Collector dla komunikatów odpowiedzi.

Komunikacja synchroniczna

W niektórych przypadkach klient może nie mieć możliwości obsłużenia asynchronicznego mechanizmu komunikacji, wymagającego podania adresu dla komunikatów z odpowiedzią. W takiej sytuacji klient może albo asynchronicznie sprawdzać co jakiś czas stan przetwarzania (polling), albo z innych względów odwołać się do usługi rejestracji dokumentów w sposób synchroniczny — na przykład gdy musi natychmiast przekazać odpowiedź użytkownikowi końcowemu.

Protokoły takie jak HTTP są protokołami żądania-odpowiedzi: przeglądarka internetowa wysyła żądanie do serwera, serwer generuje stronę HTML i w tym samym połączeniu zwraca ją do przeglądarki. W przypadku protokołu synchronicznego, odpowiedź jest faktyczną odpowiedzią usługi zdrowotnej, natomiast w przypadku komunikacji asynchronicznej może to być jedynie potwierdzenie przyjęcia żądania.

Ze względu na to, że odpowiedź dla konsumenta zależy od odpowiedzi uzyskanych z innych usług (np. usług opieki zdrowotnej lub usług narzędziowych), realizacja synchronicznego schematu komunikacji na poziomie usługi rejestracji dokumentów (a nie na poziomie usługi opieki zdrowotnej) może być niezwykle trudna. Możliwość wygenerowania odpowiedzi w trybie synchronicznym w całości zależy od tego, czy wszystkie pozostałe usługi biorące udział w procesie obsługują komunikację synchroniczną. Oznacza to, że w czasie projektowania aplikacji konsumenta należy sprawdzić, czy wykorzystywane usługi zdrowotne i usługi narzędziowe obsługują interfejsy synchroniczne i asynchroniczne.

Preferowanym sposobem komunikacji jest komunikacja asynchroniczna, jednak przez to interfejs publiczny — musząc obsługiwać sprawdzanie stanu żądania i operacje oczyszczania rejestru stanu żądań — staje się bardziej skomplikowany. Natomiast stosowanie wyłącznie synchronicznej metody komunikacji (o ile wykorzystywane usługi opieki zdrowotnej na to pozwalają) może spowodować dodatkowe problemy ze skalowalnością, które nie wystąpiłyby w przypadku rejestracji dokumentów z użyciem metody asynchronicznej. Warto zatem stosować metodę synchroniczną tylko wtedy, gdy jest to konieczne — na przykład w usłudze dostępu do skróconego rejestru zdrowia pacjenta, która pobiera dane z lokalnego magazynu danych i generuje odpowiedź w trybie natychmiastowym.

Usługi i protokoły komunikacyjne, wykorzystywane do synchronicznej i asynchronicznej wymiany komunikatów, szczegółowo opisano w sekcji *Usługi komunikacyjne* dalej w tym dokumencie.

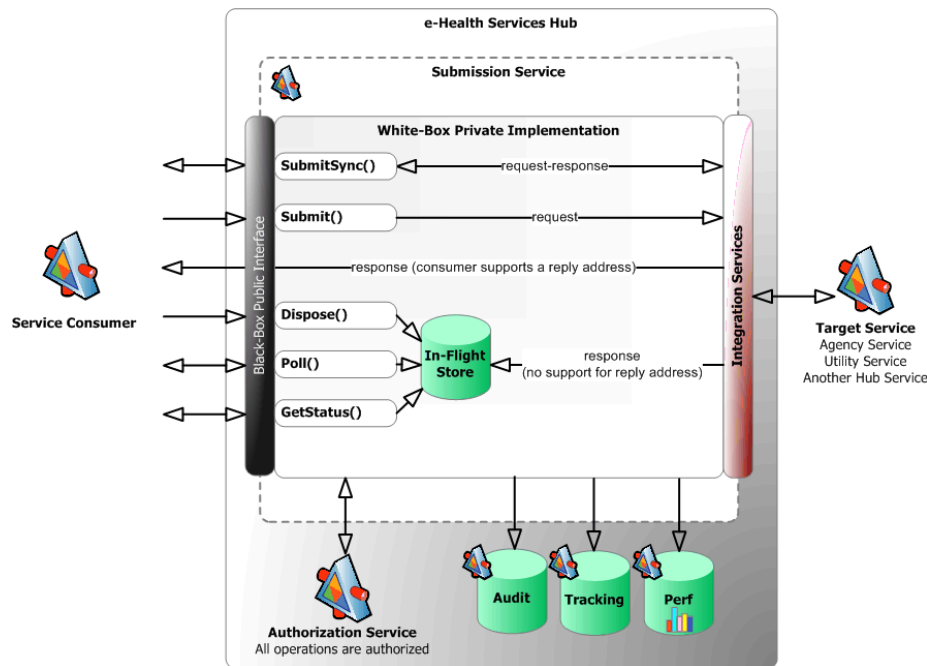
Implementacja prywatna

Zadaniem interfejsu publicznego usługi rejestracji dokumentów jest zapewnienie standardowego sposobu interakcji z konsumentami. Natomiast zadaniem implementacji prywatnej jest faktyczne przetwarzanie dokumentów, zapewnienie integracji z usługami agencji i usługami pomocniczymi, generowanie odpowiedzi oraz zagwarantowanie, że usługa będzie dostarczała innym usługom prawidłowe informacje.

Usługa rejestracji dokumentów pełni wiele różnych funkcji wymagających odpowiedniej implementacji. Niektóre z nich to:

- odbieranie i przetwarzanie żądań,
- zwracanie odpowiedzi — synchronicznie lub asynchronicznie, w zależności od wymagań agencji opieki zdrowotnej lub usługi pomocniczej,
- zapisywanie żądań, których dostarczenie do docelowej agencji lub usługi pomocniczej jest w danej chwili niemożliwe,
- zapisywanie odpowiedzi, które nie mogą być dostarczone w sposób asynchroniczny, lub gdy konsument sam cyklicznie sprawdza dostępność odpowiedzi (polling),
- autoryzacja żądań,
- sprawdzanie dostępności odpowiedzi (polling),
- oczyszczanie rejestru odpowiedzi,
- inspekcja żądań, odpowiedzi oraz operacje związane z bezpieczeństwem — na przykład autoryzacja,
- zapewnienie instrumentacji w postaci informacji o błędach, ostrzeżeń, podstawowych informacji operacyjnych, liczników wydajności umożliwiających sprawdzenie stanu usługi oraz możliwości włączania i wyłączenia dodatkowych funkcji monitorowania, ułatwiających diagnozowanie ewentualnych problemów,
- integracja z usługami agencji i usługami pomocniczymi,
- przekazywanie dokumentów do usług agencji, usług pomocniczych lub równorzędnych usług rejestracji,
- wsparcie protokołów aplikacyjnych wyższego poziomu poprzez orkiestrację procesów biznesowych.

Funkcje te omówiono bliżej w tej i w następnych sekcjach dokumentu. Na *ilustracji 18* przedstawiono zarys implementacji usługi rejestracji dokumentów.



Ilustracja 18. Usługi wysokiego poziomu świadczone przez prywatną implementację usługi rejestracji dokumentów

Format komunikatów

uzupełnić o HL7

Komunikaty przesyłane są w formacie XML, który de facto stał się standardem komunikacji pomiędzy aplikacjami (konsumentami usług) a usługami Web Services (dostawcami usług). XML pozwala na zdefiniowanie struktury, która nadaje znaczenie „suchym” danym.

Uwaga — nadzór nad specyfikacją XML utrzymuje organizacja World Wide Web Consortium (W3C). Obecnie obowiązującą wersją specyfikacji jest wersja 1.1, specyfikacja ta posiada status rekomendacji W3C. Witryna organizacji W3C znajduje się pod adresem <http://www.w3.org/>, a specyfikację XML można znaleźć pod adresem <http://www.w3.org/XML/>.

Swoją popularność standard XML zawdzięcza głównie łatwości użycia oraz faktowi, że jest on oparty na tekście, dzięki czemu komunikaty oparte na XML mogą być odczytywane nawet przez najprostsze systemy. Funkcje obsługi XML są powszechnie dostępne w wielu systemach operacyjnych, XML jest też obsługiwany przez bazy danych jako natywny typ danych.

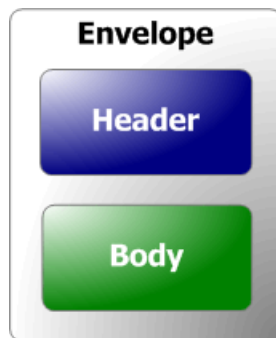
W związku z powyższym, stosowanie XML jako podstawowej struktury komunikatu w strukturze mającej zapewnić interoperacyjność pomiędzy różnymi systemami i aplikacjami w heterogenicznym środowisku opieki zdrowotnej wydaje się być rozwiązaniem jak najbardziej właściwym.

Koperty, nagłówki i zawartości komunikatów

Zastosowanie „kopertowego” formatu komunikatów pozwala na przechowywanie metadanych komunikatu wraz z treścią tego komunikatu. Format obejmuje nagłówek zawierający metadane oraz „ciało” komunikatu zawierające jego treść. Przykładem wykorzystywanego obecnie formatu kopertowego jest SOAP — protokół oparty XML (i wykorzystywany przez wielu producentów oprogramowania opartego na Web Services), służący do komunikacji pomiędzy aplikacjami i pozwalający na uzupełnienie żądań i odpowiedzi odpowiednimi metadanymi. Usługa rejestracji stosuje format SOAP do przesyłania żądań i odpowiedzi do innych usług. Ponieważ protokół SOAP jest obsługiwany praktycznie przez wszystkie usługi opieki zdrowotnej — niezależnie od platformy sprzętowej i systemu operacyjnego — zastosowanie tego protokołu w usłudze rejestracji komunikatów zapewnia wysoką interoperacyjność.

Uwaga — nadzór nad specyfikacją SOAP sprawuje organizacja W3C. Wersja 1.2 specyfikacji, posiadająca status rekomendacji W3C, dostępna jest pod adresem <http://www.w3.org/2000/xml/Group/>.

Na *ilustracji 19*. przedstawiono przykładową strukturę dokumentu o formacie kopertowym. Koperta to struktura zawierająca w sobie zarówno nagłówek, jak i treść dokumentu.

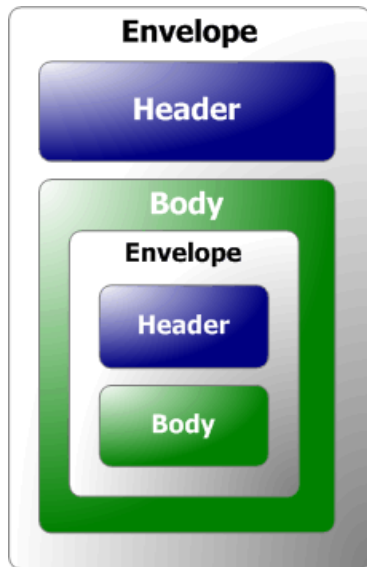


Ilustracja 19. Przykład dokumentu o formacie kopertowym

Format ten pozwala także na zagnieżdżanie dokumentów. Zaawansowany format koperty, wykorzystywany w systemach opieki zdrowotnej, może na przykład pozwalać na zagnieżdżenie treści dokumentu SOAP wewnątrz komunikatu SOAP. Pozwala to na budowanie wielopoziomowej struktury metadanych komunikatu — metadane związane z dokumentem (metadane biznesowe) mogą być oddzielone od metadanych związanych z komunikatem SOAP (metadane techniczne, dotyczące raczej kwestii bezpieczeństwa i wiarygodności).

Uwaga — przykładem kopertowego formatu wykorzystywanego w służbie zdrowia w Wielkiej Brytanii jest schemat GovTalk, wchodzący w skład biblioteki schematów dostępnej pod adresem <http://www.govtalk.gov.uk/>.

Na *ilustracji 20*. przedstawiono zagnieżdżony komunikat o formacie kopertowym — treść komunikatu pierwszego poziomu zawiera inną kopertę. Zagnieżdżanie może być wielopoziomowe — w razie potrzeby zagnieżdżone koperty mogą zawierać kolejne koperty.



Ilustracja 20. Przykład dokumentu zawierającego zagnieżdżoną kopertę

Załączniki komunikatów

Czasami konieczne jest dołączenie do dokumentu jakichś dodatkowych informacji. Mogą to być na przykład fotografie, kopia prawa jazdy, zeskanowany tradycyjny, papierowy list czy inne materiały cyfrowe.

Osadzanie załączników w dokumentach XML jest już od jakiegoś czasu możliwe technicznie dzięki różnym mechanizmom i różnym specyfikacjom, takim jak *SOAP with Attachments*. Najnowsza specyfikacja, która zastępuje wszystkie poprzednie, jest oparta na dwóch specyfikacjach organizacji W3C: XML-binary Optimized Packaging (XOP) i SOAP Message Transmission Optimization Mechanism (MTOM).

Uwaga — specyfikacja XOP znajduje się pod adresem <http://www.w3.org/TR/xop10/>, a specyfikacja MTOM pod adresem <http://www.w3.org/TR/soap12-mtom/>.

XOP pozwala na pakowanie danych binarnych w wiadomość sformatowaną zgodnie z MIME za pomocą kodowania Base64. Schemat dokumentu definiuje dane Base64 jako typ danych `xs:base64Binary` — wspieraną leksykalną formę kanoniczną ujętą w specyfikacji XML InfoSet (abstrakcyjny model danych dla serializowanych dokumentów XML).

Uwaga — znaki Base64 muszą być zapisane w postaci kanonicznej — bez dodatkowych znaków niedrukowanych na początku, wewnątrz lub na końcu zakodowanego dokumentu. Jeśli warunek ten nie zostanie dotrzymany, usługa Web Service, która odbierze komunikat, nie będzie mogła odkodować zawartości pól Base64.

Format binarny prawdopodobnie jest bardziej optymalny niż dokument zakodowany w Base64, który przed odczytaniem musi jeszcze zostać odkodowany. Dane zapisane binarnie powinny także mieć mniejszą objętość. Zamiast danych XML InfoSet, zakodowanych w Base64, element XOP zawiera łącznie do zoptymalizowanej binarnej treści komunikatu MIME. Otrzymany w ten sposób pakiet (po serializacji obiektu InfoSet) nazywany jest pakietem XOP. Zawiera on dokument XML (dokument XOP) oraz przetworzoną treść komunikatu w postaci pakietu MIME Multipart/Related.

MTOM to specyfikacja precyzująca sposoby optymalizacji transmisji komunikatów SOAP (a w szczególności koperty). W zakresie implementacji optymalizacji specyfikacja ta oparta jest na specyfikacji XOP. Usługa Web Service w momencie otrzymania komunikatu SOAP powinna odtworzyć oryginalny komunikat poprzez odkodowanie zoptymalizowanej zawartości binarnej z powrotem do reprezentacji Base64, jednak procedura ta nie jest obowiązkowa.

Bezpieczeństwo komunikatów

Podstawowa komunikacja z usługami Web Services polega na wysłaniu i odbieraniu komunikatów. Najczęściej stosowanym formatem komunikatów jest SOAP. Przesyłanie dokumentów jako treści komunikatów SOAP jest dość problematyczne, ponieważ nie ma możliwości zabezpieczenia poszczególnych komunikatów. Specyfikacja SOAP nie obejmuje żadnych mechanizmów zabezpieczeń, a jedynie podstawową strukturę komunikatu SOAP (koperta, nagłówki i treść).

Brak odpowiednich standardów i specyfikacji we wczesnych stadiach rozwoju usług Web Services i — w szczególności — protokołu SOAP powodował, że do zapewnienia bezpieczeństwa komunikacji stosowano inne mechanizmy. Stosowane mechanizmy zależały od środowiska, w którym działało rozwiązanie. Najczęściej stosowano protokoły zapewniające bezpieczeństwo na poziomie transportowym — SSL, TLS oraz IPsec. Taki poziom zabezpieczeń często nie jest jednak wystarczający.

Dlaczego zabezpieczenie tylko warstwy transportowej może nie być wystarczające?

Zabezpieczenia wprowadzone w warstwie transportowej chronią poufność informacji jedynie podczas przesyłania ich pomiędzy nadawcą a odbiorcą. Poza kanałem komunikacyjnym komunikaty są niezabezpieczone, mają postać jawnego tekstu. W takim przypadku bezpieczeństwo komunikatu zależy od zapewnianych przez platformę mechanizmów zachowania poufności i integralności komunikatów.

Z tego względu w momencie otrzymania komunikatu przez adresata nie można zagwarantować, że integralność tego komunikatu nie została naruszona i nikt nie poznał jego treści. Co gorsza, jeśli komunikat przesyłany jest z wykorzystaniem jednego lub kilku węzłów pośrednich, podczas przechodzenia przez te węzły komunikat pozostaje niezabezpieczony.

Nawet w granicach pojedynczego systemu, zabezpieczenia warstwy transportowej często zapewniane są przez specjalistyczny sprzęt i oprogramowanie (ze względu na wydajność i efektywność działania), zainstalowane na granicy systemu. Bezpieczne sesje kończą się właśnie w tym miejscu. Nawet jeśli do celów nawiązania połączenia zastosowano odpowiedni mechanizm uwierzytelnienia wzajemnego, podczas przetwarzania komunikatu przez system informacje o nadawcy tego komunikatu mogą zostać utracone.

Przyszłość to zabezpieczenia na poziomie komunikatu

Problemy związane z zapewnieniem bezpieczeństwa transmisji na poziomie transportowym można rozwiązać, stosując zabezpieczenia na poziomie pojedynczych komunikatów. Istnieje kilka specyfikacji pozwalających na umieszczenie w nagłówku SOAP informacji dotyczących bezpieczeństwa komunikatu. Najlepszą z tych specyfikacji jest WS-Security.

Specyfikacja WS-Security zawiera definicje zestawu pól nagłówkowych SOAP, umożliwiających zachowanie poufności i integralności komunikatów w trakcie przesyłania ich pomiędzy nadawcą a odbiorcą — niezależnie od rodzajów sieci, przez jakie są

przesyłane, liczby węzłów pośrednich czy typów systemów wykorzystywanych do składowania komunikatów przed wysłaniem ich w dalszą drogę.

Uwaga — pieczę nad standardem WS-Security piastuje organizacja OASIS, patrz strona http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss.

Poufność

Poufność danych chroniona jest za pomocą mechanizmów szyfrowania — jawna treść komunikatu zostaje z użyciem standardowego algorytmu szyfrowania (takiego jak potrójny DES, AES czy RSA) zamieniona na niemożliwe do odcyfrowania dane binarne. Rozróżnia się dwie metody szyfrowania — symetryczną i asymetryczną. Obie oparte są na zaawansowanych algorytmach matematycznych, a do zaszyfrowania i odszyfrowania danych niezbędne jest posiadania odpowiedniego klucza szyfrującego.

W przypadku szyfrowania symetrycznego zarówno nadawca, jak i odbiorca komunikatu dysponują tym samym kluczem szyfrującym (zwanym też wspólnym sekretem). Do stosowania szyfrowania symetrycznego niezbędne jest istnienie jakiegoś mechanizmu wymiany kluczy szyfrujących, gwarantującego, że obie strony przed rozpoczęciem zabezpieczonej transmisji dysponują identycznymi kluczami szyfrującymi.

W przypadku szyfrowania asymetrycznego każda strona posiada dwa klucze — prywatny i publiczny. Klucz publiczny służy do szyfrowania wiadomości nadawanych i odbieranych od jego właściciela; właściciel może udostępnić ten klucz wszystkim osobom, z którymi chce się komunikować. Klucz prywatny (pozostający w wyłącznej dyspozycji jego właściciela) służy do odszyfrowywania komunikatów.

Treść zaszyfrowana z użyciem klucza publicznego może zostać odszyfrowana wyłącznie za pomocą klucza prywatnego, a treść zaszyfrowana z użyciem klucza prywatnego może zostać odszyfrowana wyłącznie za pomocą klucza publicznego. Tak długo, jak długo właściciel klucza prywatnego potrafi uchronić go przed niepożądanym dostępem, szyfrowanie asymetryczne jest wygodną i pewną metodą ochrony poufności komunikatów — klucz publiczny można udostępniać dowolnym osobom.

Skoro dystrybucja kluczy w przypadku szyfrowania asymetrycznego jest tak łatwa, dlaczego ta metoda szyfrowania nie jest oczywistym wyborem za każdym razem, gdy trzeba zaszyfrować jakieś dane? Jest tak, ponieważ algorytm matematyczny oraz rozmiar stosowanych kluczy (minimalny rozmiar zapewniający ochronę przed atakami metodą przeglądu zupełnego) sprawiają, że stosowanie tej metody wymaga większej mocy obliczeniowej niż w przypadku szyfrowania symetrycznego. Dlatego tam, gdzie jest to możliwe, należy stosować szyfrowanie symetryczne, na przykład podczas wymiany komunikatów pomiędzy usługami Web Services. Szyfrowanie asymetryczne jest przydatne na etapie negocjacji „współdzielonego sekretu” albo klucza sesji, który zostanie użyty do symetrycznego szyfrowania transmisji. Przykładem protokołu opartego na takim mechanizmie jest HTTPS — HTTP over Secure Sockets Layer (SSL).

Zastosowanie standardu WS-Security pozwala na wprowadzenie szyfrowania na dowolnym poziomie. Można szyfrować całą treść komunikatu albo jedynie jej części. Można zaszyfrować nawet pola nagłówek komunikatu. W zakresie opisu konwencji stosowanych do szyfrowania poszczególnych części komunikatu SOAP, standard WS-Security opiera się na specyfikacji XML Encryption.

Integralność

O ile treść komunikatu nie musi być poufna i tajna i może nie wymagać szyfrowania, często występuje konieczność zagwarantowania, że podczas transmisji komunikatu nie doszło do żadnej manipulacji i jego integralność nie została naruszona. Mechanizm taki jest szczególnie przydatny w przypadku transmisji listu lub formularza aplikacyjnego — możliwa jest wtedy weryfikacja tożsamości nadawcy dokumentu. Mechanizm ten

nazywany jest podpisaniem dokumentu, jego wynikiem jest dołączenie do dokumentu podpisu elektronicznego.

Uwaga — więcej informacji na temat technik i funkcji podpisu elektronicznego można znaleźć w temacie *Podpisy elektroniczne i certyfikaty* w sekcji *Building Blocks* w tym przewodniku.

Comment [JB4]: brak sekcji

Podpisanie dokumentu wiąże z użyciem algorytmu funkcji skrótu (na przykład SHA-1) do obliczenia małej (i o stałym rozmiarze) wartości binarnej nazywanej wartością hasz lub skrótem dokumentu. Wartości skrótu są unikalne; wartości dwóch nawet niewiele różniących się od siebie dokumentów także są różne od siebie. Wartość skrótu dokumentu zaszyfrowana prywatnym kluczem nadawcy stanowi podpis elektroniczny tego dokumentu. Odbiorca dokumentu może odszyfrować podpis za pomocą klucza publicznego nadawcy, ponownie obliczyć wartość skrótu dokumentu za pomocą tego samego algorytmu funkcji skrótu i porównać wartość odszyfrowaną z wartością obliczoną. Jeśli wartości te różnią się od siebie, treść dokumentu uległa zmianie i komunikat powinien zostać odrzucony. Jeśli wartości są identyczne, adresat ma gwarancję, że komunikat dotarł do niego w stanie nienaruszonym.

W przypadku obliczania wartości skrótu dokumentu XML występuje dodatkowy problem — dwa dokumenty XML mogą być identyczne syntaktycznie, ale różnić się ze względu na dodatkowe znaki niedrukowane (odstępny, znaki końca linii itp.). Znaki te mają jedynie wpływ na formatowanie znaczników XML, ale nie zmieniają treści dokumentu. Zatem przed obliczeniem wartości skrótu dokumentu zachodzi konieczność doprowadzenia go do postaci kanonicznej za pomocą odpowiedniego algorytmu usuwającego niedrukowane znaki zgodnie ze ustalonymi zasadami.

Uwaga — organizacja W3C opracowała specyfikację o nazwie Canonical XML (czasem oznaczaną także symbolem C14N jako skrót słowa canonicalization), która precyzuje reguły transformowania dokumentów XML do postaci kanonicznej w celu obliczenia wartości skrótu dla podpisu cyfrowego. Specyfikacja w wersji 1.0 ma status rekomendacji W3C i dostępna jest pod adresem <http://www.w3.org/TR/xml-c14n>.

Standard WS-Security pozwala na cyfrowe podpisywanie różnych części komunikatu SOAP — tak samo, jak ma to miejsce w przypadku szyfrowania. W zakresie tworzenia podpisów cyfrowych i dołączania ich do komunikatów SOAP, standard WS-Security opiera się na specyfikacji XML Signature.

Uwaga — specyfikacja XML Signature ma status rekomendacji W3C i jest dostępna pod adresem <http://www.w3.org/TR/xmlsig-core/>.

Autoryzacja

Usługa rejestracji dokumentów powinna poprawnie obsługiwać przesłane w nagłówkach komunikatów SOAP tokeny zabezpieczeń, pozwalające adresatowi zidentyfikować nadawcę dokumentu. Nadawca przed wysłaniem dokumentu powinien uwierzytelnić się w swojej domenie zaufania, dzięki czemu — pod warunkiem, że pomiędzy domeną, która wystawiła token, a domeną, w której znajduje się usługa rejestracji dokumentów, istnieje relacja zaufania — usługa zaakceptuje uwierzytelnienie nadawcy. Możliwość manipulowania zawartością tokenu jest wykluczona przez podpis cyfrowy tokenu. Istnieje także możliwość sprawdzenia integralności komunikatu.

Po zweryfikowaniu tokena bezpieczeństwa, usługa rejestracji dokumentów musi sprawdzić, czy nadawca posiada autoryzację do przesłania dokumentu do usługi agencji lub usługi pomocniczej. Może to zrobić poprzez sprawdzenie rejestracji nadawcy w tych usługach. Poza tym sprawdzany jest także poziom uwierzytelnienia nadawcy w jego lokalnej domenie zaufania w odniesieniu do minimalnego poziomu akceptowanego przez usługę agencji lub usługę pomocniczą. Dowolna negatywna odpowiedź usługi uwierzytelniania powoduje, że usługa rejestracji dokumentów zwraca komunikat błędu

SOAP z informacją, że nadawca nie jest autoryzowany do przesłania dokumentu do tej usługi.

Walidacja komunikatu

Po zweryfikowaniu nadawcy i jego autoryzacji do przesłania dokumentu i komunikatu i sprawdzeniu nagłówek komunikatu może być konieczne walidowanie treści komunikatu. Walidacja treści pozwala przed dostarczeniem dokumentu do docelowej usługi agencji lub usługi pomocniczej upewnić się, że struktura i zawartość dokumentu mają właściwą postać. Można także przeprowadzić walidację dokumentów, które mają zostać przekazane do równorzędnej usługi rejestracji dokumentów. Podejście to można stosować na przykład wtedy, gdy usługa równorzędna nie ma wystarczających zasobów do przeprowadzenia takiej walidacji.

Jeśli walidacja dokumentu nie powiedzie się, usługa rejestracji dokumentów powinna zwrócić komunikat błędu SOAP. Zaletą wykonywania podstawowej walidacji przez usługę rejestracji dokumentów jest fakt, że usługi docelowe otrzymują wyłącznie dokumenty zgodne z ustalonym schematem.

Zwykle do walidacji wykorzystywany jest schemat zdefiniowany za pomocą XML Schema (XSD). XSD pozwala na ściśle zdefiniowanie struktury dokumentu XML, włącznie z ograniczeniem liczby powtórzeń poszczególnych elementów, obowiązkiem istnienia pewnych elementów itd. XSD pozwala także na sprawdzanie typów danych poszczególnych elementów i atrybutów, a także sprawdzanie, czy użyte wartości danych należą do dozwolonych zakresów wartości (lub zbiorów wartości typów wyliczeniowych) oraz na porównywanie danych ze złożonymi wzorcami.

Magazyn komunikatów

Usługa rejestracji dokumentów powinna zwrócić nadawcy informację o poprawnym przyjęciu komunikatu i zagwarantować, że przesłany komunikat nie zostanie zagubiony lub zignorowany. Aby dotrzymać tych warunków, kopia dokumentu na czas jego przetwarzania zostaje zapisana w tymczasowym magazynie danych. Jeśli usługa rejestracji dokumentów nie będzie mogła dostarczyć dokumentu do usługi agencji, usługi pomocniczej lub równorzędnej usługi rejestracji dokumentów, komunikat będzie przechowywany tak długo, aż jego dostarczenie będzie możliwe. Usługa rejestracji dokumentów może na przykład okresowo ponawiać próby dostarczenia dokumentu zgodnie z określonym algorytmem.

Magazyn komunikatów jest także miejscem tymczasowego składowania odpowiedzi, które nie zostały jeszcze przekazane nadawcy dokumentu (w przypadku, gdy nadawca podał adres zwrotny) lub nie zostały jeszcze pobrane przez nadawcę komunikatu (w przypadku, gdy nadawca zdecydował się na okresowe sprawdzanie dostępności odpowiedzi — polling).

Magazyn komunikatów jest elementem krytycznym dla działania usługi rejestracji dokumentów, powinien być więc odpowiednio zabezpieczony przed awariami sprzętu i oprogramowania oraz skutkami klęsk żywiołowych.

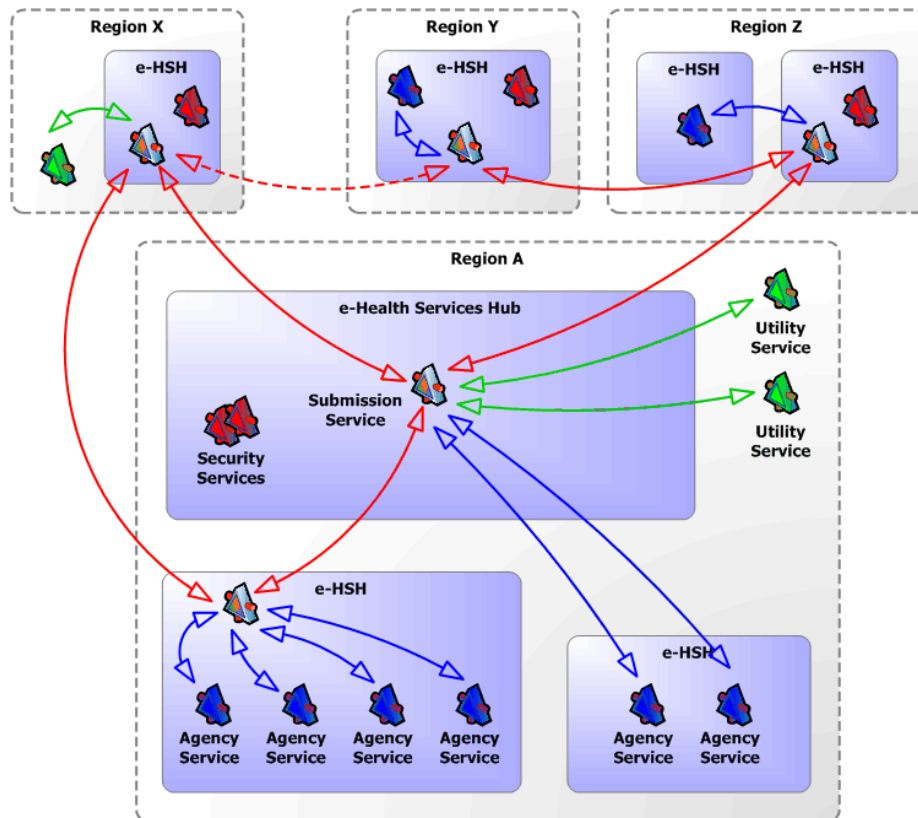
Usługa trasowania komunikatów

Jednym z głównych zadań usług integracyjnych e-zdrowia jest przekazywanie dokumentów do ich odpowiednich odbiorców. Może się to wiązać z koniecznością przekazania dokumentu do:

- stowarzyszonej usługi znajdującej się lokalnie, w tej samej agencji zdrowotnej (w przypadku dokumentów przekazywanych przez usługę rejestracji dokumentów na poziomie domenowym),
- stowarzyszonej usługi centralnej dla danej domeny (w przypadku dokumentów przekazywanych przez lokalną usługę rejestracji dokumentów),
- stowarzyszonej usługi znajdującej się w innej domenie zaufania (w przypadku dokumentów przekazywanych przez usługi rejestracji dokumentów na poziomie lokalnym lub poziomie domeny),
- usługi pomocniczej,
- usługi opieki zdrowotnej.

Na *ilustracji 21*. (uaktualnić schemat) przedstawiono różne ścieżki przekazywania dokumentu. Kolory linii oznaczają:

- linia czerwona — fizyczna droga przekazania dokumentu pomiędzy stowarzyszonymi usługami,
- przerywana linia czerwona — logiczna droga przekazania dokumentu; faktyczna fizyczna droga dokumentu może prowadzić przez inne węzły,
- linia niebieska — droga przekazania komunikatu do usługi agencji opieki zdrowotnej,
- linia zielona — droga przekazania komunikatu do usługi pomocniczej.



Ilustracja 21. Drogi przekazywania dokumentów przez usługę rejestracji dokumentów

Adresowanie usług Web Services

Lokalizacja usługi Web Services ustalana jest w czasie działania aplikacji poprzez przeszukanie katalogu UDDI. Pozwala to utrzymać jedno z podstawowych założeń architektury zorientowanej na usługi — przezroczystość lokalizacji. Adres uzyskany w wyniku wyszukiwania odpowiada fizycznej lokalizacji usługi Web Service. Może on mieć postać adresu URL protokołu HTTP — jeśli komunikacja z usługą Web Service odbywa się za pośrednictwem protokołu HTTP, ale może to być także inny typ adresu — jeśli wykorzystywany jest inny protokół komunikacyjny, na przykład podstawowy TCP/IP.

Komunikat SOAP z dokumentem biznesowym powinien zawierać nagłówki SOAP z adresem punktu końcowego, który ma otrzymać i przetworzyć dokument. Adresem tym często jest adres usługi rejestracji dokumentów, której zadaniem jest przekazanie komunikatu do docelowej usługi opieki zdrowotnej lub usługi pomocniczej. Oprócz adresu punktu końcowego, komunikat może zawierać także zestaw właściwości opisujących docelową usługę opieki zdrowotnej lub usługę pomocniczą, a także inne właściwości techniczne i specyficzne dla aplikacji, wymagane przez daną usługę opieki zdrowotnej lub usługę pomocniczą. Dzięki tym właściwościom usługa rejestracji dokumentów, do której trafi komunikat, może przekazać komunikat dalej do właściwej usługi docelowej.

Specyfikacja WS-Addressing umożliwia stosowanie zestandaryzowanego formatu adresów Web Service w nagłówkach komunikatów SOAP. Adresat komunikatu (adres punktu końcowego) jest określony przez element To, a operacja, która ma zostać wykonana przez usługę Web Service jest określana przez element Action. Element From identyfikuje nadawcę komunikatu, a element ReplyTo wskazuje adres, pod który należy skierować odpowiedź. Natomiast element FaultTo wskazuje adres, pod który należy kierować komunikaty informujące o błędach. Z każdym elementem adresu punktu końcowego mogą być (opcjonalnie) związane właściwości referencji, reprezentowane przez element ReferenceProperties.