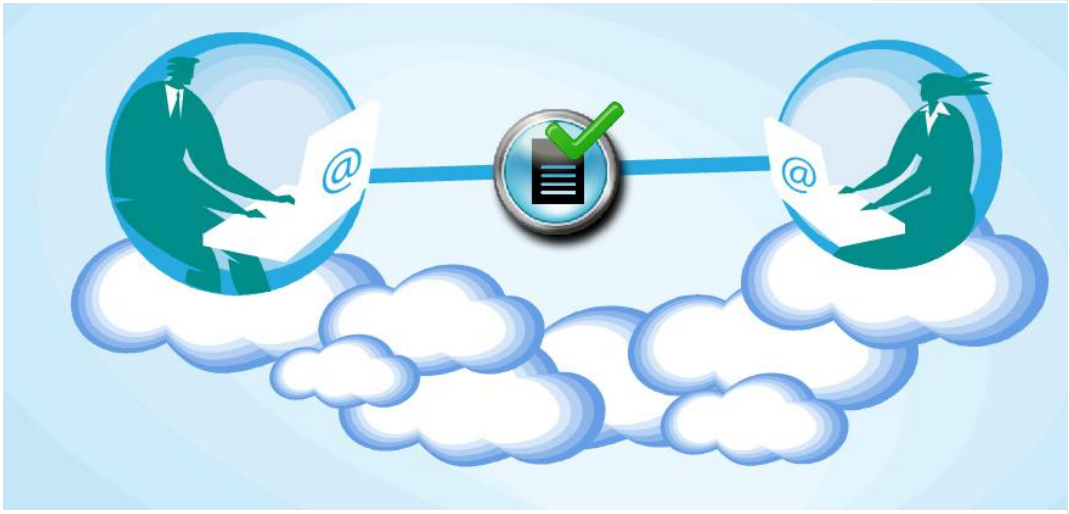
WEB.GOV.PL
WSPIERAMY E-BIZNES

2012

Tożsamość w chmurze



Jarosław Tomaszewski
Marcin Kraska

INNOWACYJNA GOSPODARKA
NARODOWA STRATEGIA SPÓJNOŚCI

PARP

UNIA EUROPEJSKA
EUROPEJSKI FUNDUSZ
ROZWOJU REGIONALNEGO

Koncepcja publikacji i współpraca merytoryczna:
Polska Agencja Rozwoju Przedsiębiorczości (PARP)
Platforma - Wspieramy e-biznes - www.web.gov.pl

Autorzy:
Jarosław Tomaszewski, Marcin Kraska,
Instytut Logistyki i Magazynowania (ILiM)
http://www.ilim.poznan.pl/

Korekta:
Michał Koralewski

Wydawca:
Polska Agencja Rozwoju Przedsiębiorczości (PARP)
ul. Pańska 81/83
00-834 Warszawa

www.parp.gov.pl

Wydanie I
Publikacja bezpłatna

Projekt współfinansowany przez Unię Europejską w ramach Europejskiego Funduszu Rozwoju Regionalnego

Wspieramy e-biznes www.web.gov.pl

Spis treści

1 Wprowadzenie

Jednym z nierozłącznych elementów e-usług oferowanych w Internecie jest konieczność zalogowania się do systemu informatycznego. Przy pierwszym użyciu e-usługi użytkownicy zazwyczaj proszeni są o założenie nowego konta, a co za tym idzie, są zobligowani do podania pewnego zakresu informacji o sobie, w tym m.in. login i hasło[1]. Są to najprostsze i dlatego najbardziej popularne elementy, ale warto pamiętać, że nie są jedynym sposobem uwierzytelniania użytkowników w systemach informatycznych. Istnieją bardziej złożone metody uwierzytelniania, które opierają się na dedykowanych urządzeniach (np. karty elektroniczne, tokeny, certyfikaty cyfrowe). Dzięki temu rozwiązania te są dużo bardziej bezpieczne, ale za to złożone i wymagające posiadania dodatkowych, kosztownych urządzeń.

Wraz z rosnącą liczbą nowych serwisów internetowych, użytkownicy, którzy chcą z nich korzystać, zmuszeni zostają do zakładania wielu odrębnych kont. Upomina się ich, aby ze względów bezpieczeństwa stosowali do uwierzytelniania unikalny login i hasło tzn. różniący się od wszystkich tych, które dotychczas zastosowali w innych serwisach internetowych. Sugestia dotycząca stosowania unikalnych haseł, ze względów bezpieczeństwa, jest w pełni zasadna – nie raz świat obiegła już informacja o tym, iż została wykradziona baza użytkowników (np. Yahoo[2] czy Twitter[3]), a ich dane osobowe wraz z przechowywanymi tam hasłami opublikowano w Internecie. Z drugiej jednak strony użytkownicy nie chcą i nie są w stanie zapamiętać wszystkich haseł do kont, które posiadają w kilku, kilkunastu czy nawet kilkudziesięciu różnych serwisach internetowych. Powstaje zatem dylemat, czy ryzykować i wykorzystywać takie same dane uwierzytelniające w różnych systemach, czy stosować do tego bezpieczniejsze, ale niewygodne w praktyce unikalne dane. Jest jeszcze trzecie wyjście, które opiszemy w tej publikacji.

E-book prezentuje metody i technologie umożliwiające rozwiązanie problemu uwierzytelniania i autoryzacji. Publikacja jest dedykowana przedsiębiorcom, którzy zarządzają popularną e-usługą lub planują uruchomić nową e-usługę wymagającą uwierzytelniania, jednak nie chcą zmuszać swoich użytkowników do pamiętania kolejnych loginów i haseł, nie zmniejszając jednocześnie poziomu bezpieczeństwa zarówno danych użytkownika, jak i samej e-usługi. Przedstawiony materiał nie wymaga specjalistycznej wiedzy dotyczącej technologii informatycznych, a wyjaśnienie związanych z nimi pojęć, można znaleźć w Słowniku w ostatnim rozdziale opracowania.

[1] Istnieją także inne metody uwierzytelniania niż podawanie login i hasła

[2] http://nt.interia.pl/internet/wiadomosci/news/wyciekly-dane-450-tys-uzytkownikow-yahoo,1821592,62

[3] http://internet.gadzetomania.pl/2012/05/09/wyciekly-dane-uzytkownikow-twittera-opublikowano-maile-i-hasla-tysiecy-uzytkownikow

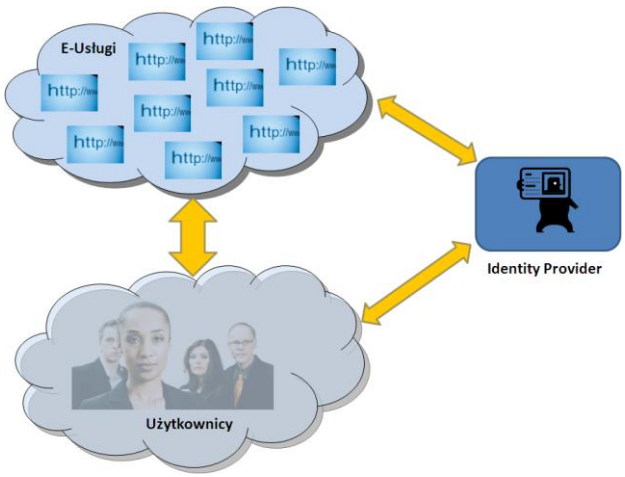
2 Uwierzytelnianie i autoryzacja w e-usłudze

Projektując nową e-usługę należy sobie odpowiedzieć na pytanie, czy potrzebuje ona dokonywać uwierzytelniania użytkowników i jeżeli tak, to w jaki sposób uwierzytelnianie powinno być realizowane. W wielu e-usługach nie ma potrzeby uwierzytelniania (np. darmowy portal informacyjny) i wtedy każdy użytkownik posiada taki sam dostęp do serwisu internetowego. Jeżeli jednak istnieje konieczność ograniczenia udostępnianych funkcji i informacji, w zależności od indywidualnego użytkownika, wtedy konieczne jest wdrożenie mechanizmów uwierzytelniania i autoryzacji.

Najprostszym sposobem na wdrożenie uwierzytelniania i autoryzacji jest zbudowanie własnej bazy użytkowników i zarządzanie we własnym zakresie informacjami na ich temat. Jak już jednak wspomniano w rozdziale 1, takie podejście coraz częściej spotyka się z niechęcią ze strony osób, posiadających już kilkanaście czy nawet kilkadziesiąt kont w różnych serwisach internetowych. Z pomocą w tym zakresie przychodzi technologia pozwalająca za pomocą jednego identyfikatora i powiązanego z nim hasła, uwierzytelniać się w wielu różnych serwisach internetowych. Dostępne na rynku rozwiązania wykorzystują kilka różnych standardów. Żaden z nich nie przewiduje przekazywania powiązanym serwisom internetowym danych użytkowników potrzebnych do uwierzytelnienia (login, hasło), przez co ryzyko ujawnienia tych danych nie rośnie wraz ze wzrostem liczby serwisów internetowych, z którymi współpracuje. Inną cenną cechą z punktu widzenia użytkownika jest możliwość zarządzania danymi uwierzytelniającymi w wielu serwisach internetowych z jednego miejsca. Przykładem takiej czynności, którą użytkownicy powinni ze względów bezpieczeństwa cyklicznie wykonywać, jest zmiana hasła. Zmienione hasło w jednym miejscu automatycznie „rozpowszechnia się"[4] na wszystkie powiązane z nim serwisy internetowe, niezależnie od tego, ile ich jest.

Architektura uwierzytelniania z wykorzystaniem zewnętrznych dostawców uwierzytelniania (*ang. Identity Providers*) różni się w szczegółach, w zależności od stosowanego protokołu. Generalna idea jest jednak podobna i polega na wydzieleniu od e-usługi funkcjonalności uwierzytelniania użytkowników. Uwierzytelnianie jest realizowane przez dedykowany serwis, podczas gdy e-usługa skupia się na funkcjach stanowiących wartość użytkową.

Rysunek 1 - Architektura uwierzytelniania z wykorzystaniem zewnętrznych dostawców



Źródło: Opracowanie własne

[4] W praktyce dane uwierzytelniające nigdzie nie są przechowywane

Oprócz prostego uwierzytelniania użytkowników w oparciu o jeden identyfikator, zachodzi czasem potrzeba, aby uwierzytelnić konkretny serwis internetowy udostępniając mu określony zakres informacji. Wyobraźmy sobie sytuację, w której użytkownik e-usługi (np. serwisu społecznościowego) przechowuje w nim swoje zdjęcia. W pewnym momencie użytkownik ten chciałby wykonać odbitki pewnych zdjęć z wykorzystaniem wybranej e-usługi. Aby to zrobić, najczęściej musi on najpierw pobrać wybrane zdjęcia na swoje urządzenie (np. komputer, tablet, telefon, itp.), a następnie przesłać je do odpowiedniego serwisu internetowego zajmującego się wykonywaniem odbitek. W przypadku wielu zdjęć, taka operacja może być długotrwała i związana z transferem pokaźnej ilości danych. Problem ten można rozwiązać poprzez udostępnienie pomiędzy poszczególnymi e-usługami wybranych danych - w tym wypadku zdjęć. Ze względów bezpieczeństwa, udostępnienie to powinno następować wyłącznie na bezpośrednie polecenie użytkownika będącego właścicielem danych. Podobnie jak w przypadku uwierzytelniania użytkowników, również i w tym wypadku zostały już opracowane odpowiednie technologie i standardy, które realizują taką funkcjonalność. Przegląd dostępnych na rynku rozwiązań zostanie opisany w następnym rozdziale.

3 Przegląd metod uwierzytelniania i autoryzacji

W rozdziale drugim wspomnieliśmy o istnieniu technologii wspierających funkcjonalność e-usług w zakresie uwierzytelniania i autoryzacji. Szczególnie duże i popularne serwisy internetowe, w momencie, w którym posiadają już znaczną liczbę użytkowników, decydują się na udostępnienie zewnętrznym serwisom funkcjonalności uwierzytelniania z wykorzystaniem stosowanych przez nich identyfikatorów. Na rynku dostępnych jest wiele takich rozwiązań, przy czym tylko niektóre z nich są oparte o standardy. Cześć dostawców funkcjonalności uwierzytelniania decyduje się na stosowanie własnych rozwiązań, przykładem których może być Facebook Connect[5], Google AuthSub[6], Yahoo BBAuth[7] czy też Amazon Web Services Identity[8]. Istnieją także na rynku standardy uwierzytelniania i autoryzacji, które coraz więcej firm decyduje się stosować w swoich e-usługach.

Niektóre z firm wykorzystują jednocześnie wiele protokołów uwierzytelnienia, w tym kilka standardów oraz swoje autorskie rozwiązania. Przykładem może być Google, który wspiera wspomniany wyżej własny protokół Google AuthSub, jednocześnie wykorzystując standardy takie jak SAML, OpenID czy OAuth. Wynika to najczęściej z chęci dostarczania coraz to bardziej zaawansowanych funkcjonalności, przy jednoczesnym zapewnieniu kontynuacji działania na starych zasadach, dla dotychczasowych serwisów internetowych korzystających z usług uwierzytelniania. Takie podejście daje istniejącym serwisom czas na wdrożenie nowoczesnych rozwiązań opartych o standardy.

W zakresie standardów związanych tożsamością można wyróżnić przede wszystkim OpenID, OAuth oraz SAML. Poniżej zaprezentowano podstawowe informacje na temat każdego z nich.

3.1 OpenID

OpenID jest standardem utrzymywanym przez organizację OpenID Foundation działającą na zasadach non-profit[9]. Zarząd organizacji składa się z osób reprezentujących społeczność związaną z OpenID oraz firmy komercyjne takie, jak Symantec, Google, Microsoft, PayPal, Verizon, Ping Identity. Za początek kształtowania się OpenID uznaje się rok 2005, kiedy to powstał pierwowzór protokołu działającego w bardzo ograniczonym środowisku. Szybko jednak protokół zaczął się rozwijać i w 2007 roku zaczęły się nim interesować duże firmy takie jak Microsoft, Symantec czy AOL i wtedy też formalnie została utworzona organizacja OpenID Foundation. Na koniec roku 2007 została opracowana specyfikacja OpenID 2.0 stosowana do dziś. W 2008 roku do organizacji przyłączyły się m.in. firmy takie jak Google, Microsoft oraz Yahoo! i powstawało coraz więcej serwisów korzystających z OpenID. Na koniec 2010 roku było już ponad miliard kont użytkowników OpenID i ponad 50 tysięcy serwisów akceptujących uwierzytelnienie oparte o ten standard.

OpenID jest standardem umożliwiającym osobom posiadającym konto u jednego z dostawców uwierzytelnienia (*ang. Identity Provider*), uwierzytelniać się także w innych serwisach wspierających OpenID. Jest wielu różnych dostawców uwierzytelnienia na świecie np. Google, Yahoo!, MySpace, WordPress. Przykładem krajowego jest Wirtualna Polska, każdy jednak może korzystać z dowolnego innego, niezależnie od tego, w jakim kraju jest zlokalizowany serwis internetowy, czy jego użytkownik. Przy tej okazji warto zwrócić uwagę na rozróżnienie roli, jaką dany serwis internetowy pełni w uwierzytelnianiu OpenID. Informacja o tym, że serwis wspiera OpenID nie jest wystarczająca, gdyż serwis może wspierać ten standard jako dostawca uwierzytelniania lub jako jego odbiorca, umożliwiając

[5] http://developers.facebook.com/blog/post/2008/05/09/announcing-facebook-connect/

[6] https://developers.google.com/accounts/docs/AuthSub

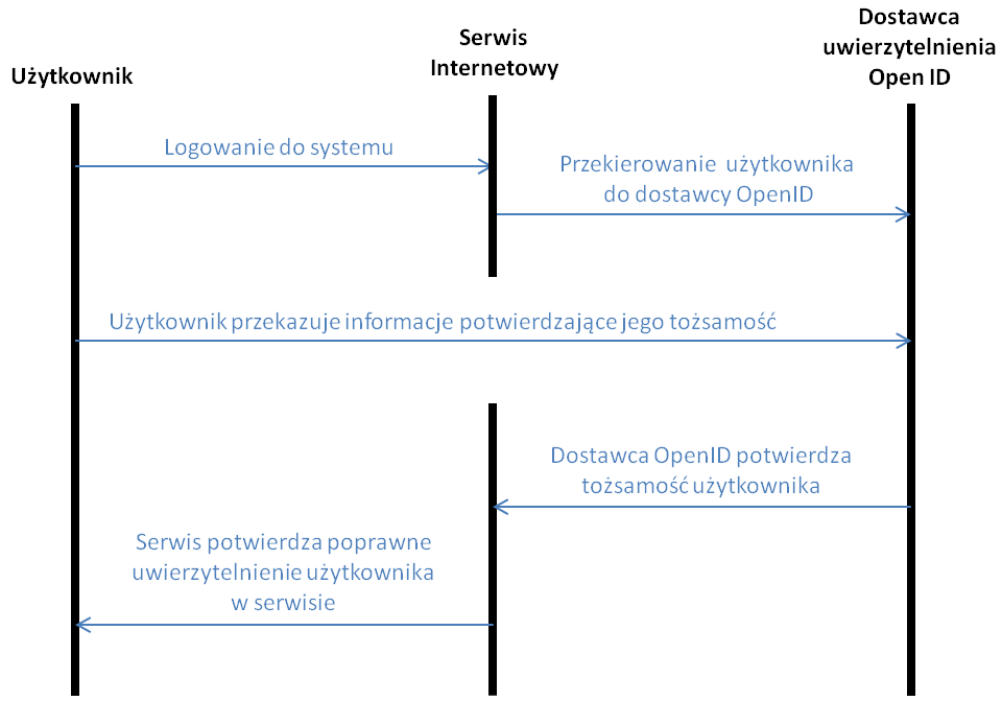
[7] http://developer.yahoo.com/auth/

[8] http://aws.amazon.com/iam/

[9] http://pl.wikipedia.org/wiki/Organizacja_non-profit

użytkownikom posiadającym konto u dostawcy OpenID uwierzytelnienie w swoim serwisie. I tak, trzymając się przykładu z polskiego rynku, Wirtualna Polska jest serwisem uwierzytelniającym, podczas gdy serwisy takie, jak Dziennik Lekcyjny, Centrum Faktur, Moi Krewni korzystają z uwierzytelniania bazując na standardzie OpenID. OpenID dodatkowo umożliwia przekazywanie informacji o użytkowniku pomiędzy dostawcą uwierzytelniania, a serwisem, który z niego korzysta. Zakresem przekazywanych danych użytkownik może zwykle zarządzać zarówno globalnie, jak i indywidualnie dla wybranych serwisów. Poniżej zamieszczono uproszczony model przepływu danych pomiędzy uczestnikami procesu uwierzytelnienia OpenID.

Rysunek 2 - Uproszczony model obrazujący uwierzytelnianie w standardzie OpenID



Źródło: Opracowanie własne

W pierwszym kroku, w celu uwierzytelnienia użytkownika, serwis internetowy przekierowuje użytkownika na serwer dostawcy uwierzytelniania OpenID. Na tym serwerze użytkownik podaje swoje dane uwierzytelniające oraz wyraża zgodę na udostępnienie serwisowi internetowemu wybranych danych z jego profilu osobowego. W przypadku, gdy wszystkie operacje są poprawne, serwis internetowy otrzymuje potwierdzenie uwierzytelnienia, a użytkownik zostaje z powrotem przekierowany do serwisu internetowego. Warto zauważyć, że dane uwierzytelniające (np. hasło) w żadnej formie nie jest przekazywane serwisowi internetowemu, zatem liczba miejsc w których są one przechowywane, ogranicza się wyłącznie do dostawcy uwierzytelnienia.

W praktyce komunikacja pomiędzy uczestnikami jest nieco bardziej złożona i szczegóły techniczne można znaleźć na portalu openid.net. Należy podkreślić, że dostawca OpenID, oprócz samego uwierzytelnienia, udostępnia także pewien zakres informacji o użytkowniku przechowywany w jego profilu. W porównaniu do innych standardów, warto zaznaczyć, że OpenID zajmuje się wyłącznie uwierzytelnianiem użytkowników, w szczególności nie służy do zarządzania autoryzacją dostępu do indywidualnych zasobów systemów komputerowych.

3.2 OAuth

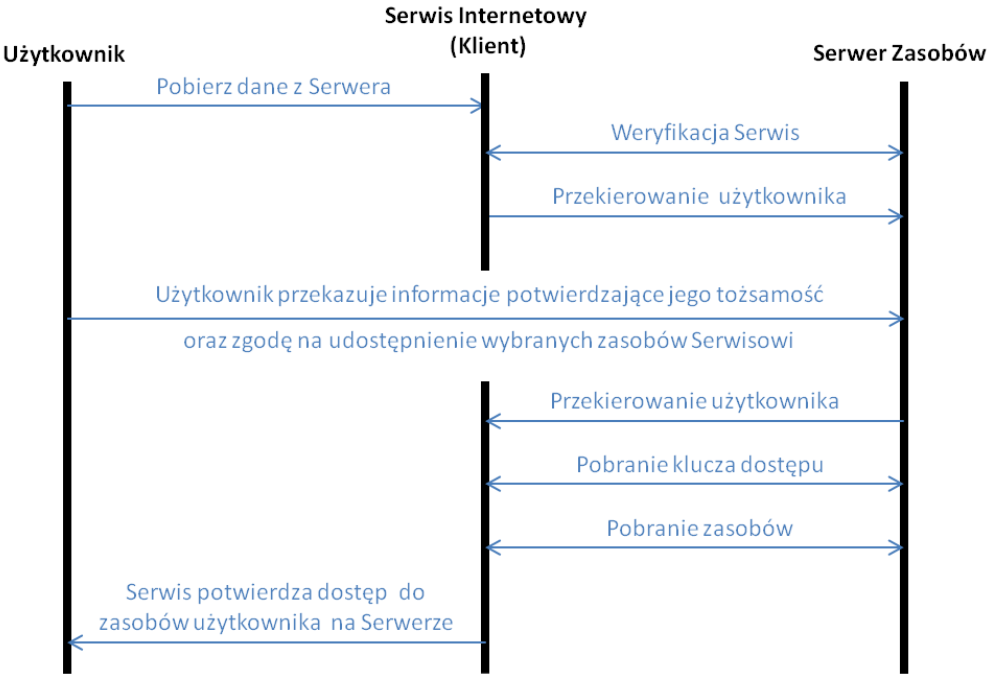
Za początek OAuth uważa się w rok 2006, kiedy to trwały już prace nad stworzeniem standardu OpenID. W tym czasie dostrzeżono potrzebę przekazywania przez użytkowników dostępu do swoich zasobów zlokalizowanych w systemach informatycznych, bez potrzeby ujawniania do tego celu swoich danych uwierzytelniających (np. login-u i hasła).

Funkcjonalność tę porównuje się do specjalnego klucza, w jaki wyposażone są niektóre luksusowe samochody. Klucz taki umożliwia jedynie przejechanie ograniczonej odległości oraz nie umożliwia m.in. otwierania bagażnika samochodu, korzystania z telefonu komórkowego zainstalowanego w samochodzie, itp. Z zasady, klucz ten służy do wręczenia osobie zajmującej się parkowaniem samochodu, bez potrzeby przekazywania normalnych kluczy pozwalających na korzystanie z samochodu bez żadnych ograniczeń. Poszukiwano w obszarze systemów komputerowych (w tym m.in. serwisów internetowych) podobnego rozwiązania, umożliwiającego udostępnienie części zasobów użytkownika za pomocą odpowiednika „specjalnego klucza".

W czasie, gdy tworzył się OAuth, nie było żadnego otwartego standardu, który wspierałby tego typu funkcjonalność. Powstała więc grupa osób związana z Google, która opracowała propozycję odpowiedniego protokołu. W 2007 roku grupa ta otworzyła się na wszystkich zainteresowanych do współuczestnictwa w opracowaniu standardu, tworząc społeczność OAuth. Pod koniec 2007 roku powstała specyfikacja OAuth Core w wersji 1.0, która została następnie w roku 2009 zaktualizowana do wersji OAuth 1.0a, rozwiązując problem bezpieczeństwa, jaki został wykryty w pierwotnej wersji. W 2010 roku OAuth 1.0a został opublikowany jako standard RFC 5849. W międzyczasie powstała także zupełnie nowa wersja protokołu - OAuth 2.0, jednak nie jest ona kompatybilna wstecz z wersją OAuth 1.0 i nie doczekała się do tej pory ostatecznej akceptacji przez organizację IETF (*ang. Internet Engineering Task Force*), zajmującą się standardami związanymi z działaniem Internetu. Nie oznacza to jednak, że OAuth 2.0 nie jest wykorzystywany – wręcz przeciwnie. Wiele dużych firm w tym m.in. Microsoft, Facebook, Google, Instagram wpiera aktualnie wyłącznie wersję 2.0 podczas, gdy inne firmy, takie jak m.in. Dropbox, LinkedIn, Yahoo!, Twitter wspierają wersję 1.0 czy też 1.0a.

Jak już wspomniano na samym początku, OAuth umożliwia użytkownikom udostępnianie swoich zasobów, znajdujących się na różnych serwisach internetowych, innym serwisom internetowym, bez potrzeby przekazywania im hasła. Dodatkowo pozwala także na ograniczenie tego dostępu ze względu na jego zakres lub czas udostępniania, itp. Poniżej zamieszczono uproszczony model przepływu danych pomiędzy uczestnikami procesu udostępniania zasobów w OAuth.

Rysunek 3 - Uproszczony model obrazujący udostępnianie zasobów w standardzie OAuth



Źródło: Opracowanie własne

W pierwszym kroku, aby otrzymać dostęp do zasobów użytkownika, serwis musi zostać zweryfikowany na serwerze udostępniającym te zasoby. W tym celu, wysyła on odpowiednie wywołanie do serwera zawierające dane identyfikujące. W przypadku, gdy dany serwis zostanie zaakceptowany, otrzyma on klucz tzw. *Request Token*, który pozwoli mu na dalszą komunikację z serwerem. Po otrzymaniu klucza, przekierowuje on użytkownika na serwer, gdzie ten użytkownik podaje swoje dane uwierzytelniające oraz wyraża zgodę na udostępnienie swoich wybranych zasobów temu serwisowi internetowemu. W przypadku, gdy wszystkie operacje są poprawne, użytkownik zostaje z powrotem przekierowany do serwisu internetowego, który dodatkowo otrzymuje z serwera specjalny klucz tzw. *Access Token*. Klucz ten pozwala serwisowi internetowemu na dostęp do wybranych zasobów użytkownika na serwerze, przez ściśle określony czas.

Powyższy opis oddaje generalny sens wymiany danych pomiędzy uczestnikami OAuth 1.0 choć technicznie jest on nieco bardziej złożony. Wersja OAuth 2.0 jest jeszcze bardziej skomplikowana, jednak nie będziemy prezentować szczegółów technicznych, które można znaleźć na portalu oauth.net. Warto zwrócić jednak uwagę na dwa istotne elementy tego standardu. Podobnie jak w przypadku OpenID, serwis uzyskujący dostęp do zasobów serwera, nie wchodzi w posiadanie danych uwierzytelniających użytkownika, w imieniu którego otrzymuje dostęp. Drugim ważnym elementem jest rejestracja serwisów na serwerze OAuth. Jest ona ważnym elementem bezpieczeństwa w komunikacji, zapewniającym dostęp do zasobów serwera wyłącznie znanym i zweryfikowanym serwisom internetowym, utrudniając próby ataku na serwer OAuth.

Należy nadmienić, iż OAuth może być także wykorzystany do uwierzytelniania użytkowników poprzez udostępnione API (*ang. Application Programming Interface*), czyli serwera do odczytu informacji użytkownika zapisanych w jego profilu. Serwis internetowy może tam znaleźć np. identyfikator użytkownika oraz inne informacje na jego temat i na tej podstawie określić, kto się uwierzytelnił. W praktyce serwisy internetowe stosują tę metodę – przykładem może być udostępnienie przez Google

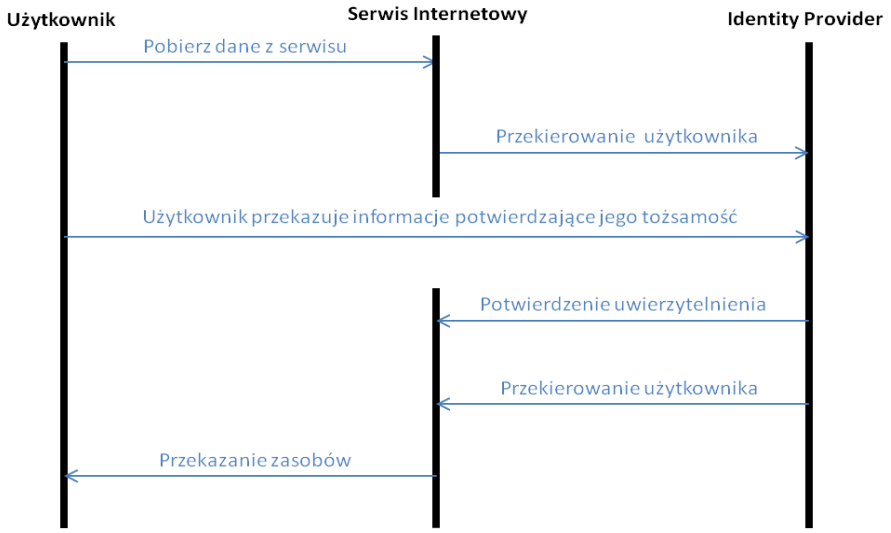
opisu technicznego, który pozwala przy wykorzystaniu OAuth 2.0 na uruchomienie funkcji logowania do własnego serwisu[10].

3.3 SAML

Początki protokołu SAML (*ang. Security Assertion Markup Language*) datuje się na rok 2001, kiedy to organizacja OASIS (*ang. Organization for the Advancement of Structured Information Standards*) zajmująca się standardami, rozpoczęła pracę nad stworzeniem założeń standardu wymiany informacji związanych z uwierzytelnianiem oraz autoryzacją przy wykorzystaniu XML. W pracach nad standardem wykorzystano istniejące rozwiązania kilku firm komercyjnych i pod koniec 2002 roku opublikowano wersję 1.0 SAML jako standard OASIS. W 2003 roku opublikowano stosunkowo niewielką aktualizację standardu do wersji 1.1, a w roku 2005 powstała wersja 2.0 standardu SAML, która nie jest kompatybilna wstecz z wersjami 1.0 i 1.1.

Standard SAML przewiduje trzy główne role w komunikacji - użytkownika, dostawcy usług (w naszym przypadku może to być serwis internetowy) oraz dostawcy identyfikacji. Zgodnie z założeniami, standard opisuje sposób wymiany informacji w kontekście uwierzytelniania i autoryzacji. Standard jest wykorzystywany zarówno w kontekście osób korzystających z serwisów internetowych, jak i w komunikacji pomiędzy systemami komputerowymi z wykorzystaniem np. web-serwisów. Poniżej przedstawiono uproszczony model przepływu danych pomiędzy uczestnikami procesu udostępniania zasobów w SAML.

Rysunek 4 - Uproszczony model obrazujący autoryzację w standardzie SAML



Źródło: Opracowanie własne

Proces komunikacji zwykle zaczyna się od próby uzyskania dostępu przez użytkownika do jego danych znajdujących się w serwisie internetowym. Jeżeli jest on niezalogowany, następuje przekierowanie go do Identity Provider-a w celu uwierzytelnienia. Użytkownik podaje swoje dane uwierzytelniające (np. login i hasło), a informacja potwierdzająca pozytywne uwierzytelnienie zostaje przekazana do serwisu internetowego. Serwis internetowy posiadając potwierdzenie z Identity Provider-a, czyli tzw. asercję (*ang. assertion*), udostępnia użytkownikowi jego zasoby. SAML wpiera także SSO (*ang. Single Sign-On*), czyli

[10] https://developers.google.com/accounts/docs/OAuth2Login

pojedyncze logowanie w grupie powiązanych serwisów internetowych. Jeżeli użytkownik zaloguje się w dowolnym serwisie internetowym z wykorzystaniem Identity Providera-a, to dopóki jego sesja jest aktywna, może on bez potrzeby ponownego logowania, korzystać z dowolnego innego serwisu internetowego powiązanego z tym Identity Provider-em. W takim wypadku różnica w przepływie danych, który został opisany powyżej polega na tym, iż po przekierowaniu użytkownika w celu uwierzytelnienia z serwisu internetowego do Identity Providera, Identity Provider sprawdza, czy istnieje aktywna sesja tego użytkownika (np. w kontekście pracy z innym serwisem internetowym) i jeżeli tak, to już bez pytania użytkownika o dane uwierzytelniające, potwierdza on serwisowi uwierzytelnienie i przekierowuje użytkownika z powrotem do serwisu internetowego. Dla użytkownika cała operacja jest niewidoczna i trafia on niemal „od razu" do właściwego miejsca (np. zasobów) serwisu internetowego. Powyższy opis oddaje generalny sens działania SAML natomiast szczegóły techniczne można znaleźć na portalu saml.xml.org.

Uwierzytelnienie z wykorzystaniem SAML jest realizowane w oparciu o zaufanie serwisów do Identity Provider-a i informacji przez niego dostarczanych. Ciekawym przykładem krajowej realizacji w praktyce SAML oraz SSO jest platforma ePUAP. Platforma ta, będąc utrzymywana przez organ administracji publicznej[11], udostępnia[12] funkcjonalność Identity Provider-a w oparciu o protokół SAML 2.0. Z funkcjonalności uwierzytelniania oraz SSO korzysta m.in. portal Pojedynczego Punktu Kontaktowego eu-go.gov.pl, który oprócz informacji na temat podejmowania, prowadzenia i zakończenia działalności gospodarczej, umożliwia także realizację wybranych procedur administracyjnych przy wykorzystaniu ePUAP. Wystarczy, że użytkownik raz się zaloguje (nie ma znaczenia czy zrobi to na ePUAP czy EU-GO) i może bez przeszkód korzystać z obu tych systemów. Przechodzenie pomiędzy serwisami internetowymi powiązanymi SSO może być na tyle płynne, że użytkownikom może się wydawać, że działają cały czas w ramach jednego serwisu. Przykładem takiego połączenia jest również Google, który w swoich aplikacjach, takich jak Web Picasa, Gmail, Google Calendar, stosuje właśnie SSO oparte o SAML.

[11] ePUAP jest zarządzany i utrzymywany przez Ministerstwo Administracji i Cyfryzacji

[12] http://epuap.gov.pl/wps/portal/!ut/p/c0/04_SB8K8xLLM9MSSzPy8xBz9CP0os3g3Z4-gYG93QwMLRydXA89go2CXYENnAwtDM_2CbEdFAKyGzHM!/?WCM_PORTLET=PC_7_47JL5I93007KD0I2FVBNKG0OK1_WCM&WCM_GLOBAL_CONTEXT=/wps/wcm/connect/epuap2/ePUAP2/PL/Pomoc/Integratorzy/Specyfikacja+WSDL/

3.4 Porównanie standardów

Opisane powyżej standardy różnią się od siebie, ponieważ każdy z nich powstał w odpowiedzi na inne zapotrzebowanie. Różnice polegają głównie na stosowaniu odmiennej technologii oraz dostarczaniu innych funkcjonalności, choć z perspektywy użytkownika korzystającego z tych rozwiązań może wydawać się, że sposób działania tych standardów jest bardzo podobny.

Przed wyborem konkretnego standardu należy się zastanowić, jakie są nasze oczekiwania w zakresie uwierzytelniania i autoryzacji, w kontekście działania konkretnego serwisu internetowego. Jeżeli szukamy prostych rozwiązań w celu umożliwienia korzystania z istniejących już w innych serwisach kont, to dobrym wyborem wydaje się być OpenID. Stosunkowo najprostszy do uruchomienia standard uwierzytelniania oraz szeroka gama dostawców uwierzytelniania może być w tym przypadku dodatkowym atutem. Jeżeli jednak planujemy, aby nasz serwis internetowy pozwalał na udostępnianie lub korzystanie z zasobów swoich użytkowników w innych serwisach, OpenID już nie wystarczy. W takiej sytuacji należy rozważyć wybór protokołu OAuth, weryfikując wcześniej, czy konkretne serwisy, z którymi nasz serwis miałby współpracować, wspierają OAuth i jeżeli tak, to w jakiej wersji. Jak już wcześniej wspomniano, OAuth może być także wykorzystywany do uwierzytelniania co poszerza zakres jego stosowania. Standard SAML wydaje się być najbardziej złożonym rozwiązaniem stosowanym do uwierzytelniania oraz autoryzacji użytkowników[13] w ramach zaufanego kręgu aplikacji i systemów komputerowych. Oferuje on funkcjonalność SSO, która jest w stanie połączyć różne serwisy internetowe w taki sposób, że użytkownik ma wrażenie poruszania się po jednym dużym systemie. Ten standard zatem dedykowany jest przede wszystkim do rozwiązań stanowiących grupę ściśle ze sobą współpracujących serwisów.

[13] SAML służy także do uwierzytelniania dostępu do interfejsów komunikacyjnych, ale nie jest to przedmiotem niniejszego opracowania.

4 Podsumowanie i wnioski

Opisane w rozdziale trzecim standardy stanowią podstawę, w oparciu o którą tworzone są federacje serwisów internetowych, mających na celu wykorzystanie jednej bazy użytkowników do ich uwierzytelniania i autoryzacji. Każda firma będąca uczestnikiem federacji, przystępuje do niej ze względu na korzyści jakie z tego tytułu oczekuje uzyskać. Dla przedsiębiorcy oferującego e-usługi ma to tym większe znaczenie, im większa jest liczba użytkowników serwisu uwierzytelniającego, gdyż wraz z jej wzrostem rośnie prawdopodobieństwo, iż potencjalny użytkownik e-usługi posiada konto w tym serwisie uwierzytelniającym. Poniżej wymieniono kilka ważniejszych korzyści z perspektywy właścicieli serwisów internetowych, jakie można uzyskać stosując uwierzytelnianie w chmurze.

- **Wzrost popularności serwisu**

  Firma wykorzystująca uwierzytelnianie w chmurze jest postrzegana jako nowoczesna i dbająca o wygodę użytkowników. Jej rozpoznawalność może także ulec poprawie w wyniku zarówno wzrostu liczby użytkowników, jak i obecności danego serwisu w innych, powiązanych w kontekście wspólnego uwierzytelniania i autoryzacji serwisach. Dla Identity Provider-a natomiast, im więcej serwisów korzysta z jego usług uwierzytelniania, tym większą ma on rozpoznawalność wśród użytkowników.

- **Przywiązanie do serwisu i marki firmy**

  Korzyść ta głównie dotyczy serwisów uwierzytelniających, którzy udostępniając swoje usługi zewnętrznym serwisom internetowym, pośrednio budują swoją markę. Użytkownik posiadając już konto w jednym serwisie uwierzytelniającym, które wykorzystuje w kilku serwisach internetowych, nie będzie skłonny tego serwisu zmieniać w związku z uciążliwością takiego działania. Taka funkcjonalność sprzyja zatem lojalności i przywiązania klientów do serwisu.

- **Nowi użytkownicy**

  Wzrost popularności danego serwisu może przełożyć się bezpośrednio na liczbę jego nowych użytkowników. Im łatwiej jest założyć nowe konto, tym więcej użytkowników może zdecydować się na korzystanie z serwisu. Jeżeli użytkownik w praktyce nie musi się rejestrować, bo może wykorzystać posiadane już przez niego konto, to tym łatwiej podejmie decyzję o skorzystaniu z serwisu.

- **Wzrost zaufania użytkowników**

  Generalnie im więcej serwis ma użytkowników, tym większym zaufaniem cieszy się on na rynku. Fakt, iż posiadane przez użytkownika konto u jednego ze znanych dostawców uwierzytelniania można wykorzystać również w danym serwisie internetowym, powoduje wzrost zaufania do tego serwisu. Wynika to m.in. z faktu współpracy znanej firmy z danym serwisem internetowym oraz brakiem konieczności przekazywania mu bezpośrednio danych uwierzytelniających (np. haseł).

- **Bardziej przyjazny interfejs**

  Jak zostało to opisane w powyższych rozdziałach, funkcjonalność uwierzytelniania i autoryzacji w chmurze pozwala na automatyzację pewnych operacji, które użytkownik inaczej musi realizować osobiście. Dotyczy to zarówno samego procesu rejestracji, jak i udostępniania swoich zasobów innym serwisom. Przytoczony przykład z udostępnianiem zdjęć w celu ich wydrukowania pokazał, że zamiast czynności pobierania w jednym serwisie i ładowania w drugim pojedynczych zdjęć, można je po prostu udostępnić pomiędzy serwisami. Jest to dużo szybsze i wygodniejsze rozwiązanie, które użytkownicy z pewnością docenią.

Stosowanie technologii uwierzytelniania i autoryzacji, przy wykorzystaniu zewnętrznych dostawców uwierzytelnienia niesie ze sobą pewne zagrożenia. Poniżej przedstawiono kilka najważniejszych z nich, które pozwolą na podjęcie racjonalnych decyzji związanych z wdrażaniem opisanych technologii:

- **Zagrożenie utraty danych przez użytkowników**

  Zagrożenie wynika głównie z ryzyka przejęcia przez obcą osobę danych uwierzytelniających konto użytkownika, co umożliwia dostęp do jego prywatnych danych we wszystkich powiązanych serwisach. W skrajnych wypadkach może dojść do przejęcia przez obcą osobę konta w wyniku zmiany danych uwierzytelniających (np. hasła). W takich wypadkach użytkownik traci dostęp swoich danych na koncie. Należy dodać, że to zagrożenie występuje zarówno przy stosowaniu uwierzytelniania w chmurze, jak i przy lokalnym uwierzytelnianiu. Różnica polega wyłącznie na skali problemu – w przypadku uwierzytelniania lokalnego, ryzykiem obarczone jest wyłącznie konto w jednym serwisie, natomiast przy uwierzytelnianiu w chmurze, może to dotyczy wszystkich serwisów powiązanych z kontem u danego dostawcy uwierzytelnienia.

- **Obawa przed udostępnianiem danych zagranicznym podmiotom**

  Tworzenie konta u dostawcy uwierzytelnienia, nierozłącznie związane jest z podaniem podstawowych danych dotyczących użytkownika. Większość ze znanych serwisów uwierzytelniających zlokalizowana jest poza granicami naszego kraju, co może u niektórych użytkowników rodzić obawę o bezpieczeństwo swoich danych. Dodatkowo użytkownicy mogą obawiać się, iż wykorzystywanie uwierzytelnianie w chmurze zmniejsza ich prywatność, poprzez zbieranie przez dostawcę uwierzytelniania informacji dotyczących, w jakich serwisach dany użytkownik ma konta.

Wszystkie powyższe zagrożenia są ściśle związane z solidnością i zaufaniem, jakim darzą dostawcę uwierzytelniania zarówno właściciele serwisów internetowych, jak i sami ich potencjalni użytkownicy. Dlatego też wydaje się, iż decyzja o wyborze konkretnego partnera w tym zakresie stanowi istotny element, który może przyczynić się do powodzenia wdrożenia uwierzytelniania w chmurze.

W dzisiejszym świecie, w którym jest niezliczona ilość e-usług i stale powstają nowe, wydaje się, że uwierzytelnianie w chmurze stanowi właściwy kierunek powalający użytkownikom zarządzać swoimi kontami. Pomimo istnienia pewnego ryzyka, korzyści wynikające z zastosowania uwierzytelniania w chmurze są atrakcyjne zarówno dla dostawców e-usług, jak i dla ich użytkowników. Stały rozwój standardów uwierzytelniania i autoryzacji powoduje wzrost zainteresowania tymi technologiami, co daje pozytywne perspektywy na przyszłość.

5 Słownik

Autoryzacja – (*ang. authorization*) jest to proces, którego celem jest weryfikacja i potwierdzenie faktu posiadania przez użytkownika systemu uprawnień do korzystania z wybranego zasobu.

Dostawca uwierzytelniania – (*ang. Identity Provider*) jest modułem informatycznym umożliwiającym tworzenie, zarządzanie i utrzymywanie identyfikacji swoich użytkowników oraz udostępniającym zewnętrznym serwisom usługi uwierzytelniające.

e-Usługi – (*ang. e-services*) „usługi świadczone drogą elektroniczną przez sieć telekomunikacyjną, a w tym sieć komputerową, np. Internet, z wykorzystaniem technologii informacyjnej, których świadczenie jest zautomatyzowane i które wymagają niewielkiego udziału człowieka"[14]. W niniejszej publikacji, e-usługi są tożsame z pojęciem serwisu internetowego.

Serwis internetowy – w niniejszej publikacji pojęcie tożsame z definicją „e-usługi".

Serwis społecznościowy – „serwis internetowy, który istnieje w oparciu o zgromadzoną wokół niego społeczność. Tworzy tak zwane media społecznościowe (*ang. social media*)"[15].

SSO – (*ang. Single Sign-On*) jest właściwością polegającą na tym, iż użytkownik logując się jednokrotnie otrzymuje dostęp do wszystkich powiązanych systemów komputerowych, bez potrzeby logowania się indywidualnie w każdym z nich.

Uwierzytelnianie – (*ang. authentication*) zwane czasem potocznie autentykacją, jest to proces, którego celem jest weryfikacja i potwierdzenie tożsamości deklarowanej przez użytkownika będącego osobą, urządzeniem lub usługą. Najbardziej popularnym przykładem uwierzytelniania jest podanie login-u i hasła.

XML – (*ang. Extensible Markup Language*) jest uniwersalnym językiem, niezależnym od stosowanej platformy sprzętowej i programowej, przeznaczony do przechowywania danych w sposób ustrukturyzowany, umożliwiający ich odczytanie zarówno przez człowieka jak i maszynę. XML jest stworzony w oparciu o specyfikację zarządzaną przez organizację W3C.

[14] http://pl.wikipedia.org/wiki/E-us%C5%82ugi

[15] http://pl.wikipedia.org/wiki/Serwis_spo%C5%82eczno%C5%9Bciowy