Projekt nr. POIG.02 03. 00-00-028/08-01 www.platon.pionier.net.pl
PLATFORMA OBSŁUGI NAUKI PLATON
KOORDYNATOR: INSTYTUT CHEMII BIOORGANICZNEJ PAN
POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO - SIECIOWE
ul. Noskowskiego 12/14, 61-704 Poznań, (+48 61) 858 20 00, fax: (+48 61) 852 59 54, e-mail: office@man.poznan.pl, www: http://www.man.poznan.pl

Federacyjne zarządzanie tożsamością a eduroam

Tomasz Wolniewicz, UCI UMK (twoln@umk.pl)
dokument przygotowany w ramach projektu PLATON
wersja 2.0 – sierpień 2012

Spis treści

1. Wstęp

Użytkownicy Internetu są zmuszeni do posiadania wielu kont. Zapamiętanie dużej liczby identyfikatorów i haseł jest praktycznie niemożliwe, więc stosuje się wiele technik, które mają ułatwić rozwiązanie tego problemu.

Drugim, istotnym problemem w dostępie do chronionych zasobów internetowych jest kwestia autoryzacji, a wiec potwierdzenia uprawnień konkretnego użytkownika do korzystania z danego zasobu. Zwłaszcza w przypadku dostępu opłacanego poprzez instytucje, potwierdzenie uprawnień użytkowników staje się złożonym problemem.

Należy zwrócić uwagę na fakt, ze terminy ***Federated Login***, czy ***Federated Identity*** funkcjonują obecnie w oderwaniu od tego, co tradycyjnie nazywało się ***Federacją***. ***Federated Login***, to przede wszystkim technologia, która powstała w ramach i na potrzeby federacji zarządzania tożsamością, a następnie została przejęta i rozbudowana przez instytucje komercyjne. Jednym z najważniejszych przykładów takiej technologii jest standard OpenID, zaliczany do logowania federacyjnego, chociaż w prawdziwych federacja nieużywany.

Celem niniejszego dokumentu jest przedstawienie zagadnienia federacyjnego zarządzania tożsamością w znaczeniu takim, jakie występuje w środowiskach naukowo-akademickich całego świata, ilustrując prezentowane zagadnienia konkretnym przykładem jakim jest eduroam, pomimo że rozwiązania techniczne stosowane przez eduroam są inne niż w tym, co typowo nazywało się federacją zarządzania tożsamością. W Polsce mamy do czynienia z inna sytuacją niż w większości krajów UE. eduroam stał się usługą znaną i dobrze rozumianą, natomiast federacyjne podejście do zarządzania

tożsamością, ciągle nie może wyjść z fazy planów. Model eduroam powinien ułatwić zrozumienie na czym polega bardziej abstrakcyjny schemat zarządzania tożsamością, ale dodatkowo, fakt, ze eduroam w Polsce już działa, może się stać znaczącym ułatwieniem przy wprowadzaniu federacji o szerszych celach.

W dalszym ciągu przedstawione zostaną różne przykłady konkretnych rozwiązań, ale zaczniemy od opisania usługi eduroam, rozwijanej w Polsce w ramach projektu PLATON.

2. eduroam

2.1.1. Model

Celem usługi eduroam jest zapewnienie powszechnego, gościnnego dostępu do sieci dla członków środowiska nauki. eduroam jest zazwyczaj postrzegany jako ściśle związany z sieciami bezprzewodowymi i tak jest zazwyczaj realizowany, chociaż w rzeczywistości infrastruktura eduroam wspiera wszelkie sieci chronione przy pomocy standardu IEEE 802.1X. Istotą eduroam jest mechanizm uwierzytelnienia i autoryzacji. Kiedy na terenie instytucji włączonej do eduroam pojawia się użytkownik z innej instytucji i uruchamia urządzenie, przy pomocy którego chce korzystać z sieci, to urządzenia dostępowe sieci uruchamiają proces uwierzytelnienia. Urządzenie użytkownika zapytane o identyfikator przesyła łańcuch znaków skonstruowany na tej samej zasadzie, co adres e-mail. Podobnie, jak w przypadku e-mail, na podstawie części domenowej lokalizowany jest serwer macierzysty dla danego użytkownika, a w następstwie procesu właściwego uwierzytelnienia realizowanego pomiędzy urządzeniem użytkownika i jego serwerem macierzystym, urządzenia dostępowe instytucji, we której użytkownik przebywa otrzymują zgodę na umożliwienie dostępu.

W ramach powyższego procesu pojawia się kilka elementów, których zrozumienie jest kluczowe.

2.1.2. Zaufanie między instytucjami

Instytucja goszcząca użytkownika ufa zapewnieniu jego instytucji macierzystej, że ta użytkownika rozpoznaje i, że jest on uprawniony do skorzystania z usługi. Ustalenie odpowiedniej relacji zaufania miedzy instytucjami wymaga wcześniejszych uregulowań, określenia zasad działania usługi, akceptacji tych zasad przez obie instytucje, określenia i wdrożenia infrastruktury technicznej, która realizuje procesy uwierzytelnienia i wypełnienia relacji zaufania.

2.1.3. Bezpieczeństwo procesu uwierzytelnienia

Użytkownik korzysta z konta w swojej instytucji macierzystej, jego hasło musi zostać przekazane do serwera macierzystego w sposób gwarantujący jego bezpieczeństwo. W żadnym razie użytkownik nie może być zmuszany do wprowadzenia swojego hasła do obcej strony internetowej. W eduroam, bezpieczeństwo hasła jest realizowane poprzez zestawienie szyfrowanego kanału pomiędzy urządzeniem użytkownika, a jego serwerem macierzystym. Hasło jest przekazywane tym kanałem i jest niewidoczne dla infrastruktury pośredniczącej w transmisji, w szczególności dla urządzeń instytucji goszczącej.

2.1.4. Ochrona prywatności użytkownika

eduroam, podobnie jak wiele innych usług, jest realizowany w oparciu o zasadę, że nie wolno zbierać niepotrzebnych informacji na temat tożsamości użytkownika. W szczególności użytkownik ma prawo i możliwości techniczne do ukrycia swojego pełnego identyfikatora, tak że jedyna informacja którą dysponuje instytucja goszcząca jest to jaka instytucja odpowiada za danego użytkownika.

2.1.5. Rozpoznawanie użytkowników powracających

Możliwość anonimizacji użytkowników jest pożądana z punktu widzenia ochrony ich prywatności, ale z drugiej strony utrudnia lub uniemożliwia stwierdzenie, że kolejne logowania dotyczą tej samej osoby. W konsekwencji zablokowanie dostępu pojedynczej osobie, która narusza regulamin, albo nadanie komuś szczególnych uprawnień jest niemożliwe bez współpracy z instytucją macierzystą użytkownika. W eduroam prowadzone są prace, które mają zlikwidować ten problem poprzez

przydzielanie użytkownikom indywidualnych pseudo-identyfikatorów. Identyfikatory byłyby stałe dla dostępów tej samej osoby w tej samej instytucji goszczącej, ale zmieniałyby się przy przejściu do innej instytucji.

3. Bardziej ogólnie

Opisane powyżej elementy, czyli:

1. zaufanie między instytucjami,
2. bezpieczeństwo procesu uwierzytelnienia,
3. ochrona prywatności użytkownika i,
4. rozpoznawanie użytkowników powracających

mogą być traktowane całkowicie abstrakcyjnie i w oderwaniu od konkretnej platformy technologicznej. Stanowią one bazę działania każdego federacyjnego systemu zarządzania tożsamością.

Jeżeli w poprzednim przykładzie zmienimy instytucję udostępniającą eduroam na firmę udostępniającą czasopisma elektroniczne, to możemy stworzyć nowy przykład, w którym osoby związane z określonymi instytucjami są w stanie skorzystać z czasopism elektronicznych po zalogowaniu się w swojej instytucji macierzystej. Usługodawca udostępniający czasopisma otrzyma od instytucji macierzystej użytkownika potwierdzenie, że dana instytucja upoważnia danego użytkownika do korzystania z zasobu. Równolegle z tym potwierdzeniem przesłany zostanie pseudoidentyfikator, a być może również jakieś dodatkowe atrybuty zagwarantowane w kontrakcie miedzy instytucją macierzystą a usługodawcą. Usługodawca nie powinien otrzymać danych pozwalających na zidentyfikowanie konkretnej osoby, ponieważ historia przeglądanych zasobów z całą pewnością musi być traktowana jako sprawa poufna.

Logowanie za pomocą jednego konta może być realizowane w różnych technologiach. eduroam korzysta ze standardu 802.1x i związanych z nim standardów takich jak EAP. EAPOL, czy RADIUS. W dostępach poprzez WWW z reguły stosuje się OAIS SAML. Od strony czysto technicznej, w powyższych przykładach występują tylko dwie strony – usługodawca oraz instytucja poświadczająca tożsamość. Poza sama technologią, kluczowymi elementami są: zaufanie oraz semantyka przekazywanych atrybutów. Zaufanie jest niezbędne zarówno do poświadczenia uprawnić użytkownika do konkretnej usługi jak i do tego, by instytucja poświadczającą tożsamość przekazała w jego imieniu jakieś informacje na jego temat (dodatkowe atrybuty). Uzgodnienia dotyczące znaczenia atrybutów pozwalają na spójna interpretację atrybutów i ich wartości przez obie strony komunikacji.

W pewnych przypadkach instytucja poświadczającą tożsamość może być nawet sam użytkownik. Dotyczy to np. sytuacji kiedy użytkownik sam tworzy konto w jakieś usłudze i wskazuje na system, który będzie poświadczał jego tożsamość (np. serwer OpenId). Usługodawca nie oczekuje żadnych istotnych atrybutów, potrzebne jest jedynie rozpoznanie użytkownika, aby udostępnić mu za każdym razem to samo konto. Taki model jest wystarczający w usługach darmowych, gdzie posiadanie przez użytkownika konta jest jedynie elementem ułatwiającym korzystanie z systemu i nie służy żadnym celom rozliczeniowym.

W przypadku usług odpłatnych, potwierdzenie, że użytkownik jest faktycznie tym za kogo się podaje jest znacznie bardziej istotne, a jeżeli usługa jest opłacana przez instytucję, to potwierdzenie uprawnienia do korzystania z usługi powinno pochodzić właśnie z tej instytucji.

W przypadku eduroam mamy wprawdzie do czynienia z usługa darmową, ale ograniczoną do zamkniętej grypy użytkowników związanych ze środowiskiem naukowo-akademickim. Uprawnienie użytkownika do korzystania z usługi musi zatem pochodzić od odpowiedniej instytucji. Dodatkowo, instytucja poświadczająca tożsamość użytkownika w eduroam, gwarantuje, że w przypadku gdyby użytkownik popełnił wykroczenie, będzie w stanie zidentyfikować go i przedstawić odpowiednim władzom dowody, które tę identyfikację potwierdzą.

4. Federacje zarządzania tożsamością

W modelu usługodawca – instytucja uwierzytelniająca, mamy tylko dwie strony i takie rozwiązanie może działać poprawnie. Ostatnio obserwuje się trend, że wielkie firmy obsługujące miliony kont (np. Google, czy Facebook) staja się instytucjami uwierzytelniającymi na powszechny użytek. To one tworzą warunki współpracy z usługodawcami i narzucają zasady gry swoim użytkownikom. Tym niemniej, od wielu lat obserwuje się wyraźną tendencję, w której instytucje o podobnym profi-

lu – np. naukowo-akademickie, skupiają się w federacje, aby uprościć kwestie formalne i techniczne. eduroam jest znowu bardzo dobrym przykładem pokazującym w jaki sposób federowanie się nie tylko ułatwia, ale w zasadzie umożliwia funkcjonowanie usługi. W eduroam instytucje deklarują chęć skorzystania z usługi swojemu lokalnemu operatorowi i od tego momentu staja się częścią globalnego systemu. Nie muszą zawierać porozumień z innymi instytucjami, z którymi de facto współpracują. Takie działanie jest możliwe dzięki przyjęciu wspólnych zasad działania usługi. Instytucja przystępująca do eduroam zobowiązuje się do przestrzegania tych zasad, przyjmując jednocześnie, że inne instytucje, również takie zobowiązanie podjęły. eduroam wprowadza nie tylko regulamin (tzw. politykę), ale również mechanizmy transportowe, zapewniające odpowiedni routing pakietów oraz odpowiednie mechanizmy bezpieczeństwa, które gwarantują, że komunikacji można ufać.

Stworzenie federacji pozwala na wprowadzenie wspólnych zasad, co do znaczenia atrybutów używanych w komunikacji uprawnień (np. w jakich atrybutach przekazuje się informację o statusie osoby, co oznaczają określenia typu student, pracownik, pracownik naukowy, osoba stowarzyszona itp.) Grupa instytucji posiadająca tego typu wspólne zasady, zdecydowanie łatwiej porozumie się z usługodawcą, który nie będzie musiał uwzględniać specyfiki każdej instytucji.

Federacja, jako instytucja, może również ułatwić proces weryfikacji usługodawców. Nie ma zakazów prawnych, aby pewne dane osobowe były przekazywane z jednej instytucji do drugiej, ale musi się to odbywać w sposób odpowiednio kontrolowany. Niezbędne jest zapewnienie, aby przekazywać tylko dane niezbędne do działania konkretnej usługi, aby usługodawca zapewniał odpowiedni poziom przetwarzania i ochrony danych i aby użytkownik miał świadomość i wpływ na to, że jego dane są przekazywane i przetwarzane. Federacja może prowadzić proces weryfikacji, ułatwiając w ten sposób indywidualnym instytucjom decyzję o współpracy z konkretnym usługodawcą. Federacja może również negocjować wspólne kontrakty, ale ten aspekt wykracza poza ramy niniejszego opracowania.

Federacja, to również uzgodnienie co do konkretnej technologii, co oznacza, że usługodawca będzie miał pewność interoperacyjności ze wszystkimi członkami federacji. Federacje prowadzą również repozytoria tzw. metadanych, a więc bezpieczne archiwa, z których można pobierać listę parametrów technicznych określających usługodawców i instytucje uwierzytelniające.

5. Przykłady usług

5.1. Dostęp do czasopism elektronicznych

Podany wcześniej przykład dostępu do czasopism elektronicznych był jedną z pierwszych usług, w których pojawiło się uwierzytelnianie federacyjne. Negocjowanie konsorcjalnego dostępu do takich usług od dawna było normą, a wiec budowa wspólnego mechanizmu uwierzytelnienia była tego naturalnym następstwem. Początkowo usługodawcy stosowali kontrolę dostępu bazującą na adresach IP, ale uprawnienie było związane z osobami a nie adresami sieciowymi, w szczególności dostęp z innych sieci (np. z domu) wymuszał stosowanie dodatkowych mechanizmów takich jak VPN czy specjalne proxy. Zastosowanie logowania federacyjnego eliminuje te wszystkie niedogodności.

5.2. Dostęp do oprogramowania

Niektóre programy dystrybucji oprogramowania dla środowisk akademickich (np. Microsoft MSDNAA) pozwalają, aby studenci zarejestrowanych uczelni mogli pobierać oprogramowanie użytkowe. Warunkiem takie dostępu jest poświadczenie, że dana osoba faktycznie jest studentem wydziału uczelni, który taki dostęp zapewnił. Takie poświadczenie może zostać dokonane w oparciu o logowanie federacyjne.

6. Modele federacji

W środowisku naukowo-akademickim wypracowano dwa modele federacji – rozproszony i scentralizowany.

W modelu rozproszonym federacja jest odpowiedzialna za ustalanie regulaminów, semantyki atrybutów, negocjacje z instytucjami wstępującymi do Federacji, określenie protokołu komunikacji,

wsparcie dla instytucji – członków Federacji. Sam proces uwierzytelnienia i autoryzacji następuje jednak bezpośrednio pomiędzy usługodawca i dostawca tożsamości.

Model scentralizowany obejmuje wszystkie funkcje modelu rozproszonego, ale dodaje centralny punkt, poprzez który przechodzi cała komunikacja. Od strony dostawcy usługi widoczny jest tylko jeden dostawca tożsamości, od strony dostawców tożsamości – cała komunikacja niezbędna w procesie uwierzytelnienie i autoryzacji pochodzi z jednego, zaufanego punktu. Model scentralizowany wprowadza szereg ułatwień technicznych, pozwala na generowanie centralnych statystyk, pozwala na przeniesienie części odpowiedzialności oraz większości ustaleń formalnych z odbiorców końcowych na operatora federacji. Koszty działania operatora federacji scentralizowanej są jednak znacząco wyższe, a członkowie federacji muszą być gotowi na scedowanie szeregu działań na operatora.

eduroam może być postrzegany jako federacja o modelu scentralizowanym. Uwierzytelnienie między partnerami jest przekazywane poprzez serwery pośredniczące i zaufanie jest budowane poprzez zaufanie między kolejnymi krokami, raczej niż między faktycznym usługodawcą i instytucja uwierzytelniającą. Plany rozwojowe eduroam idą jednak w kierunku likwidacji pośredniczącej infrastruktury serwerów i ograniczenie roli eduroam do wydawania dla serwerów instytucji, w ten sposób tworząc system całkowicie rozproszony.

W ocenie autora niniejszego dokumentu, najwłaściwszym rozwiązaniem dla polskiego środowiska naukowo-akademickiego jest federacja rozproszona.

7. Konfederacje

W tym co zostało napisane powyżej, eduroam był przedstawiany jako rodzaj usługi federacyjnej, a zatem ograniczonej do jednej federacji (jednego kraju). W rzeczywistości eduroam jest usługą międzynarodową tworzona poprzez umowę między federacjami krajowymi. Mamy tu zatem do czynienia z federacja federacji, czyli konfederacją.

Konfederacja działa w oparciu o własny regulamin, który określa minimalne poziomy, które muszą być zapewnione przez regulaminy członkowskich federacji. Przystąpienie do konfederacji jest zadaniem Operatora Federacji i do jego obowiązków należy dbanie o synchronizację zapisów pomiędzy regulaminem federacji a regulaminem konfederacji.

eduroam jest pierwszą konfederacją o szerokim zasięgu. W obszarze federacji opartych o SAML podobna rolę ma odgrywać eduGAIN.

To co odróżnia obecny eduroam od tego co jest planowane w ramach eduGAIN, to pełna centralizacja eduroam. W eduGAIN centralne jest jedynie repozytorium metadanych, natomiast połączenia między stronami odbywają się jak w ramach federacji rozproszonych. W eduroam komunikacja jest przesyłana poprzez statyczna sieć serwerów pośredniczących; ten model będzie jednak zastępowany systemem rozproszonym, zbliżając się w ten sposób do koncepcji eduGAIN.

8. Porównanie technologii eduroam oraz federacji opartych o OASIS SAML

eduroam na swoim obecnym poziomie rozwoju jest oparty w całości na protokole RADIUS. Ostatnio wprowadza się odmianę tego protokołu – RADIUS over TLS, ale zmiana w tym przypadku jest w zasadzie kosmetyczna, tzn. wyłącznie zastępuje warstwę transportowa UDP szyfrowanym transportem na protokole TCP. Ponieważ RADIUS over TLS stosuje certyfikaty, to otwiera możliwość na uwierzytelnianie połączeń międzyserwerowych. Oczekuje się, że ta ważna cecha będzie wykorzystana w kolejnych fazach eduroam i odniesiemy się do niej nieco później.

W czasie uwierzytelnienia w protokole RADIUS, pomiędzy serwerem instytucji udostępniającej sieć a serwerem instytucji uwierzytelniającej wymieniane są (za pośrednictwem infrastruktury serwerów eduroam) pakiety czterech typów: Access-Request, Access-Challenge, Access-Accept, Access-Reject.

Model SAML jest koncepcyjnie podobny, z tym, że wraz z potwierdzeniem uwierzytelnienia przekazywany jest zestaw atrybutów dotyczących konkretnego użytkownika. Zestaw przekazywanych atrybutów może być ustalany w ramach uzgodnień między współpracującymi stronami, ale typowo powinien być określony w opisie usługi (tzw. metadanych usługodawcy). Usługodawca powinien po-

dać listę atrybutów wymaganych i pożądanych (opcjonalnych). Instytucja potwierdzająca tożsamość użytkownika przekazuje zestaw atrybutów wynikający z lokalnej polityki udostępniania danych oraz z uzgodnień z konkretnym usługodawcą. Zestaw przekazywanych atrybutów powinien zawierać atrybuty wymagane przez konkretnego usługodawcę, jeżeli zestaw atrybutów jest niekompletny, to najprawdopodobniej usługa będzie niedostępna.

Jak już wcześniej wspomniano, pomiędzy stronami musi funkcjonować mechanizm zaufania, tak by z jednej strony, instytucja uwierzytelniająca miała pewność, że udostępnia dane o użytkowniku wyłącznie właściwemu odbiorcy, a z drugiej, by usługodawca miał pewność, że udostępnia swoją usługę wyłącznie tym, którzy mają do niej uprawnienie.

A modelu federacji SAML zaufanie opiera się na wspólnej zaufanej stronie, jaką jest Federacja. Federacja tworzy zbiór metadanych i podpisuje go cyfrowo w sposób, który może być zweryfikowany przez wszystkich członków Federacji. Opisy zawarte z zbiorze metadanych zawierają parametry niezbędne do zestawienia połączeń między stronami oraz certyfikaty, które pozwalają na potwierdzenie autentyczności stron połączenia.

Techniczna realizacja wymiany danych w modelu SAML jest bardziej skomplikowana niż w przypadku modelu eduroam. W najprostszej sytuacji nośnikiem informacji wymienianych między stronami jest przeglądarka użytkownika, która jest przekierowywana pomiędzy stronami WWW usługodawcy i instytucji uwierzytelniającej. To właśnie przeglądarka poprzez skomplikowany system przekierowań oraz ustawienia sesyjnych ciasteczek jest zasadniczym medium transmisyjnym danych uwierzytelnienia. W bardziej skomplikowanych modelach pojawia się dodatkowa wymiana danych bezpośrednio między usługodawcą a instytucją uwierzytelniającą (tzw. backchannel). Regularne pobieranie pliku metadanych federacji jest podstawą zaufania pomiędzy stronami. W przeciwieństwie do technologii RADIUS stosowanej w eduroam, w przypadku zdecentralizowanej federacji SAML nie ma żadnej transmisji danych poprzez elementy Federacji.

Model bezpieczeństwa polegający na zaufaniu do jednej instytucji – Federacji poprzez publikowaną przez tę stronę informację identyfikującą strony, może być zastosowany również w modelu eduroam. Zamiast jednego centralnego repozytorium metadanych, w eduroam przygotowano rozwiązanie polegające na wystawianiu specyficznych certyfikatów – zawierających odniesienie do polityki eduroam. Serwery eduroam mogą się odnajdować, albo za pośrednictwem dotychczasowej, statycznej hierarchii eduroam (która jest jednocześnie strukturą zapewniającą zaufanie), albo korzystając z wpisów do bazy DNS. W tym drugim przypadku serwer instytucji udostępniającej sieć korzysta z nazwy domenowej zawartej w identyfikatorze użytkownika i na jej podstawie odszukuje w DNS właściwy serwer uwierzytelniający. Nawiązując połączenie z odszukanym serwerem musi uzyskać potwierdzenie, że serwer rzeczywiście należy do instytucji stowarzyszonej w eduroam. To potwierdzenie następuje w wyniku sprawdzenia certyfikatu, którym przedstawia się serwer. Akceptowane są wyłącznie certyfikaty pochodzące z jednego z akredytowanych urzędów certyfikacyjnych, a dodatkowo certyfikaty muszą zawierać specyficzny atrybut zarezerwowany dla usługi eduroam. W opisanym modelu rolę centralnego, zaufanego repozytorium metadanych pełni zaufane repozytorium akredytowanych urzędów certyfikacyjnych.

O ile RADIUS jest typowym protokołem sieciowym, to SAML jest standardem wymiany informacji nałożonym na protokoły wyższej warstwy, np. html. SAML jest nie tylko podstawą uwierzytelnienia, ale również autoryzacji, tzn. kontroli uprawnień. Oczywiście dostawca usługi może tworzyć własny system kontroli uprawnień bazując na stałym pseudoidentyfikatorze użytkownika, ale w większości przypadków dostawca usługi nie ma informacji, które pozwoliłyby na przypisanie użytkownika do konkretnej polityki uprawnień. W praktyce jedyną metodą jest przekazanie takich informacji przez instytucję uwierzytelniającą w postaci atrybutów SAML. Ponieważ różni usługodawcy mogą mieć różne polityki autoryzacji, a zatem różne zapotrzebowanie na dostarczane atrybuty, to na instytucji uwierzytelniającej leży dodatkowy obowiązek analizowania zasadności przekazywania konkretnych atrybutów, ponieważ często mogą one być traktowanie jako dane osobowe. Federacja może unifikować standardy, dokonywać analizy usługodawców i dostarczać swoim członkom informacji, na których mogą opierać decyzje o udostępnianiu danych, należy jednak zwrócić uwagę, że jest to zagadnienie dużo bardziej złożone niż w przypadku eduroam.

9. Federacja w Polsce

9.1. Usługa eduroam jako podstawa powstania polskiej federacji

Tak, jak wcześniej wspomniano, sytuacja w Polsce jest inna niż w większości krajów europejskich, gdzie federacje zarządzania tożsamością funkcjonują od wielu lat i eduroam pojawił się wyraźnie później.

Jednym z najważniejszych czynników warunkujących powstanie federacji jest powszechność zarządzania kontami użytkowników w jednostkach macierzystych. W Polsce takiej powszechności nadal nie ma, ale wdrażanie eduroam zdecydowanie pomaga.

Systemy uwierzytelniające działające na potrzeby eduroam, z reguły są powiązane z jakąś bazą danych użytkowników. Uruchomienie mechanizmów instytucji uwierzytelniającej na potrzeby logowania federacyjnego jest stosunkowo proste. Niezbędne może się okazać wprowadzenie modyfikacji do lokalnej bazy danych, tak by zawierała ona informacje o uprawnieniach do konkretnych usług.

Bardzo ważne jest to, że wokół eduroam zbudowana została struktura organizacyjna, która może się stać podstawą struktury zaufania polskiej federacji. Wydaje się, że docelowo najwłaściwsze jest powielenie podejścia szwedzkiej federacji, w której eduroam jest po prostu jedna z usług federacji, a regulamin eduroam jest częścią regulaminu federacji.

Usługi WWW stowarzyszone z eduroam, takie jak dostęp do portalu administracyjnego, powinny zostać wyposażone w mechanizm logowania federacyjnego. Taki system z jednej strony ułatwi dostęp do portalu, a z drugiej będzie pierwszą centralną usługą PIONIER-a, która z mechanizmów federacyjnych korzysta.

9.2. Rola federacyjnego zarządzania tożsamością w usługach projektu PLATON

Projekt PLATON składa się z pięciu usług, z których cztery z całą pewnością wymagają uwierzytelnienie użytkownika. Są to:

U1 – wideokonferencje

U2 – eduroam

U3 – usługi kampusowe

U4 – archiwizacja

Uwierzytelnianie w U5 – telewizji interaktywnej może być niezbędne w sytuacjach, gdy dystrybuowana treść nie będzie dostępna powszechnie.

Na obecnym stopniu wdrożenia, usługi korzystają z niezależnych mechanizmów uwierzytelniania. Z wyjątkiem U2, te mechanizmy wymagają tworzenia kont bezpośrednio w usłudze. Przewiduje się, że wraz ze wzrostem zainteresowania samymi usługami, jak i wzrostem popularności mechanizmów federacyjnych w Polsce, usługi PLATON-a również wdrożą model logowania federacyjnego.

9.3. Model polskiej federacji zarządzania tożsamością

Federacja zarządzania tożsamością powinna bazować na doświadczeniach polskiego eduroam, ale również europejskich federacji SAML. Konsorcjalny charakter organizowania dostępu do usług sieciowych w ramach polskiego środowiska nauki, wskazuje na celowość rozpraszania systemu zarządzania poprzez tworzenie reprezentacji usługi w regionach. W taki sposób została zbudowana polska usługa eduroam. Partnerzy konsorcjum nie tylko są usługodawcami eduroam względem swoich abonentów, ale również tworzą istotny element infrastruktury uwierzytelniającej poprzez utrzymanie serwerów regionalnych. W technologii SAML serwery pośredniczące nie występują, a dodatkowo technologia SAML jest uważana za trudną. Wynika stąd, że nie ma potrzeby budowania jakiejkolwiek infrastruktury technicznej w regionach, natomiast regionalne wsparcie techniczne w pewnych przypadkach może być niedostępne.

Biorąc pod uwagę te wszystkie okoliczności najwłaściwszy wydaje się być model mieszany. Polski Operator Federacji zapewnia infrastrukturę techniczną (serwer metadanych) i wsparcie dla instytucji stowarzyszonych w Federacji. Operator centralny działa bezpośrednio lub za pośrednictwem operatorów regionalnych. Zasady działania w stosunku do abonentów danego członka konsorcjum

PIONIER są uzgadniane między operatorem centralnym a danych członkiem Konsorcjum PIONIER. Należy oczekiwać, że w fazie początkowej przeważać będzie bezpośrednia obsługa przez operatra centralnego, a w miarę rozrostu Federacji, niektórzy członkowie konsorcjum będą przejmowali obsługę swoich abonentów.

Materiały towarzyszące

[1] *eduroam Service Definition*, http://www.eduroam.pl/regulamin/GN3-12-192_eduroam-policy-service-definition_ver28_26072012.pdf
[2] *Polski regulamin eduroam*, http://www.eduroam.pl/regulamin/
[3] *Koncepcja wdrożenia usługi eduroam w sieci Pionier*, T. Wolniewicz, M. Górecka-Wolniewicz, Z. Ołtuszyk http://www.eduroam.pl/Dokumentacja/koncepcja_polska-1.0.pdf
[4] *Zabezpieczenie przez zmianą adresu IP przez Użytkownika,* A. Angowski, http://www.eduroam.pl/Dokumentacja/eduroam_zapobieganie_zmianie_IP.pdf
[5] *Chargeable User Identity*, F. Adrangi, A. Lior, J. Korhonen, J. Loughney, RFC 4372
[6] *Instalacja i konfiguracja serwera FreeRADIUS v.2*, M. Górecka-Wolniewicz, http://www.eduroam.pl/Dokumentacja/freeradiusv2-09-2012.pdf