IV Konferencja i3: internet - infrastruktury - innowacje

Wszechobecny Internet - X lat Polskiego Internetu Optycznego PIONIER

Poznań 15 - 19 kwietnia 2013

Federacja zarządzania tożsamością PIONIER.Id

Tomasz Wolniewicz
Maja Górecka-Wolniewicz

Uniwersytet Mikołaja Kopernika w Toruniu

Federacje zarządzania tożsamością

- Pomysł pochodzący i rozwijany przez środowiska akademickie całego świata od roku 2000
- Zarządzanie dostępem do usług w oparciu o uprawnienia poświadczane przez instytucję macierzystą użytkownika
- W ostatnich latach idea logowania federacyjnego pojawiła się w wydaniu Google, Facebook, LinkedIn, Twitter, Microsoft itp.
- Zasady logowania federacyjnego zostały wdrożone również w polskim systemie ePUAP
- eduroam jest pochodną idei federacji

Logowanie federacyjne w działaniu

- Podstawowe elementy
  - Konto użytkownika w instytucji macierzystej
  - Przekierowanie logowania z portalu usługi do portalu instytucji macierzystej
  - Zalogowanie użytkownika w instytucji macierzystej
  - Przekazanie potwierdzenia i opcjonalne przekazanie dodatkowych atrybutów (np. przynależność do grupy, adres e-mail, imię nazwisko)

- Zalety stosowania logowania federacyjnego
  - Dostawca usługi nie musi utrzymywać kont użytkowników
  - Użytkownik nie musi pamiętać danych do wielu kont
  - Weryfikacja uprawnień może być scedowana na instytucję macierzystą

Przykład

https://foodl.org

Logowanie do usług WWW (1)

- Przykłady
  - Dostęp do portali zarządzania usługami
  - Dostęp do czasopism elektronicznych
  - Dostęp do portali współpracy – np. Wideokonferencje, Foodle
  - Rekrutacja studentów w programie MOST
  - Pobieranie oprogramowanie MS w programach typu IT-Academy

Logowanie do usług WWW (2)

- Zasada działania
  - dwie strony – dostawca usługi i instytucja uwierzytelniająca
  - zasada wzajemnego zaufania oparta o podpisane umowy dwustronne lub współpraca z zaufaną stroną
  - dostawca usługi uwierzytelnia użytkownika przekierowując go na jego domową stronę logowania
  - instytucja uwierzytelniająca potwierdza uwierzytelnienie i odsyła uzgodnione atrybuty dodatkowe (autoryzacja)
  - jedno konto w instytucja uwierzytelniającej daje dostęp do wszystkich usług
  - dostawca usługi nie musi znać rzeczywistej tożsamości użytkownika (ochrona danych)

Logowanie federacyjne a ochrona danych osobowych (1)

- Problem ochrony danych osobowych jest bardzo ważny i administratorzy powinni przykładać do niego należytą wagę
- Różne poziomy problemu
  - Wyłącznie uwierzytelnienie
    - Sytuacja podobna jak przy dostępie do czasopism elektronicznych po IP
    - Użytkownik loguje się w instytucji macierzystej
    - Instytucja macierzysta zwraca informację, że zalogowanie przebiegło poprawnie i dodaje tymczasowy token ważny przez jedną sesję
    - Nie są przekazywane żadne dane osobowe

Logowanie federacyjne a ochrona danych osobowych (2)

- Uwierzytelnienie i pseudoindentyfikator
  - Sytuacja jak wyżej, z tym że dodatkowo przekazywany jest stały token użytkownika
  - Token jest taki sam dla danego użytkownika logującego się do danej usługi
  - Różni usługodawcy odbierają różne tokeny dla tego samego użytkownika
  - Stały token pozwala na stworzenie przez dostawcę profilu użytkownika
  - Dostawca nie zna żadnych danych pozwalających na identyfikację użytkownika bez kontaktowania się z instytucją macierzystą
  - Taki stały token w niektórych krajach jest uważany za element danych osobowych w innych nie

Logowanie federacyjne a ochrona danych osobowych (3)

- Dodatkowe dane osobowe – email, imię i nazwisko
  - Dane mogą być potrzebne, np. do przesyłania komunikatów z usługi
  - Decyzja o tym czy dane powinny być przekazywane, czy nie zależy do instytucji macierzystej
  - Instytucja macierzysta może uruchomić formularz potwierdzania zgody przez samego użytkownika
  - Brak zgody na udostępnienie danych może mieć skute w postaci braku dostępu do usługi
- Informacja o tym, jakie atrybuty są wymagane lub opcjonalnie używane przez usługę jest zapisana w tzw. metadanych usługi
- Administratorzy instytucji macierzystej mogą konfigurować zestaw udostępnianych danych dla każdej usługi

Rola Federacji

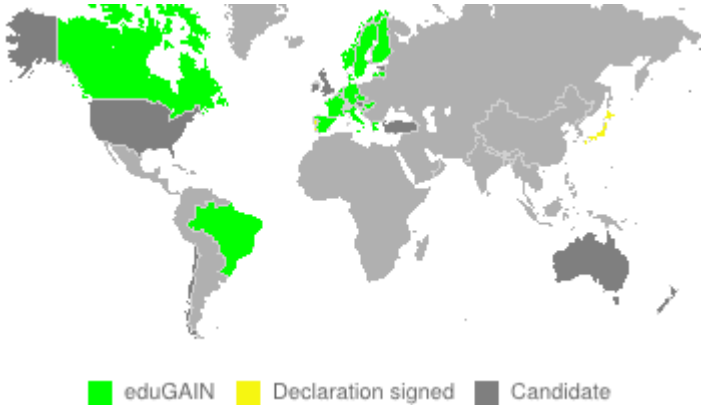
- Uzgadnianie regulaminów współpracy
- Uzgadnianie słowników atrybutów
  - np. komu przysługuje atrybut „pracownik” lub „student”
- Utrzymywanie punktu wymiany informacji o usługach i instytucjach uwierzytelniających
- Przygotowywanie wstępnej informacji o usługodawcach i ich wymaganiach, wiarygodności itp.
- Pozyskiwanie usługodawców
- Działanie w roli „trzeciej zaufanej strony”
- Pośredniczenie w zawieraniu usług dwustronnych
- Współpraca międzynarodowa

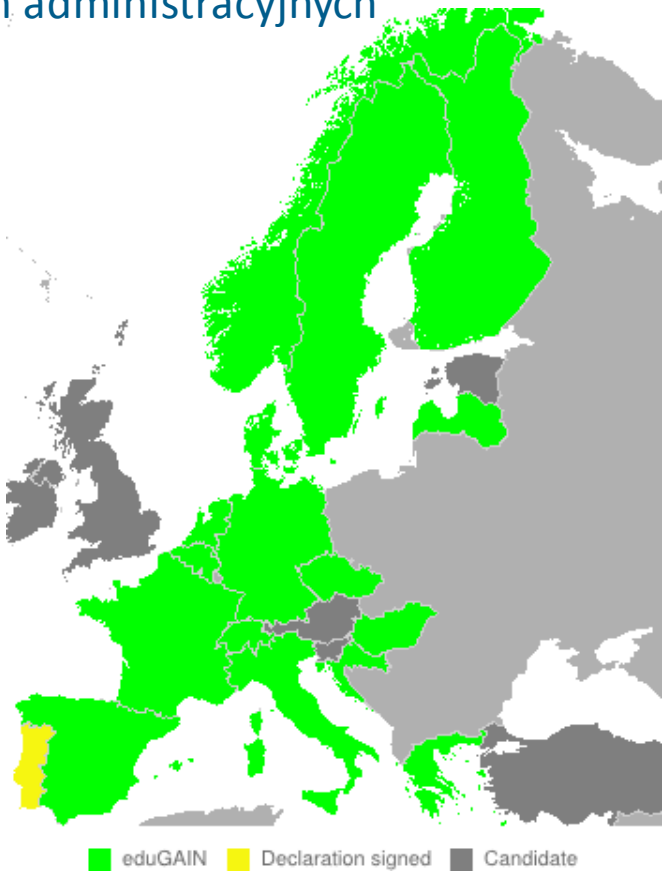
Federacje na świecie (przykłady)

Kraj	Liczna instytucji uwierzytelniających	Liczba usług
USA	292	1079
W. Brytania	726	798
Szwajcaria	52	674
Niemcy	104	119
Czechy	24	106
Francja	175	375
Australia	34	58

Konfederacje

- Współpraca federacji w celu zmniejszenia obciążeń administracyjnych
- Ułatwienie pracy projektów międzynarodowych
- Uzgadnianie słowników i terminologii
- REFEDS: https://refeds.terena.org/
- eduGAIN http://www.edugain.org





Polska federacja PIONIER.Id

- Regulamin federacji oczekuje na zatwierdzenie przez Konsorcjum PIONIER
- Partnerzy Federacji - usługodawcy
- Członkowie Federacji – instytucje akademickie poświadczające tożsamość własnych użytkowników
  - Członkowie mogą też występować w roli usługodawców
- Przystąpienie do federacji – złożenie deklaracji członkowskiej podpisanej przez upoważnionego reprezentanta instytucji
- Schemat Federacji
  - Operator Federacji (PCSS plus ew. instytucje współpracujące)
  - Operatorzy Regionalni
    - Operatorzy naukowych sieci MAN **mogą** pełnić funkcję operatorów regionalnych, tzn. przyjmować deklaracje, świadczyć lokalne wsparcie techniczne
  - Partnerzy
  - Członkowie

Przygotowanie polskich instytucji do współpracy w ramach Federacji

- Uniwersytet Mikołaja Kopernika i PCSS są członkami technicznej federacji współpracującej z niektórymi usługodawcami
- Uczelnie współpracujące w inicjatywie IRK-MOST mają gotową infrastrukturę techniczną i przystąpienie do Federacji będzie tylko formalnością
  - Uniwersytet Adama Mickiewicz
  - Uniwersytet Jagielloński
  - Uniwersytet Mikołaja Kopernika
  - Uniwersytet Opolski
  - Uniwersytet w Białymstoku
  - Uniwersytet Śląski
  - Uniwersytet Warszawski
- Instytucje współpracujące z eduroam mogą łatwo dostosować swoją infrastrukturę i w efekcie przystąpić do federacji

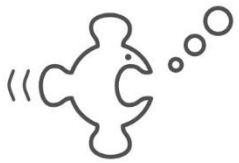
Przykłady usługodawców

- https://foodl.org/
- https://atlases.muni.cz/
- https://cat.eduroam.org/
- https://tnc2013.terena.org/
- https://most.uka.uw.edu.pl/
- http://karo.umk.pl
- http://www.sciencedirect.com/
- https://applications.eumedgrid.eu/
- https://earthserver-sg.consorzio-cometa.it
- https://filesender.funet.fi

Włączenie nowej instytucji do federacji PIONIER.Id - strona techniczna

- Instytucja musi realizować funkcję dostawcy tożsamości (SAML Identity Provider)
- Sporo uczelni w Polsce korzysta obecnie z baz danych, np. LDAP, do przechowywania danych dotyczących użytkowników
- Uczelnie aktywne w usłudze eduroam (http://eduroam.pl) korzystają z bazy użytkowników oraz uwierzytelniania RADIUS – te narzędzia mogą zostać użyte w logowaniu federacyjnym
- Dostawca tożsamości spełnia dwie funkcje:
  - Uwierzytelnia użytkownika (loguje)
  - Przekazuje do aplikacji współpracującej z IdP atrybuty dotyczące danego użytkownika, na podstawie których można podjąć decyzję o nadaniu uprawnień (autoryzacja)

Oprogramowanie używane do realizacji logowania federacyjnego



- simplesamlphp http://simplesamlphp.org/
  - aplikacja napisana w języku PHP
  - możliwość użycia jednego z wielu źródeł bazy danych użytkowników:
    - LDAP (jedna baza lub wiele źródeł danych LDAP),
    - SQL,
    - CAS (Central Authentication Service),
    - uwierzytelnianie RADIUS,
    - OpenID
    - Facebook
    - Twitter

Oprogramowanie używane do realizacji logowania federacyjnego

- Użycie simplesamlphp jako IdP
  - jeżeli modułem uwierzytelniającym jest CAS, to źródłem danych służącym do pobrania atrybutów użytkownika jest LDAP
  - jeżeli chcemy użyć RADIUS-a, to serwer RADIUS powinien zwracać w odpowiedzi atrybuty użytkownika (są one przekazywane przez specjalne atrybuty RADIUS)
  - jest możliwe tworzenie własnych modułów uwierzytelniania
- simplesamlphp jako SP
  - SP musi deklarować z jakich atrybutów korzysta
  - SP współpracuje z dostawcami tożsamości (IdPs), których metadane są zdefiniowane dla danego SP

Oprogramowanie używane do realizacji logowania federacyjnego

- Shibboleth http://shibboleth.net/ 

  - Oprogramowanie pełniące funkcje logowania federacyjnego
  - Oddzielne paczki dla Shibboleth IdP i Shibboleth SP
  - Shibboleth IdP – aplikacja w Javie może korzystać z konteneru Apache Tomcat / Jetty / JBoss Tomcat
    - dużo modułów uwierzytelniania: LDAP, CAS, SQL
  - Shibboleth SP – moduł mod_shib.so dla Apache'a oraz niezależna aplikacja shibd (Shibboleth deamon)

IV Konferencja i3: internet - infrastruktury - innowacje

Wszechobecny Internet
X lat Polskiego Internetu Optycznego

PIONIER

Poznań 15 - 19 kwietnia 2013

http://www.i3conference.net/

KONSORCJUM PIONIER

PIONIER

ORGANIZATORZY

POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO-SIECIOWE

POZNAN