Federacyjne zarządzanie tożsamością

Tomasz Wolniewicz
Uczelniane Centrum informatyczne
Uniwersytet Mikołaja Kopernika w Toruniu

Korzystanie z usług zewnętrznych (typowy scenariusz)

- czasopisma elektroniczne
  - kontrola dostępu po IP
  - rozszerzenia poprzez proxy lub VPN
- wirtualne organizacje (np. projekty badawcze)
  - dedykowane systemy kont
- mobilność studentów (proces boloński)
  - konieczność tworzenia kont dla studentów obcych
- wspólne platformy e-learningowe
  - ???

Problemy modelu tradycyjnego

- Czasopisma elektroniczne
  - skomplikowane administrowanie
    - konieczność określania zakresu uprawnionych IP)
  - trudny dostęp spoza uczelni
    - wymaga proxy lub VPN-a
    - zaburza zbieranie statystyk
  - brak możliwości tworzenia specyficznych licencji
    - np. dostępność pewnych funkcji tylko dla określonej grupy osób)
- Wirtualne organizacje
  - utrudnione zarządzanie uprawnieniami
    - na ogół wymaga przepływu informacji poza systemem
  - konieczność tworzenia systemów kont
  - przetwarzanie danych osobowych
- Mobilność studentów i platformy e-learningowe
  - konieczność przekazywania dokumentów
    - instytucja macierzysta deleguje studenta
  - konieczność tworzenia kont
    - student musi mieć konto (w celu uwierzytelnienia, dostępu do Internetu – np. w DS.)

Model dostępu do usługi poprzez zdalne uwierzytelnianie i autoryzację

- Usługodawca (Service Provider)
  - dysponent zasobu np. portalu WWW
- Instytucja uwierzytelniająca (Identity Provider)
  - instytucja, która „zna” użytkownika i może za niego ręczyć, może nadawać uprawnienia
- Model korzystania z usługi
  - *użytkownik* – mam uprawnienie do zasobu i chcę z niego skorzystać
  - *usługodawca* – kto może to potwierdzić?
  - *użytkownik* – potwierdzić może moja instytucja X
  - *usługodawca* – zaloguj się w swojej instytucji, a ona wyśle potwierdzenie
  - *inst. uwierz.* – potwierdzam poprawność tożsamości i przekazuję identyfikator użytkownika (12cb23a8901287daf)
  - *usługodawca* – czy użytkownik 12cb23a8901287daf to pracownik, czy student?
  - *inst. uwierz.* - student
  - *usługodawca* – otwiera dostęp do usługi

Wszystkie problemy rozwiązane !!!

- Czasopisma elektroniczne
  - logowanie poprzez własną instytucję
  - dostęp z dowolnego miejsca
  - możliwość tworzenia własnego profilu
  - anonimowość względem usługodawcy
  - możliwość ograniczania usługi ze względu na grupę użytkowników
- Wirtualne organizacje
  - logowanie poprzez własną instytucję
  - możliwość zarządzania uprawnieniami poprzez instytucję własną (ale zarządzenie na poziomie WO jest nadal możliwe)
  - możliwość uniknięcia przetwarzania danych osobowych przez WO
- Mobilność studentów i platformy e-learningowe
  - brak konieczności tworzenia kont na potrzeby uwierzytelnienia
  - możliwość zautomatyzowania procesu kierowania studenta do innej uczelni
  - możliwość automatyzacji procesu przekazywania dokumentacji

No, może niezupełnie….

- Wiarygodność instytucji uwierzytelniającej
  - usługodawca musi mieć pewność, że otrzymał potwierdzenie od instytucji, z którą podpisał umowę
- Ochrona danych użytkownika
  - instytucja uwierzytelniająca nie może przekazać danych na temat użytkownika każdemu, kto o nie poprosi
  - użytkownik powinien mieć świadomość jakie dane są komu przekazywane
  - identyfikator użytkownika nie powinien zdradzać jego tożsamości i nie powinien się powtarzać przy dostępie do różnych usługodawców
- Wspólny język
  - protokół
  - uzgodnienie atrybutów i ich znaczenia

Federacja

- Umowa instytucji w sprawie stosowania wspólnych standardów
  - protokół komunikacyjny
  - atrybuty i ich znaczenie
  - wiarygodność
- Udzielenie delegacji w sprawie uzgodnień technicznych z usługodawcami
  - federacja przedstawia założenia techniczne i formalne
  - federacja może negocjować warunki finansowe, ale nie jest to niezbędne (może być poza obszarem działania federacji)
- Prowadzenie katalogu instytucji uwierzytelniających i zaufanych usługodawców (metadane)

Korzyści z udziału w federacji

- Uproszczenie procedur zawierania umów z usługodawcami
- Możliwość stosowania systemów Single-Sign-On w odniesieniu do wielu usługodawców
- Możliwość tworzenia wspólnych systemów informatycznych

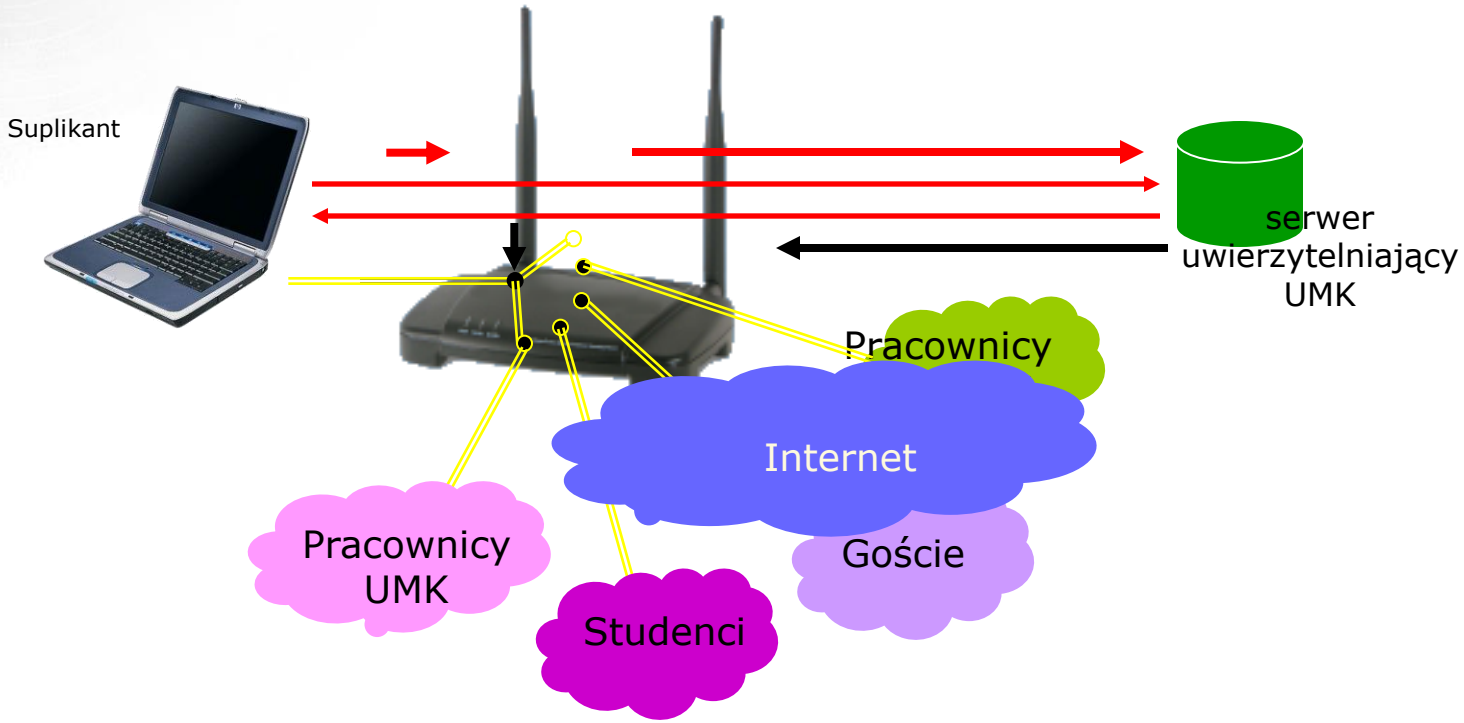
Mobilność studenta *(model przykładowej implementacji)*

- Uczelnia macierzysta X deleguje studenta do uczelni Y
  - w USOS wpisywane są niezbędne dane
    - okres na jaki student jest delegowany
    - parametry uczelni Y
    - wymagania
- Student pojawia się w uczelni Y
  - loguje się do systemu uczelni Y wskazując, ze pochodzi z uczelni X
  - system Y prosi X o potwierdzenie delegacji i okresu ważności
  - po potwierdzeniu, zakładane jest konto lokalne, działające w oparciu o uwierzytelnienie w uczelni macierzystej
  - student może korzystać z niektórych uwierzytelnionych systemów w Y
    - dostęp do sieci
    - biblioteka
    - czasopisma elektroniczne
- Dziekanat Y
  - ma już w swoim systemie podstawowe dane studenta
  - pobiera z X niezbędne dane dodatkowe
  - ustawia parametry przypisania do własnego toku studiów

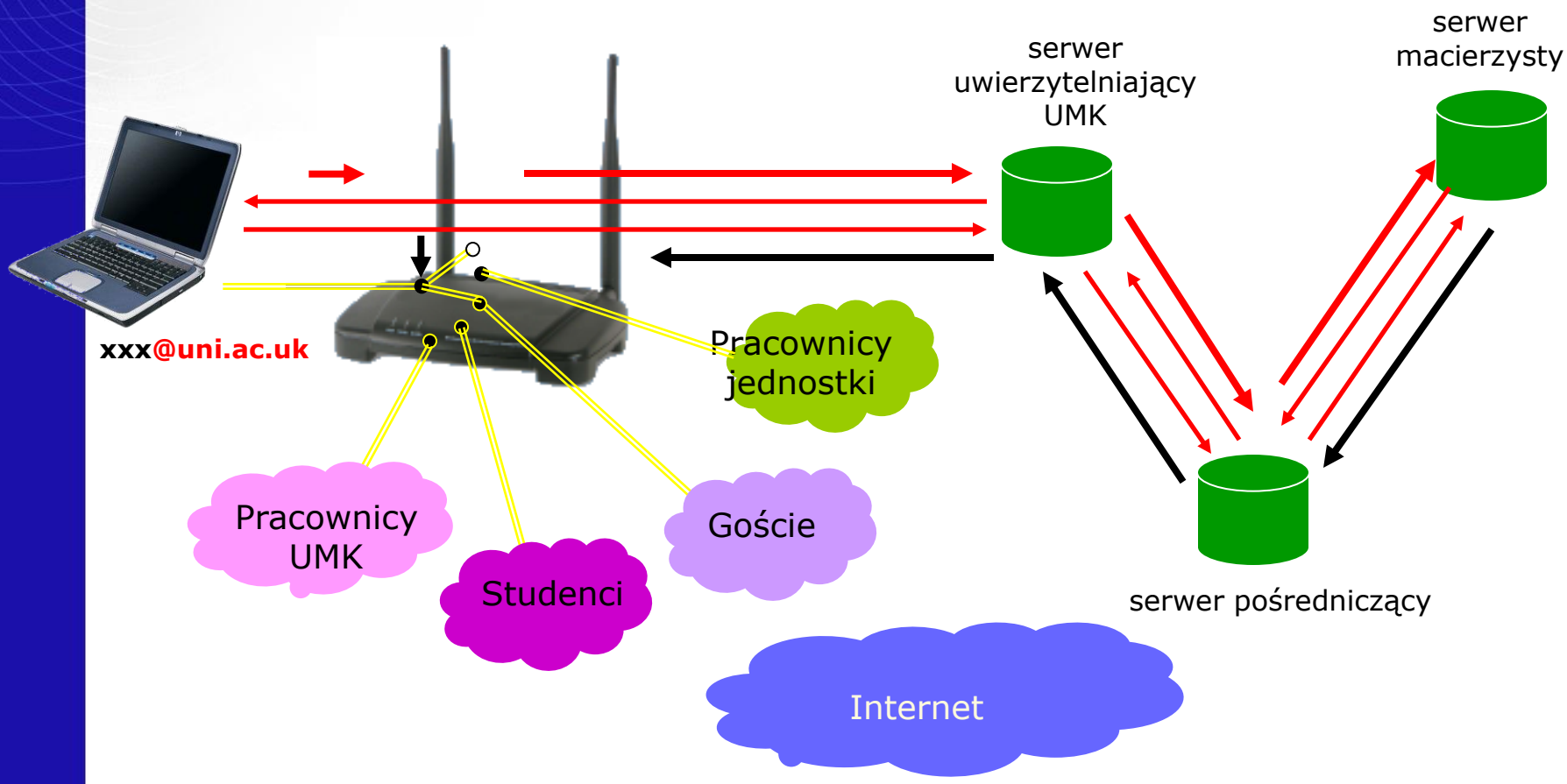
eduroam jako przykład federacji

- eduroam pozwala na wzajemne umożliwianie dostępu do sieci pracownikom i studentom
- instytucja macierzysta „odpowiada” za swojego pracownika, studenta
  - odnotowywane są uwierzytelnienia
  - przechowywane są dane pozwalające na zidentyfikowanie użytkownika
- ochrona instytucji udostępniającej sieć
  - instytucja nie zna danych osobowych gości
  - w przypadku problemów może wskazać informacje, które następnie (przy współpracy z instytucja macierzystą) mogą do prowadzić do wskazania winnego
- formalności
  - instytucje podpisują zobowiązania do przestrzegania regulaminu
  - usługa jest świadczona w sieci PIONIER bez dodatkowych opłat
- implementacja
  - stosuje się mechanizmy związane z 802.1x – nietypowe jak dla federacji
  - uwarunkowania formalne są typowe dla federacji

dostęp do sieci w oparciu o 802.1x *(użytkownik lokalny)*



dostęp do sieci *(gość eduroam)*



Federacje środowisk naukowo-akademickich na świecie

- Federacje istnieją w zdecydowanej większości krajów Unii, w USA, Kanadzie, Australii
- Istnienie federacji może być uważane za wyznacznik informatyzacji obszaru nauki i szkolnictwa wyższego
- Z reguły federacje działają w oparcie o finansowanie rządowe
- Na ogół operatorem federacji jest instytucja odpowiedzialna również za utrzymanie krajowej naukowo-akademickiej sieci informatycznej
- Konieczność tworzenia federacji (nie tylko w środowisku naukowo-akademickim) jest szeroko uznawana
  - tematyka konferencji TERENA i EUNIS (w tym wazny referat J-M. Lowendahla z Gartner. Inc.)
  - projekt STORK - http://www.eid-stork.eu/

Federacje na świecie *(kilka wybranych przykładów)*

- InCommon - http://www.incommonfederation.org/
  - Federacja w USA stworzona na potrzeby szkolnictwa wyższego i otwarta dla wszystkich instytucji uznawanych przez Departament Edukacji
  - płatne członkostwo
  - 113 instytucji członkowskich (z zakresu Hi Ed)
  - 6 instytucji naukowych
  - 41 „sponsored partners” (w tym Apple - iTunes, EBSCO, Elsevier, Microsoft)
- UK Access Management Federation for Education and Research - http://www.ukfederation.org.uk/
  - Federacja prowadzona przez JANET
- SWITCHaai Federation - http://www.switch.ch/aai/about/federation/
  - Szwajcarska federacja prowadzona przez SWITCH
  - duża aktywność w rozwijaniu oprogramowania Shibboleth i w działaniach międzynarodowych
- Kraje skandynawskie
  - FEIDE - http://feide.no (Norwegia - UNINET)
  - DK-AAI, WAYF - https://www.wayf.dk (Dania)
  - HAKA - http://www.csc.fi/english/institutions/haka (Finlandia - CSC)
  - SWAMID - http://www.swamid.se (Szwecja)

Konfederacja, czyli jeden krok dalej

- Federacje są (typowo) zawiązywanie w obrębie jednego kraju
- Często sensowne jest poszerzenie obszaru działania usług
  - eduroam
  - proces boloński
- Federacje mogą współpracować pod warunkiem wypracowania wspólnej platformy
  - protokoły
  - atrybuty i znaczenie
  - zgodne ustalenia formalne
- Działania konfederacyjne
  - GEANT3 – eduroam, eduGAIN, koordynacja federacji, koordynacja PKI
  - TERENA REFEDs - http://www.terena.org/activities/refeds/
  - Kalmar Union - http://rnd.feide.no/content/kalmar-union - federacja krajów skandynaskich

Polskie doświadczenia

- eduroam
  - pierwsza udana federacja w Polsce
- UMK
  - od wielu lat współpracuje w ramach działań TERENY
  - pierwsze instalacje CAS-a
  - wprowadzenie CAS-a do usług USOS-owych
  - pilotowa instalacja Shibboletha
  - koordynacja eduroam
  - pilotowa instalacja eduGAIN
- UW
  - instalacje CAS-a
  - pilotowa instalacja Shibboletha
  - czasopisma w ICM ???
- PCSS
  - operator sieci PIONIER i usług w tej sieci
  - partner w GEANT3
  - wbudowanie Shibboletha do oprogramowania dLibra

Co z federacją w Polsce?

- Ważni gracze
  - MNiSW
    - powinno być motorem działań *(ale nie jest i pewnie nie będzie)*
  - Konsorcjum PIONIER
    - zarządza eduroam
    - przygotowuje działania w zakresie PKI
    - uruchamia usługi w projekcie PLATON, gdzie federacyjny model zarządzania tożsamością powinien być bardzo istotny
    - problemem jest ograniczony zasięg działania
  - MUCI
    - brak (na razie) wspólnych usług (z wyjątkiem Biura Karier)
    - ograniczony zasięg działania
  - konsorcja dostępu do czasopism elektronicznych
    - organizowanie na potrzeby konkretnej usługi
    - brak wiedzy informatycznej
    - brak struktury formalnej
  - PCSS
    - operator sieci PIONIER
    - twórca dLibry
  - ICM
    - dostawca czasopism elektronicznych

Federacja ma koszty działania

- Utrzymanie metadanych
- Utrzymanie regulaminów itp.
- Kwestie członkostwa w federacji
- Uzgodnienia z dostawcami usług

- InCommon – ma składki
- Niektóre federacje europejskie działają w oparciu o projekty rządowe
- Niektóre federacje biorą pieniądze od dostawców usług