

Dokumentacja elektroniczna w podmiotach publicznych - ze szczególnym uwzględnieniem szkół wyższych

Zarządzanie tożsamością w uczelni wyższej

Janina Mincer-Daszkiewicz
Uniwersytet Warszawski, MUCI
jmd@mimuw.edu.pl

Warszawa, 2015-03-25

Plan prezentacji

1. Podstawowe pojęcia (uwierzytelnianie, autoryzacja, zarządzanie tożsamością i dostępem).
2. Dlaczego centralne uwierzytelnianie i zarządzanie tożsamością w środowisku akademickim jest tak ważne?
3. Aspekty polityki zarządzania tożsamością i dostępem.
4. Aspekty techniczne zarządzania tożsamością i dostępem.
5. Rozwiązanie dla uczelni wyższej.
6. Federacyjne zarządzanie tożsamością.
7. Polska Federacja Zarządzania Tożsamością PIONIER.Id.
8. Zarządzanie elektroniczną dokumentacją a zarządzanie tożsamością i dostępem.
9. Puśćmy wodze fantazji, czyli gdzie można by wykorzystać federacyjne zarządzanie tożsamością w szkolnictwie wyższym w Polsce.

Podstawowe pojęcia

1. **Uwierzytelnianie** (ang. *authentication*) - weryfikowanie tożsamości osoby ubiegającej się o dostęp do zasobów.
2. **Autoryzacja** (ang. *authorization*) - proces określania rodzaju dostępu przyznanego użytkownikowi.
3. **Zarządzanie tożsamością** (ang. *identity management, IdM*) - zarządzanie prawami dostępu do zasobów informacyjnych, czyli:
 1. procedury określające kto może mieć dostęp do zasobów informacyjnych oraz co może z tymi zasobami zrobić oraz
 2. systemy nadzorujące realizację tych ustaleń.

Zakres dostępu powinien być minimalny, ale zarazem wystarczający do pełnienia wyznaczonych obowiązków.

5. **Zarządzanie dostępem** (ang. *access management, AM*) - procesy i technologie służące do sterowania i monitorowania dostępem do chronionych zasobów; obejmuje uwierzytelnianie, autoryzację, zaufanie i audyt bezpieczeństwa.

Dlaczego?

Dlaczego centralne uwierzytelnianie i zarządzanie tożsamością w środowisku akademickim jest tak ważne:

1. Uczelnie wyższe muszą zapewnić dostęp do wielu usług, często rozproszonych, wielu użytkownikom (studenci, pracownicy, goście).
2. Użytkownicy pełnią wiele ról, wymagających różnych uprawnień.
3. Zbiór użytkowników jest płynny, często zmienia się w czasie.
4. Wszyscy członkowie społeczności powinni mieć równy dostęp do zasobów informacyjnych (z dokładnością do pełnionych ról) - nikt nie może być wykluczony.
5. Pracownicy i studenci są mobilni, w podróży także potrzebują dostępu do zasobów informacyjnych.
6. Uczelnie powinny stać w awangardzie rozwiązań informatycznych, ze względu na swoją rolę edukacyjną.
7. Europa, w tym europejskie szkolnictwo wyższe, integruje się także na poziomie informatycznym - polskie uczelnie nie mogą być wykluczone.

A Państwa zdaniem?

Aspekty polityczne i techniczne IAM*

1. **Nadawanie uprawnień** (ang. *provisioning*).
2. **Odbieranie uprawnień** (ang. *deprovisioning*).
3. Schemat nadawania uprawnień:
 1. określenie zadań użytkownika (roli w organizacji) - wykonuje „przełożony”,
 2. określenie systemów informacyjnych jakie będą mu potrzebne do wykonywania tych zadań - wykonuje „właściciel systemu”,
 3. określenie zakresu dostępu do danych w tych systemach - wykonuje „właściciel systemu”,
 4. weryfikacja uprawnień - wykonuje komórka bezpieczeństwa,
 5. nadanie uprawnień - wykonują administratorzy.
4. **SSO** (ang. *Single Sign-On*) - zasada pojedynczego logowania.

* IAM - Identity and Access Management

Zadania związane z IAM

1. Analiza istniejących procedur zarządzania tożsamością i dostępem oraz ich optymalizacja - projektowanie procesów w celu zwiększenia ich wydajności i niezawodności oraz ułatwienia automatyzacji.
2. Projektowanie reguł dostępu - uporządkowanie istniejących definicji uprawnień, umożliwienie zautomatyzowanego nadawania uprawnień na bazie ról pełnionych w organizacji.
3. Implementacja standardów bezpieczeństwa i standardów zarządzania w obszarze zarządzania tożsamością i dostępem. Zapewnienie zgodności ze standardami, wymogami prawnymi i najlepszymi praktykami branżowymi. Zmniejszenie ryzyk związanych z obszarem zarządzania tożsamością i dostępem.
4. Wdrożenie centralnego katalogu tożsamości - pojedynczego wiarygodnego repozytorium wszystkich niezbędnych danych dotyczących tożsamości.
5. Integracja katalogu tożsamości z systemami i aplikacjami używanymi w organizacji - możliwość zcentralizowanego i zautomatyzowanego zarządzania nadawaniem i odbieraniem dostępu dla systemów i aplikacji objętych integracją.

IAM na uczelni wyższej

1. **Jak minimalizować koszt i wysiłek zarządzania tożsamością:**
 1. uczelnia wyższa to często duży twór organizacyjny,
 2. często złożony z mniejszych jednostek,
 3. często rozproszonych geograficznie na dużych obszarach,
 4. udostępniających użytkownikom wiele usług informatycznych,
 5. często niezintegrowanych i pochodzących od różnych dostawców?
2. Rozwiązanie problemu **od strony technicznej** jest relatywnie proste, gdyż istnieje dużo narzędzi, zarówno darmowych, jak i komercyjnych.
3. Rozwiązanie problemu **od strony organizacyjnej** to prawdziwe wyzwanie i wymaga dobrze przemyślanego projektu

Przykładowe systemy uczelniane wymagające uwierzytelniania i autoryzacji

1. USOSweb - system informacyjny dla studentów i nauczycieli akademickich (może być kilka instalacji)
2. UL - system rejestracji żetonowej na zajęcia oferowane centralnie (lektoraty, WF, egzaminy z języków obcych)
3. APD - Archiwum Prac Dyplomowych
4. SRS - System Rezerwacji Sal
5. OSA - Otwarty System Antyplagiatowy
6. Ankieter - studenci, pracownicy, absolwenci, kandydaci na studia
7. Platforma zdalnego nauczania (oparta na Moodle)
8. Centralne serwery pocztowe (studenci, nauczyciele akademicy, administracja)
9. Systemy biblioteczne (wypożyczalnia książek, czasopisma on-line), MSDN
10. Sieć bezprzewodowa
11. Portal centralny, portale wydziałów, instytutów, grup badawczych
12. Inne systemy informacyjne (np. wiki, fora dyskusyjne)
13. Systemy komputerowe (laboratoria)

Zarządzanie tożsamością w praktyce

1. **Centralny Serwer Uwierzytelniania** zapewnia usługę pojedynczego logowania (SSO) i implementuje protokół CAS (ang. *Central Authorization Service*).
2. Zapleczem dla CAS jest **centralna baza danych o użytkownikach** (LDAP lub Active Directory).
3. Dane o użytkownikach i ich rolach są przekazywane do tej bazy automatycznie z innych repozytoriów (system do obsługi toku studiów, baza kadrowa).
4. **Zalety:**
 1. Wygoda - jednokrotne wprowadzenie danych konta daje dostęp do wszystkich serwisów.
 2. Bezpieczeństwo - dane umożliwiające zalogowanie są przekazywane do jednego miejsca i tam są weryfikowane, logowanie do wszystkich serwisów odbywa się na tej samej stronie, w ten sam sposób.
 3. Prostota - prosto rozszerza się tę usługę na inne serwisy.

Zarządzanie tożsamością w praktyce

Role są tworzone automatycznie poprzez **widoki** założone na bazie centralnej i migrowane automatycznie raz dziennie do bazy danych o użytkownikach. Polityka dostępu jest realizowana na poziomie aplikacji.

Przykładowe role:

- Pracownik etatowy
- Pracownik nieetatowy
- Absolwent
- Doktorant
- Student studiów stacjonarnych, niestacjonarnych wieczorowych, niestacjonarnych zaocznych

Inne przykładowe role użyteczne przy definiowaniu uprawnień do serwisów uczelnianych:

- członek senatu
- członek Rady Wydziału, Instytutu
- członek komisji rektorskiej, wydziałowej
- członek koła naukowego
- członek samorządu studenckiego
- studenci uczestniczący w wymianie zagranicznej

Centralny Serwer Uwierzytelniania UW okno logowania



Uniwersytet Warszawski

Centralny Serwer Uwierzytelniania

Aby móc korzystać z serwisów internetowych Uniwersytetu Warszawskiego, musisz być studentem lub pracownikiem uczelni.

Wprowadź swój numer PESEL i hasło, aby kontynuować.

PESEL:

Hasło:

Ukryj mój PESEL

ZALOGUJ

[zapomniane hasło](#) | [lista serwisów](#) | [o tej stronie](#) | [English version](#)

CAS - strona informacyjna

Centralny Serwer Uwierzytelniania

Centralny System Uwierzytelniania (tzw. CAS, od angielskiego *Central Authentication Service*) ułatwia użytkownikowi korzystanie z grupy serwisów webowych wymagających autoryzacji. Przy próbie logowania do jednego z takich serwisów użytkownik zostaje przekierowany na stronę logowania CAS, a po zalogowaniu uzyskuje przezroczyste dostępowe do **wszystkich** serwisów, które współdziałają z CAS. CAS korzysta z jednego, wspólnego dla wszystkich serwisów repozytorium kont. Na Uniwersytecie Warszawskim tę rolę pełni CUS.

Ważną zaletą takiego systemu jest zwiększenie bezpieczeństwa, ponieważ:

- dane umożliwiające zalogowanie są zawsze przekazywane do jednego miejsca i tam są weryfikowane (hasło użytkownika nie przechodzi przez serwis webowy i nie może być przez niego *wykradzione*),
- nie ma potrzeby tworzenia niezależnych kont w serwisie, jedno konto otwiera drogę do wszystkich serwisów korzystających z centralnego uwierzytelniania.

Korzystając z Centralnego Systemu Uwierzytelniania, należy pamiętać, że:

- strona logowania musi mieć zawsze tę samą postać, zmiana wyglądu strony powinna być dla użytkownika sygnałem do zwiększonej ostrożności,
- strona musi być 'bezpieczna', o czym świadczy przedrostek `https://` w adresie,
- strona musi być chroniona certyfikatem uczelni macierzystej.

Jeśli formularz logowania znajdziesz na stronie, która nie spełnia tych warunków, to może to oznaczać, że ktoś uruchomił fałszywy serwis i chce wykraść hasła użytkowników. W takim przypadku należy zrezygnować z logowania i powiadomić o problemie administratora.

Jeśli adres strony i jej postać są poprawne, to należy wprowadzić swój identyfikator i hasło, przy czym na Uniwersytecie Warszawskim rolę identyfikatora pełni numer PESEL, a w przypadku osób nie posiadających tego numeru tzw. sztuczny PESEL, przydzielany podczas tworzenia konta.

Jeśli po zalogowaniu pojawi się komunikat **Brak autoryzacji, użytkownik <nazwa_konta> nie jest zarejestrowany w systemie**, to oznacza to, że konto nie jest znane w systemie. W celu wyjaśnienia problemu należy się skontaktować z dziekanatem macierzystej jednostki.

Oficjalne serwisy UW dostępne poprzez CAS



Oficjalne serwisy internetowe Uniwersytetu Warszawskiego
współdziałające z Centralnym Systemem Uwierzytelniania.

Serwery USOSweb	Pozostałe serwisy systemu USOS
<ul style="list-style-type: none">USOSweb Kampusu CentralnegoUSOSweb Wydziału ChemiiUSOSweb Wydziału Dziennikarstwa i Nauk PolitycznychUSOSweb Wydziału FizykiUSOSweb Wydziału Matematyki, Informatyki i MechanikiUSOSweb Wydziału Nauk Ekonomicznych	<ul style="list-style-type: none">USOSowniaRejestracja żetonowa (WF, lektoraty)Archiwum Prac DyplomowychSystem Rezerwacji SalInformator ECTSUniwersytecki System Ankietyjący

Pozostałe serwisy

- Centrum Otwartej i Multimedialnej Edukacji
- Zakładanie kont w poczcie studenckiej
- Portal UW
- System obsługi zgłoszeń JIRA

Serwisy wydziałowe

- Portal Wydziału Matematyki, Informatyki i Mechaniki
- Ankieter Wydziału Matematyki, Informatyki i Mechaniki
- Platforma e-learningowa Wydziału Matematyki, Informatyki i Mechaniki
- System Rezerwacji Sal Wydziału Matematyki, Informatyki i Mechaniki
- Portal Wydziału Fizyki
- Platforma e-learningowa Instytutu Lingwistyki Stosowanej
- Wiki Wydziału Biologii
- System rejestracji na praktyki studenckie Wydziału Prawa i Administracji

USOSweb Wydziału MIM

Serwis internetowy Uniwersytetu Warszawskiego | **USOSownia** - uniwersyteckie forum USOSowe

***** Nie jesteś zalogowany | [zaloguj się](#)

USOSweb [AKTUALNOŚCI](#) [KATALOG](#) [MÓJ USOSWEB](#) [DLA STUDENTÓW](#) [DLA PRACOWNIKÓW](#) [MODUŁY DODATKOWE](#)

DOKUMENTY
▶ [strona główna](#)
▶ [aktualności](#)
▶ [APD](#)

KALENDARZ REJESTRACJI

KONTAKT

ostatnia migracja danych: ok. 19 godzin temu

ostatnia modyfikacja tego dokumentu: 4 dni temu

Witaj w systemie USOSweb Wydziału Matematyki, Informatyki i Mechaniki Uniwersytetu Warszawskiego

Pamiętaj, że serwerów USOSweb na Uniwersytecie Warszawskim jest wiele. Na tym serwerze logować się mogą wyłącznie pracownicy i studenci Wydziału Matematyki, Informatyki i Mechaniki.

UWAGA: komunikat przy logowaniu treści 'Nieznany użytkownik' świadczy o nieaktualnych danych w USOS. Należy w tej sprawie napisać do Sekcji Studenckiej (student) bądź do sekretariatu instytutu (pracownicy). Proszę *nie pisać* w tej sprawie do uosweb@mimuw.edu.pl, gdyż administratorzy serwisu i tak nie będą w stanie pomóc.

Oświadczenia o spełnieniu warunków do podjęcia i kontynuowania studiów stacjonarnych w uczelni publicznej bez wnoszenia opłat

Zgodnie z decyzją Pani Prorektor ds. studentów i jakości kształcenia, prof. dr hab. Marty Kicińskiej-Habior, informujemy, że została otwarta tura składania oświadczeń w USOSweb.

W roku akademickim 2013/2014 do złożenia oświadczenia zobowiązani są:
1. Studenci nowoprzyjęci na I r. studiów stacjonarnych w ramach rekrutacji otwartej.
2. Studenci podejmujący studia w ramach wznowienia studiów (dotyczy studiów podjętych po 1.10.2011 r.).
3. Studenci przyjęci w trybie przeniesienia z innej uczelni (kontynuujący na UW studia podjęte począwszy od 1.10.2011 r.).

Portal Wydziału MIM

Serwis internetowy Uniwersytetu Warszawskiego

***** Logowanie dla studentów i pracowników | [zaloguj się](#)

Wydział Matematyki, Informatyki i Mechaniki
Uniwersytetu Warszawskiego

[Strona główna](#) | [Wiadomości](#) | [Dla kandydata](#) | [Dla studenta](#) | [Dla pracownika](#) | [Badania](#) | [Wydział](#)

Konkurs WCNM
Kolejny konkurs o stanowiska po-doktorskie Warszawskiego Centrum Nauk Matematycznych został otwarty. Wnioski można składać na stronie <http://wcnmcs.edu.pl/submit-application/postdocs> do 15 października.

Więcej [»](#)

Wyszukiwarka

Najczęściej szukane strony

- [Poczta pracownicza](#) | [Poczta studencka](#)
- [USOSweb](#) | [APD](#) | [SRS](#)
- [Plany](#) | [Kalendarz semestru zimowego](#)
- [Sukcesy studentów i pracowników](#)
- [Lista pracowników Wydziału](#)
- [Instrukcja dotarcia do Wydziału](#) | [plan budynku](#)

Strona	Opis
Poczta pracownicza	
Poczta studencka	
USOSweb	
APD	
SRS	
Plany	
Kalendarz semestru zimowego	
Sukcesy studentów i pracowników	
Lista pracowników Wydziału	
Instrukcja dotarcia do Wydziału	
plan budynku	

Portal informacyjny dla studentów

Serwis internetowy Uniwersytetu Warszawskiego

***** Nie jesteś zalogowany | [zaloguj się](#)

Czym jest: [USOSweb](#) | [UL](#) | [APD](#) | [IRK](#) | [CAS](#) | [CUS](#) | [Inne serwisy](#)

OSWAJAMY USOS

ENGLISH-SPEAKING USERS
[Click here for English versions of our guides and articles](#)

SZUKAJ
Wyszukiwanie w witrynie:

SUBSKRYBUJ FORUM I STRONĘ GŁÓWNIĄ

MENU

- [Podręcznik USOS-owicza](#)
 - [Zanim powstał USOS...](#)
 - [Czy USOSweb to USOS?](#)
- [USOSweb](#)
- [UL](#)
- [APD](#)
- [IRK](#)
- [Logowanie i uwierzytelnianie](#)
- [Inne serwisy](#)

Rzecznik akademicki do spraw studenckich i pracowniczych

Konflikt, problem, trudności? MAMY NA TO SPOSÓB!
Ombudsman na Uniwersytecie Warszawskim

Artykuły o USOS w miesięczniku Delta

W miesięczniku popularnonaukowym **Delta** rozpoczął się druk serii artykułów o USOS. Miesięcznik ma swój portal internetowy pod adresem <http://www.deltami.edu.pl>. Pierwszy artykuł z serii ma tytuł **Skład USOS** mniej zna i jakie są moje prawa, czyli o zarządzaniu tożsamością. Zapraszamy do lektury.

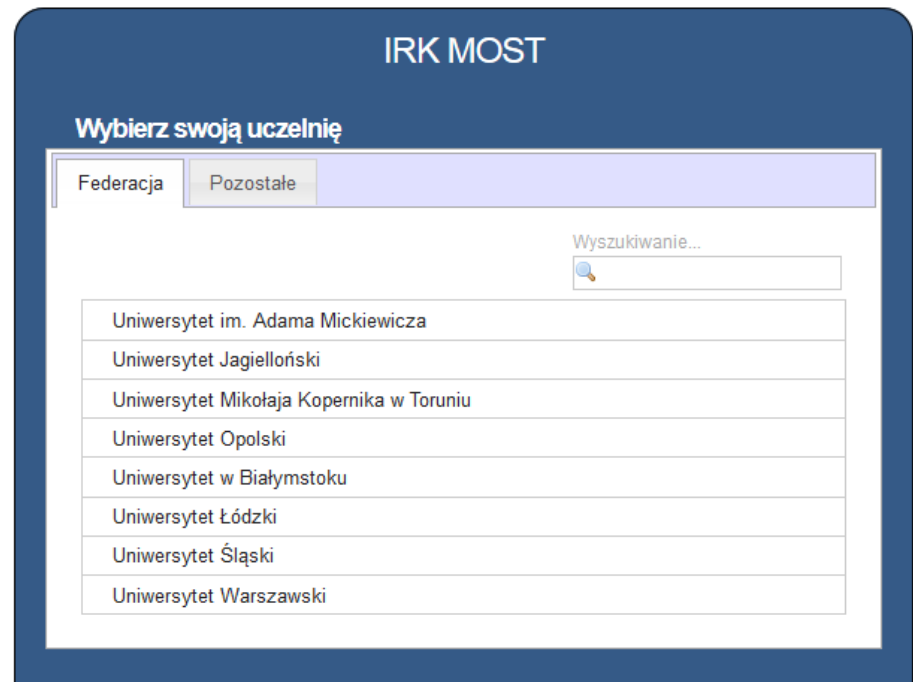
Uczelnia nie jest samotną wyspą ...

1. **Zaufanie** - porozumienie między różnymi instytucjami lub systemami dotyczące współdzielenia danych na temat tożsamości.
2. **Federacja** - specjalny rodzaj relacji zaufania między różnymi instytucjami, które godzą się na współużytkowania danych na temat tożsamości ponad granicami wewnętrznymi sieci. Zwykle mają zasięg krajowy.
3. **Konfederacja** - związek federacji.

Federacyjne zarządzanie tożsamością MOST - Program Mobilności Studentów

Program Mobilności Studentów **MOST** jest formą studiowania, prowadzoną od ponad dziesięciu lat przez uczelnie - strony *Porozumienia na Rzecz Jakości Kształcenia*. Opiera się na zasadach, jakie obowiązywały przy wyjazdach w ramach Programu Socrates. Koordynatorem MOST jest **Uniwersytecka Komisja Akredytacyjna**, działająca na zlecenie **Konferencji Rektorów Uniwersytetów Polskich**. W programie uczestniczy 20 polskich uniwersytetów i kilka uczelni stowarzyszonych. Rejestracja na wyjazdy od 2010 roku odbywa się centralnie. Część uczelni uczestniczy w federacyjnym zarządzaniu tożsamością.

<http://most.uka.uw.edu.pl>



The screenshot shows the IRK MOST website interface. At the top, it says "IRK MOST". Below that, the heading "Wybierz swoją uczelnię" is displayed. There are two tabs: "Federacja" (selected) and "Pozostałe". A search bar with the placeholder "Wyszukiwanie..." and a magnifying glass icon is present. Below the search bar is a list of universities:

Uniwersytet im. Adama Mickiewicza
Uniwersytet Jagielloński
Uniwersytet Mikołaja Kopernika w Toruniu
Uniwersytet Opolski
Uniwersytet w Białymstoku
Uniwersytet Łódzki
Uniwersytet Śląski
Uniwersytet Warszawski

CENTRALNY SYSTEM UWIERZYTELNIANIA

Wprowadź swój numer PESEL i hasło

Numer PESEL:

Hasło:

Ukryj mój numer PESEL

ZALOGUJ | wyczyść | [Polski](#) | [English](#)

UNIwersYTET IM. ADAMA MICKIEWICZA W POZNANIU

<https://cas.amu.edu.pl/cas-server-webapp-3.3.5/login>

UNIwersYTET MIKOŁAJA KOPERNIKA

Centralny punkt logowania

Z usług internetowych UMK mogą korzystać pracownicy i studenci Uniwersytetu Mikołaja Kopernika mający konto na serwerach UMK.

Jeżeli jeszcze nie masz konta - załóż konto.

Wprowadź swój identyfikator w sieci UMK oraz hasło:

Identyfikator:
np. login@umk.pl, login@his.umk.pl

Hasło:

Zaloguj

► pomoc ► lista usług ► o tej stronie ► English version

<https://login.umk.pl/login>

Uniwersytet Opolski
Centralny Punkt Logowania

Aby korzystać z serwisów internetowych Uniwersytetu Opolskiego, musisz być jego pracownikiem lub studentem.

Wprowadź swój login i hasło, aby kontynuować. Nie wiesz jak się zalogować? Kliknij [tutaj](#).

Login:

Hasło:

Ostrzegaj przed zalogowaniem do innych usług

WYCZYŚĆ | **ZALOGUJ**

[zapomniane hasło](#) | [lista serwisów](#) | [o tej stronie](#) | [English version](#)

<https://login.uni.opole.pl/cas/login>

IRK MOST

Nazwa użytkownika

Hasło

Login »

Zarządzanie tożsamością w sieciach bezprzewodowych

eduroam (ang. *education roaming*) - sieć umożliwiająca bezpieczny roaming dla użytkowników jednostek naukowych i szkolnictwa wyższego.

Cel: Student wyjeżdżający na inną uczelnię w ramach wymiany międzynarodowej czy pracownik uczestniczący w konferencji naukowej na innej uczelni od razu jest uwierzytelniany przez jej serwisy. Konta są wprowadzane przez lokalnych administratorów w lokalnych bazach. Przyznawane role zależą od uzgodnień między uczelniami.

W niektórych krajach (Szwecja, Norwegia) dostępny nawet na lotniskach.

Zainicjowana przez organizację **TERENA** w 2003 roku.

Jest **konfederacją**, czyli federacją federacji (działających na szczeblu krajowym).

Użyteczne:

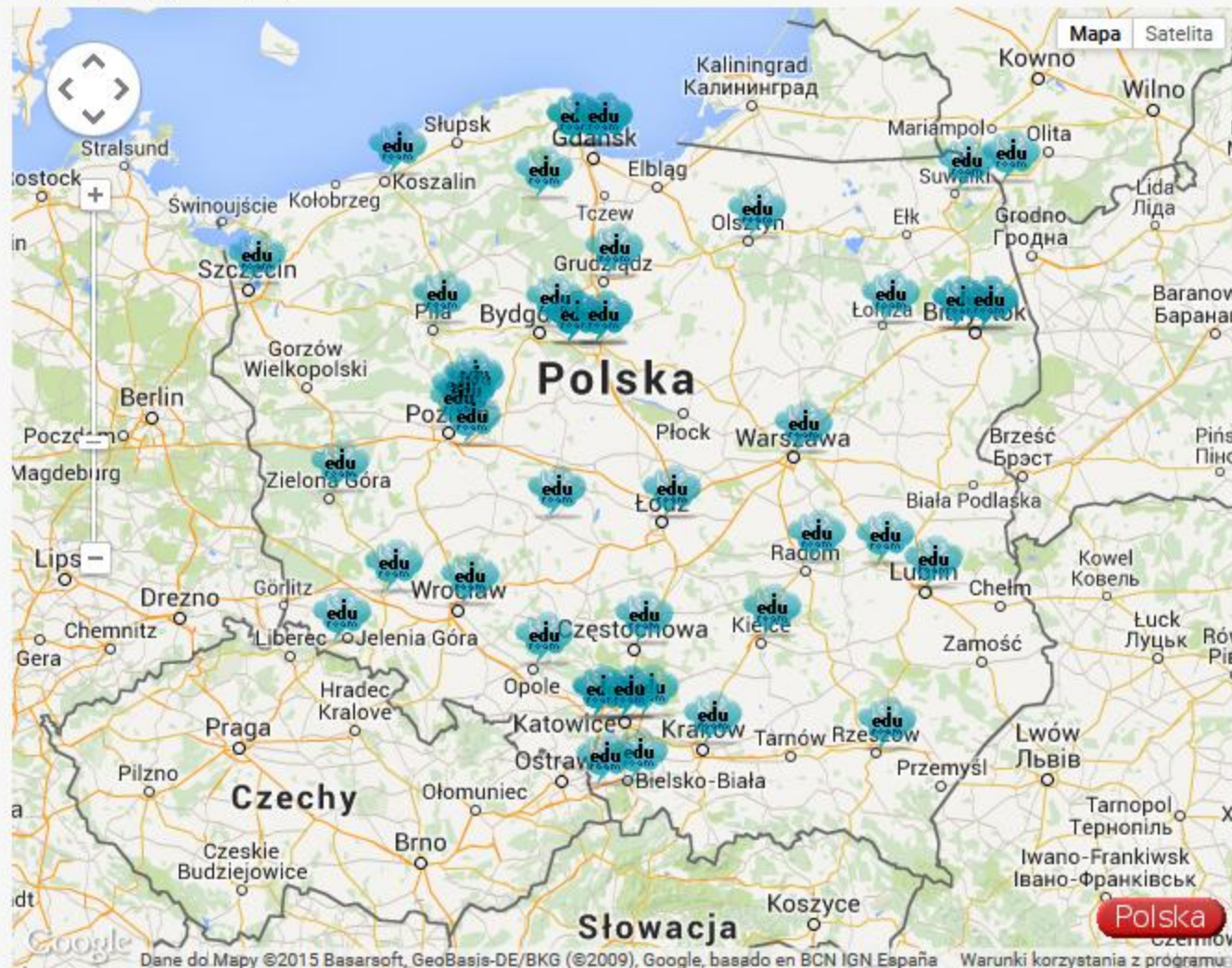
1. Bogumiła Czerniak, *Charakter prawny i obowiązki podmiotu oferującego dostęp do sieci Internet w ramach usługi eduroam*, ICM UW
2. Strona domowa eduroam, <http://www.eduroam.org>
3. eduroam w Polsce, <http://www.eduroam.pl>

eduroam na terenie Polski

eduroam w Polsce jest dostępny poprzez infrastrukturę sieci PIONIER i podłączonych do niej sieci miejskich zarządzanych przez instytucje będące członkami [Konsorcjum PIONIER](#). Infrastruktura **eduroam** w Polsce została zbudowana w ramach projektu [PLATON](#).

eduroam jest dostępny w **70** polskich instytucjach, w **661** lokalizacjach (rozumianych jako odrębne budynki bądź ich grupy, bądź wspólne obszary na zewnątrz budynków), w **48** miejscowościach.

Zobacz pełną [listę](#) lub [mapę](#) w większym rozmiarze.



PIONIER.Id

- Strona główna
- Dokumenty Federacji
- Członkowie Federacji
- Partnerzy Federacji
- Informacje techniczne
- Po co przystępować?
- Jak zostać członkiem?
- Procedura rejestracji
- Opracowania i prezentacje
- Kontakt

Świat federacji

- eduGAIN
- REFEDS

Strona główna

Witamy na stronach Polskiej Federacji **PIONIER.Id**.

- Federacyjne Zarządzanie Tożsamością jest procesem, w którym dostawca usługi świadczonej drogą elektroniczną (zwany dalej Dostawcą Usługi) ufa innemu podmiotowi (zwanemu Dostawcą Tożsamości) w zakresie zweryfikowania tożsamości i uprawnień użytkownika końcowego. Dostawca Tożsamości ufa Dostawcy Usługi w zakresie procedur przetwarzania danych osobowych niezbędnych do świadczenia usługi, które to dane są dostarczane przez Dostawcę Tożsamości w procesie uwierzytelnienia i autoryzacji użytkownika.
- Zaufanie między Dostawcą Tożsamości a Dostawcą Usługi jest oparte o dwustronne umowy lub inne procedury i ustalenia zastępujące takie umowy.
- Proces uwierzytelnienia jest chroniony za pomocą parametrów zawartych w opisach technicznych Dostawcy Usługi i Dostawcy Tożsamości (tzw. metadanych).
- Celem tworzenia Federacji Zarządzania Tożsamością jest uproszczenie i zunifikowanie procedur tworzenia umów dwustronnych oraz dostarczenie bezpiecznego źródła metadanych. Federacje Zarządzania Tożsamością mogą zawierać porozumienia o współpracy z innymi Federacjami tworząc konfederacje.
- Usługa Federacji PIONIER.Id polega na dostarczaniu procedur i środków technicznych niezbędnych do zapewnienia sprawnej współpracy członków i partnerów federacji PIONIER.Id w celu ułatwienia członkom federacji uwierzytelnionego i autoryzowanego dostępu do usług. Usługa Federacji PIONIER.Id jest kierowana w pierwszej kolejności do podmiotów należących do sektora badań i edukacji.
- Federacja PIONIER.Id jest wspólnym działaniem członków [Konsorcjum PIONIER](#).
- Operatorem Federacji PIONIER.Id jest Poznańskie Centrum Superkomputerowo-Sieciowe. Prace rozwojowe i operacyjne koordynuje Uczelniane Centrum Informatyczne Uniwersytetu Mikołaja Kopernika w Toruniu.

PIONIER.Id

- Strona główna
- Dokumenty Federacji
- Członkowie Federacji
- Partnerzy Federacji
- Informacje techniczne
- Po co przystępować?
- Jak zostać członkiem?
- Procedura rejestracji
- Opracowania i prezentacje
- Kontakt

Świat federacji

- eduGAIN
- REFEDS

Członkowie PIONIER.Id

1. [Politechnika Świętokrzyska](#)
2. [Politechnika Wrocławska](#)
3. [Poznańskie Centrum Superkomputerowo-Sieciowe](#)
4. [Uniwersytet Marii Curie-Skłodowskiej](#)
5. [Uniwersytet Mikołaja Kopernika w Toruniu](#)

w trakcie przystępowania

1. [Uniwersytet Opolski](#)
2. [Uniwersytet Warszawski](#)

About eduGAIN

eduGAIN is a service developed within the GÉANT project. eduGAIN interconnects identity federations around the world, simplifying access to content, services and resources for the global research and education community. eduGAIN enables the trustworthy exchange of information related to identity, authentication and authorisation (AAI) by coordinating elements of the federations' technical infrastructure and providing a policy framework that controls this information exchange.

This exchange of information contributes to the seamless operation of services developed within the GÉANT project and services provided by other communities represented by, or associated with, the GÉANT Partners.

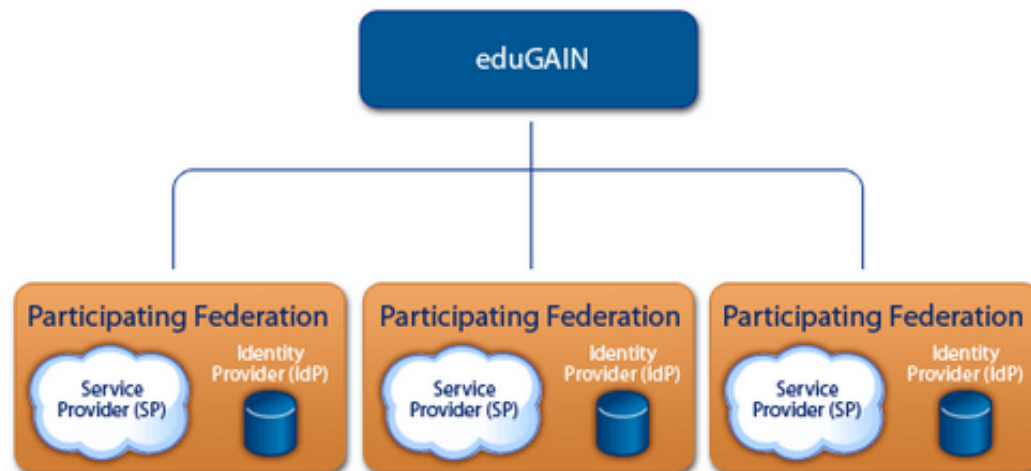


Useful links

[Why Use eduGAIN](#)

[How eduGAIN works](#)

[Who benefits from eduGAIN?](#)



Features:

- Enables trustworthy exchange of information between federations
- Reduces the costs of developing and operating services
- Improves the security and end-user experience of services
- Enables service providers to greatly expand their user base
- Enables identity providers to increase the number of services available to their users



STORK 2.0 project

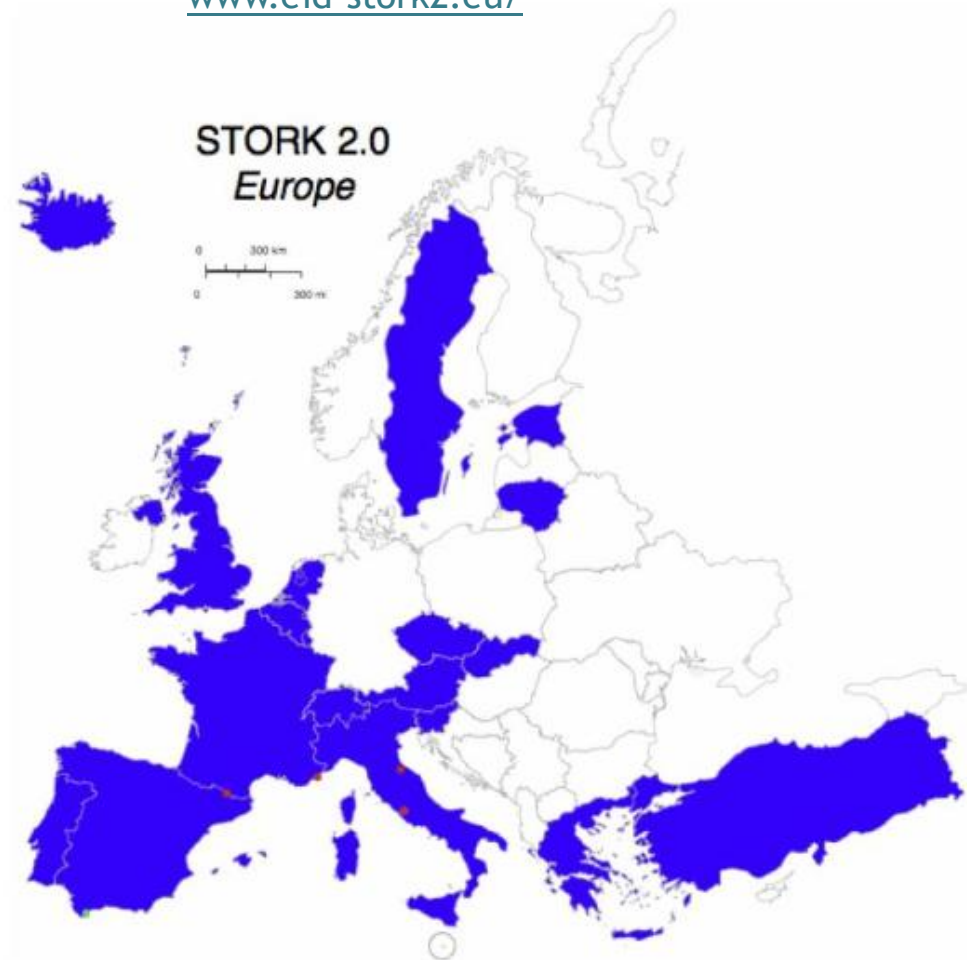
www.eid-stork2.eu/

STORK 2.0
Secure identity across
borderS linked 2.0

3 year duration:
from 2012 to 2015

19 participating
countries

58 partners



Puśćmy wodze fantazji ...

Gdzie można wykorzystać federacyjne zarządzanie tożsamością w szkolnictwie wyższym w Polsce i poza granicami:

1. [Program MOST](#)
2. [Biurokarier.edu.pl](#)
3. [POL-on](#), [OSF](#) i inne systemy MNiSW
4. EMREX Project - *Field trial on the impact of enabling easy mobility on recognition of external studies*
5. Erasmus without Paper Project

Ale:

1. Trzeba rozwiązać problem aktywności kont absolwentów uczelni.
2. ePUAP mógłby rozwiązać problem uwierzytelniania we wszystkich serwisach na terenie Polski
3. STORK mógłby rozwiązać problem uwierzytelniania we wszystkich serwisach w Europie

A Państwa zdaniem?

Zarządzanie elektroniczną dokumentacją a zarządzanie tożsamością i dostępem:

1. Dostęp do dokumentów elektronicznych wymaga uwierzytelniania i autoryzacji.
2. System EZD (Elektronicznego Zarządzania Dokumentami) powinien być zintegrowany z systemami dostarczającymi lub pobierającymi dokumenty elektroniczne.
3. System EZD powinien być zintegrowany z systemem zarządzania tożsamością i dostępem.

1. Podstawowe cechy wygodnego mechanizmu uwierzytelniania i autoryzacji:
 1. użytkownik ma jedno konto dostępne do wszystkich serwisów, loguje się jeden raz, żeby uzyskać dostęp do wszystkich,
 2. dane o kontach i rolach są wprowadzane w jednym miejscu i dystrybuowane wszędzie tam, gdzie są potrzebne,
 3. aktualizacja kont i ról odbywa się automatycznie,
 4. w razie problemów można użytkownika obsłużyć osobiście blisko jego miejsca pobytu.
2. Projektując system zarządzania tożsamością należy wziąć pod uwagę koszt zarządzania danymi, ich aktualizowania i dystrybuowania.
3. Jeśli uczelnia chce brać aktywny udział w elektronicznym obiegu informacji musi być elementem polskiej federacji.