Janina Mincer-Daszkiewicz

Wydział Matematyki, Informatyki i Mechaniki

Uniwersytet Warszawski

jmd@mimuw.edu.pl
http://www.mimuw.edu.pl/~jmd

Zarządzanie tożsamością w systemach internetowych uczelni wyższej

Koniec z chaosem?

Plan prezentacji

- Pojęcia
- Cele, metody
- Studium przypadku – Uniwersytet Warszawski
- Podsumowanie

Zarządzanie tożsamością (ang. *Identity Management*)

(według Wikipedii)

to zarządzanie prawami dostępu do zasobów informacyjnych, czyli:

- procedury określające kto może mieć dostęp do zasobów informacyjnych oraz co może z tymi zasobami zrobić oraz
- systemy nadzorujące realizację tych ustaleń.

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

Kluczowe pojęcia

- **autentykacja** (ang. *authentication*) – proces uwierzytelniania (weryfikowania tożsamości) osoby ubiegającej się o dostęp do zasobów
- **autoryzacja** – (ang. *authorization*) proces określania rodzaju dostępu przyznawanego użytkownikowi
- **atrybuty** – informacje o użytkowniku, takie jak przynależność do określonej grupy czy rola w społeczności uczelni
- **zaufanie** – porozumienie między różnymi instytucjami lub systemami dotyczące współdzielenia danych na temat tożsamości

Kluczowe pojęcia - cd

- **zarządzanie dostępem** – procesy i technologie służące do sterowania i monitorowania dostępem do chronionych zasobów; obejmuje autentykację, autoryzację, zaufanie i audyt bezpieczeństwa

- **federacja** – specjalny rodzaj relacji zaufania między różnymi instytucjami, które godzą się na współużytkowanie danych na temat tożsamości ponad granicami wewnętrznych sieci

Schemat nadawania uprawnień

- określenie zadań pracownika (roli w organizacji) - wykonuje przełożony
- określenie systemów informacyjnych jakie będą mu potrzebne do wykonywania tych zadań - wykonuje „właściciel systemu”
- określenie zakresu dostępu do danych w tych systemach - wykonuje „właściciel systemu”
- weryfikacja uprawnień - wykonuje komórka bezpieczeństwa
- nadanie uprawnień - wykonują administratorzy

Problem ...

Jak **minimalizować koszt** i **wysiłek** zarządzania tożsamością w dużych instytucjach, złożonych z wielu mniejszych jednostek, często rozproszonych geograficznie na dużych obszarach (jak uczelnia wyższa z filiami w innych miastach), udostępniających użytkownikom wiele usług informatycznych, często niezintegrowanych i pochodzących od różnych dostawców?

Rozwiązanie problemu od strony technicznej ...

jest relatywnie proste, bo istnieje dużo narzędzi zarówno darmowych, jak i komercyjnych

Systemy zarządzania tożsamością

- Listy dostępu (ang. *Access Control Lists*), np. systemy uniksowe, NTFS
- Active Directory (systemy Windowsowe)
- Central Authentication Service (CAS)
- Microsoft Passport Network
- eDirectory dawniej znane jako Novell Directory Services (NDS)
- Novell Identity Manager
- Open LDAP (Lightweight Directory Access Protocol)
- Oracle Identity Manager
- Pluggable Authentication Modules (PAM)
- Single sign-on

Rozwiązanie problemu od strony organizacyjnej ...

to prawdziwe wyzwanie i wymaga dobrze przemyślanego projektu

Studium przypadku

Uniwersytet Warszawski

system obsługi studentów – USOS

Systemy uczelniane wymagające uwierzytelniania i autoryzacji

- USOSweb – system informacyjny dla studentów i nauczycieli akademickich (może być kilka instalacji)
- UL – system rejestracji na zajęcia oferowane centralnie (lektoraty, WF, egzaminy z języków obcych)
- APD – Archiwum Prac Dyplomowych
- SRS – System Rezerwacji Sal
- Ankieter
- Platforma zdalnego nauczania (oparta na Moodle)
- Centralne serwery pocztowe (studenci, nauczyciele akademiccy, administracja)

Systemy uczelniane wymagające uwierzytelniania i autoryzacji - cd

- Systemy biblioteczne (wypożyczalnia książek, czasopisma on-line)
- Sieć radiowa
- Portal centralny, portale wydziałów, instytutów, grup badawczych
- Inne systemy informacyjne (np. USOSownia, fora dyskusyjne)
- Systemy komputerowe (laboratoria)

Architektura z lotu ptaka

http://usos.edu.pl/USOS-architektura2.pdf

Modele zarządzania tożsamością – 1

Dane o kontach i profilach są trzymane w bazie centralnej USOS, skąd są migrowane automatycznie do lokalnych baz aplikacji; aplikacje autoryzując użytkowników sięgają do danych dostępnych lokalnie, ale zmiana tych danych (np. hasła) w lokalnej bazie aplikacji nie propaguje się wcale lub wolno do innych serwisów, profile określają uprawnienia do aplikacji

Zalety:

- Działa ☺
- Hasło wprowadza student w IRK, skąd trafia ono do USOS (odpada problem dystrybucji haseł)

Modele zarządzania tożsamością – 2

- Jak w punkcie (1), ale dochodzi autoryzacja poprzez lokalne bazy NIS, wykorzystywane w laboratoriach komputerowych jednostek
- Zalety:
  - W lokalnej instalacji USOSweb obowiązuje ten sam identyfikator i hasło co w lokalnym serwerze pocztowym i laboratorium komputerowym
  - Zakładanie, aktualizowanie, usuwanie kont w NIS można zautomatyzować

Modele zarządzania tożsamością – 3

Powstaje **CUS** – centralna baza danych o użytkownikach (wykonana przez DS ICM, udostępniana na licencji GPL). Dane do bazy CUS są przekazywane na bieżąco z bazy USOS, aplikacje internetowe podczas autoryzacji odpytują bezpośrednio CUS

Zalety:

- Zmienione dane konta są od razu dostępne dla wszystkich serwisów

Modele zarządzania tożsamością – 4

Powstaje CAS – *Centralny Serwer Uwierzytelniania* zapewniający usługę pojedynczego logowania

Zalety:

- Wygoda – jednokrotne wprowadzenie danych konta daje dostęp do wszystkich serwisów
- 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
- Prostota – prosto rozszerza się tę usługę na inne serwisy

Modele zarządzania tożsamością – 5

Powstają role tworzone automatycznie przez widoki założone na bazie centralnej USOS. Role są migrowane raz dziennie do bazy CUS przez demon systemowy. Docelowo role w całości zastąpią profile. Przykładowe role:

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

Modele zarządzania tożsamością – 5 cd

- Widok to zbiór trójek (osoba, role, jednostka)
- Zalety:
  - Polityka dostępu realizowana na poziomie aplikacji, a nie USOS
  - Profile trzeba było obsługiwać ręcznie, role są obsługiwane automatycznie (rozwiązuje problem aktualizacji danych)
  - Zbiór ról można łatwo rozszerzać

Modele zarządzania tożsamością – 5 cd

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

Bezpieczny mechanizm przypominania hasła

- Użytkownik otwiera ekran logowania CAS
- Wybiera opcję „Zmiana hasła”
- Wpisuje nowe hasło (z potwierdzeniem)
- System wyświetla krótki, czytelny kod aktywacyjny
- Użytkownik odwiedza najbliższy dziekanat
  - Pracownik dziekanatu sprawdza jego tożsamość
  - Wprowadza do USOS przekazany przez użytkownika kod aktywacyjny
  - USOS przesyła kod do CAS
  - CAS aktywuje konto

Bezpieczny mechanizm przypominania hasła

- Pomysłodawca: DS ICM
- Zalety:
  - Nikt poza użytkownikiem nie widzi nowego hasła
  - Kod aktywacyjny jest jednorazowy i ma ograniczony termin ważności
  - Użytkownik jest uwierzytelniany przez „żywą osobę”

Inne metody przypominania hasła

- Hasło jest wysyłane mailem – możliwość podsłuchania
- Hasło jest wysyłane SMS-em – kosztowne i złożone organizacyjnie
- Pracownik dziekanatu generuje użytkownikowi nowe losowe hasło, które trzeba zmienić przy pierwszym logowaniu
  - Konieczność ręcznego przepisania hasła na kartkę (możliwość pomyłki)
  - Hasło widzi osoba postronna
  - Użytkownicy miewają problemy z wymuszoną operacją natychmiastowej zmiany hasła

Centralny Serwer Uwierzytelniania UW okno logowania

CAS – strona informacyjna

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 przezroczyście dostęp 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

USOSweb Kampusu Centralnego
USOSweb Wydziału Chemii
USOSweb Wydziału Fizyki
USOSweb Wydziału Matematyki, Informatyki i Mechaniki
USOSweb Wydziału Nauk Ekonomicznych
USOSweb Wydziału Prawa i Administracji

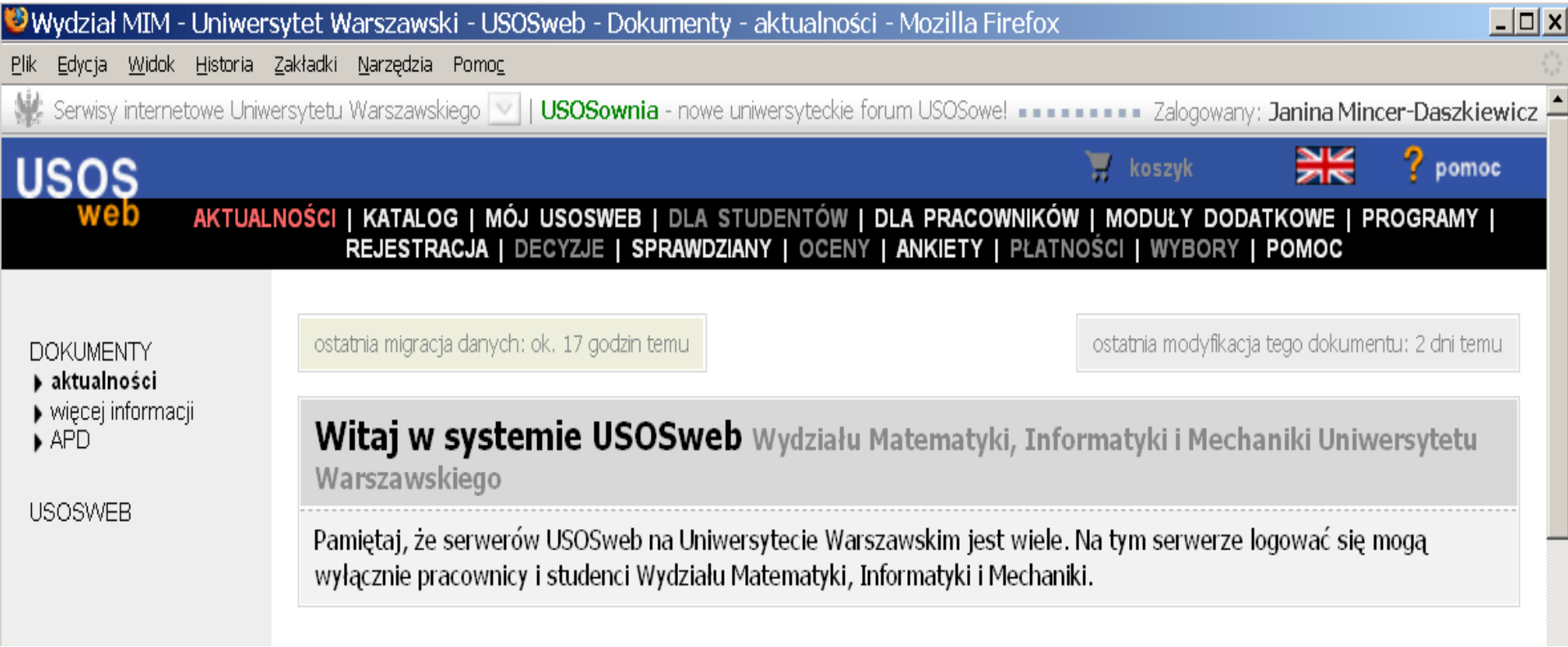
Pozostałe serwisy systemu USOS

USOSownia
Rejestracja żetonowa (WF, lektoraty)
Archiwum Prac Dyplomowych

Pozostałe serwisy

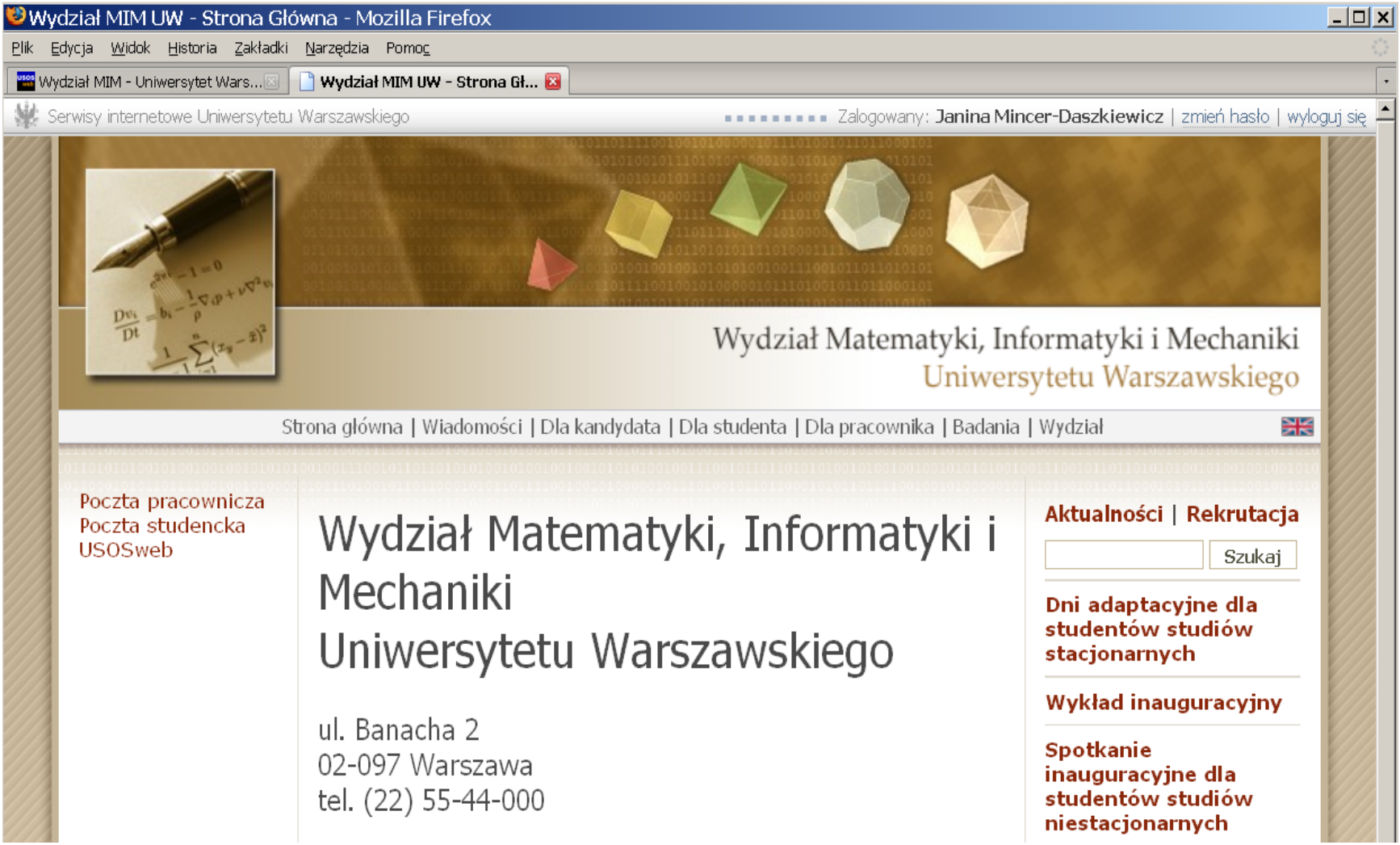
Portal Wydziału Matematyki, Informatyki i Mechaniki
Portal Wydziału Fizyki
Centrum Otwartej i Multimedialnej Edukacji (wkrótce)
Poczta Studencka (wkrótce)

USOSweb Wydziału MIM

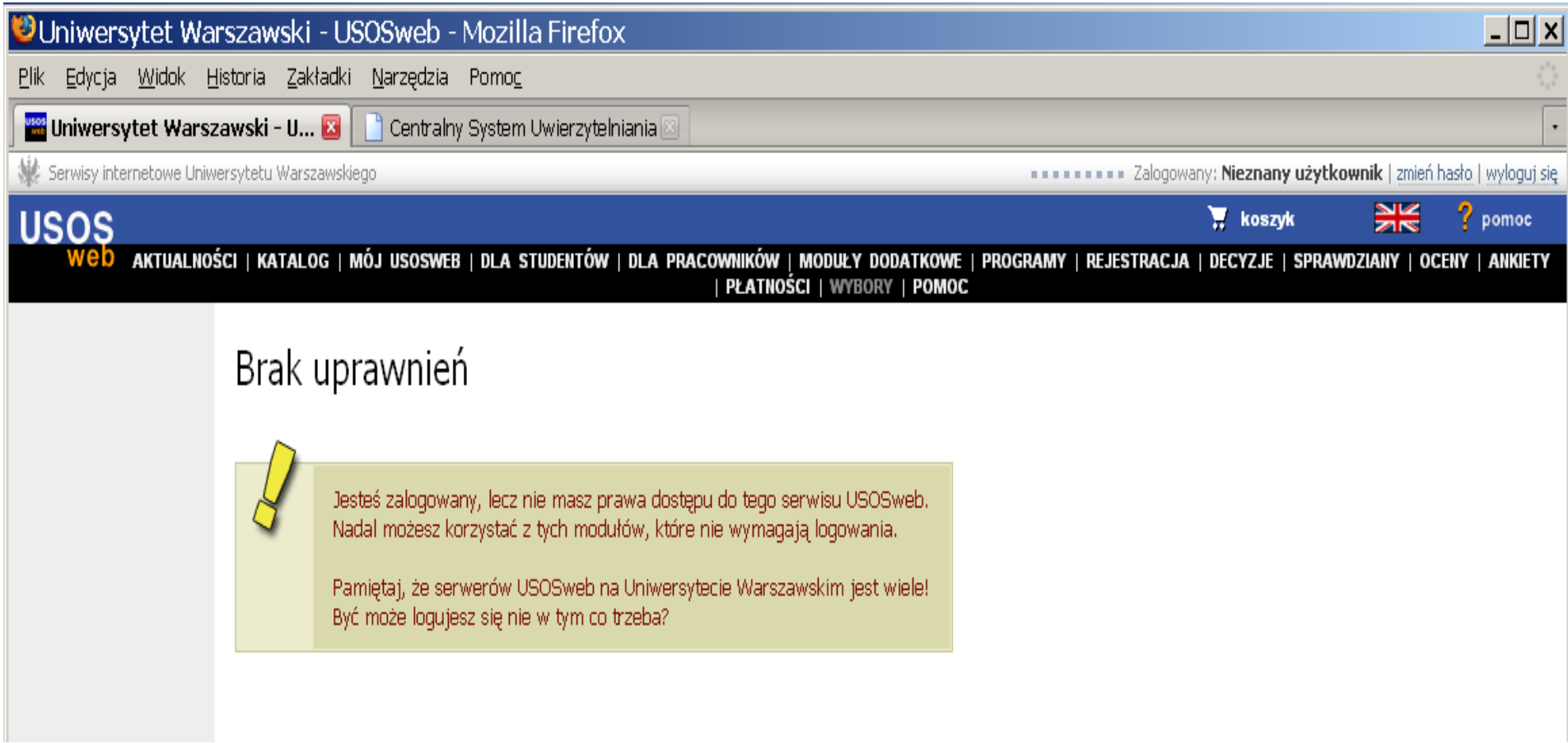


USOSweb Wydziału MIM

Portal Wydziału MIM



USOSweb innego wydziału



Zarządzanie tożsamością w federacjach (ang. *Federated Identity Management*)

- Studium przypadku

  eduroam (ang. *education roaming*)

- 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

http://www.eduroam.org

http://www.eduram.pl

eduroam w Polsce

Podsumowanie

- Podstawowe cechy wygodnego mechanizmu uwierzytelniania i autoryzacji:
  - użytkownik ma jedno konto dostępowe do wszystkich serwisów, loguje się jeden raz, żeby uzyskać dostęp do wszystkich
  - dane o kontach i rolach są wprowadzane w jednym miejscu i dystrybuowane wszędzie tam, gdzie są potrzebne
  - aktualizacja kont i ról odbywa się automatycznie
  - w razie problemów można użytkownika obsłużyć osobiście blisko jego miejsca pobytu

Podsumowanie - cd

- Projektując system zarządzania tożsamością należy wziąć pod uwagę:
  - koszt zarządzania danymi
  - koszt aktualizowania danych
  - koszt dystrybuowania danych
- Są dostępne darmowe narzędzia
- Problem zarządzania tożsamością jest w centrum uwagi wielu uczelni europejskich (por. EUNIS'2008, osobna sesja, 10 referatów)

czyli ...

sprawny mechanizm zarządzania tożsamością jest sposobem na

... uniknięcie chaosu ;)

Adresy

- USOS
  http://usos.edu.pl
- CAS na UW
  http://logowanie.uw.edu.pl
- Pasek logowania CAS
  http://usosweb.mimuw.edu.pl
- EUNIS 2008, zarządzanie tożsamością na uczelniach wyższych w Europie
  http://eunis.dk/papers/