POZNAŃSKIE CENTRUM SUPERKOMPUTEROWO-SIECIOWE

Rozproszone systemy uwierzytelniania użytkowników

Marcin Werla

Poznańskie Centrum Superkomputerowo-Sieciowe

IV Warsztaty „Biblioteki cyfrowe”

Toruń, 2007

Wprowadzenie

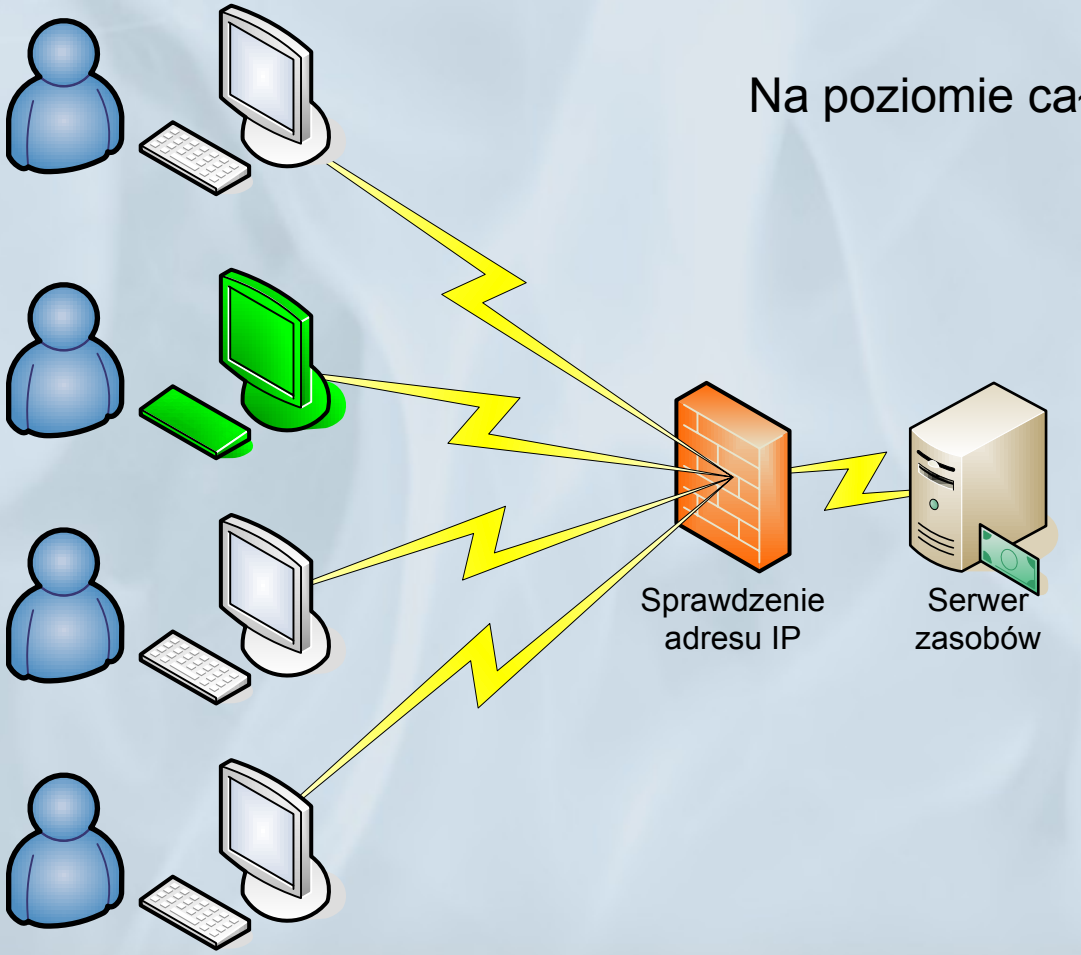
- Uwierzytelnianie – proces polegający na zweryfikowaniu tożsamości osoby, urządzenia lub usługi biorącej udział w wymianie danych
- Autoryzacja – proces, w którym sprawdzane jest czy dany podmiot (o ustalonej właśnie tożsamości) ma prawo dostępu do zasobów, o które prosi

Wprowadzenie

- Metody uwierzytelniania:
  - Nazwa użytkownika (*login*) i hasło lub fragment hasła
  - Kryptografia asymetryczna (klucz prywatny i publiczny)
  - Listy i generatory haseł jednorazowych
  - Cechy biometryczne (dla człowieka, np. wygląd tęczówki)
  - „Parametry” techniczne (dla urządzenia, np. adres IP)

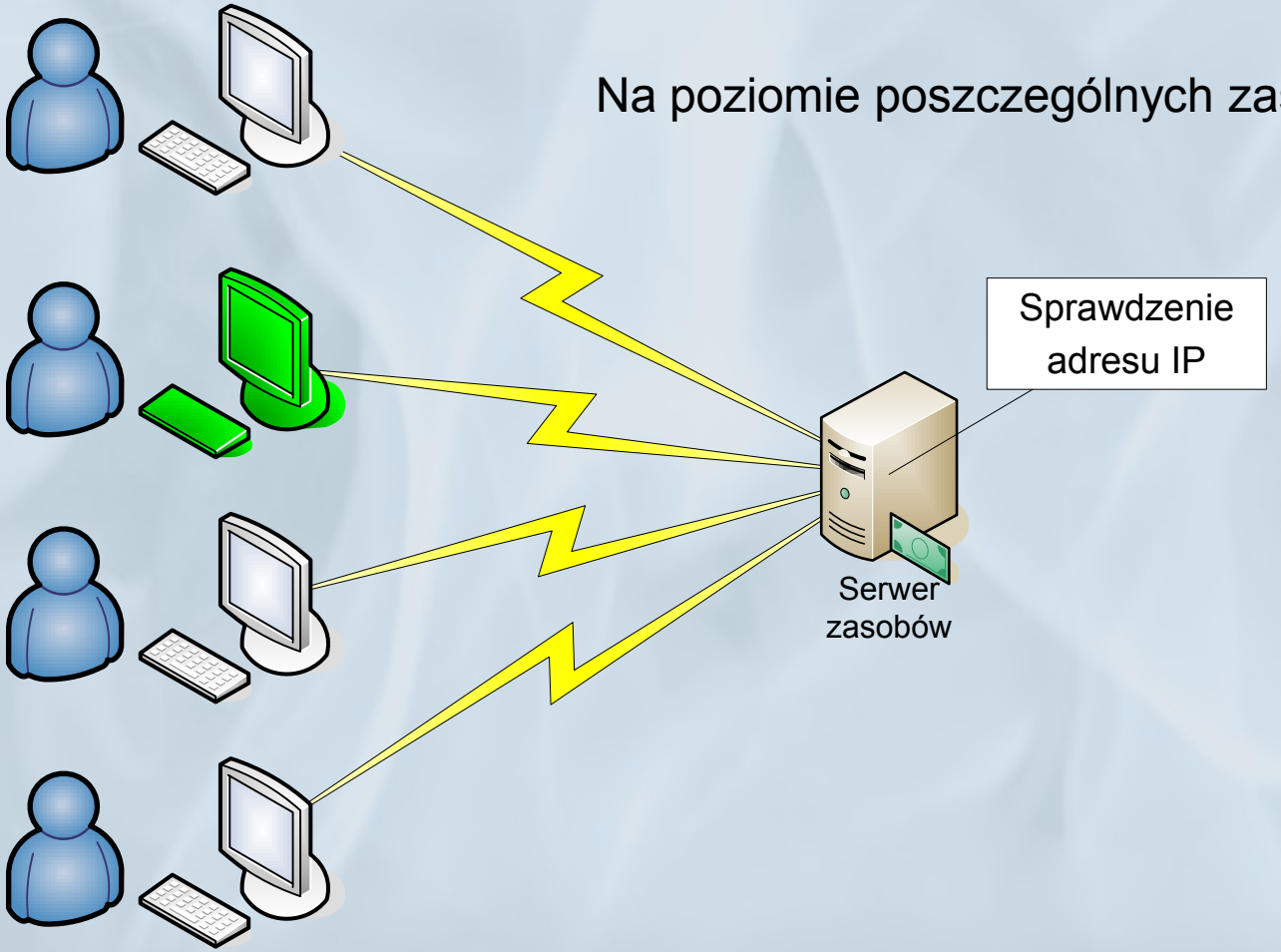
Autoryzacja w oparciu o adres IP

Na poziomie całego systemu

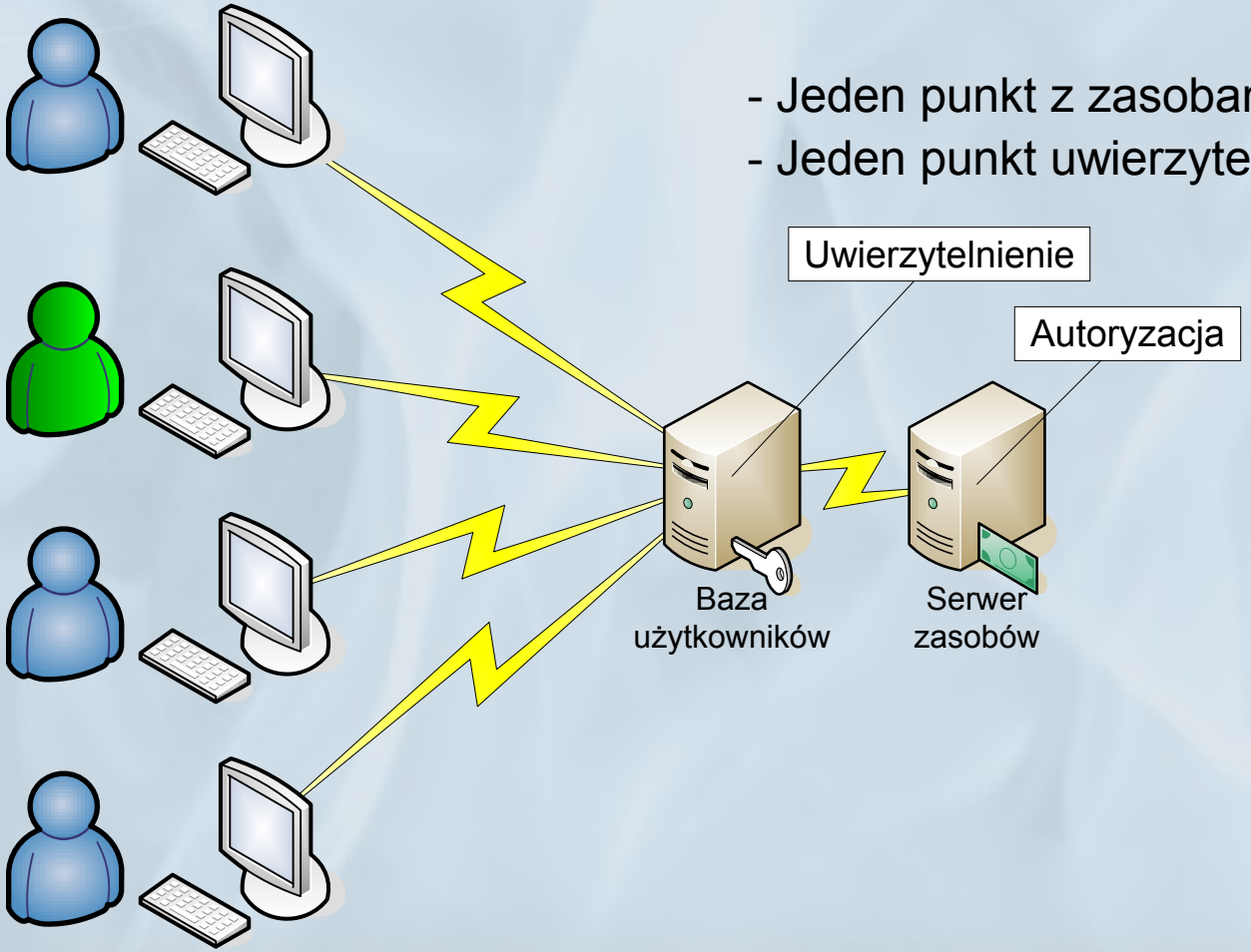


Autoryzacja w oparciu o adres IP

Na poziomie poszczególnych zasobów

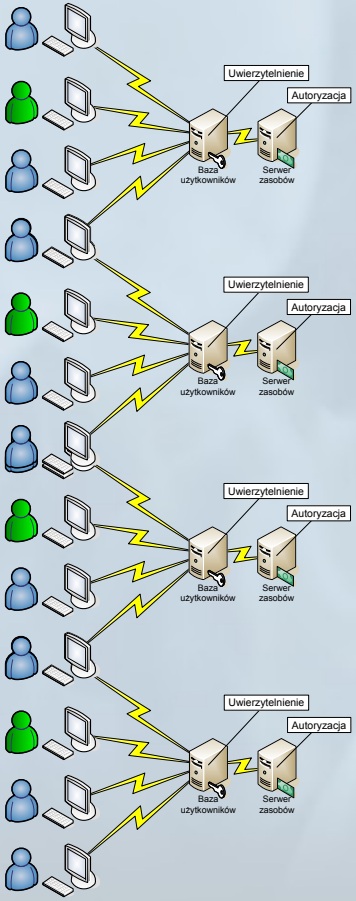


Scenariusz podstawowy



- Jeden punkt z zasobami
- Jeden punkt uwierzytelniania

Problem



Wiele punktów z zasobami

=

Wiele punktów autoryzacji

=

Wiele punktów uwierzytelniania

=

Wiele baz użytkowników

=

Wiele nazw użytkownika i hase

Rozwiązanie nr 1

- System jednokrotnego logowania - pozwala na podstawie jednokrotnego zalogowania się uzyskać dostęp do skojarzonych z tym systemem zasobów

Sposób realizacji

- Wiele punktów z zasobami = wiele punktów autoryzacji
- Jeden punkt uwierzytelniania = jedna baza użytkowników = jedna nazwa użytkownika i hasło
- Obszar zastosowania: wszędzie tam, gdzie można się ograniczyć do jednej bazy użytkowników

System jednokrotnego logowania

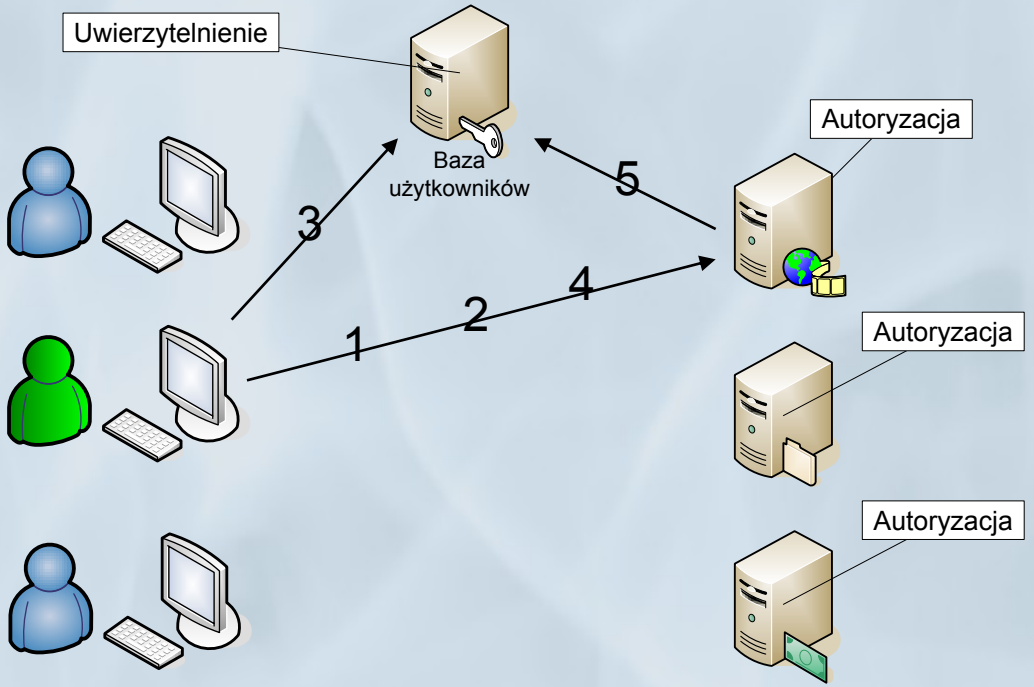
1 – Próba pobrania zasobu

2 – Nakaz uwierzytelnienia

3 – Uwierzytelnienie

4 – Powtórna próba pobrania zasobu

5 – Potwierdzenie tożsamości



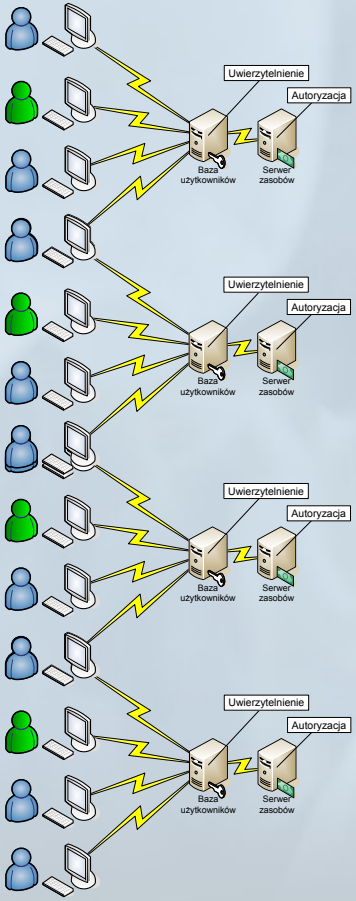
Przy dostępie do innego zasobu scenariusz powtarza się, ale użytkownik zostaje automatycznie rozpoznany przez usługę uwierzytelniającą. Dzieję się tak do momentu, aż użytkownik się z tej usługi nie wyloguje.

Centralny punkt uwierzytelniania określa tylko tożsamość. O prawach dostępu do zasobów decydują poszczególne usługi odpowiedzialne za te zasoby, na podstawie informacji otrzymanych z punktu uwierzytelniania.

System jednokrotnego logowania

- Przykłady:
  - Interkl@sa - Polski Portal Edukacyjny
  - Uniwersytet Mikołaja Kopernika w Toruniu
    - Również KPBC

Problem



Wiele punktów z zasobami

=

Wiele punktów autoryzacji

=

Wiele punktów uwierzytelniania

=

Wiele baz użytkowników

=

Wiele nazw użytkownika i hase

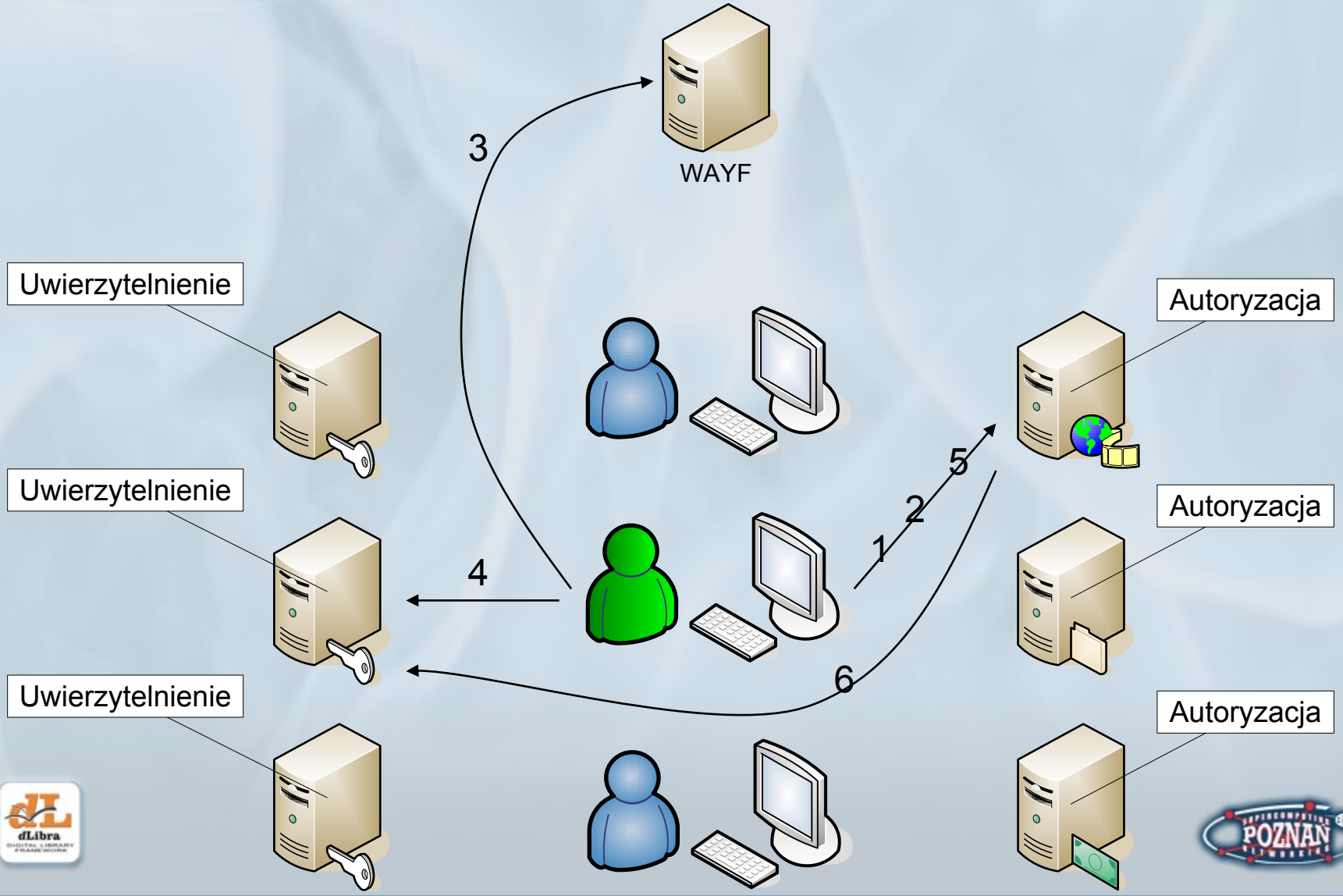
Rozwiązanie nr 2

- Połączenie wielu usług uwierzytelniających i wielu usług wymagających autoryzacji w *federację*
- *Federacja* to zbiór organizacji, które używają wspólnych zestawu atrybutów, praktyk i polityk do wymiany informacji o użytkownikach i zasobach w celu umożliwienia współpracy
- Wymiana informacji między organizacjami
  - *Niezbędne* jest zaufanie

Rozwiązanie nr 2

- Prace rozpoczęto w ramach programu Internet2 w USA
- Opracowano
  - system Shibboleth (http://shibboleth.internet2.edu/)
  - protokół SAML (http://www.oasis-open.org/committees/security/)

Shibboleth


WAYF
3
Uwierzytelnienie
Uwierzytelnienie
Uwierzytelnienie
Autoryzacja
Autoryzacja
Autoryzacja
1
2
4
5
6

Shibboleth

1. Próba pobrania zasobu
2. Nakaz uwierzytelnienia
3. Określenie instytucji macierzystej

   WAYF = *Where Are You From?* (Skąd jesteś?)
4. Uwierzytelnienie
5. Powtórna próba pobrania zasobu
6. Potwierdzenie tożsamości

Kto jest zgodny z Shibboleth?

- American Chemical Society
- ArtSTOR
- Atypon
- CSA
- Digitalbrain PLC
- EBSCO Publishing
- Elsevier ScienceDirect
- ExLibris
- JSTOR
- NSDL
- OCLC
- Ovid Technologies Inc.
- Project MUSE
- Proquest Information and Learning
- Serials Solutions
- SCRAN
- Thomson Gale
- Thomson ISI/Scientific

Shibboleth i dLibra

- Od wersji 4.0 dLibra w pełni zgodna z protokołem SAML
  - Możliwość wykorzystania konta z zewnętrznego systemu w bibliotece cyfrowej
  - Możliwość wykorzystania konta z biblioteki cyfrowej w zewnętrznym systemie
  - A więc również: możliwość wykorzystania konta z jednej biblioteki cyfrowej w innej bibliotece cyfrowej

Shibboleth i dLibra

- Nowe możliwości
  - Wykorzystanie danych z zewnętrznej bazy użytkowników przy autoryzacji dostępu do treści publikacji
    - Dotychczas możliwe tylko w oparciu o LDAP (np. KPBC - UMK)
  - Sieciowy profil czytelnika

Shibboleth i dLibra

- Realizacja
  - Budowa federacji (w znaczeniu Shibboleth) z kolejnych bibliotek cyfrowych przechodzących na dLibrę 4.0
  - Punkt WAYF zainstalowany w FBC

Shibboleth i dLibra

- Dalsze kroki
  - Udostępnianie kolejnych zewnętrznych baz użytkowników poprzez Shibboleth
  - Wykorzystanie tych baz do autoryzacji w bibliotekach cyfrowych
  - Wykorzystanie tych baz do dostępu do innych materiałów?

Pytania?

Dziękuję za uwagę!