Zarządzanie tożsamością

Grzegorz Ziemiański

Wydział Matematyki, Informatyki i Mechaniki
Uniwersytet Warszawski
gz235233@students.mimuw.edu.pl

22.10.2009

Tożsamość

Tożsamość

Łączy użytkownika z aplikacją, określa kim jest dany użytkownik i jakie ma uprawnienia

Zarządzanie tożsamością

> *Zbiór procesów i infrastruktura do tworzenia, utrzymywania i używania elektronicznych tożsamości*

Barton Group

Mały przykład

Ile tożsamości musi zapamiętać student na UW?

Mały przykład

Ile tożsamości musi zapamiętać student na UW?

1. IRK + USOS + portal wydziałowy
2. Konto na students + komputery w lab
3. Biblioteka

Mały przykład

Ile tożsamości musi zapamiętać student na UW?

1. IRK + USOS + portal wydziałowy
2. Konto na students + komputery w lab
3. Biblioteka

A niedługo będzie jeszcze lepiej.

Mały przykład

Ile tożsamości musi zapamiętać student na UJ?

Mały przykład

Ile tożsamości musi zapamiętać student na UJ?

1. USOS
2. Rejestracja do grup
3. Intranet
4. Windows
5. Linux
6. Stacje bezdyskowe
7. Poczta wydziałowa
8. Biblioteka

Proste rozwiązania

- System poziomów haseł
- Hasła zapisane na karteczkach

Dlaczego są złe?

- Zalogowanie do jednego serwisu może dać możliwość dostania się do innego
- Utrata jednego kompromituje tożsamość w wielu serwisach
- Panie sprzątające mają dostęp do komputera szefa ☺

Początki - application silos

- Każda aplikacja przechowuje tylko informacje o własnych użytkownikach
- Nie widać potrzeby współpracy między aplikacjami (w kwestii użytkowników)
- Nie jest to wtedy jeszcze aż tak uciążliwe

Plusy:

- Każdy zarządza tylko swoimi użytkownikami
- Utrata hasła naraża tylko jedną aplikację

Minusy:

- Milion nazw użytkowników i haseł do zapamiętania
- Zapisywanie danych na kartkach
- Słaba ochrona danych

Scentralizowane bazy danych

- Skoro mamy jedną organizację to po co przechowywać wiele kopii tożsamości tego samego użytkownika?
- Z pomocą przychodzi LDAP

Plusy:

- Mniej danych, którymi trzeba zarządzać
- Mniej pieniędzy na wypłaty dla adminów
- Jeden login i jedno hasło w danej organizacji

Minusy:

- Trzeba uwierzytelniać się za każdym razem
- Utrata hasła kompromituje wszystkie serwisy w organizacji

SSO - Single Sign-On

- Skoro mamy to samo hasło to po co je wpisywać wiele razy?
- Z pomocą przychodzi np. nasz ulubiony CAS (aka CSU)

Plusy:

- Aplikacja nie ogląda hasła użytkownika
- Logujemy się tylko raz
- Aplikacje mniej przejmują się logowaniem

Minusy:

- Utrata hasła kompromituje wszystkie serwisy w organizacji
- Trochę kulawe wylogowywanie

Czym jest federacja?

http://www.syfy.com/enterprise/gallery

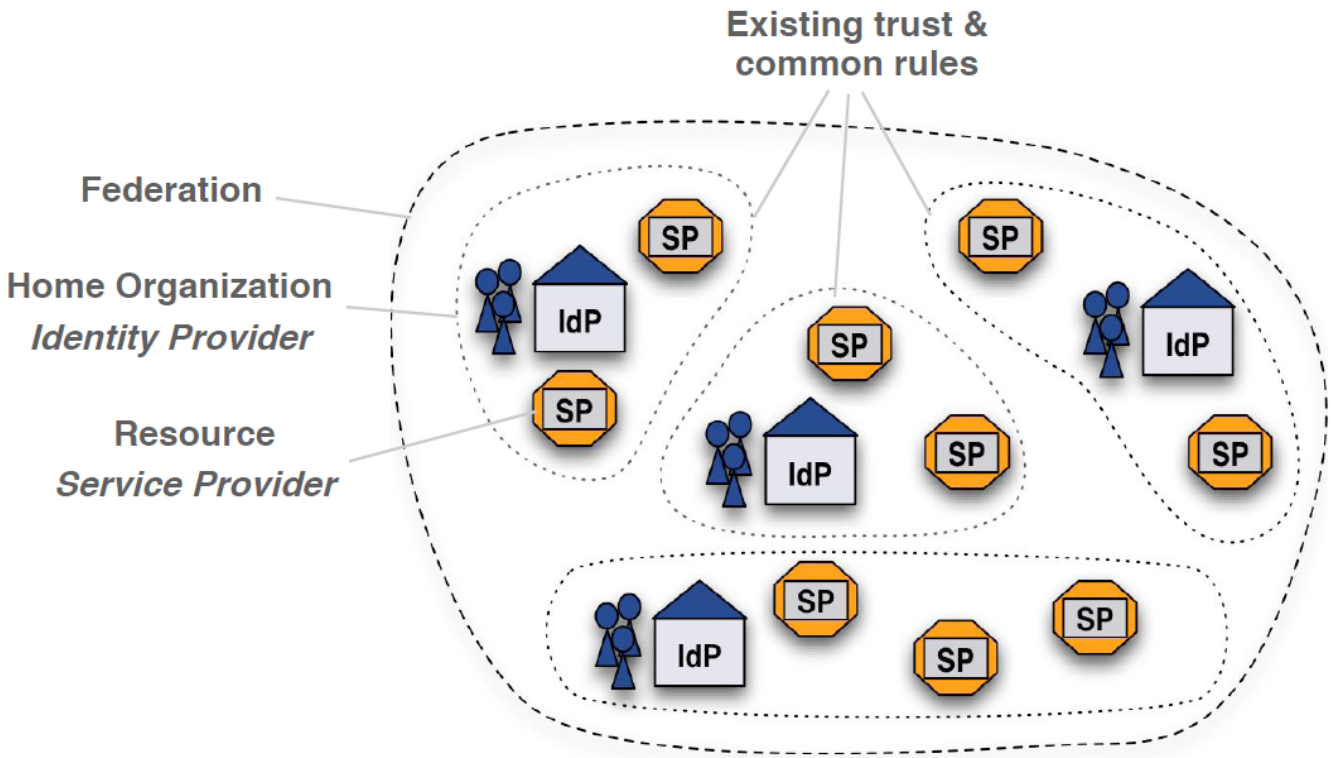
Czym jest federacja?

Federacja

Zjednoczona Federacja Planet (ang. United Federation of Planets) to międzygwiezdny twór państwowy zbudowany jako porozumienie rządów istot rozumnych zamieszkujących część Kwadrantu Alfa.
Organizacja ta zrzesza światy, których mieszkańcy dysponują napędem warp (lub inną metodą przemieszczania się z prędkością większą niż prędkość światła).

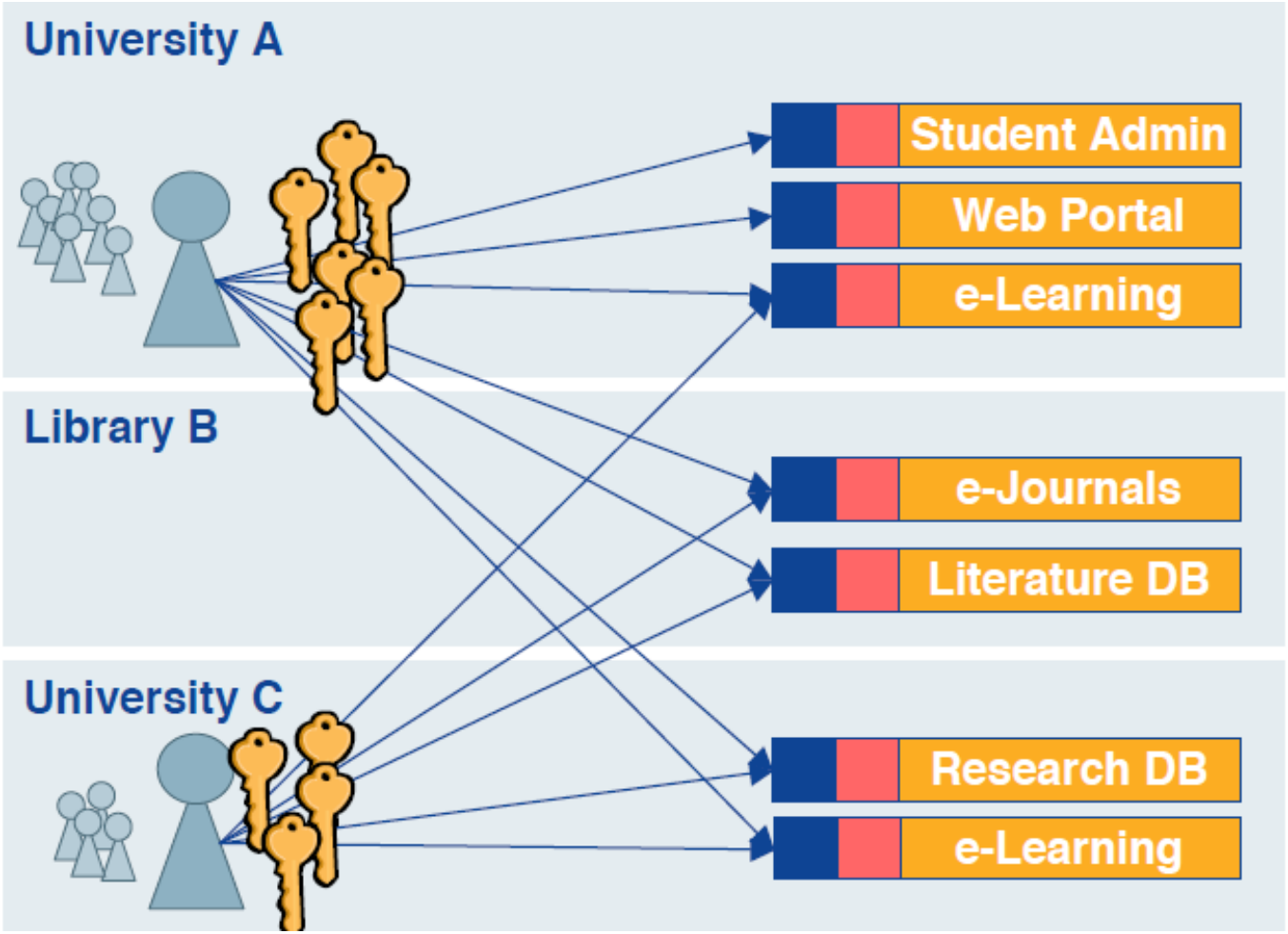
http://memory-alpha.org/pl/wiki/Zjednoczona_Federacja_Planet

Czym jest federacja?



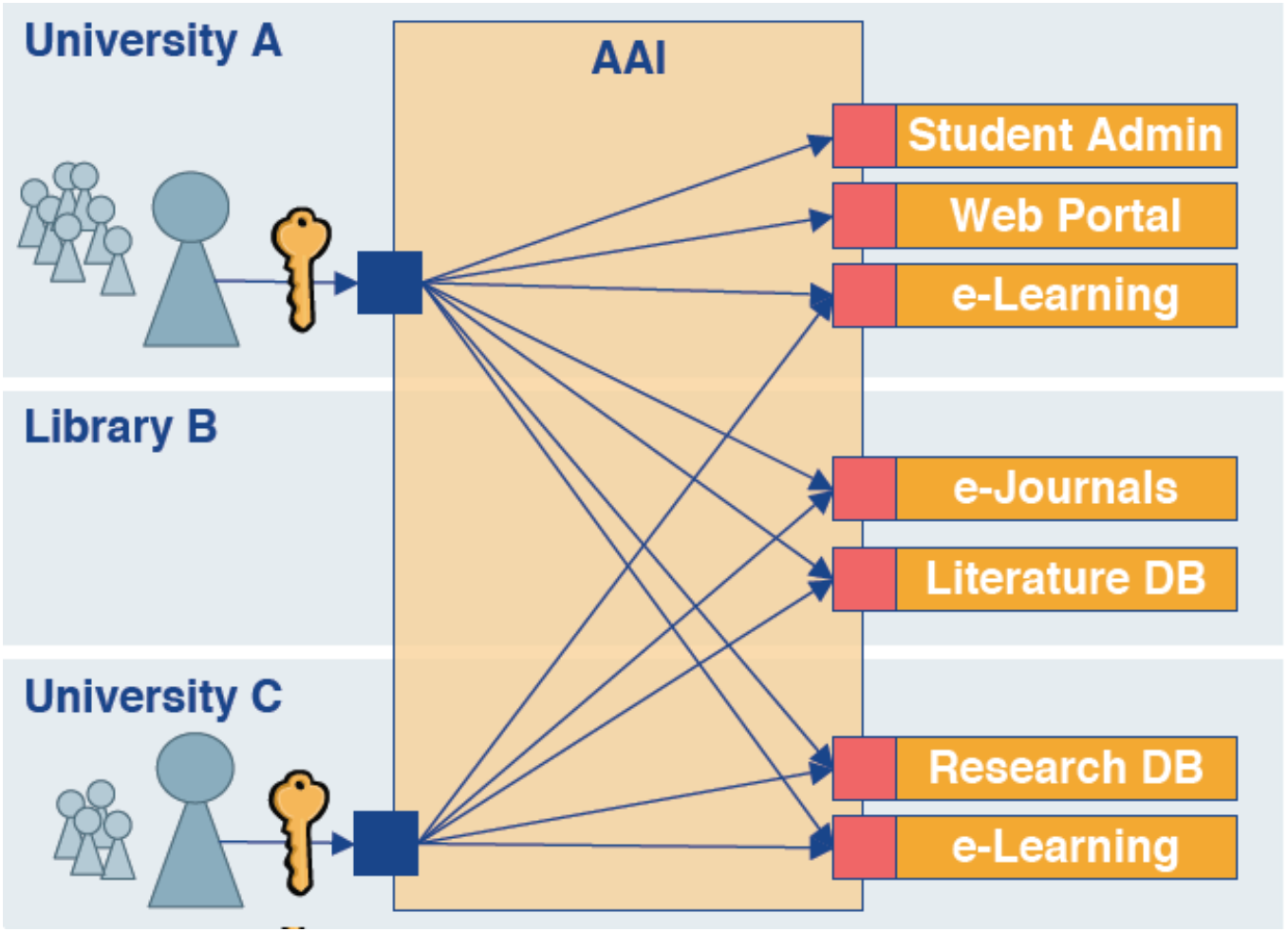
http://www.switch.ch/aai/support/presentations/ws-webres-2007-ls/AAI-Res-WS-Intro.pdf

Bez federacji



http://www.switch.ch/aai/support/presentations/ws-webres-2007-ls/AAI-Res-WS-Intro.pdf

Z federacją

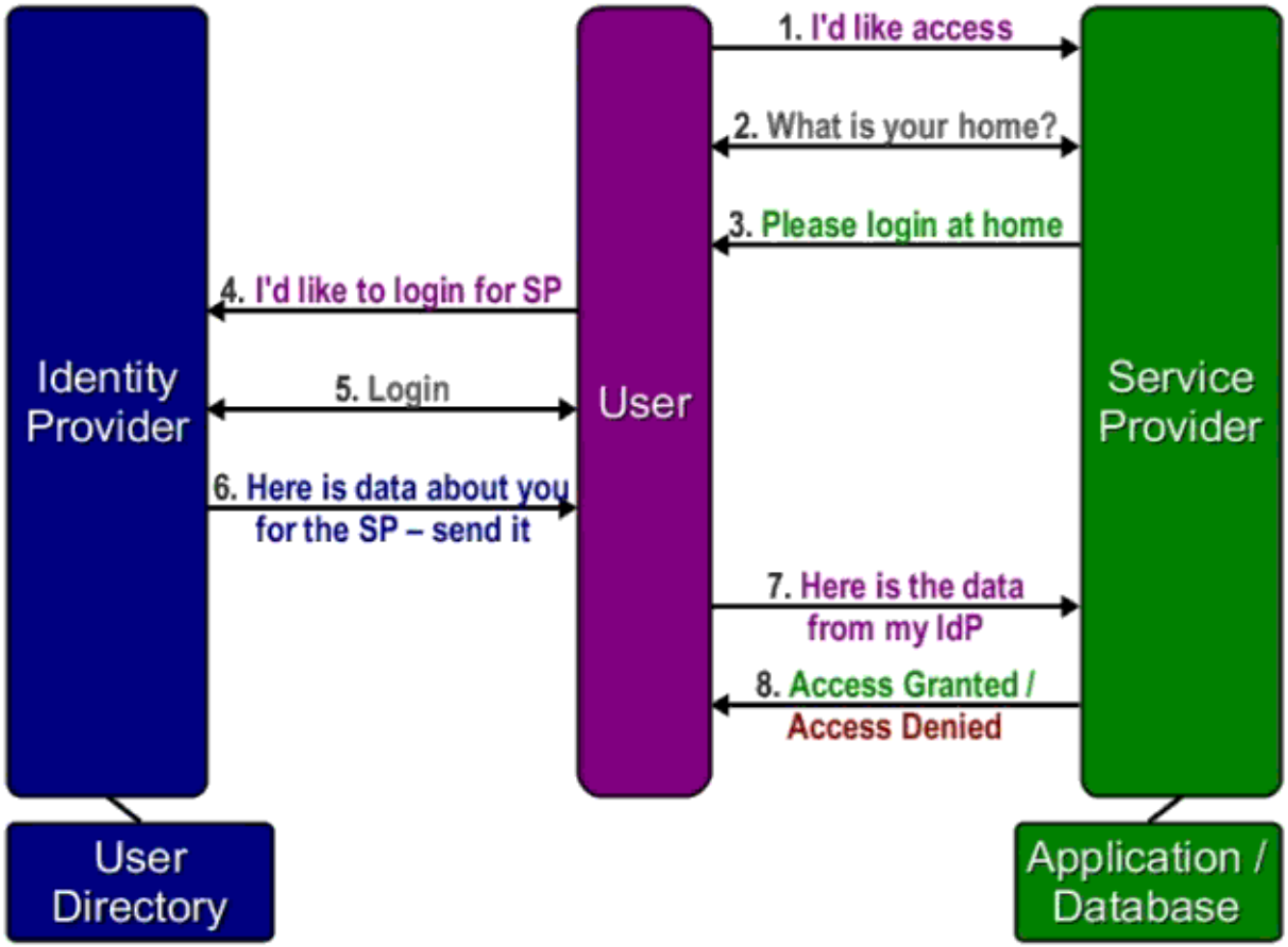


http://www.switch.ch/aai/support/presentations/ws-webres-2007-ls/AAI-Res-WS-Intro.pdf

Federacyjne zarządzanie tożsamością

- Rozszerzenie systemów SSO o zaufanie do innych wewnątrz federacji
- Każdy system utrzymuje informacje o własnych użytkownikach
- Udostępnia je poprzez system atrybutów
- Potrzebny serwis umożliwiający odnalezienie „domu” użytkownika
- Hasło nie jest oglądane przez aplikacje

Schemat działania



Dlaczego federacja?

- Upraszcza zarządzanie atrybutami, przywilejami, użytkownikami
- Poprawia bezpieczeństwo
- Chroni prywatność
- Oszczędza pieniądze
- Bo tak mówi Gartner

Dlaczego federacja na uniwersytecie?

- I tak przechowuje dużo informacji o użytkownikach
- Dokładny proces weryfikacji osoby w rzeczywistości
- Studenci i pracownicy korzystają z wielu aplikacji i programów również innych instytucji (np. MSDN AA, współpraca między uczelniami)

Skąd jestem?

- Przyciski
- Lista (pull-down)
- OpenID url, domena, e-mail
- Smart clients
- Cryptographic cards

Kim jestem?

- Nick
- Mail
- Imię i nazwisko
- Trwałe identyfikatory
- Tymczasowe identyfikatory

Problemy

- Trzeba zaufać innym
- Problem z atrybutami (eduPerson, inetOrgPerson)
- Czy każdy student ma mieć dostęp?
- Kompromitacja hasła naraża dostęp do serwisów całej federacji...
- ...ale jest mniejsza szansa, że do tego dojdzie

Czym jest LDAP?

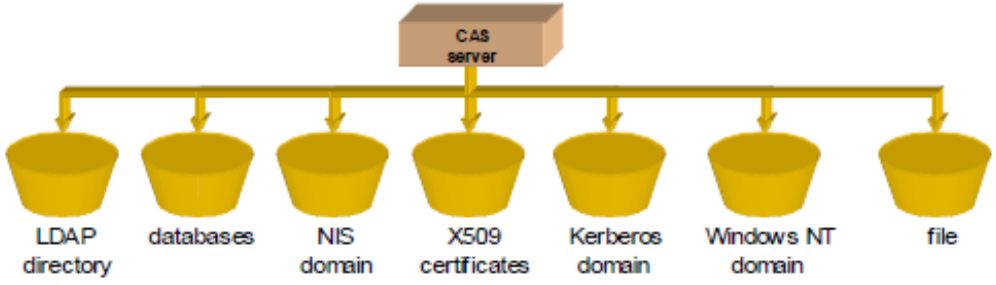
- Lightweight Directory Access Protocol
- Protokół dostępu do usług katalogowych
- Dane tworzą strukturę drzewa
- Umożliwia szybkie wyszukiwanie, ale wolniejsze wstawianie i modyfikację
- Każdy wpis ma swój unikalny identyfikator (Distinguished Name)

Przykład LDIF

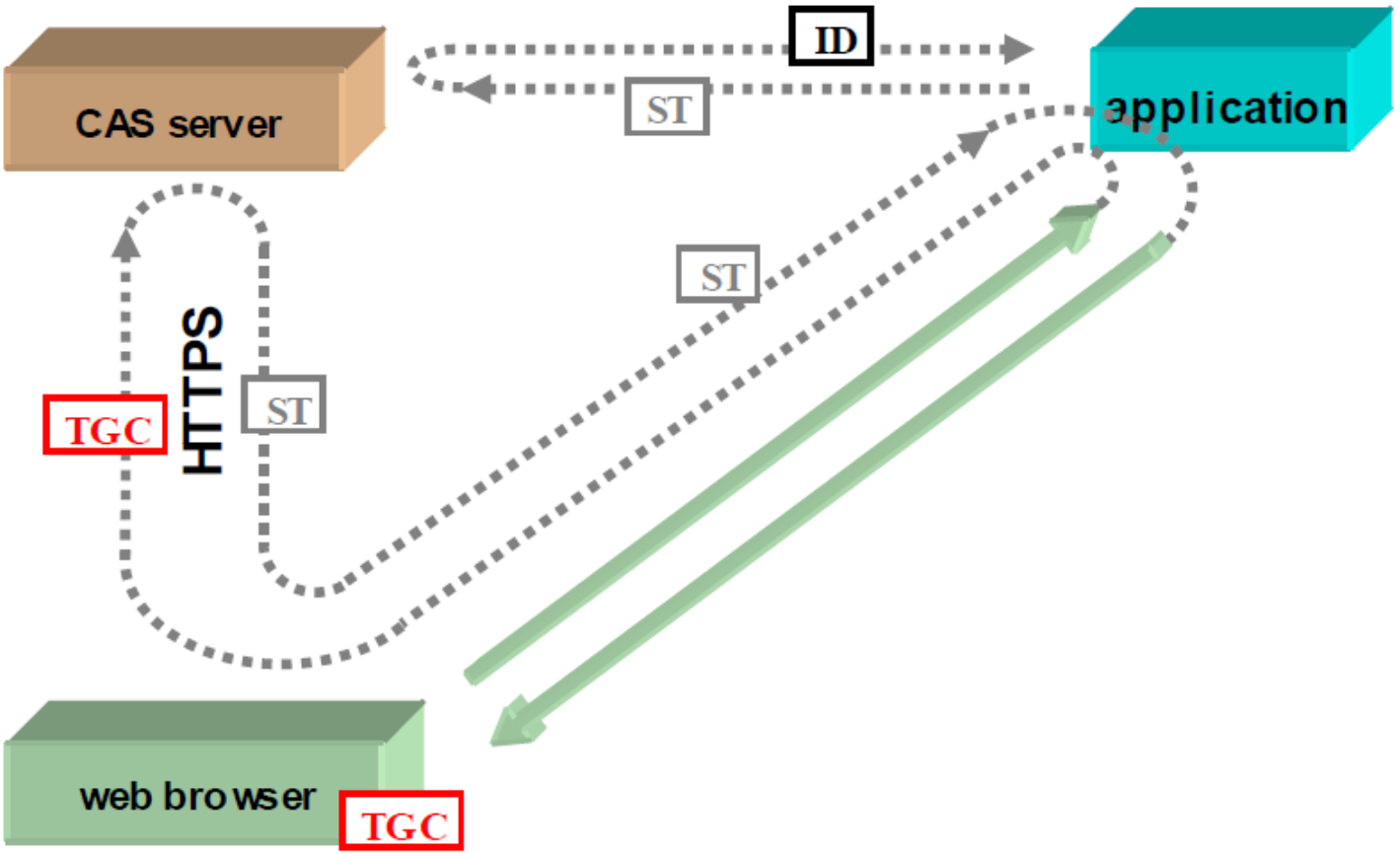
```
dn: cn=John Doe,dc=example,dc=com
cn: John Doe
givenName: John
sn: Doe
telephoneNumber: +1 888 555 6789
telephoneNumber: +1 888 555 1232
mail: john@example.com
manager: cn=Barbara Doe,dc=example,dc=com
objectClass: inetOrgPerson
objectClass: organizationalPerson
objectClass: person
objectClass: top
```

Kilka słów o CAS

- Powstał na YALE
- Obecnie prowadzony przez JASIG
- Serwer działa jako Servlet
- Klienci dostępni dla Javy, PHP, Perl, ASP, .Net
- Wersja 2.0 wprowadza proxy
- Aplikacja dowiaduje się kim jest użytkownik bez oglądania hasła
- Ale sama musi wiedzieć jakie ma uprawnienia
- I co najważniejsze jest za darmo

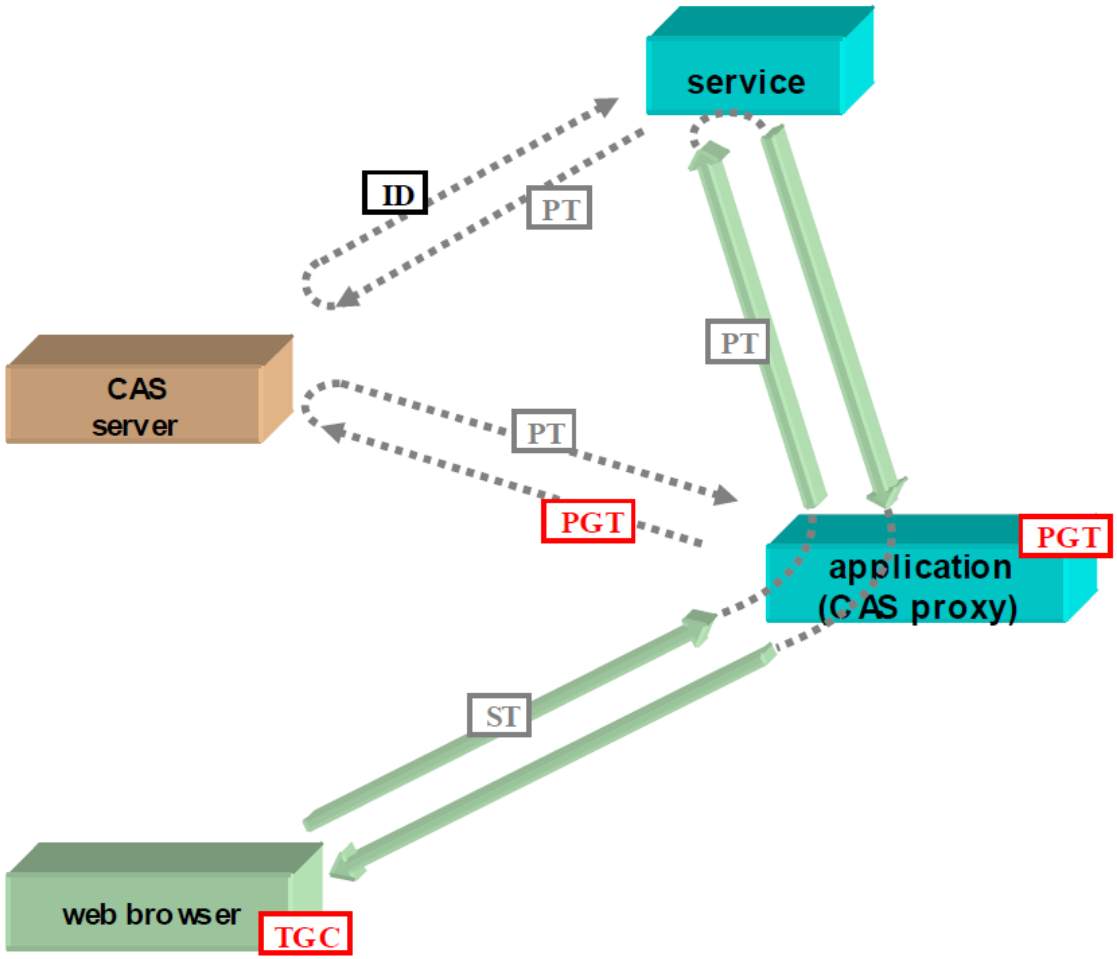


Zasada działania



http://www.esup-portail.org/consortium/espace/SSO_1B/cas/eunis2004/cas-eunis2004-article.pdf

Dla dociekliwych proxy



http://www.esup-portail.org/consortium/espace/SSO_1B/cas/eunis2004/cas-eunis2004-article.pdf

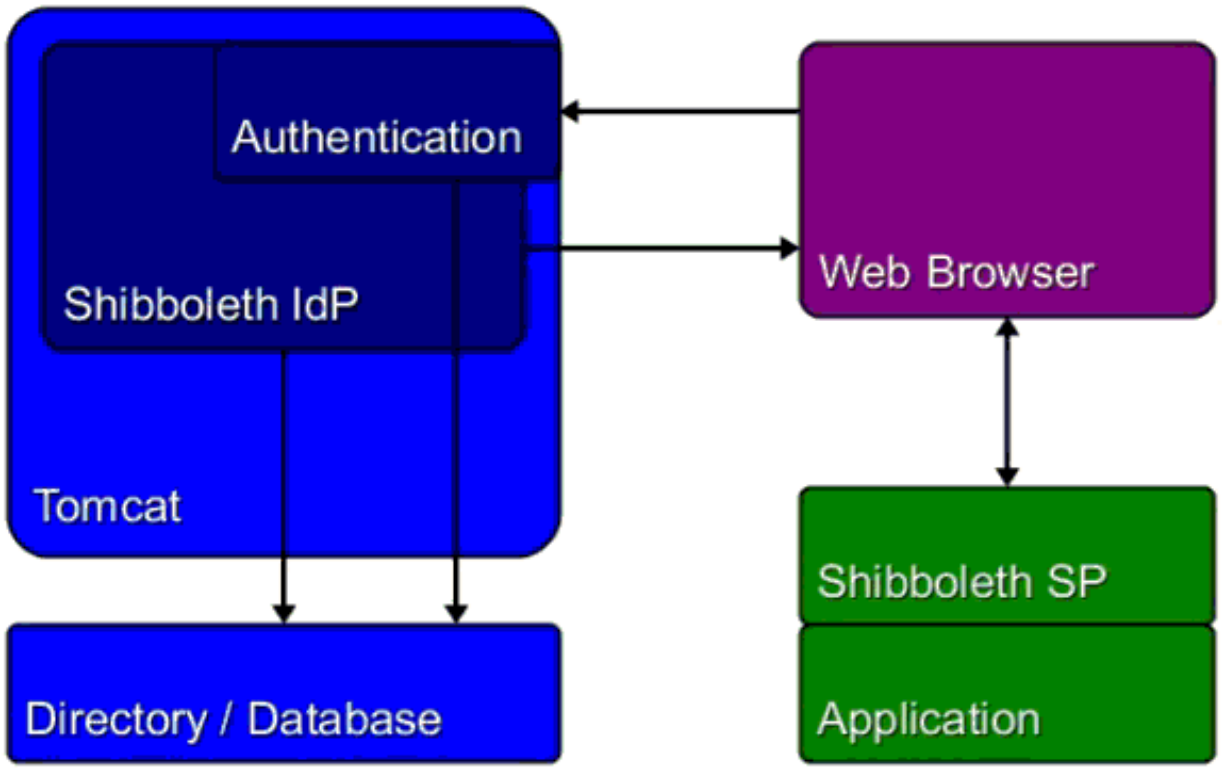
Shibboleth

1. Początki projektu w roku 2000, kod w 2003
2. Licencja Apache 2.0
3. Oparty na SAML
4. Używany w dużych federacjach np. InCommon
5. http://shibboleth.internet2.edu

Shibboleth®

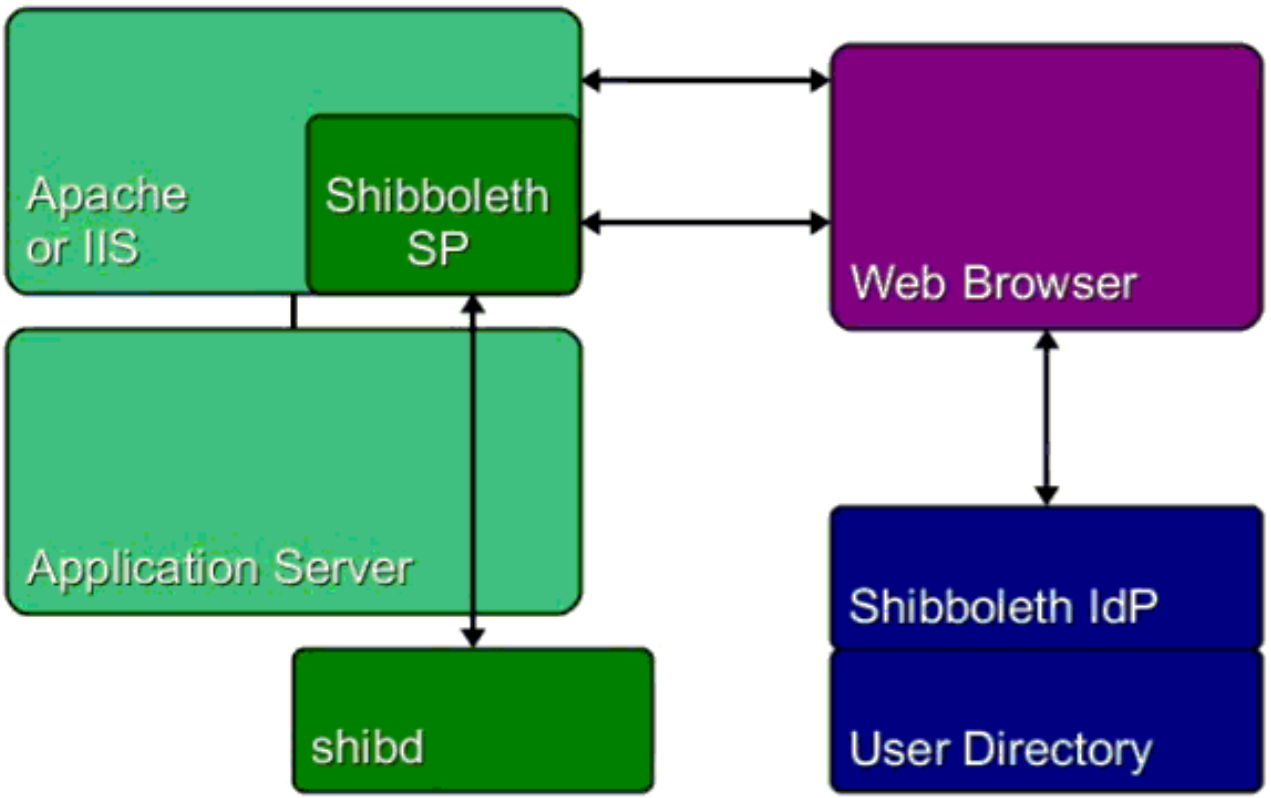
Identity Provider (IP)

1. Działa jako servlet
2. Sam nie przechowuje danych, pobiera je z innych źródeł (np. LDAP)

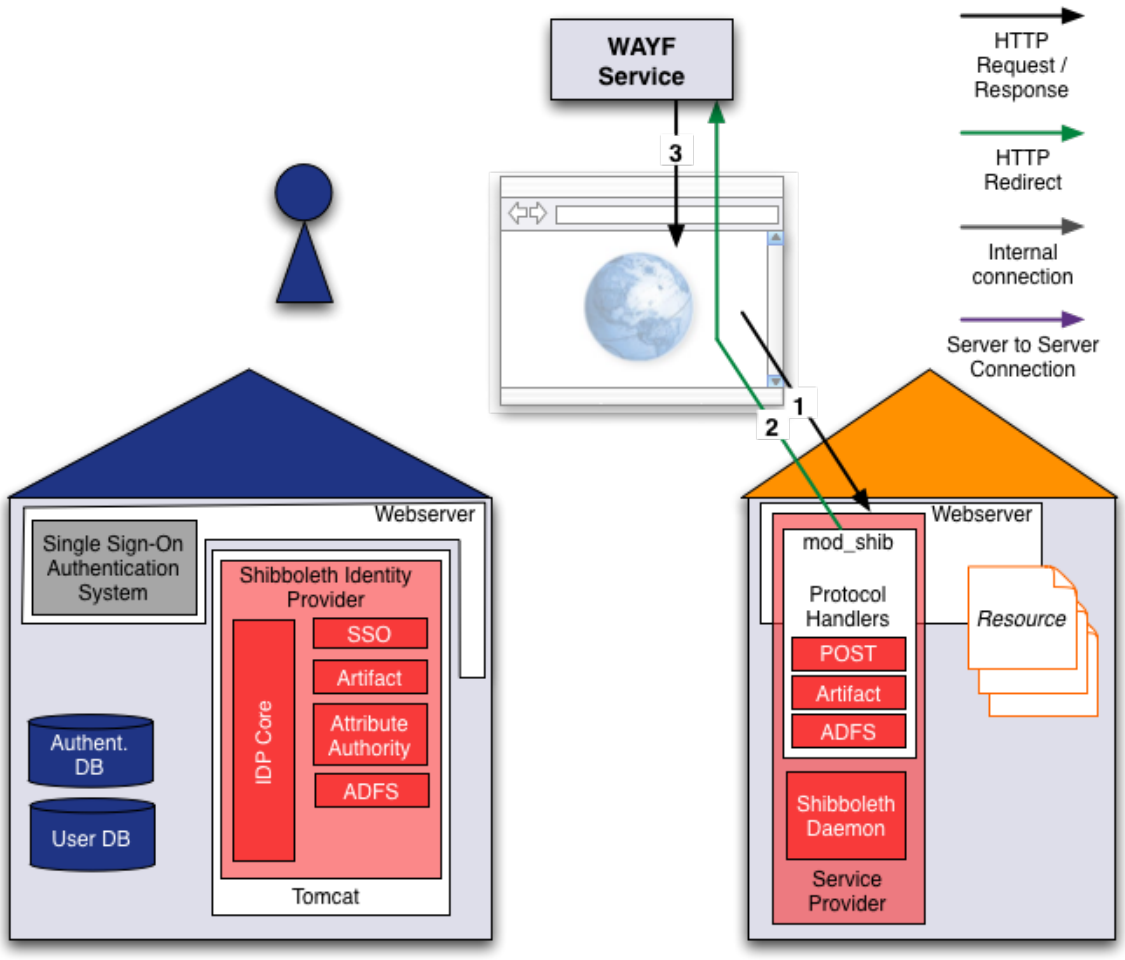


Service Provider (SP)

1. Napisany w C++ jako plugin m. in. do Apache i IIS
2. Wersja servlet
3. Nie ma API, przekazuje dane jako atrybuty

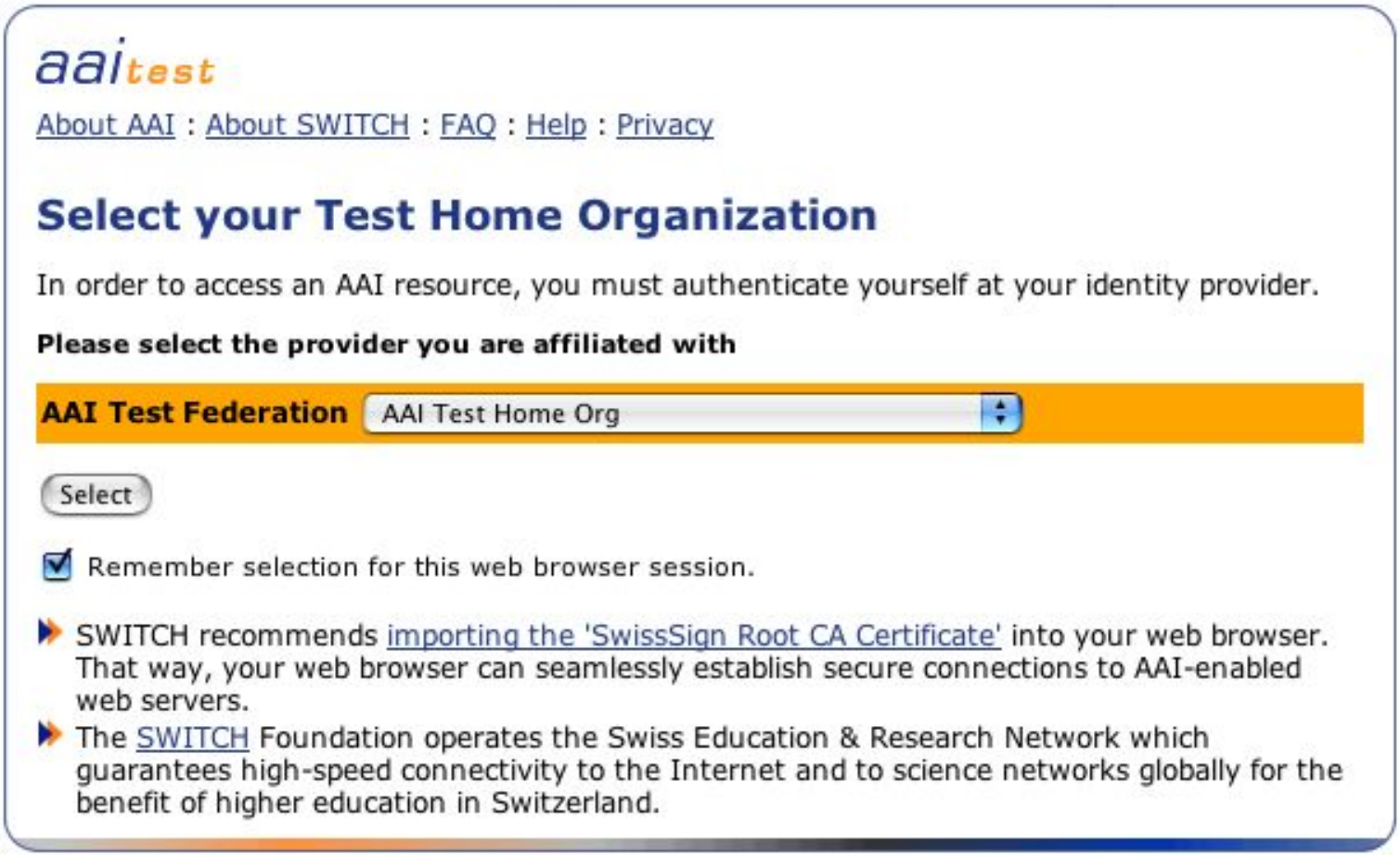


Działanie



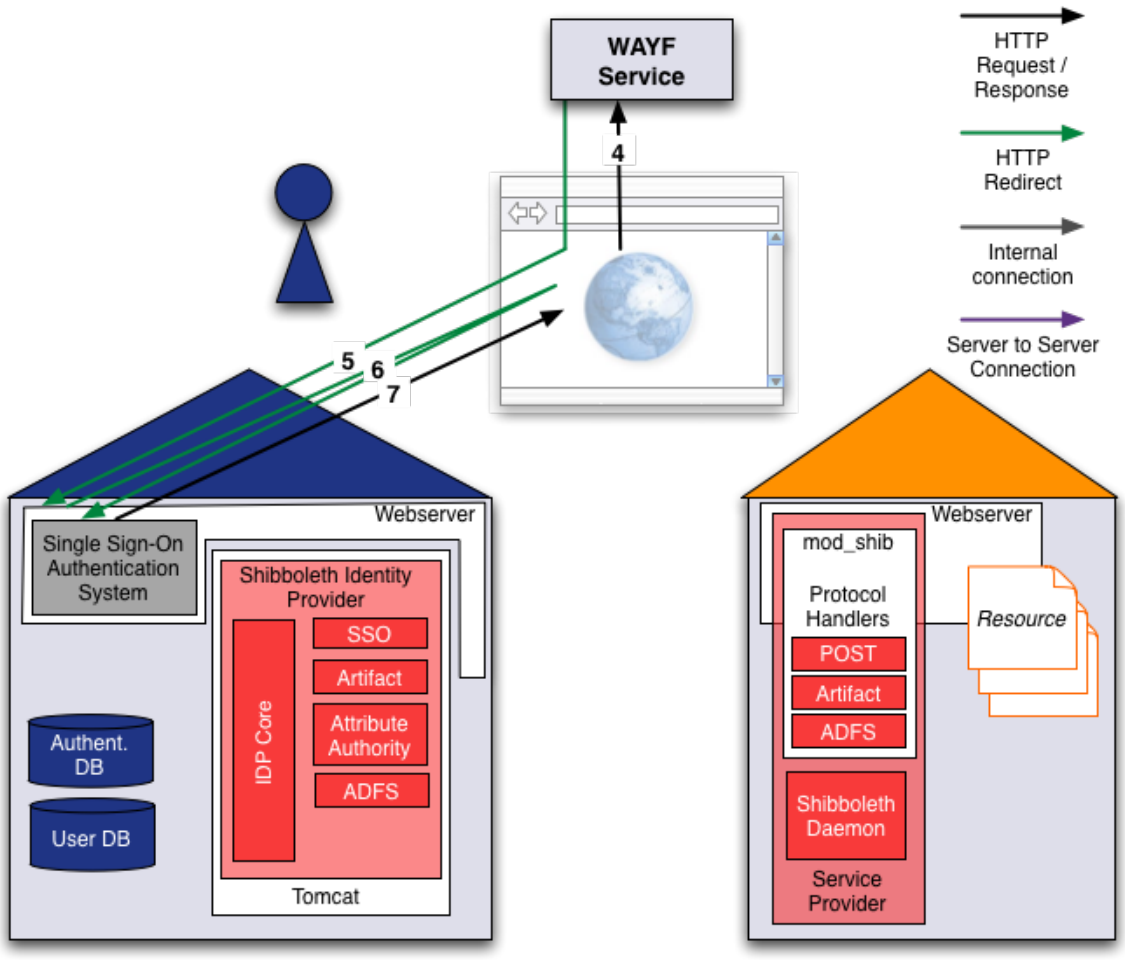
http://www.switch.ch/aai/demo/expert.html

Działanie



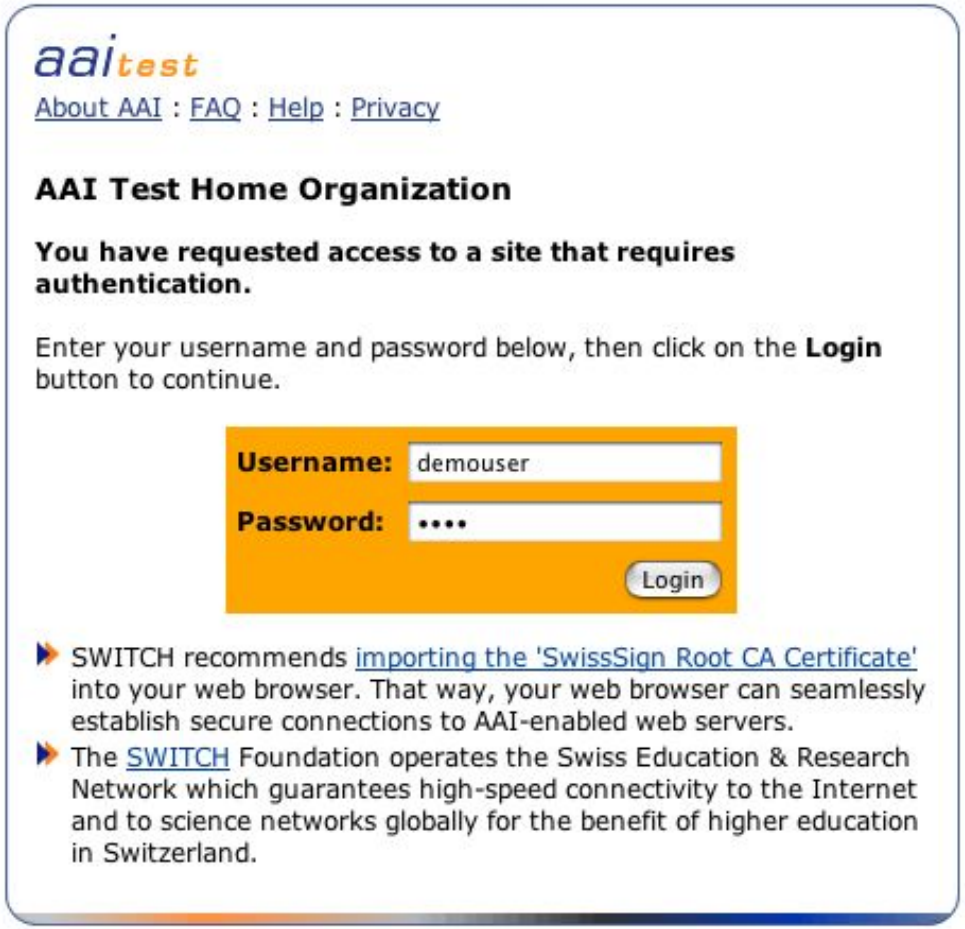
http://www.switch.ch/aai/demo/expert.html

Działanie



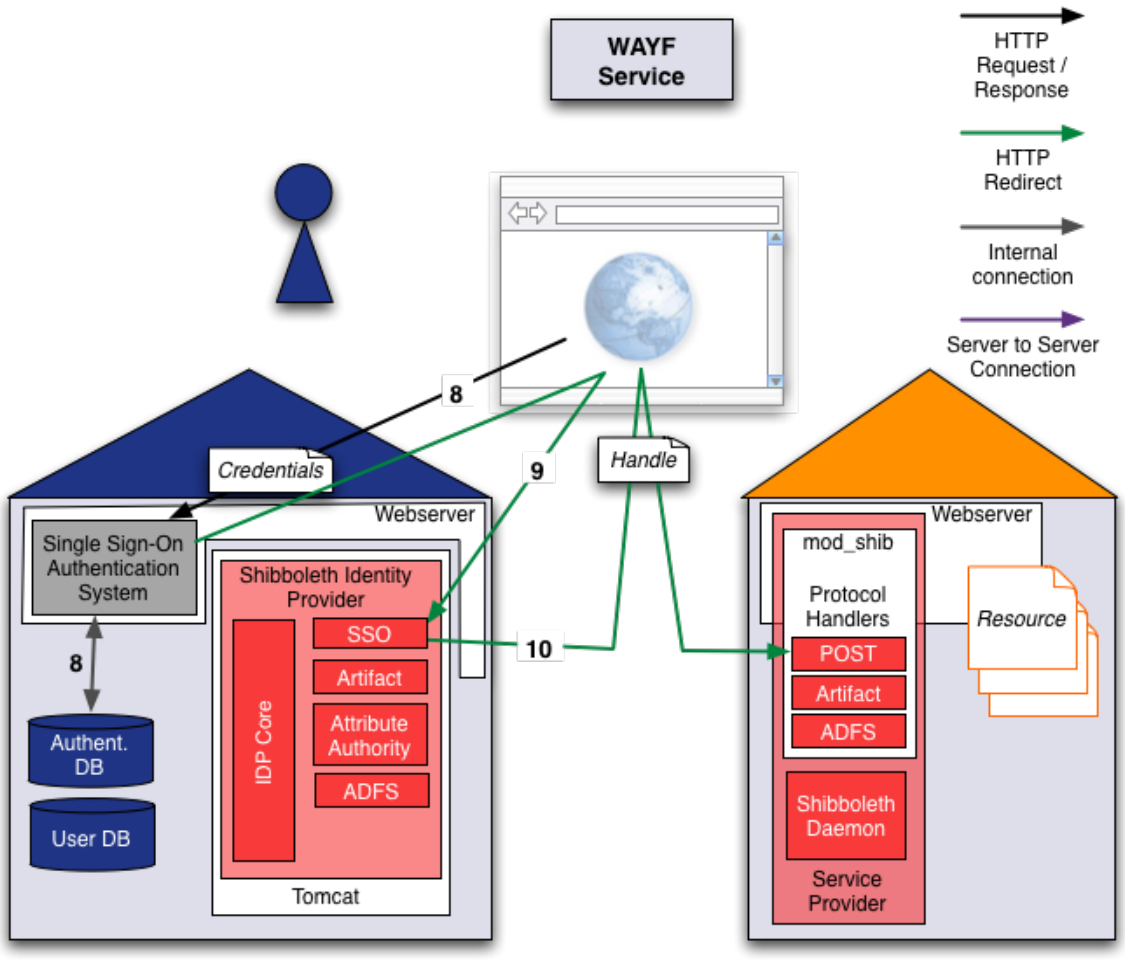
http://www.switch.ch/aai/demo/expert.html

Działanie



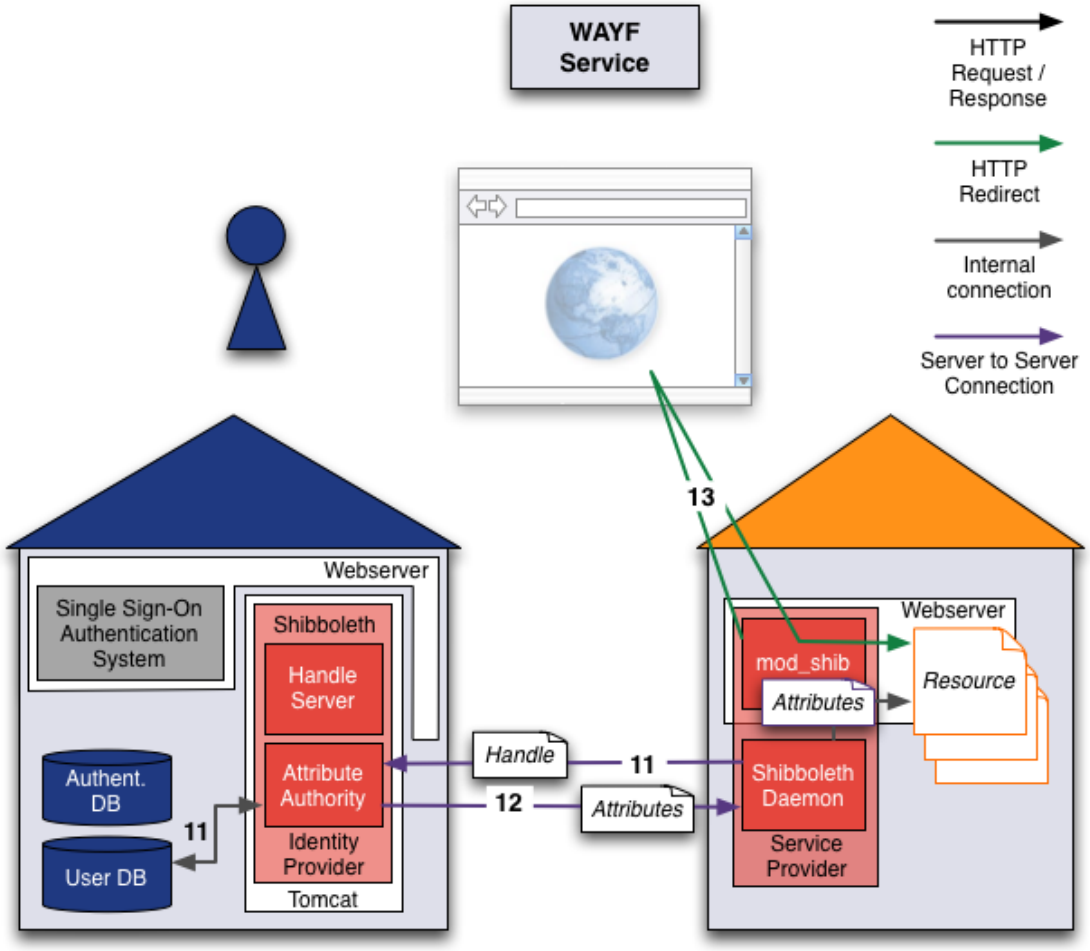
http://www.switch.ch/aai/demo/expert.html

Działanie



http://www.switch.ch/aai/demo/expert.html

Działanie



http://www.switch.ch/aai/demo/expert.html

Wylogowanie

1. Duży problem
2. Czy każda aplikacja może zakończyć wszystkie sesje?
3. Co w przypadku problemów czy braku łączności?
4. Obsługuje dopiero SAML 2.0...
5. ...a Shibboleth jeszcze nie za bardzo.
6. https://spaces.internet2.edu/display/SHIB2/SLOWebappAdaptation
7. https://www.aai.niif.hu/software

Po co nam to?

1. W skrócie MOST i Erasmus
2. Ułatwiony dostęp do zasobów (np. biblioteki) dla studentów na wymianie
3. Możliwość dostępu do USOSweb dla innych
4. Można rozszerzyć obieg dokumentów
5. Czyli możemy nadać uprawnienia osobom spoza uczelni

X.509 i PKI

1. Zabezpieczenie tym co znamy i tym co mamy
2. Legitymacja studencka dużo potrafi ☺
3. Sam certyfikat to za mało
4. Trzeba ograniczyć długość ścieżki certyfikatów
5. Można cyfrowo podpisywać dokumenty

Linki

1. https://aai-demo.switch.ch
2. http://www.switch.ch/aai/
3. http://www.jasig.org/cas
4. http://www.terena.org/activities/idm/moldova/intro2LDAP.pdf
5. http://www.oasis-open.org/committees/download.php/13525/sstc-saml-exec-overview-2.0-cd-01-2col.pdf