AAI & Shibboleth

HBONE Workshop

Bajnok Kristóf
NIIF Intézet
bajnokk@niif.hu

2007. november 7.

AAI

- **Cél 1: az autentikációt és az autorizációt leválasztani az alkalmazásról**
  - biztonságosabb
  - egyszerűbb
    - Single Sign on
  - egységesebb
- **Cél 2: Föderáció**
  - elosztott felhasználó menedzsment

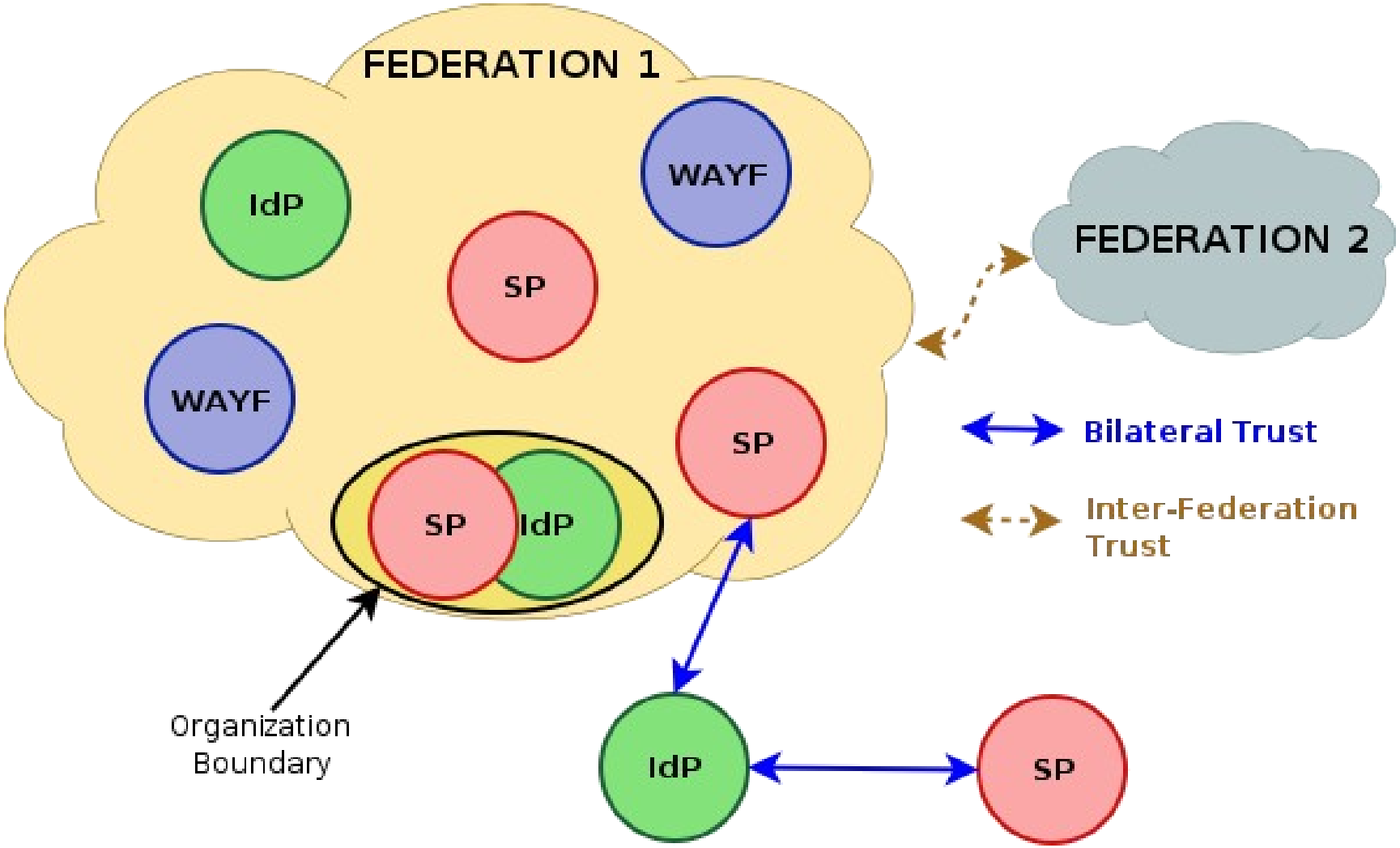
Federation

- Több intézmény közösen dolgozik
  - A közösen használt erőforrásokhoz szabályozott keretek között kell hozzáférni
  - **Legyen elég egyetlen identitás!**
- Az intézmények **megbíznak** egymás *Identity Managementjében*
  - eljárások
  - attribútumok használata

Federation elemek

- **Identity Provider (IdP)**: „anyaintézmény”
  - azonosítást végez (SSO domainek között is)
  - felügyeli az identitásokat
  - felhasználói adatokat szolgáltat
- **Service Provider (SP)**: tartalomszolgáltató
  - megbízik az IdP-ben
    - nincsenek saját felhasználói
- Federation management
  - Home location (**WAYF**), metadata, stb
    - WAYF = Where Are You From?

Federation Topológia



Kommunikáció az AAI-n belül

- **SAML** (Security Assertion Markup Language)
  - OASIS nyílt szabvány, XML alapú
  - **Assertion**: állítás + paraméterek + aláírás
    - autentikációs esemény
    - attribútumok (+ egyéb...)
  - Profilok:
    - Browser profilok: az üzenetek továbbítása a böngészőn keresztül (POST)
    - SOAP-alapú profilok: közvetlen

SAML Assertion

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion"
                MajorVersion="1" MinorVersion="1"
                AssertionID="a76adf55-01d7-40cc-929f-dbd8372ebdfc"
                IssueInstant="2005-09-22T08:59:12Z"
                Issuer="https://idp.example.org/shibboleth">
  <saml:Conditions      NotBefore="2005-09-22T08:59:12Z"
                        NotAfter="2005-09-22T09:29:12Z">
    <saml:AudienceRestrictionCondition>
      <saml:Audience>http://sp.example.org/shibboleth</saml:Audience>
    </saml:AudienceRestrictionCondition>
  </saml:Conditions>
  <saml:AuthenticationStatement AuthenticationInstant="2005-09-22T08:59:08Z"
                                AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
    <saml:Subject>
      <saml:NameIdentifier      Format="urn:mace:shibboleth:1.0:nameIdentifier"
                                NameQualifier="https://idp.example.org/shibboleth">
        7ab1827f-771bed71-55412a-121332ffe
      </samlNameIdentifier>
      <saml:SubjectConfirmation>
        <saml:ConfirmationMethod>
          urn:oasis:names:tc:SAML:1.0:cm:bearer
        </saml:ConfirmationMethod>
      </saml:SubjectConfirmation>
    </saml:Subject>
  </saml:AuthenticationStatement>
</saml:Assertion>
```

„Handle”:
A Subject azonosítója

Shibboleth

Forrás:
http://www.thebricktestament.com

Bírák 12,4-5: És elfoglalák a Gileádbeliek Efraim előtt a Jordán réveit...

Forrás:
http://www.thebricktestament.com

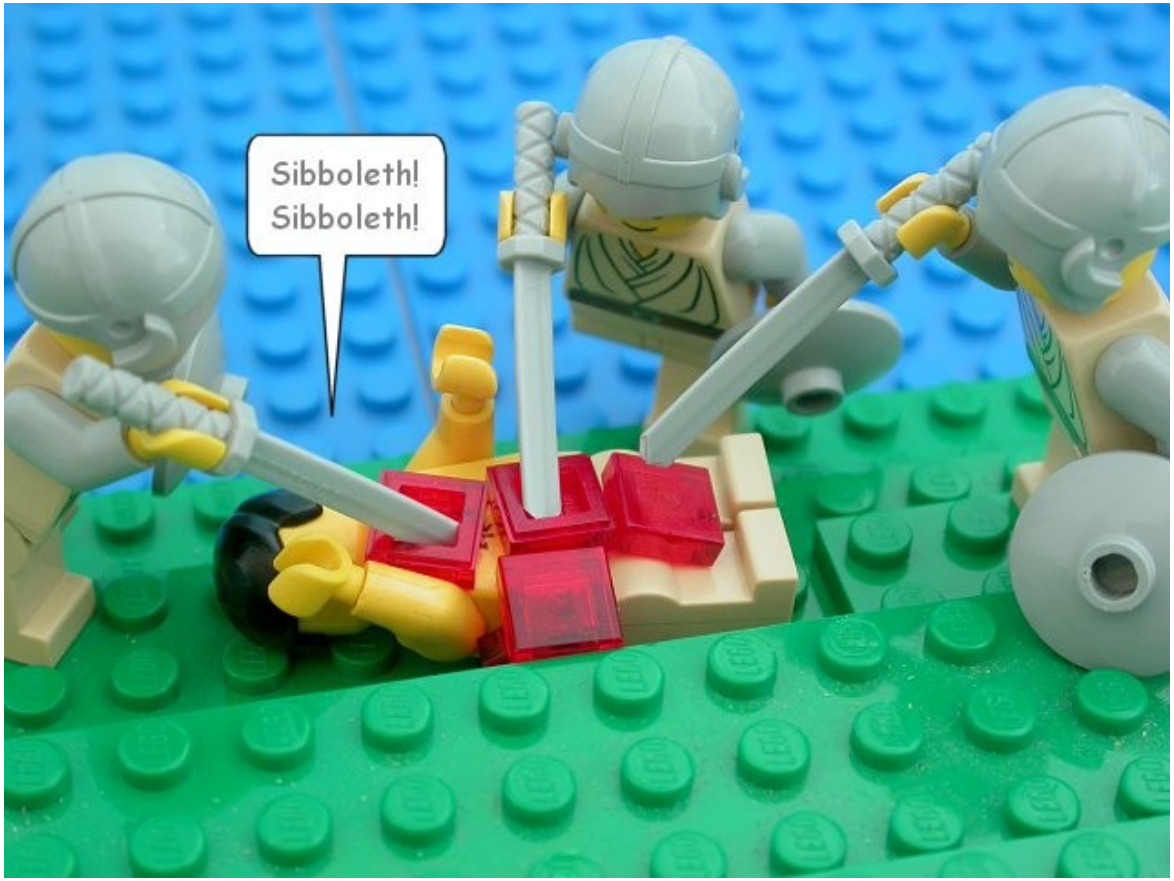
Bírák 12,5: ... és lőn, hogy mikor az Efraim közül való menekülők azt mondják vala: Hadd menjek által: azt kérdezték tőlük a gileádbeli férfiak: Efraimbeli vagy-é? ...

Forrás:
http://www.thebricktestament.com

Bírák 12,5-6: ... és ha azt mondotta: nem!
Akkor azt mondák néki: Mondd: Sibboleth! ...

Forrás:
http://www.thebricktestament.com

Bírák 12,6: ... És ha Szibbolethet mondott, mert nem tudta úgy kimondani, ...



Bírák 12,6: ... akkor megfogták őt és megölték a Jordán réveinél, ...

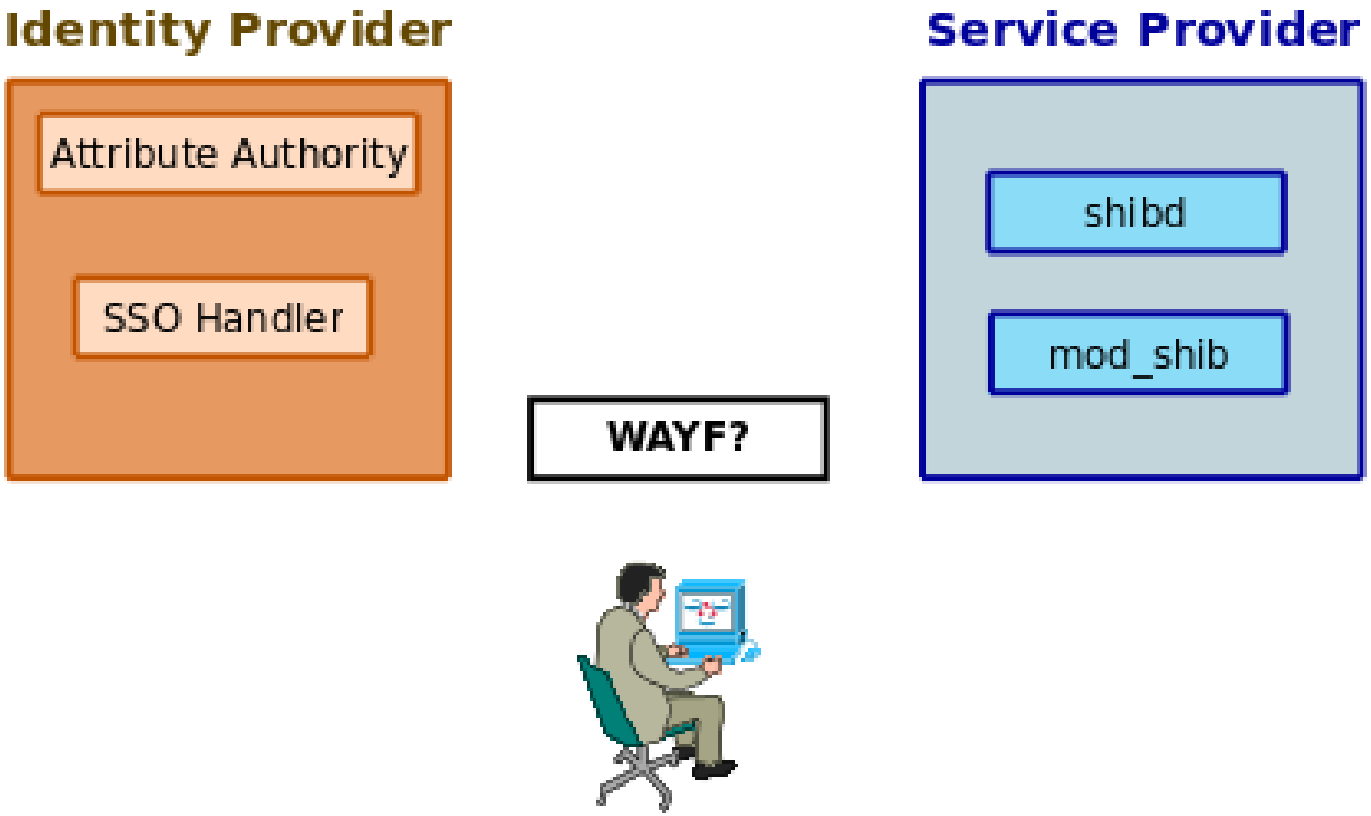
Forrás:
http://www.thebricktestament.com

Bírák 12,6: ... és elesett ott abban az időben az Efraimbeliek közül negyvenkétezer.

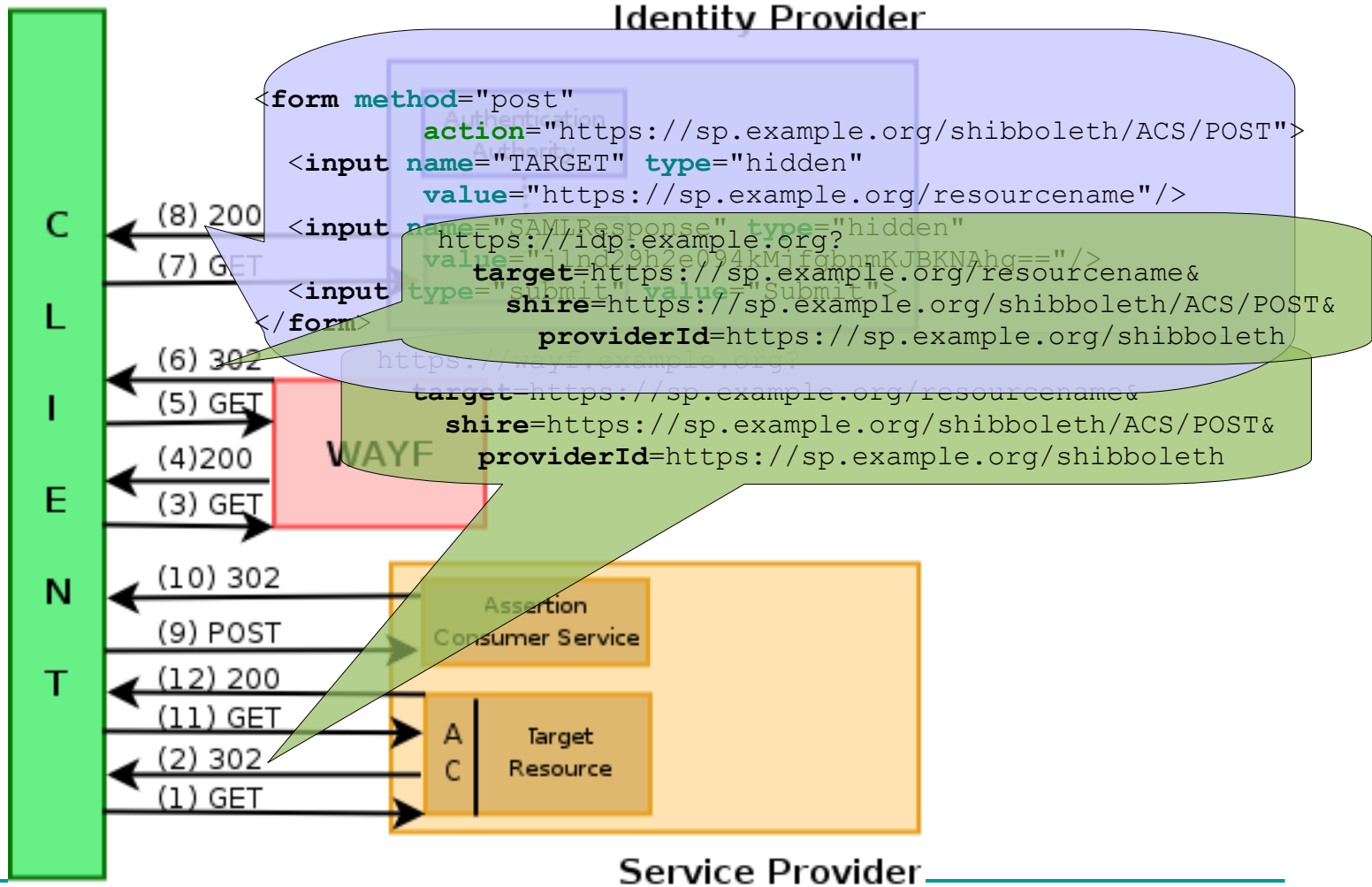
Shibboleth

- **Internet2** által fejlesztett szoftver
  - Webes Single Sign-On
  - Föderáció
  - SAML 1.1 kompatibilitás
    - részben... a Shibboleth 1.3 egy protokoll is egyben
  - nyílt forráskódú
- **IdP**: Java
- **SP**: Apache / IIS modul
- (**WAYF**): Java (proof-of-concept)

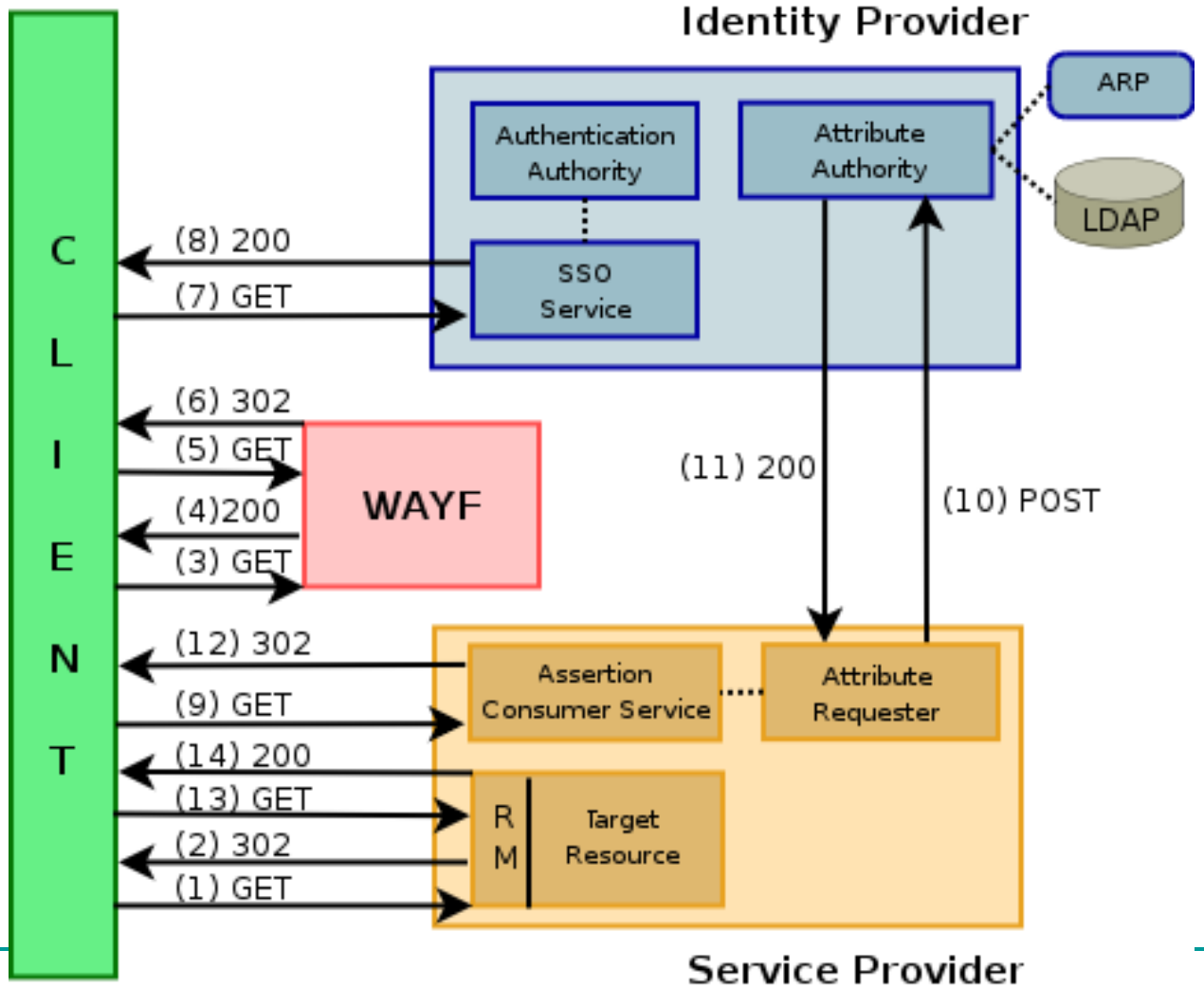
Shibboleth architektúra áttekintés



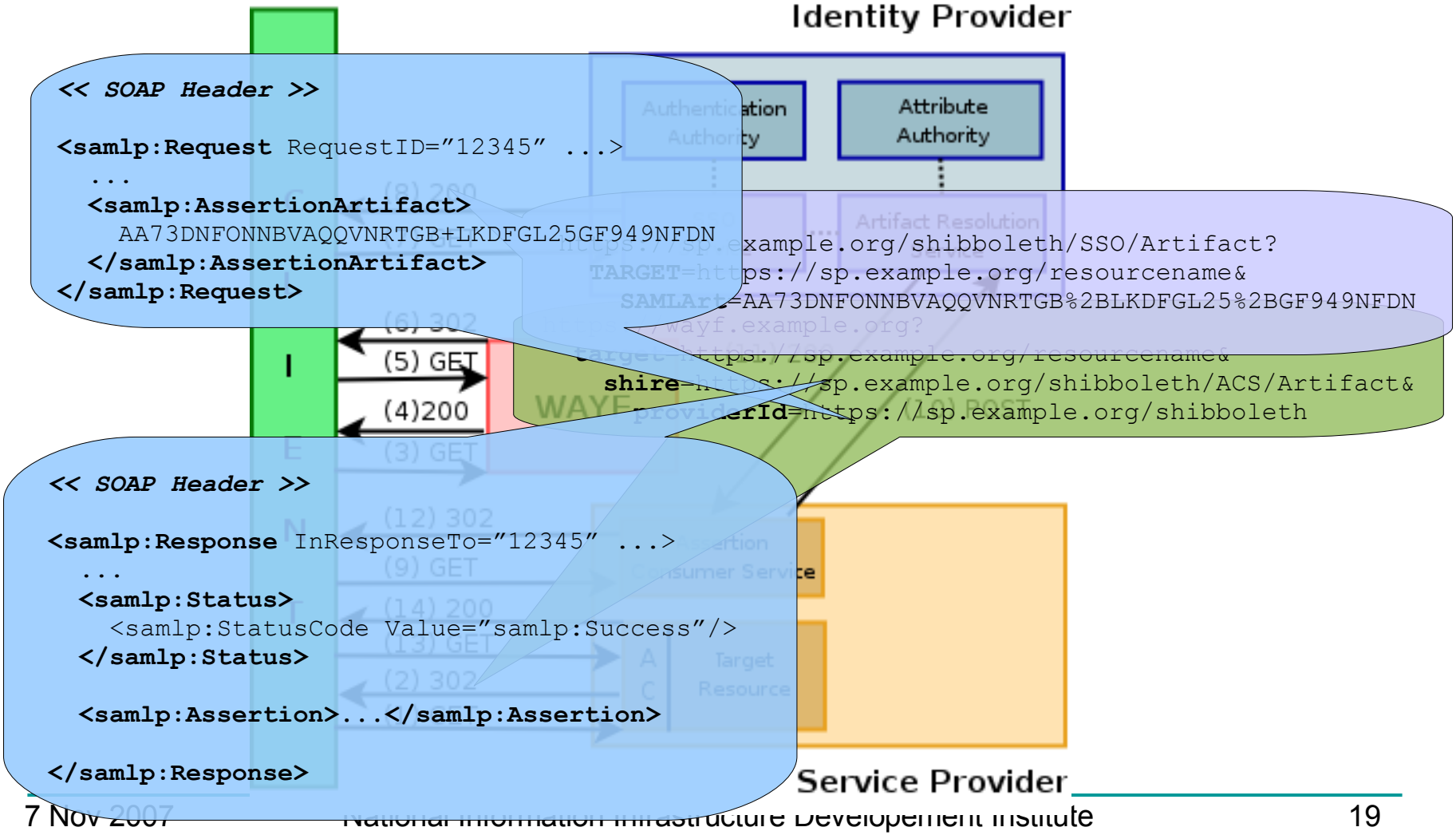
Browser/POST Profile



Attribute Exchange



Browser/Artifact Profile



Metaadatok

- Metadata
  - IdP metaadatok: intézményi adatok + cert +
    - Scope
    - SSO
      - Artifact Resolution Service URL
    - AA
  - SP metaadatok: intézményi adatok + cert +
    - Assertion Consumer Service URL
      - Browser/POST és Browser/Artifact profile-ra

Alkalmazások levédése

- Forced Session (default)
  - webszerver modul véd
  - request csak autentikálva és autorizálva kerülhet az alkalmazáshoz

```
<Location />
  AuthType shibboleth
  require affiliation employee@niif.hu
  require user jako@bme.hu ritter@elte.hu
</Location>
```

Alkalmazások levédése

- Lazy Session
  - „Login with Shibboleth” gomb
  - Az alkalmazáshoz eljuthat a kérés szűrés nélkül
  - A bejelentkezés státusza pl. a HTTP_SHIB_APPLICATION_ID vizsgálatával kérdezhető le
    - nem spoof-olható

```
<Location /shiblazy>
    AuthType shibboleth
    ShibRequireSession Off
    require shibboleth
</Location>
```

Kilépés

- Nehéz...
- Biztos módszer: böngésző bezárása
  - cookie-k, HTTP autentikáció törlése
- IdP: függ az autentikációs metódustól
  - pl. session lejárat
- SP: session törlése

Attribútumok

- IdP kiadja
  - Attribute Release Policy (ARP)
- SP ellenőrzi, elfogadja
  - Attribute Acceptance Policy (AAP)
    - pl. Scope ellenőrzés metadata alapján
  - Az alkalmazás HTTP változókban kapja meg
    - HTTP_SHIB_*
      - spoofing védelem

Nemzetközi kapcsolatok

- **EduGAIN**: Géant 2 JRA5 munkacsoport
  - föderációk közti kapcsolat
    - ún. Bridging Element-ek segítségével
    - a távoli föderáció egy IdP-ként vagy SP-ként jelenik meg
  - pl.: https://kelimutu.switch.ch/aai/

Mit tegyenek a HBONE intézmények?

- IdP telepítés, csatlakozás
  - Cél: központi szolgáltatások „shibbolizálása”
    - CA, VoD, Videokonferencia booking, stb
    - Projekt és egyéb központi oldalak
- Részvétel a végleges föderációs szabályok kidolgozásában
- Belső SSO kialakítás
  - pl. e-learning

Bővebb információ:

http://wiki.aai.niif.hu