Felhaszáló központú és föderatív azonosítási megoldások webalkalmazásokban

Szalai Ferenc – Web Service Bricks
(szferi@wsbricks.com)

Mi a probléma?

a felhasználó érték

“mindannyian az adatbázis marketing üzletben vagytok”


THE UNITED STATES OF AMERICA
FIVE DOLLARS
L 53700859 B
B 31542485 A

a weboldalak minél többet
szeretnének tudni felhasználóikról

a felhasználók csak annyit akarnak elárulni, amennyit mindenképen szükséges

a felhasználót azonosítani kell

a felhasználóról adatok kellenek

(lehetőleg minél több, hagy örüljenek a marketingesek)

Register: Enter Information

Help

1 **Enter Information** 2. Check Your Email

Register now to bid, buy, or sell on any eBay site worldwide. It's easy and **free**. Already registered? Sign in now.

Your Personal Information - All fields are required

Want to register as a business?

First name

Last name

Street address

City

State / Province

-Select-

Zip / Postal code

Country or Region

United States

Primary telephone

( ) - ext.:

Telephone is required in case there are questions about your account.

Email address

Valid email address is required to complete registration. Example: myname@yahoo.com

Re-enter email address

Your privacy is important to us
eBay does not rent or sell your personal information to third parties without your consent.
To learn more, read our privacy policy.

Your address will be used for shipping your purchase or receiving payment from buyers.

PayPal

Log In | Help | Security Center

Choose Account Type → **Enter Information** → Confirm → Done

Account Sign Up
Business Account

Secure Transaction

Business Name:

Category: -- Choose a category --

Address Line 1:

Address Line 2: (optional)

City:

State / Province / Region:

Postal Code:

Country: Hungary

Customer Service Email :

Customer Service Phone: (optional) **ext.**

Business URL: (optional)

Your Business Information
Please enter the information for your group, organization, government entity, non-profit, individual business, or partnership.

Please enter the full email address, for example, **name@domain.com**

This email address will be shared only with those who purchase from you. It will be provided to buyers during payment so that they can contact you if needed.

You will be asked to enter an email address for your PayPal profile on the next page. It can be the same or different from your Customer Service Email.

Please enter your Business URL, for example, **www.businessname.com**

First Name:

Last Name:

Country of Citizenship: Hungary

Business Owner Contact Information
Please enter the contact information for the owner of this business. If you are the owner or contact person, enter your

és meg a ismerőseidet és bekattintgathatod

Hol itt a probléma?

a felhasználók nem szeretik

felhasználók 33%-a egy elmegy, a egy új regisztrációs formot lát, 20%-a nem akar emlékezni egy újabb felhasználónév jelszó pára

(ask500peope.com survay 2007 október)

a felhasználók hazudnak

központosított

alkalmazás központú

a fehasználónév jelszó nem biztosít semmit

“adatbázis bejegyzés vagy”

egyszerűbb

megbízhatóbb

Felhasználóközpontú

- Felhasználó dönt, milyen információt ad ki magáról kinek
- Csak azt az információt kell kiadni, ami feltetlenül szükséges a szolgáltatás igénybevételéhez.
- A felhasználó dönt, hogy milyen harmadik szervet von be a műveletekbe (pl.: IdP).
- Pseudonymity
- Független a technológiától és annak üzemeltetőjétől
- Adathalászat mentes (Anti-phishing)
- Minden körülmények között hasonló élményt nyújt a felhasználónak.

Szereplők

- Service Provider – akaromazadatod.hu

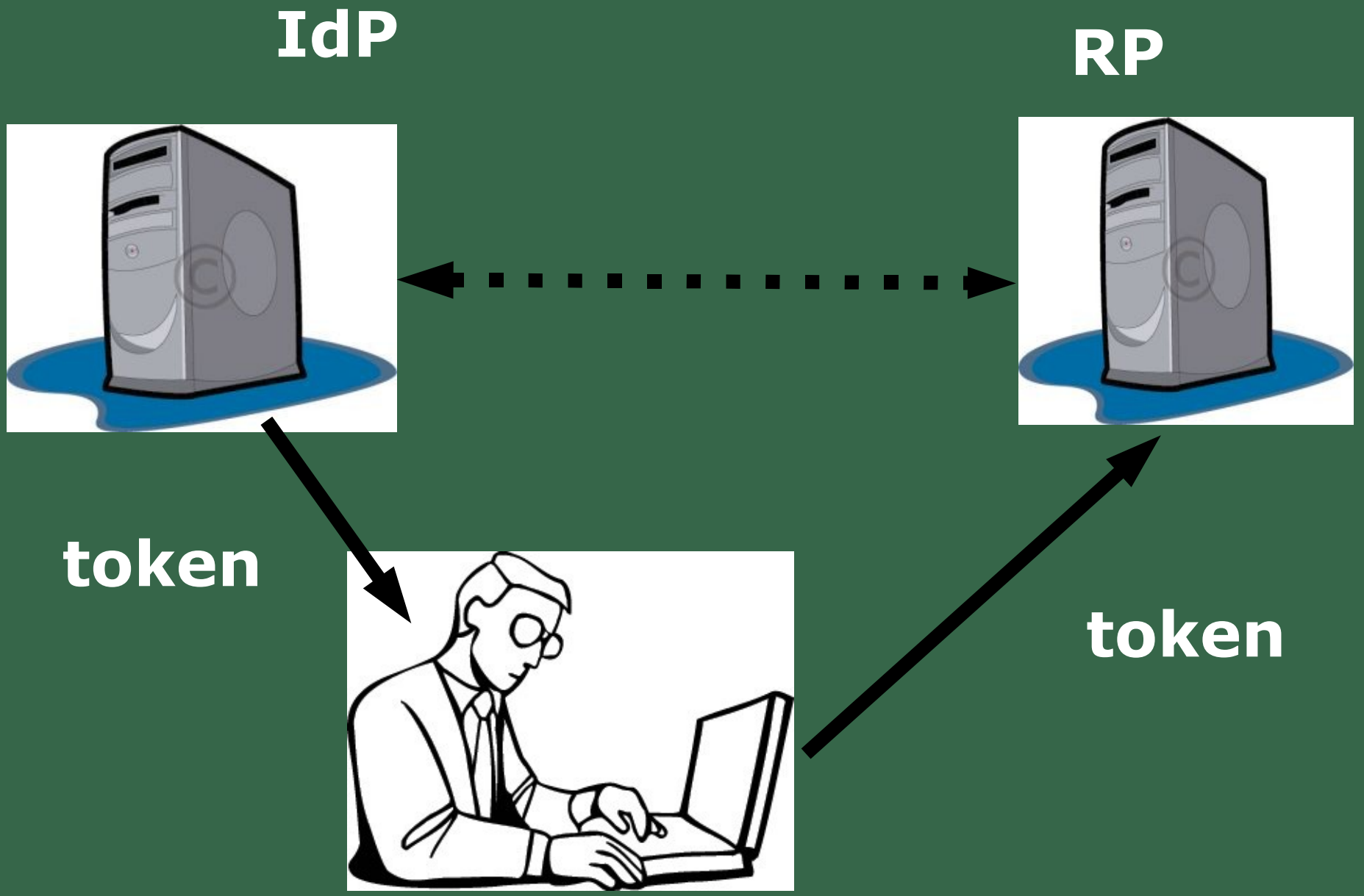
(Felhasználja az infomációt)

- Identity Provider – nalamvanazadatod.hu

(Rendelkezik az információval)

- Identity Agent - envagyokaz.hu

(Szabályozza a hozzáférész az adatokhoz)


IdP
RP
token
token

Rendezők

	Eredetileg	Klalakíás	Felhasználók	Megvalósítás
Liberty Alliance	Gyártói konzorcium	Web Services a federated személyazo-nossághoz	Pénzügy, egészségügy, államigazgatás, utazás	OpenLiberty, Novell, Sun, IBM, Oracle, HP, CA, Nokia
OpenID	Blogoszféra és open Internet fejlesztés	Egyszerű URL-alapú hitelesítés	Több ezer weboldal LiveJournal, Technocrati AOL, MS	Nyílt forrású bővítmények, Apache, Drupal, Wordpress, MediaWiki
Information Cards	Microsoft- és felhasználó-központú közösség	Felhasználó-alapú személy-azonossági szolgáltatások	Windows Vista IE7	MS Cardspace, Higgins, Ping, Pamela Project, Sxip

Products	OpenID	inames	**iCards** Bandit
Projects	LID Yadis	XDI	The Pamela Project Higgins
Companies	NetMesh JANRAIN	Cordance ooTao PARITY	Microsoft Novell
People	Johannes Ernst Brad Fitzpatrick	Drummond Reed Andy Dale	Paul Trevithick John Clippinger Kim Cameron


OpenID

OpenID

- Azonosító: URL (https://szferi.myopenid.com)
- Az azonosítás nem automatikus, azt minden esetben SP oldalról kezdeményezni kell.
- Nincs bizalmi viszony az IdP és SP között.
- Attribútumcsere szabványos 2.0 óta.
- Nagy szolgáltatók támogatják: AOL, Yahoo, Google, MS, stb.
- Független IdP-k pl.: myopenid.com
- OpenID IdP-k integrációs pontok más technológiákkal.
- Rengeteg probléma vár megoldásra pl.: phishing

Hogy működik?

1. azonosító

URL
https://szferi.myopenid.com

XRI

=Mary.Jones
+phone.number/(+area.code)
@Jones.and.Company/((+phone.number)/(+area.code))


inames

FoXRI Explorer

Exploring xri://=wil

URI(s):
http://xri.dready.org/=wil

Type: friendfeed
Path: friendfeed [
xri://=wil/friendfeed]
URI(s):
http://friendfeed.com/dready

Type: (+sip)
Path: (+sip) [xri://=wil/(+sip)]
URI(s):
sip:7930@voip.neustarlab.biz

Type: http://openid.net/signon/1.0
URI(s):
http://2idi.com/openid/
https://2idi.com/openid/

Type:
xri://+i-service*(+contact)*($v*1.0)
Path: (+contact) [
xri://=wil/(+contact)]
URI(s):
http://2idi.com/contact/


WordPress
Username
Password
Or login using your OpenID url:
Remember Me
Log In
Lost your password?

2. meg kell találni az OpenID IdP-t (szervert)


Yadis

URL esetén: HTTP header

X-XRDS-Location: https://szferi.myopenid.com/xrds

XRD példa

```
<xrds:XRDS
    xmlns:xrds="xri://$xrds"
    xmlns:openid="http://openid.net/xmlns/1.0"
    xmlns="xri://$xrd*($v*2.0)">
  <XRD>

    <Service priority="0">
      <Type>http://specs.openid.net/auth/2.0/signon</Type>
      <Type>http://openid.net/sreg/1.0</Type>
      <Type>http://openid.net/extensions/sreg/1.1</Type>

  <Type>http://schemas.openid.net/pape/policies/2007/06/ph
  ishing-resistant</
Type>
      <Type>http://openid.net/srv/ax/1.0</Type>
      <URI>https://www.myopenid.com/server</URI>
      <LocalID>https://szferi.myopenid.com/</LocalID>
    </Service>
  </XRD>
</xrds>
```

3. asszociáció: shared secret megegyezés, kulcscsere (HMAC-SHA1, HMAC-SHA256)

4. azonosítás kérés:
HTTP redirect
(openid.return_to paraméter)

5. IdP login kepernyő (vagy nem)

6. (opcionális)
felhasználó nyilatkozik, hogy engedi-e az RP-nek az azonosítást és ha igen ilyen attribútumokat kaphat meg

7. azonosítási kérésre válasz:
HTTP redirect
(openid.claimed_id)
aláírás

És mi van az attribútumokkal?

OpenID Attribute Exchange 1.0

```
openid.ns.ax=http://openid.net/srv/ax/1.0
openid.ax.mode=fetch_request
openid.ax.type.fname=http://example.com/schema/fullname
openid.ax.type.gender=http://example.com/schema/gender
openid.ax.type.fav_dog=http://example.com/schema/favourit
e_dog
openid.ax.type.fav_movie=http://example.com/schema/favour
ite_movie
openid.ax.count.fav_movie=3
openid.ax.required=fname,gender
openid.ax.if_available=fav_dog,fav_movie
openid.ax.update_url=http://idconsumer.com/update?
transaction_id=a6b5c41
```

```
openid.ns.ax=http://openid.net/srv/ax/1.0
openid.ax.mode=fetch_response
openid.ax.type.fname=http://example.com/schema/fullname
openid.ax.type.gender=http://example.com/schema/gender
openid.ax.type.fav_dog=http://example.com/schema/favourit
e_dog
openid.ax.type.fav_movie=http://example.com/schema/favour
ite_movie
openid.ax.value.fname=John Smith
openid.ax.count.gender=0
openid.ax.value.fav_dog=Spot
openid.ax.count.fav_movie=2
openid.ax.value.fav_movie.1=Movie1
openid.ax.value.fav_movie.2=Movie2
openid.ax.update_url=http://idconsumer.com/update?
transaction_id=a6b5c41
```

Integráció

http://wiki.openid.net/Libraries
RP oldal sok jó
IdP oldal kevés
Python: python-openid (JanRain)
Django:
http://django-openid.googlecode.com/svn/trunk/openid.html

“Huston we have a problem”

NO TRUST!

mindenki IdP akar lenni

adathalászat

Mi lesz a nem humanoidokkal?

Tapasztalatok

2007 május - szeptemer
6730 felhasználó
448 OpenID
(< 10 db magyar,
külföldiek kb. 23%-a)
309 myopenid.com

attribute exchange támogatást nem lehet feltételezni az IdP-éknél

e-mail cím attribútum nem megbízható, de nagyobb valószínűséggel élő

kicsit másképpen

föderatív megoldások

nagyvállalati igények


LIBERTY
ALLIANCE
PROJECT

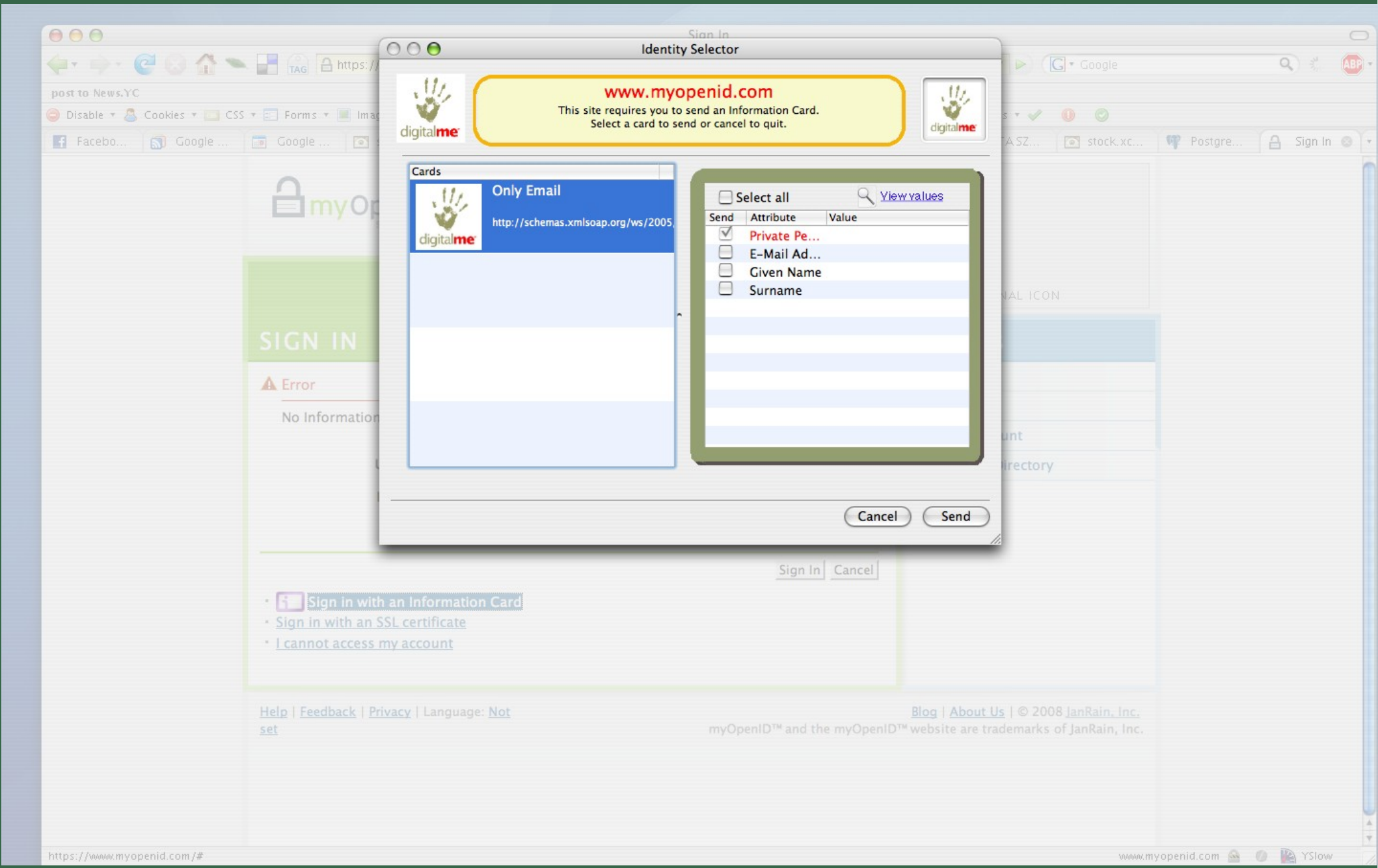

OASIS
Advancing E-Business Standards Since 1993

nem csak Web Wan a Wilágon!

InfoCard/CardSpace

- Felejtsük el végre a jelszót!
- A valós személyazonosító kártyákat mintázza.
- Minden kártyának globális egyedi azonosítója van.
- Saját kibocsátású (Self-issued) és IdP által kibocsátott kártyákat is kezel.
- WS-* protokollokra és SAML igazolásokra épül.
- Nem csak Windows!


myOpenID
SECURE OPENID PROVIDER
SIGN IN
Username
Password
Stay signed in
Sign in with an Information Card
Sign in with an SSL certificate
I cannot access my account


Identity Selector
www.myopenid.com
This site requires you to send an Information Card.
Select a card to send or cancel to quit.
Cards
Only Email
http://schemas.xmlsoap.org/ws/2005
Select all
View values
Send
Attribute
Value
Private Pe...
E-Mail Ad...
Given Name
Surname
Cancel
Send
SIGN IN
Error
No Information
Sign In
Cancel
Sign in with an Information Card
Sign in with an SSL certificate
I cannot access my account
Help | Feedback | Privacy | Language: Not set
Blog | About Us | © 2008 JanRain, Inc.
myOpenID™ and the myOpenID™ website are trademarks of JanRain, Inc.

```
<form method="post" action="https://www.myopenid.com/signin_infocard"
id="infocard-form" class='noline'>
  <input type="hidden" name="tid" value="da2363ec" />
  <input type="hidden" name="resume_action" value="signin_password" />
  <input type="image" id="infocard-logo-button"
         value="Choose an Information Card"

src="https://www.myopenid.com/static/InformationCards/images/infocard_30x21
.png">
  <label for='infocard-logo-button'><a id="infocard-label"
onclick="document.getElementById('infocard-form').submit(); return
false;">Sign in with an Information Card</a></label>
  <noscript>
<OBJECT type="application/x-informationCard" name="xmlToken" class="skip">
  <PARAM Name="tokenType" Value="urn:oasis:names:tc:SAML:1.0:assertion">
  <PARAM Name="issuer"
        Value="http://schemas.xmlsoap.org/ws/2005/05/identity/issuer/self">
  <PARAM Name="requiredClaims"
Value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersona
lidentifier">
  <PARAM Name="optionalClaims"
Value="http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddres
         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname
         http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname">
</OBJECT>
  </noscript>
  <input type="hidden" name="token"
value="414c702680f1884dcd1cac62f94a2bd10000000000000502d3" /></form>
```

WS-*

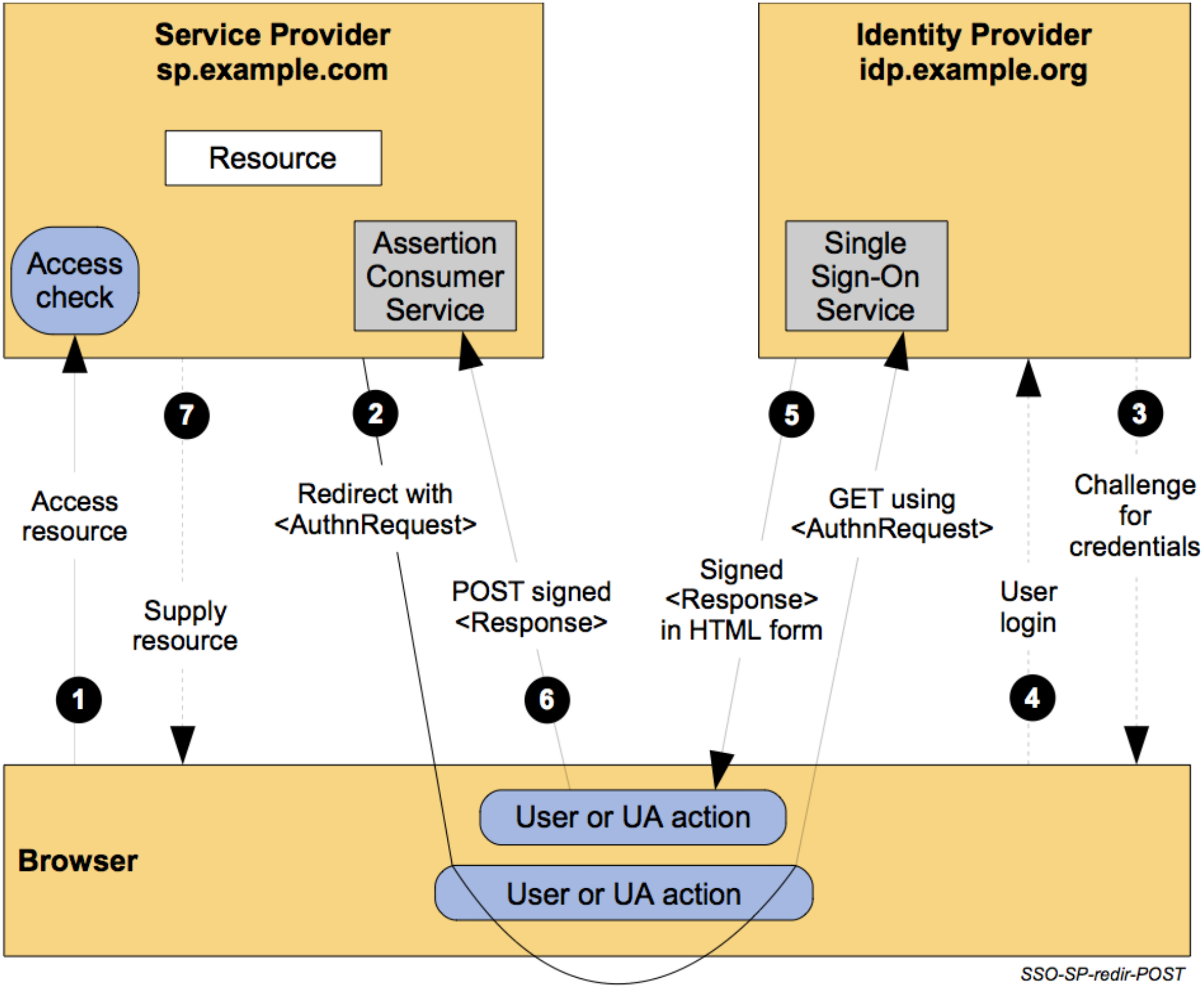
- WS-Policy: kommuniáció előfeltételeinek meghatározása (algoritmus, elvárt tokenváltozat stb.)
- WS-Trust: fő komponense az STS (Security Token Service) – általános keret (Username, Kerberos, X509, stb.) tokenek biztonságos továbbítására
- WS-Federation: AuthN, AuthZ, Attribútum, Pseudonym szolgáltatások integrációja WS-Trust alapon

SAML 2.0

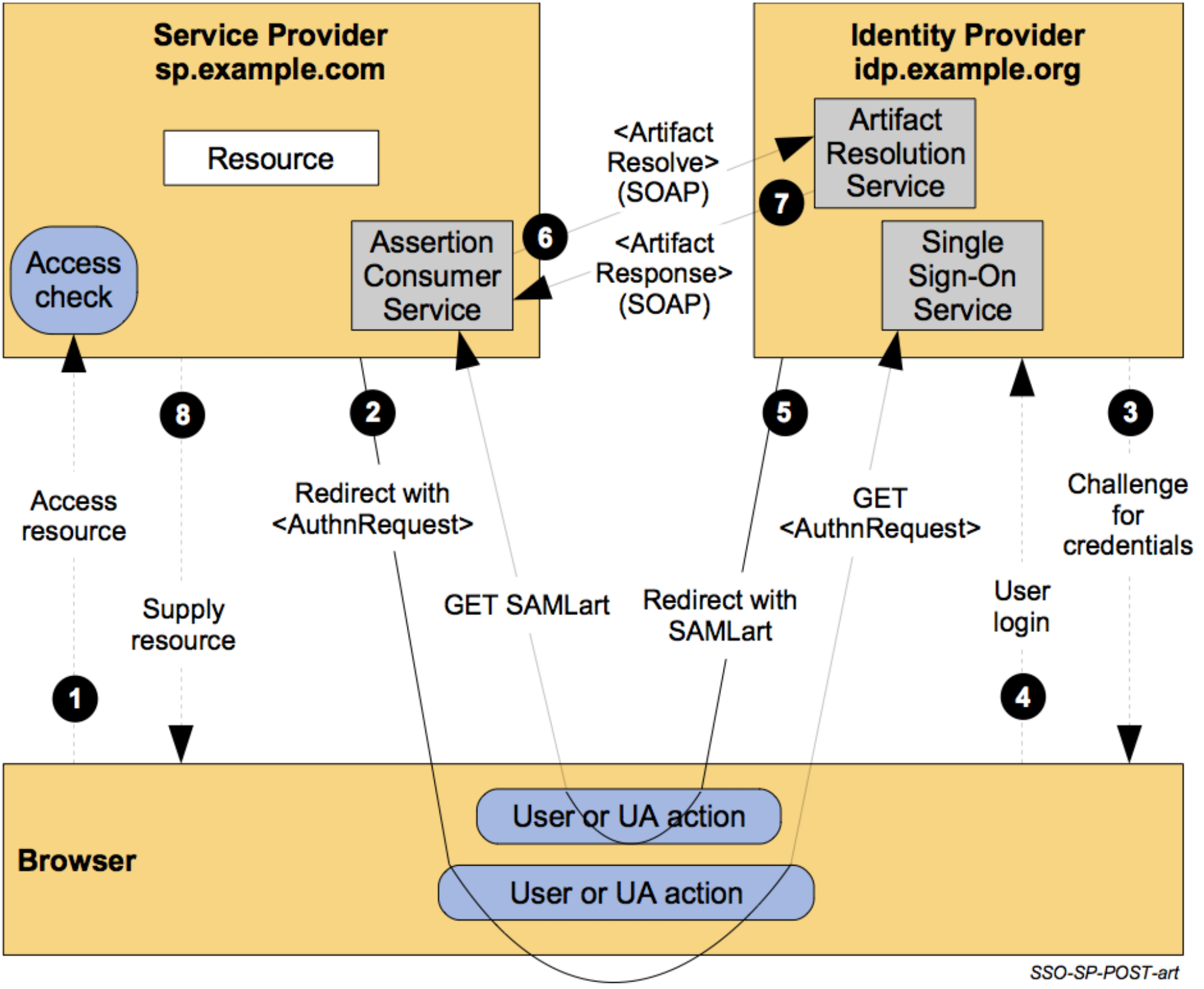
- Security Assertion Markap Language
- Igazolások (assertion) leírásának nyelve
  - kire vonatkozik?, kinek szól?, meddig érvényes?, attribútumok
- IdP és RP közötti protokoll-profilok
  - pl.: WebSSO
- Bindings: hogyan kell SAML igazolást küldeni pl. SOAP üzenetben
- Metadata: az IdP és RP leírása XML-ben
- Profilok: az elfogadott attribútumok specifikációja

Explicit TRUST szükséges!

Hogy működik?


Service Provider
sp.example.com
Resource
Access check
Assertion Consumer Service
Identity Provider
idp.example.org
Single Sign-On Service
7
2
5
3
Access resource
Redirect with <AuthnRequest>
GET using <AuthnRequest>
Challenge for credentials
Supply resource
POST signed <Response>
Signed <Response> in HTML form
User login
1
6
4
Browser
User or UA action
User or UA action
SSO-SP-redir-POST


Google™
Apps


Service Provider
sp.example.com
Resource
Access check
Assertion Consumer Service
Identity Provider
idp.example.org
Artifact Resolution Service
Single Sign-On Service
<Artifact Resolve> (SOAP)
<Artifact Response> (SOAP)
6
7
8
2
5
3
Access resource
Supply resource
Redirect with <AuthnRequest>
GET SAMLart
Redirect with SAMLart
GET <AuthnRequest>
User login
Challenge for credentials
1
4
Browser
User or UA action
User or UA action
SSO-SP-POST-art

Interoperability

User Centric Identity Interop at RSA 2008

Companies

Projects



Mit csinálunk?

nyílt forrású SAML 2.0 alapú felhasználó központú IdP-t

Kinek?

lusta programozónak és magunknak

Miért?

mert meg tudjuk csinálni

meg mert 1-nél több alkalmazást fogunk fejleszteni a közel jövőben és nem akarunk a google, inda stb. sorsára jutni

Hogyan?

Python, Django

SAML 2.0: Lasso
http://lasso.entrouvert.org/
(C, wrappers: python, php, java, perl)
SAML 2.0 IdP, SP

PyInfocard:
http://ww.wsbricks.com/pyinfocard/

fő üzenet

legyél RP!

hova tovább, hovatovább?

Identity 2.0

Mi szeretnénk, mi várható?

1. egyre kevesebb jelszó

2. gazdag, hordozható profilok

3. hordozható azonosítók

4. működő, finoman hangolható delegáció

5. reputáció szolgáltatók

6. személyazonosság (identity) szolgáltatások

“kérem kapcsolja ki”