SAML

Security Assertion Markup Language

Jan Asle Kroknes
TANDBERG

Web Single-sign On

NTLM
Kerberos
CAS, JOSSO, ...

SAML

Assertions

```
<saml:Assertion>
    <saml:Issuer/>
    <ds:Signature/>
    <saml:Subject/>
    <saml:Conditions/>
    <saml:AudienceRestriction/>
    <saml:AuthnStatement/>
    <saml:Attribute/>
 </saml:Assertion>
```

Protocols

```
<saml:AuthnRequest>
      <saml:Issuer/>
      <saml:NameIDPolicy/>
</saml:AuthnRequest>
```

Bindings

```
<form method="post"
        action="http://sp.taa.com/SAML2/POST">
    <input type="hidden" name="SAMLResponse"
        value="response" />
    <input type="submit" value="Submit" />
</form>
```

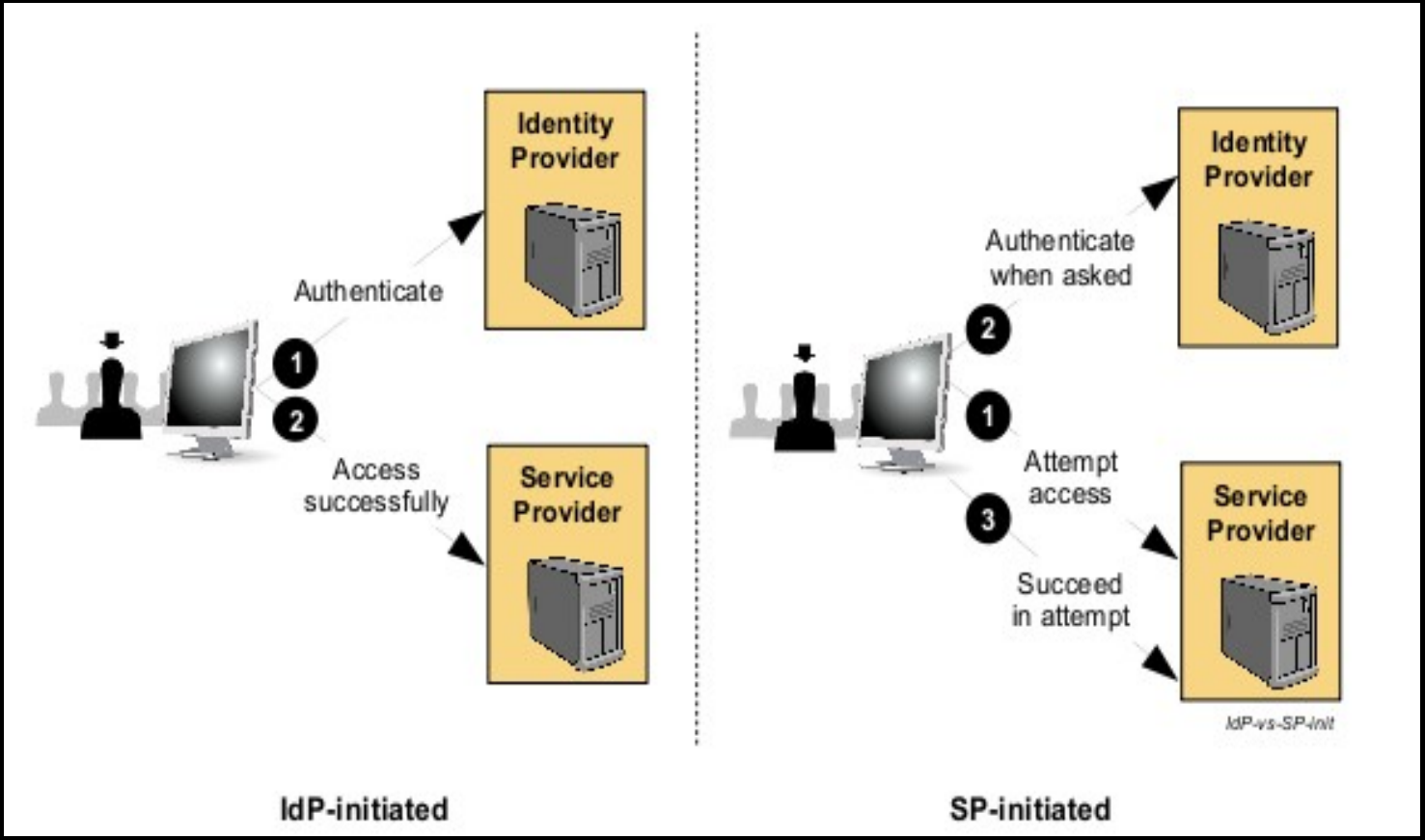
```
window.onload = function () { document.forms[0].submit(); }
```

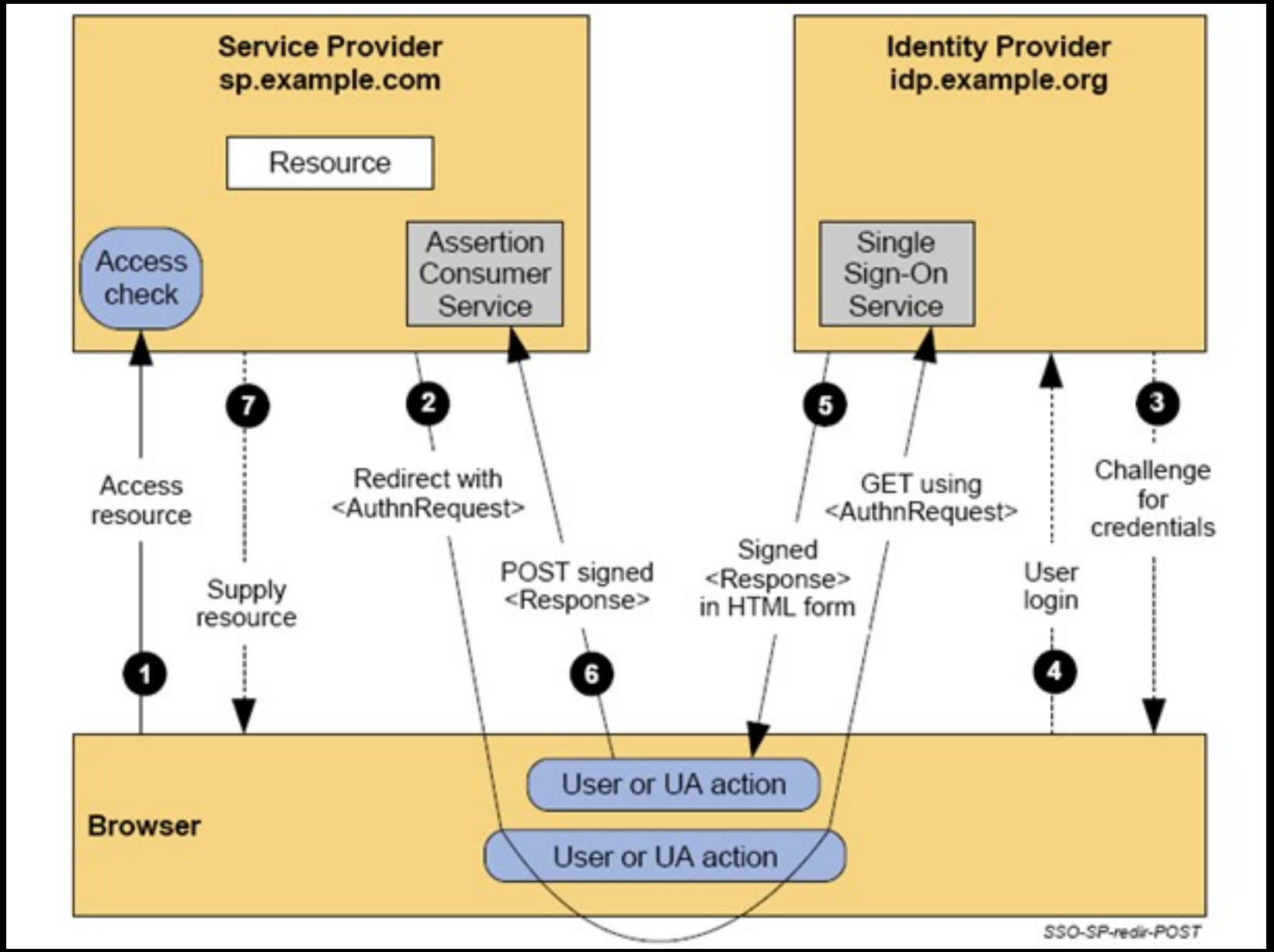
Profiles

Web Browser SSO
Single Logout

Web Browser SSO

IdP-Initiated SSO
SP-Initiated SSO


Identity Provider
Authenticate
1
2
Access successfully
Service Provider
IdP-initiated
Identity Provider
Authenticate when asked
2
1
Attempt access
3
Service Provider
Succeed in attempt
IdP-vs-SP-Init
SP-initiated


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

Federation
Pseudonymer
Web Service Security

DEMO