FUNCTIONALITY AND USE OF SAML 2.0

AI - PROJEKTSTUDIUM
HTW BERLIN

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

SPEAKER

FUNCTIONALITY AND USE OF SAML 2.0

BIJAN SELLAHI

STUDENT
ANGEWANDTE
INFORMATIK

htw

Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

WAS IST SAML 2.0?

SECURITY ASSERTION MARKUP LANGUAGE

XML BASIERTES PROTOKOLL

ERMÖGLICHT AUSTAUSCH VON AUTHENTIFIZIERUNGS- UND AUTORISIERUNGSINFORMATIONEN ÜBER ORGANISATIONSGRENZEN HINWEG

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

WAS IST SAML 2.0?

SAML AB 2001 VON DEM OASIS-KONSORTIUM ENTWICKELT. (SUN/ORACLE, IBM, NOKIA UND SAP)

SAML 2.0 WURDE 2005 ALS OASIS-STANDARD RATIFIZIERT UND ERSETZT SAML 1.1.

DIE KRITISCHEN ASPEKTE VON SAML 2.0 WERDEN AUSFÜHRLICH IN DEN OFFIZIELLEN DOKUMENTEN SAMLCORE, [1] SAMLBIND, [2] SAMLPROF [3] UND SAMLMETA [4] BEHANDELT.

OSASIS: ORGANIZATION FOR THE ADVANCEMENT OF STRUCTURED INFORMATION STANDARD

WOZU IST SAML 2.0 GUT?

ERMÖGLICHT WEBBASIERTES DOMAINÜBERGREIFENDES SINGLE SIGN ON (SSO)

VERRINGERT DEN VERWALTUNGSAUFWAND FÜR DEN BENUTZER

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

ANWENDUNGSBEREICHE

IDENTITY FEDERATION

WEB SINGLE SIGN-ON (SSO)

htw.
Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

WIE FUNKTIONIERT SAML 2.0?

ES VERWENDET SICHERHEITSTOKEN, DIE ASSERTIONS ENTHALTEN, UM INFORMATIONEN ÜBER EINEN ENDNUTZER ZWISCHEN EINER SAML AUTORITÄT (IDENTITY PROVIDER) UND EINEM SAML CONSUMER (SERVICE PROVIDER) ZU ÜBERGEBEN.

Identity Provider
IdP

Service Provider
SP

Identity Provider
IdP

Service Provider
SP

Info über identität von Subjekt
Unterstützt den SP seine Dienste auszuführen

Asserting party
(SAML Authority)

Identity Provider
IdP

Relying party

Service Provider
SP

Info über identität von Subjekt
Unterstützt den SP seine Dienste auszuführen

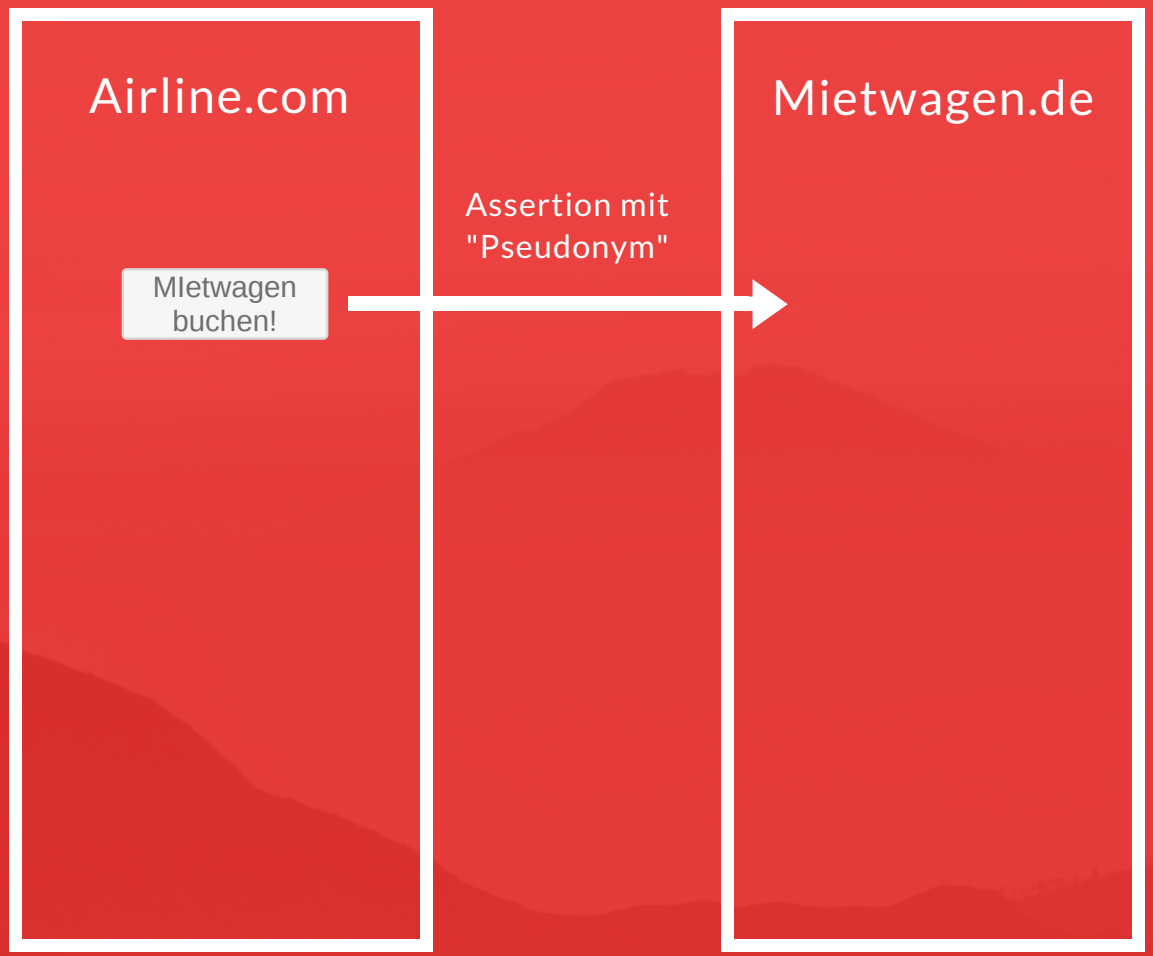
SAML Assertions

IDENTITY FEDERATION

BSP: URLAUB

FLUG BUCHEN
MIETWAGEN BUCHEN
HOTEL BUCHEN

Hochschule für Technik
und Wirtschaft Berlin
University of Applied Sciences

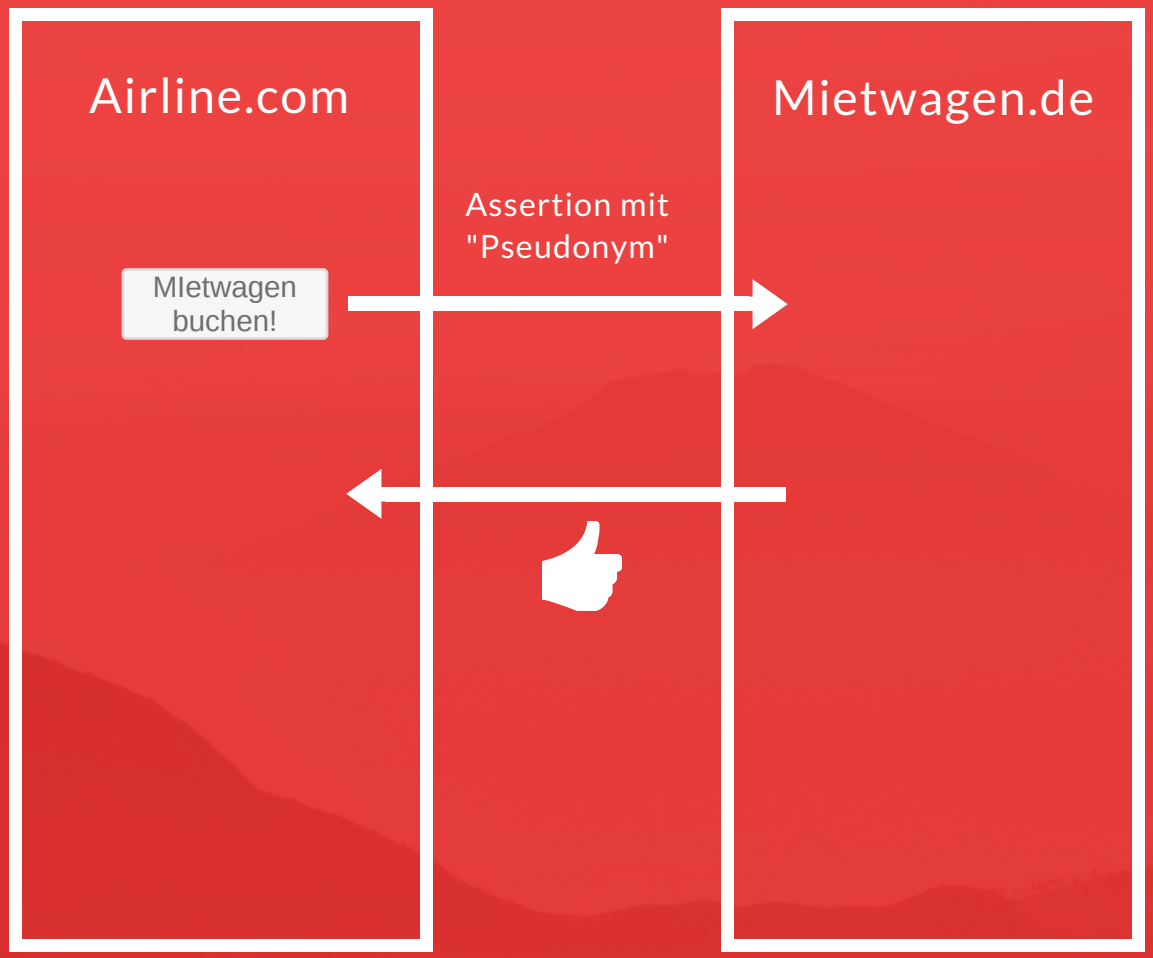


1.
Airline.com erzeugt ein Pseudonym und überträgt es in signierter SAML Assertion an Mietwagen.de

2. Mietwagen.de erkennt die Assertion und liest Pseudonym aus

3. Mietwagen.de fordert User auf sich einzuloggen

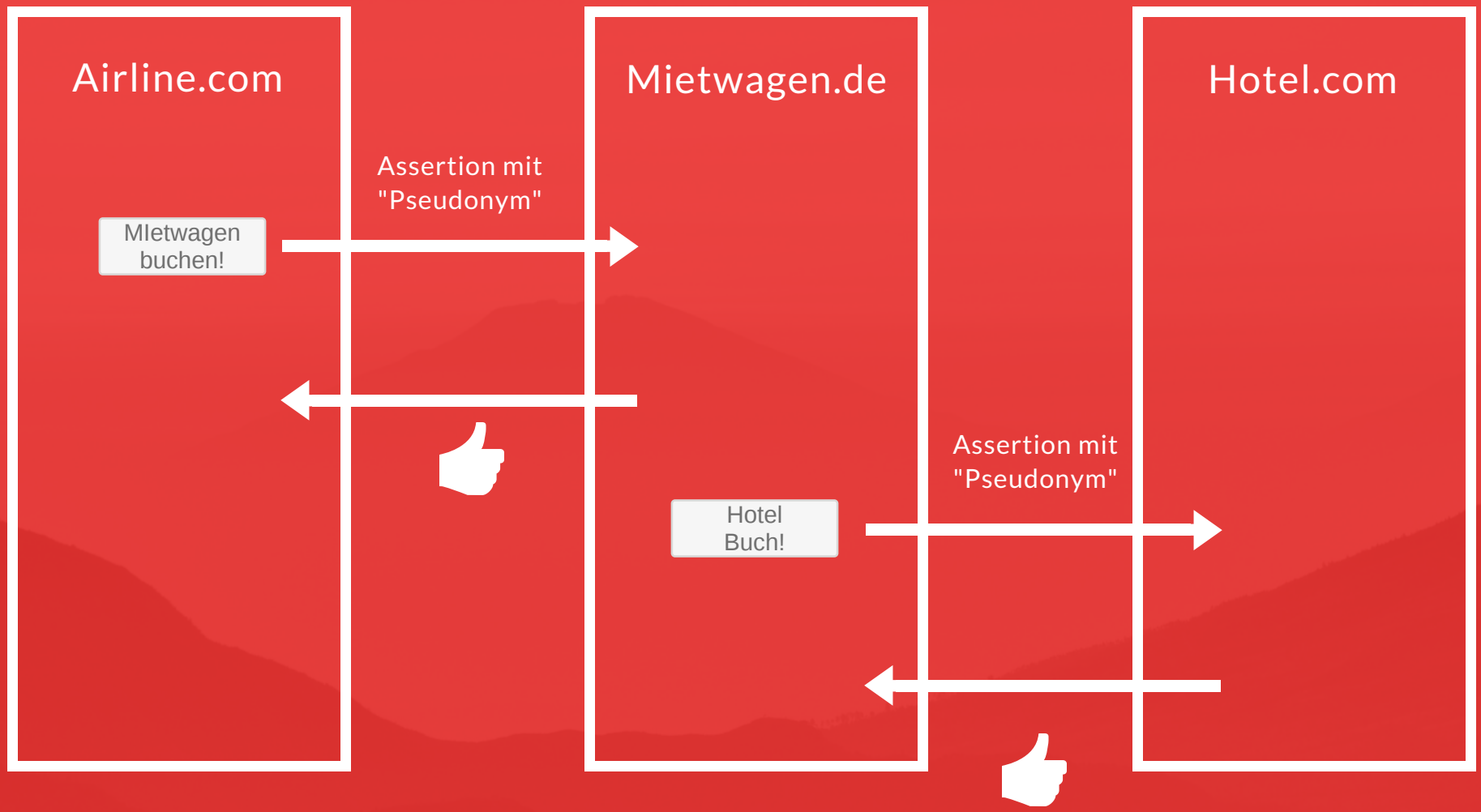
4. User eingeloggt. Mietwagen.de fragt ob User der ID Federation zustimmt



5.
Zustimmung erfolgt?
Mietwagen.de verknüpft das Pseudonym mit dem Account und persistiert es

6.
Informiert Airline.com über die Zustimmung

8.
Account Linking abgeschlossen.
Danach muss sich der User nicht mehr bei Mietwagen.de anmelden


Airline.com
Mietwagen.de
Hotel.com
Assertion mit "Pseudonym"
MIetwagen buchen!
Hotel Buch!
Assertion mit "Pseudonym"

ASSERTION

KANN BIS ZU 3 STATEMENT TYPEN ENTHALTEN

Authentication Assertion: Definiert, dass und wie eine Authentifizierung stattgefunden hat

Attribute Assertion: Enthält beliebige Anzahl von Atributen (Eigenschaften) zum Subjekt

Authorization Decision Assertion: Definiert welche Rechte ein Subjekt hat. (Welche Aktionen er beim Service Provider ausführen kann)

```
<Assertion Version="2.0"
    IssueInstant="2007-01-22T12:00:00.00+01:00" ID="11111">
  <Issuer>AirlineInc.com</Issuer>

  <Subject>
    <NameID Format=
      "urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress"
    >azqu3H7@airlineinc.com</NameID>
  </Subject>

  <Conditions
    NotOnOrAfter="2007-01-22T12:05:00.00+01:00"
    NotBefore="2007-01-22T11:31:30.048+01:00">
    <AudienceRestriction>
      <Audience>CarRental.com</Audience>
    </AudienceRestriction>
  </Conditions>

  <AuthnStatement AuthnInstant="2007-01-22T12:00:00.00+01:00">
    <AuthnContext>
      <AuthnContextClassRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:Password
      </AuthnContextClassRef>
    </AuthnContext>
  </AuthnStatement>

  <AttributeStatement>
    <Attribute NameFormat="urn:x-aol:attribute"
               Name="CreditLimit">
      <AttributeValue xsi:type="ns8:number"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xmlns:ns8="http://www.w3.org/2001/XMLSchema"
      >500</AttributeValue>
    </Attribute>
  </AttributeStatement>

  <AuthzDecisionStatement
    Resource="http://www.airlineinc.com/viewbill.html"
    Decision="Permit">
  </AuthzDecisionStatement>

</Assertion>
```

Assertion wurde erzeugt
vom IdP Airline.com

Authentifiziert wurde der User mit der
eMail Adresse: azqu3H7@airlineinc.com

Gültigkeitszeitraum

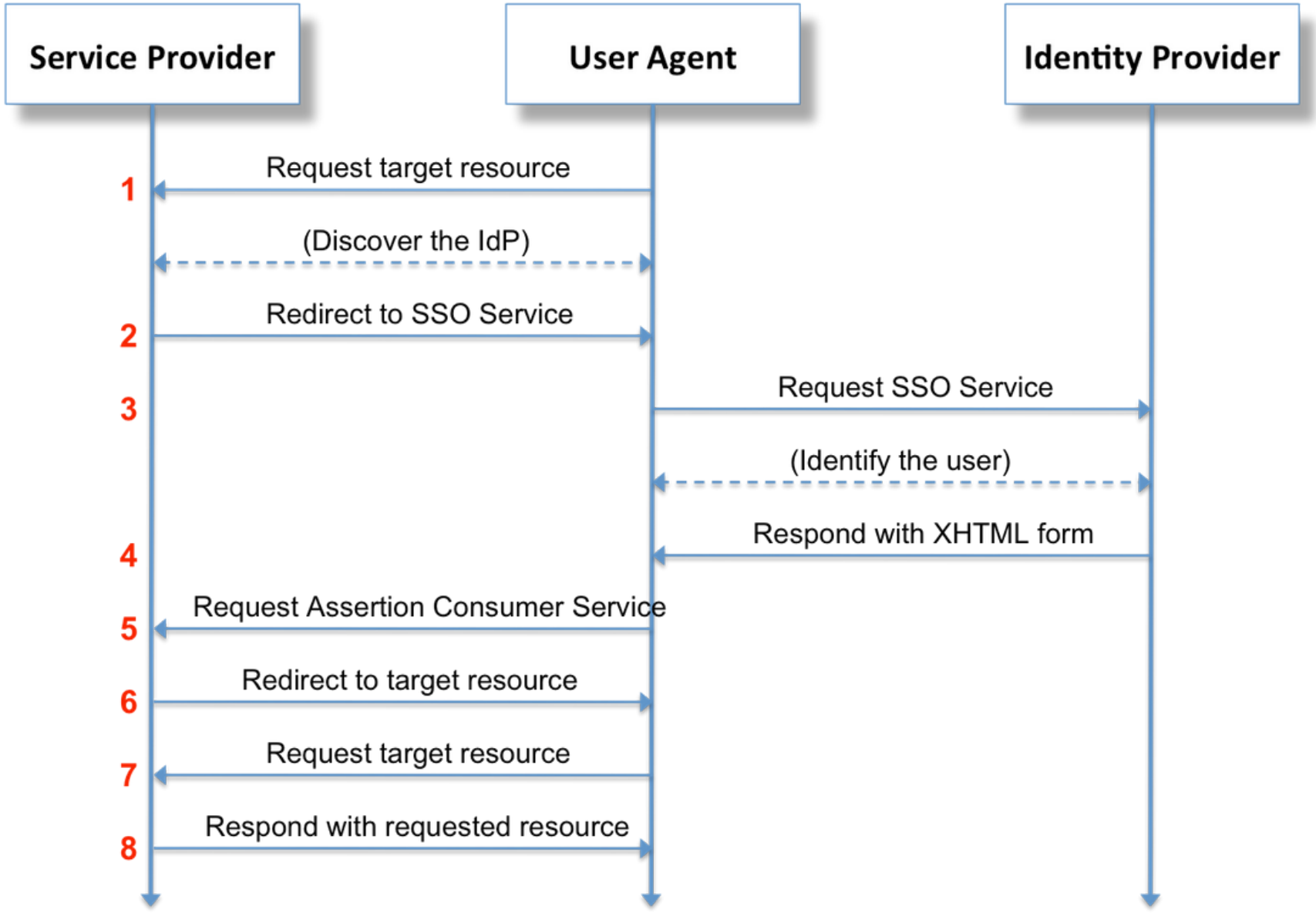
Bestimmt für

Art der Authentifizierung

Attribut mit Wert
= Nutzer hat Kreditlimit von 500 €

Recht auf genannte URL zuzugreifen

Web Single Sign-On (SSO)



QUELLEN

HTTPS://EN.WIKIPEDIA.ORG/WIKI/SAML_2.0

HTTPS://WWW.ACANDO.DE/FILEADMIN/REDAKTION/NEWS/2016/PUBLIKATIONEN/KAIN_KELLER_JS_05_07.PDF

HTTPS://DE.WIKIPEDIA.ORG/WIKI/SECURITY_ASSERTION_MARKUP_LANGUAGE

HTTPS://EN.WIKIPEDIA.ORG/WIKI/FILE:SAML2-BROWSER-SSO-REDIRECT-POST.PNG

Hochschule für Technik
und Wirtschaft Berlin

University of Applied Sciences

VIELEN DANK

FRAGEN?