Identity Authentication & Authorization

Diogo Gomes dgomes@ua.pt

Identity Management

- ▶ Provisioning. Adds new users to network operating system directories and application server directories, both inside an enterprise and outside at partner information systems.

- ▶ Password management. Enables users to have a single set of credentials to sign on to the company information systems. Additionally, it enables users to self-administer their passwords, user account data, and privileges.

- ▶ Access control. Enables the system to recognize security policies for groups of users. For example, a security policy would prevent people from changing their own job title and instead route a request for a job title change to the appropriate authority.

SAML

- Security Assertion Markup Language

- Approved by OASIS, March 2005

- "SAML is a protocol specification to use when two servers need to share authentication information. Nothing in the SAML specification provides the actual authentication service…" – in IBM Developerworks

- "SAML is different from other security approaches mostly because of its expression of security in the form of assertions about subjects. Other approaches use a central certificate authority to issue certificates that guarantee secure communication from one point to another within a network. With SAML, any point in the network can assert that it knows the identity of a user or piece of data. It is up to the receiving application to accept if it trusts the assertion. Any SAML-compliant software can assert its authentication of a user or data "– in IBM Developerworks

- Example: Univ. Aveiro IDP

What is SAML?

- Industry standard way of representing and exchanging assertions about identity, attributes and entitlements
- Vendor neutral
- XML based
- Uses SOAP, XMLDSig, XMLEnc
- SSL is required between servers

- SAML falls under the broader topic of Identity Management.
- Identity management applies to both network and federated identity.
- Federated Identity refers to the use of identity or authorization decisions across organizational boundaries.
- Identity management includes the consideration of identity registration, revocation and termination.
- SAML's focus is on single sign on by applications.

SAML Terminology:

- Assertions are declarations of facts about subjects.

- The Identity Provider or SAML Authority or Asserting Party is the entity that makes assertions.

- The Service Provider or Relying party relies on information provided by the identity providers.

SAML Provides:

- Assertions about:

  - authentication acts (e.g., YES, the entity did authenticate in this way at this time)

  - attributes of subjects (e.g., access rights, credit limits, status) name, value pairs

  - authorization decisions already made

- A Simple Request / Reply protocol

  - Request Types (queries): authentication, authorization, attribute

  - One reply format containing assertions. (authentication, authorization or attribute statements)

  - The requests and replies occur on an SSL channel. The requestor is typically a service provider and the responder an identity provider.

How does it work ?
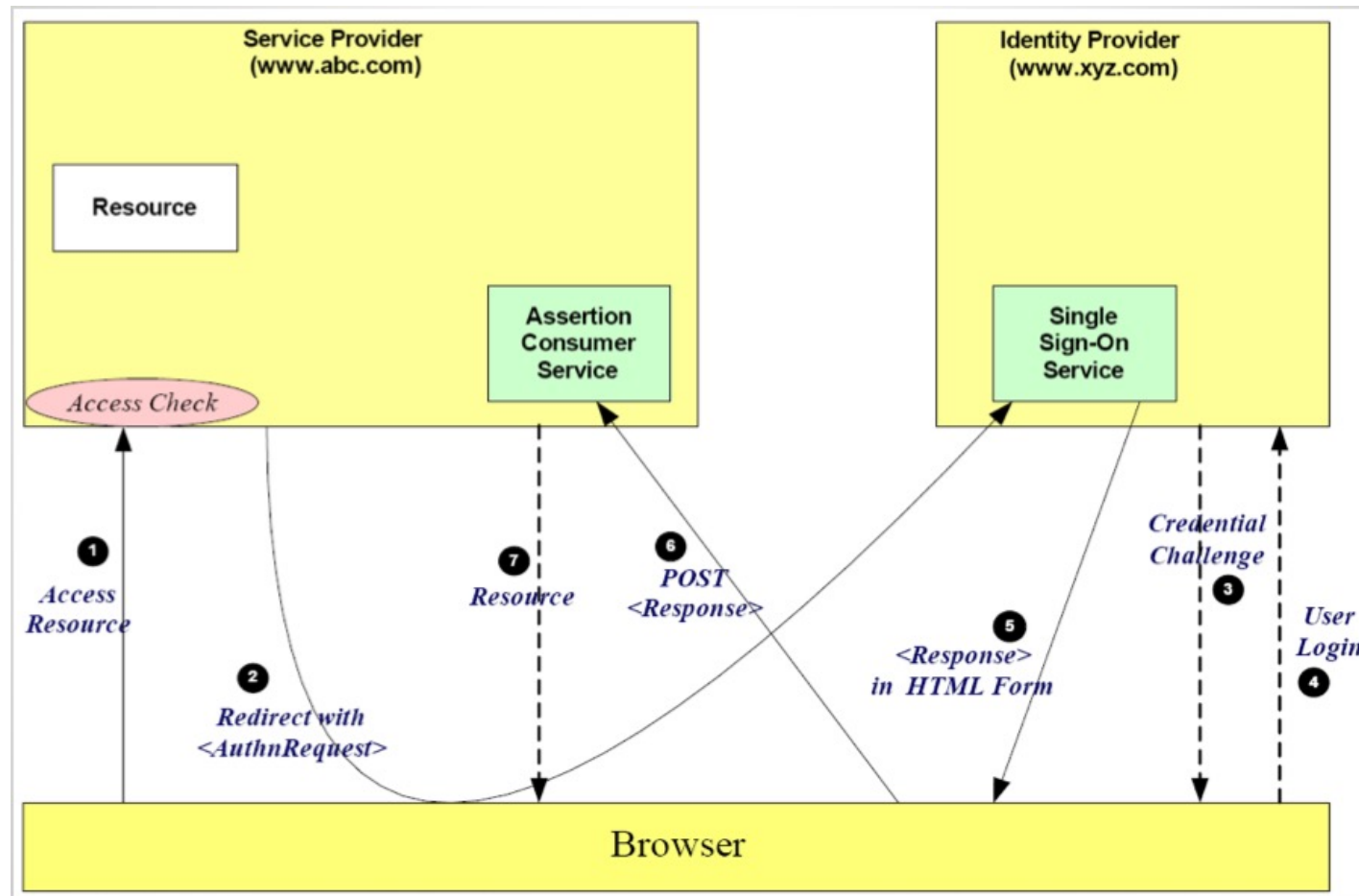
XACML

- Approved by OASIS March 2005

- XML Access Control Markup Language

- Industry standard way of representing and processing access control policies.

- Vendor neutral & XML based

- Provide for "rule combining algorithms"
  - eg: "Deny overrides" or "Permit Overrides"

- An XACML policy may specify what a provider should do when it receives a SAML assertion.

- Separation of concerns: Don't bake authorization policies into code.

XACML

▶ Policy Language

  ▶ Used to describe access control requirements. Who is allowed to do what?

▶ Request/Response Language

  ▶ The request is a query about permissions associated with x.

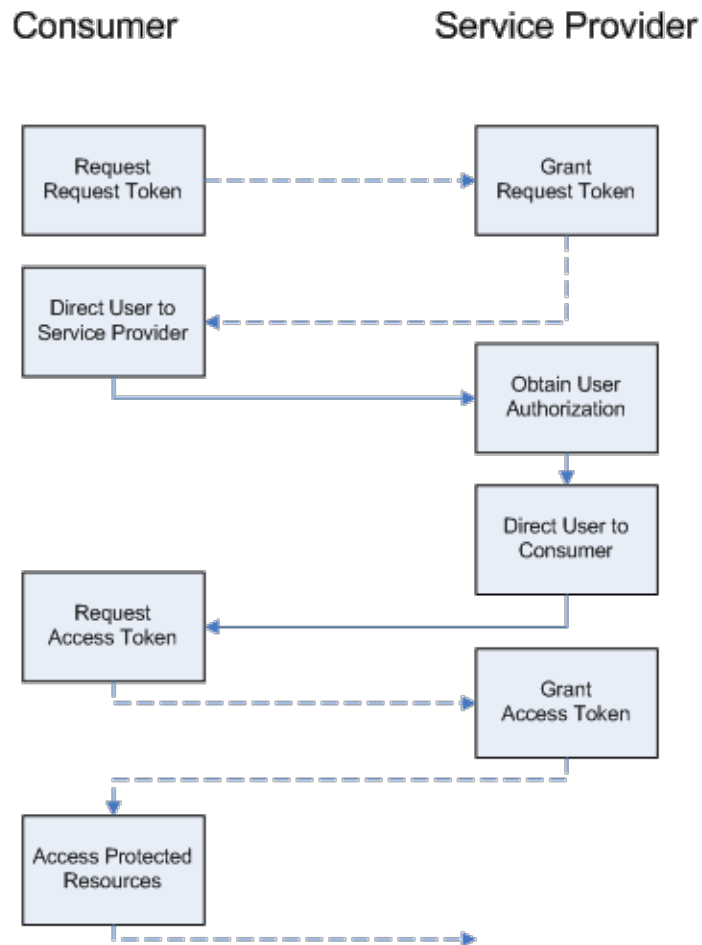 ▶ The response is permit, deny, indeterminate, or not applicable.

OpenID

- Grassroots effort since 2005

- Web user identification and authentication

- OpenID used and provided by: AOL, BBC, Google, IBM, PayPal, Verisign, etc.

- Compares a bit with the heavy weight SAML.

- Highly scalable – does not depend on pre-existing agreements.

- Losing industry traction to OAuth…

OAuth

- Open Standard for Secure API authentication
- Started by twitter in 2006
- IETF RFC 5849 in 2010
- Token-based, logged-in user has a unique token used to access data from the site
- Not extendable
- Not "Enterprise-ready"

How ?

Consumer   Service Provider

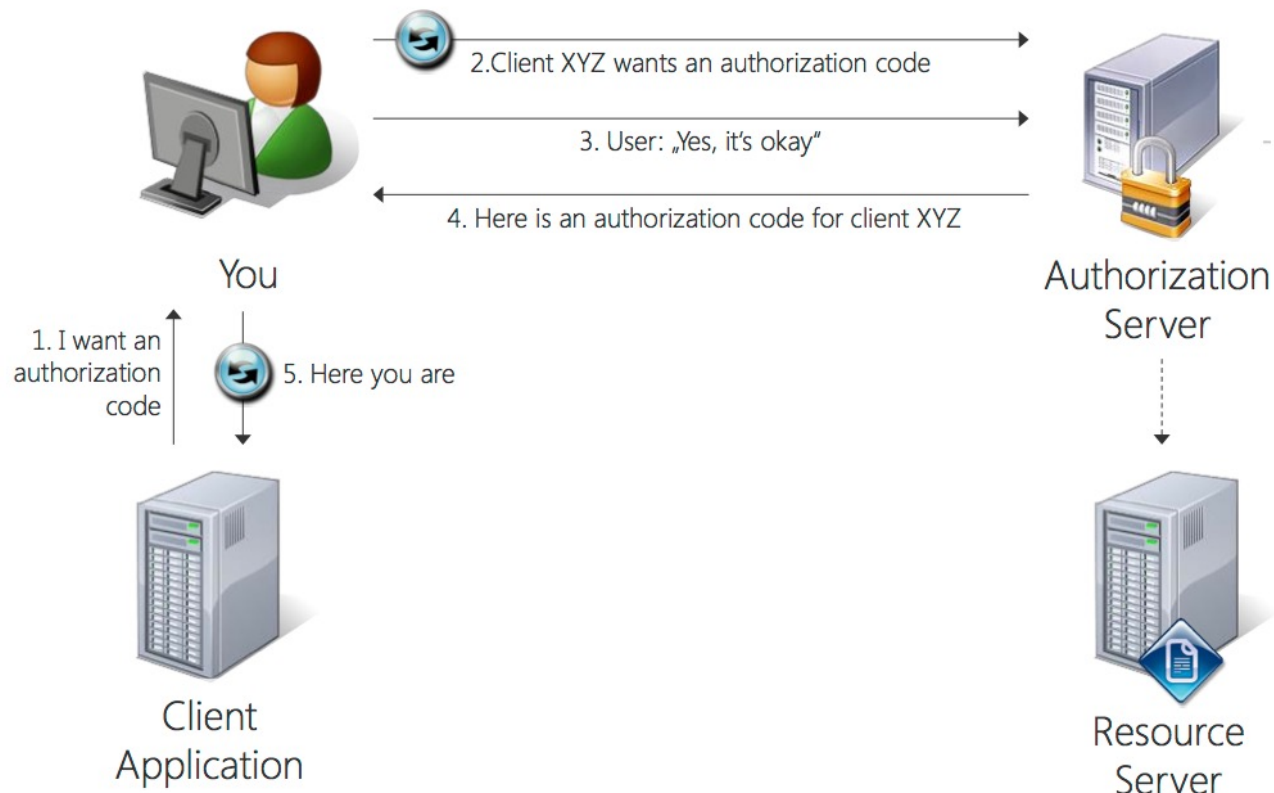| Consumer	Service Provider
Request Request Token	Grant Request Token
Direct User to Service Provider	Obtain User Authorization
	Direct User to Consumer
Request Access Token	Grant Access Token
Access Protected Resources	

- ▶ Obtain request token
- ▶ User authorizes request token
- ▶ Exchange request token for access token
- ▶ Use access token to obtain protected resources
- ▶ HTTP Authorization header
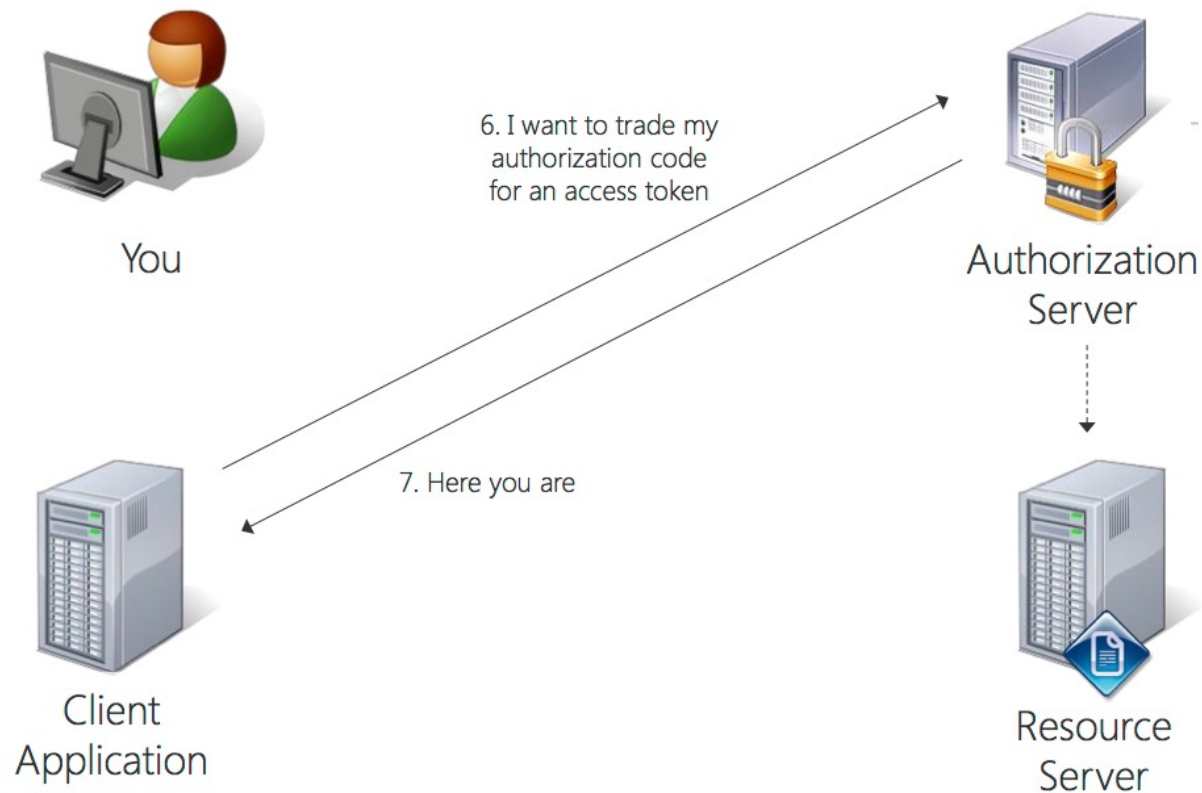- ▶ HTTP POST
- ▶ URL query string

OAuth2

- Completely new protocol (started in 2010)
- IETF RFC 6749 in 2012
- Oauth Server will validate Service Provider based on HTTPS
- Improvements:
  - Authorization:
    - Scoping (different rights)
    - Revoke rights once they where granted

Oauth2 steps

2.Client XYZ wants an authorization code

3. User: „Yes, it's okay"

4. Here is an authorization code for client XYZ

You

Authorization Server

1. I want an authorization code

5. Here you are

Client Application

Resource Server

Oauth2 steps

Oauth2 steps