Federazioni: Visione dall'esterno

Giuseppe Attardi

Università di Pisa

CTS GARR

Definition

- A **federated identity** is the means of linking a person's electronic identity and attributes, stored across multiple distinct identity management systems.

Problems

- Too many identities
- Too many identity providers
- Identity theft
- Impersonation
- Privacy

Federated Identity Management

- Within an organization, a single digital identity allows access to all resources to which the user is entitled
- Federated identity management permits extending this beyond the organization
- Participating institutions share identity attributes based on agreed-upon standards, facilitating authentication from other members of the federation and granting appropriate access to online resources
- This approach streamlines access to digital assets while protecting restricted resources

How does it work

- When an affiliated user requests a protected resource from another member organization, he is prompted for identifying information including his “home” organization
- This request is passed to the home organization, which verifies the user’s credentials and confirms whether the user has been authenticated.
- Federation members determine individually which attributes about users to share, such as name, title, or role.
- Based on this information and their respective policies, member organizations then grant or deny access to particular resources.

Benefits

- Federated identity management separates access from the establishment of identity and authorization.
- Institutions no longer have to create and maintain large numbers of user credentials
- Attributes about users are verified by the home institution, providing current, accurate information about the user, without the need to propagate status changes across multiple institutional identity systems.

Drawbacks

- Costs to modify existing applications
- Participating in a federation might require:
  - different or more stringent identity protocols
  - developing thorough institutional policies
- Risks associated with unauthorized access to certain services might induce organizations to demand more stringent policies from federation members
- This might slow adoption leading to a chicken-and-egg situation

Evolution

- Outsourcing identity management?
- Cloud-based service (IdP hosting)
- Identity management becoming user-centric rather than institution-centric
- Concerns about user privacy will need to be worked out

Broader outlook

- Identity management can support institutional policies for extending access to valuable resources to certain groups of users
- Integration of identity management systems across academic, governmental, and commercial spheres further broadens the horizon for inter-disciplinary, inter-institutional activities

Solutions

- Eduroam
- Idem
- eduGAIN (InterFederation)
- SPID
- OpenID

Shibboleth

- Library OpenSAML
- Java or C++
- Deals with SAML objects
- Clients use SOAP

Sample Client

```
Request request = buildSAML1ArtifactResolve(base64Artifact);
Envelope envelope = buildSOAP11Envelope(request);
BasicSOAPMessageContext soapContext = new
        BasicSOAPMessageContext();
soapContext.setOutboundMessage(envelope);
X509Credential clientTLSCred =
        getClientTLSCred(clientTLSPrivateKeyResourceName,
        clientTLSCertificateResourceName);
StaticClientKeyManager keyManager =
      new StaticClientKeyManager(clientTLSCred.getPrivateKey(),
        clientTLSCred.getEntityCertificate());
HttpClientBuilder clientBuilder = new HttpClientBuilder();
clientBuilder.setHttpsProtocolSocketFactory(
         new TLSProtocolSocketFactory(keyManager, new
        DelegateToApplicationX509TrustManager()));
HttpSOAPClient soapClient = new
        HttpSOAPClient(clientBuilder.buildClient(), parserPool);
soapClient.send(serverEndpoint, soapContext);
Envelope soapResponse = (Envelope) soapContext.getInboundMessage();
```

OpenID Connect

- Interoperable authentication protocol based on the OAuth 2.0 specifications
- OpenID Connect = (Identity, Authentication) + OAuth 2.0
- Provides authentication across websites
- Simple REST/JSON + HTTPS
- Uses token to avoid impersonation
- Several implementations, including GÉANT Federation Lab

Facebook	OpenID Connect
Signed request • Proprietary signature format • Works only with a single identity provider	**ID token** • IETF JSON signature • Works with multiple identity providers

Identity Layer

Who	is the user who got authenticated
Where	was he authenticated
When	was he authenticated
How	was he authenticated
What	attributes he can give you
Why	he is sending them

Personal Experience

- Providing access to NLP services, e.g. parsing natural language documents with the Tanl pipeline
- http://tanl.di.unipi.it/en/
- Users can get an access token from an OpenID provider

Tanl API: User side

Python code

```
import requests

params = {'token':'XXXXXXXXXX', 'service':'parser',
'authentication':'facebook', 'format':'plain'}

r = requests.post(url='http://tanl.di.unipi.it/en/api',
 data = params, files = {'file':f})
```

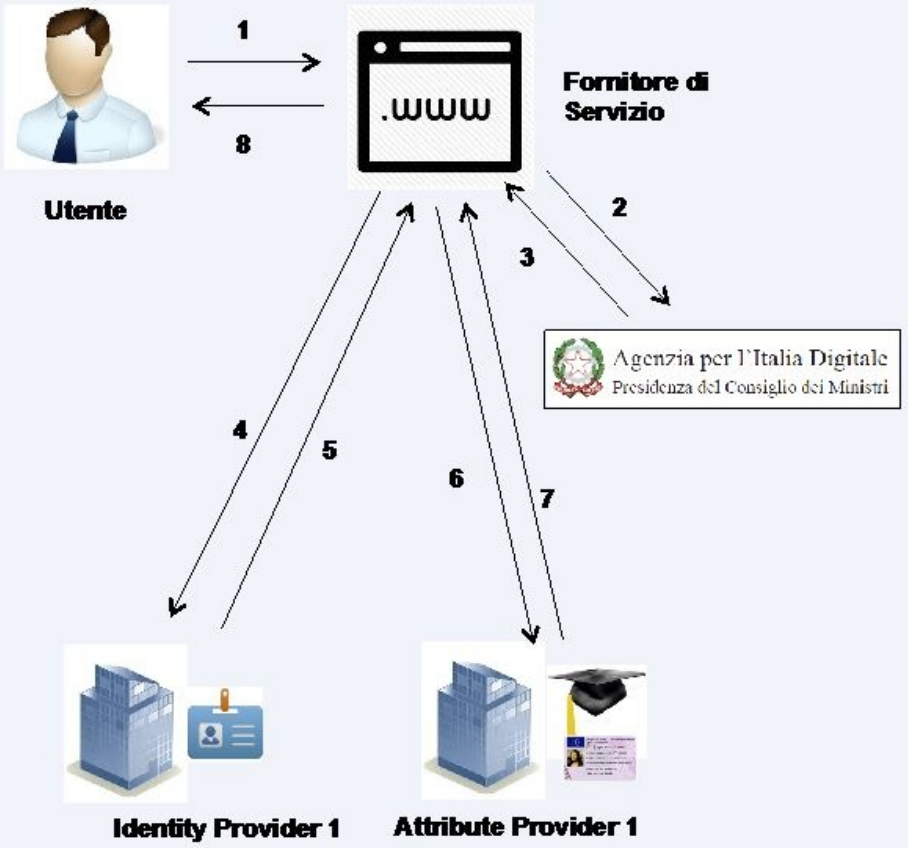
Tanl API: Server Side

```
token = self.getToken()
service = self.getService()
email = self.getEmail()
authentication = self.getAuthentication()
if authentication == 'facebook':
        FacebookHandler.validate(token, email)
text = self.getText()
self.write(Pipe(service).process(text))
```

OpenID Connect vs SAML

- Similar functionality
- OpenID supports IdP discovery, dynamic client registration, and session management
- OpenID Connect easier solution to provide access to backend API
- SAML 2.0 currently the protocol of choice for federations
- OpenID Connect might replace SAML 2.0 in the long run

Sistema Pubblico di Identità Digitale



Le interazioni Fondamentali

- 1: L'Utente richiede l'accesso ad un Servizio, fornendo il proprio identificativo e presentando una credenziale valida
- 2: Il fornitore di Servizio interroga il registro degli Identity Provider e Attribute Provider presso AgID
- 3. AgID restituisce copia del registro
- 4. Il Fornitore di servizio inoltra la richiesta di autenticazione all'Identity Provider corretto
- 5. L'identity provider, nel caso in cui l'utente disponga del corretto livello di credenziale, ne verifica la corrispondenza, fornendo al fornitore di servizio l'asserzione di identità e gli eventuali attributi richiesti.
- 6. (opzionale) Il Fornitore di servizio invia la richiesta di attributi all'Attribute Provider
- 7. (opzionale) L'Attribute Provider fornisce al fornitore di servizio gli attributi richiesti
- 8. L'utente autenticato viene autorizzato ad accedere al servizio o alla funzione richiesta

Parties

- **Gestore delle Identità**
  - soggetto accreditato presso l'Agenzia per l'Italia Digitale
- **Gestori di Attributi qualificati**
  - soggetti che per legge sono titolati a certificare alcuni attributi, come un titolo di studio
- **Gestori di Identità Digitale accreditati**
  - fornisce una Identità Digitale
  - controlla attributi sull'ANPR, l'Anagrafe Nazionale della Popolazione Residente
  - accetta CIE, CNS o Tessera Santaria

Sistema di Autenticazione

- **SPID non prevede a priori uno specifico sistema di autenticazione**
- **Consente al Gestore di Identità Digitale di scegliere la tecnologia da usare**
- **Tre livelli secondo Standard ISO/IEC 29115 :2013**
  1. **Autenticazione a un fattore (password)**
  2. **A due fattori (es. one time password)**
  3. **A due fattori con certificati digitali**

Attivazione

- Decreto entro giugno 2014
- Avviato Pilota per 6 mesi
- **Tutti i siti della Pubblica Amministrazione dovranno adeguarsi allo SPID**

Alphabet soup

- Liberty Alliance
- FIDO Alliance
- Shibboleth
- OSIS
- SAML
- OAuth
- SSO

Questions

- Participate in SPID?
- Simplified API?
- Consider OpenID Connect

References

- http://www.agendadigitale.eu/identita-digitale/700_come-funzionera-il-sistema-di-identita-digitale-italiano.htm
- http://openid.net/developers/specs/
- http://shibboleth.net/products/opensaml-java.html