XACML
eXtensible Access Control Markup Language

Antonio Lioy
< lioy @ polito.it >

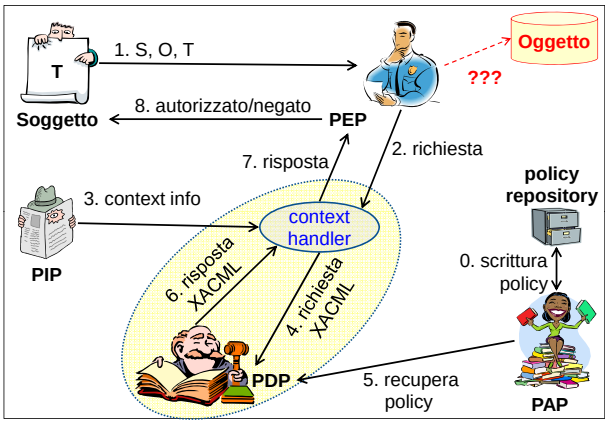
Politecnico di Torino
Dip. Automatica e Informatica

Cos'è XACML?

- **uno standard OASIS basato sulla sintassi XML**
- **un linguaggio per descrivere politiche di autorizzazione, definito in termini di:**
  - subject (utenti, computer, servizi)
  - resource (documenti, file, dati) identificati tramite URI
- **un linguaggio per gestire accessi a risorse protette da politiche di autorizzazione:**
  - formato dati per esprimere richiesta/risposta
  - da veicolare su un protocollo client-server a scelta

Componenti controllo accessi policy-based

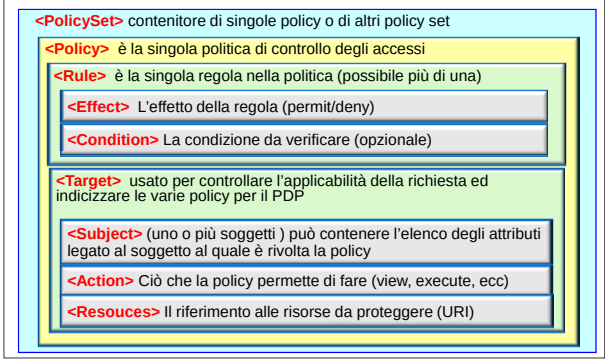
- **PEP = Policy Enforcement Point**
  - protegge una risorsa e ne permette l'accesso solo se le verifica di compatibilità con la policy è positiva
- **PDP = Policy Decision Point**
  - riceve tutte le informazioni (policy, soggetto, risorsa, tipo di accesso, contesto) e decide se concedere o meno l'accesso
- **PIP = Policy Information Point**
  - fornisce le informazioni relative all'accesso richiesto
- **PAP = Policy Access Point**
  - fornisce la policy applicabile all'accesso richiesto



Context handler

- **il PEP:**
  - è strettamente legato all'applicazione o servizio (es. web server, firewall XML)
  - usa formati specifici per richieste/risposte (pochi PEP sono in grado di usare direttamente XACML)
- **context handler:**
  - traduce richieste/risposte di accesso da/a XACML
  - arricchisce le richieste coi valori degli attributi (ottenuti dal PIP) spesso nella forma di asserzioni SAML

XACML: formato policy



XACML: formato richiesta

<Request> contiene le specifiche per i soggetti, le risorse, l'azione e l'ambiente ricavati dal contesto di richiesta

- **<Resource>** specifica le informazioni sulla risorsa alla quale è stato richiesto l'accesso, descritta tramite i suoi **<Attribute>**
- **<Action>** specifica l'azione sulla risorsa, elencando un insieme di elementi **<Attribute>** connessi con l'azione
- **<Subject>** è il soggetto richiedente l'azione, descritto tramite un insieme di suoi **<Attribute>**

<Attribute> (di Subject, Request, Resource)

- **<AttributeID>** (es. username, DN, action, URI)
- **<AttributeValue>**

XACML: formato risposta

<Response> incapsula la decisione del PDP

<Result> rappresenta un'unica decisione di autorizzazione

- **<Decision>** contiene il risultato dell'applicazione della policy sulla richiesta (Permit / Deny / Indeterminate / NotApplicable).
- **<Status>** rappresenta lo stato del risultato della decisione di autorizzazione (contiene un codice di stato, un messaggio di stato e i dettagli di stato)

SAML
Security Assertion Markup Language

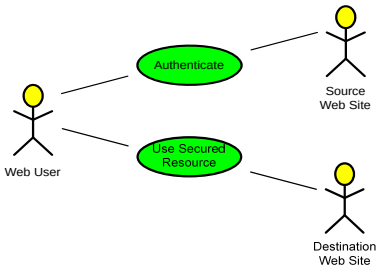
Antonio Lioy
< lioy @ polito.it >

Politecnico di Torino
Dip. Automatica e Informatica

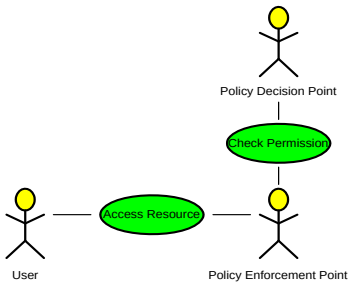
Cos'è SAML?

- **uno standard OASIS basato sulla sintassi XML**
- **un formato dati per:**
  - esprimere vari tipi di affermazioni
  - formulare richieste di affermazioni
  - esprimere risposte contenenti affermazioni
- **affermazione = ASSERTION (oggetto base di SAML)**
- **ha lo scopo di rendere standard e semplificare le interazioni relative a stabilire dei permessi in un sistema distribuito multi-dominio**

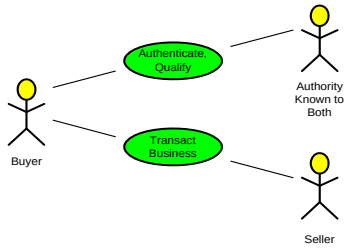
SSO use case



Authorization service use case



Back office transaction use case



SAML assertion

- **un'assertion è:**
  - una dichiarazione relativa ad un fatto pertinente ad un soggetto (es. il ruolo ricoperto da un utente)
  - dichiarazione fatta da un certo issuer
- **tre tipi di assertion (tutte relative a sicurezza):**
  - autenticazione
  - attributi
  - decisione di autorizzazione
- **estensibile per aggiungere altri tipi di assertion**
- **assertion può essere firmata digitalmente (tramite XML signature)**

Authentication assertion

- **un issuer afferma che:**
  - il soggetto S
  - è stato autenticato col meccanismo M
  - al tempo T
- **attenzione! SAML non effettua lui l'operazione di autenticazione (es. richiesta di password, sfida e risposta) …**
- **… ma fornisce un meccanismo per creare un collegamento col risultato di un'autenticazione svoltasi in precedenza da parte di un agente di autenticazione**

Esempio di authentication assertion

```
<saml:Assertion
    MajorVersion="1" MinorVersion="0"
    AssertionID="192.168.1.1.12345678"
    Issuer="Politecnico di Torino"
    IssueInstant="2007-12-03T10:02:00Z">
    <saml:Conditions
      NotBefore="2007-12-03T10:00:00Z"
      NotAfter="2007-12-03T10:05:00Z" />
    <saml:AuthenticationStatement
      AuthenticationMethod="password"
      AuthenticationInstant="2007-12-03T10:02:00Z">
      <saml:Subject>
        <saml:NameIdentifier
          SecurityDomain="polito.it"
          Name="alioy" />
      </saml:Subject>
    </saml:AuthenticationStatement>
  </saml:Assertion>
```

Attribute assertion

- **un issuer afferma che:**
  - il soggetto S
  - è associato agli attributi A, B, C, …
  - che hanno attualmente I valori "a", "b", "c", …
- **tipicamente ottenuto da una query LDAP**
- **esempio:**
  - "alioy" in "polito.it"
  - è associato all'attributo "Dipartimento"
  - con valore "DAUIN"

Esempio di attribute assertion

```
<saml:Assertion ...>
   <saml:Conditions .../>
   <saml:AttributeStatement>
      <saml:Subject>
         <saml:NameIdentifier
            SecurityDomain="polito.it"
            Name="alioy" />
      </saml:Subject>
      <saml:Attribute
         AttributeName="Dipartimento"
         AttributeNamespace="http://polito.it">
         <saml:AttributeValue>
            DAUIN
         </saml:AttributeValue>
      </saml:Attribute>
   </saml:AttributeStatement>
</saml:Assertion>
```

Authorization decision assertion

- **un issuer afferma di aver preso una decisione circa la richiesta di accesso:**
  - da parte del soggetto S
  - per un accesso di tipo T
  - alla risorsa R
  - basandosi sull'evidenza E
- **il sogegtto può essere un individuo o un programma**
- **la risorsa potrebbe essere una pagina web, un file, l'invocazione di un webservice, ...**

Esempio di authorization decision assertion

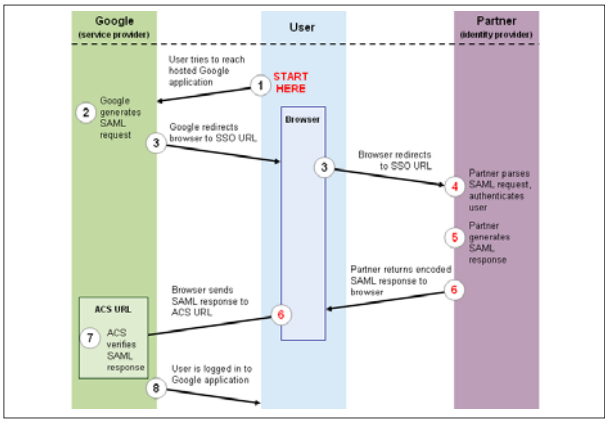
```
<saml:Assertion ...>
  <saml:Conditions .../>
  <saml:AuthorizationStatement
    Decision="Permit"
    Resource="http://did.polito.it/m2170.htm">
    <saml:Subject>
      <saml:NameIdentifier
        SecurityDomain="polito.it"
        Name="alioy"/>
    </saml:Subject>
  </saml:AuthorizationStatement>
</saml:Assertion>
```

Relazione di fiducia

- **spesso le asserzioni fanno parte di una triangolazione**
- **chi accetta l'asserzione deve "fidarsi" di chi genera l'asserzione**
- **nella pratica la relazione di fiducia si stabilisce fissando gli aspetti di sicurezza dello scambio dell'asserzione**
  - push o pull diretto su canale sicuro (es. SSL)
  - chiave condivisa o pubblica per XMLsignature

SAML SSO per Google Apps

- **una ditta (partner) installa la propria applicazione su Google (service provider)**
- **il partner vuole mantenere il controllo della parte di autenticazione ed autorizzazione (identity provider)**
- **lo scambio è basato su SAML-2.0 con firma XML**



SAML SSO per Google Apps: dettagli

- **il partner deve fornire a Google:**
  - la URL del proprio servizio di SSO
  - il certificato X.509 per verificare le proprie firme
- **il passo 3 contiene (in modo opaco):**
  - la URL del servizio Google richiesto dall'utente
  - la richiesta SAML di autenticazione
  - la URL dell'ACS (Assertion Consumer Service)
- **il passo 6 contiene (in modo opaco):**
  - la URL del servizio Google richiesto dall'utente
  - la risposta SAML di autenticazione con firma XML
  - la URL dell'ACS