L’ABC di IDEM – parte II

davide.vaghetti@garr.it

...per rompere il ghiaccio

Quante risorse con un'unica password

video a cura di Marco MALAVOLTI, GARR

http://www.garr.tv/hwdvideos/uploads/v3thk4mmcwqja0.mp4

SAML: il protocollo

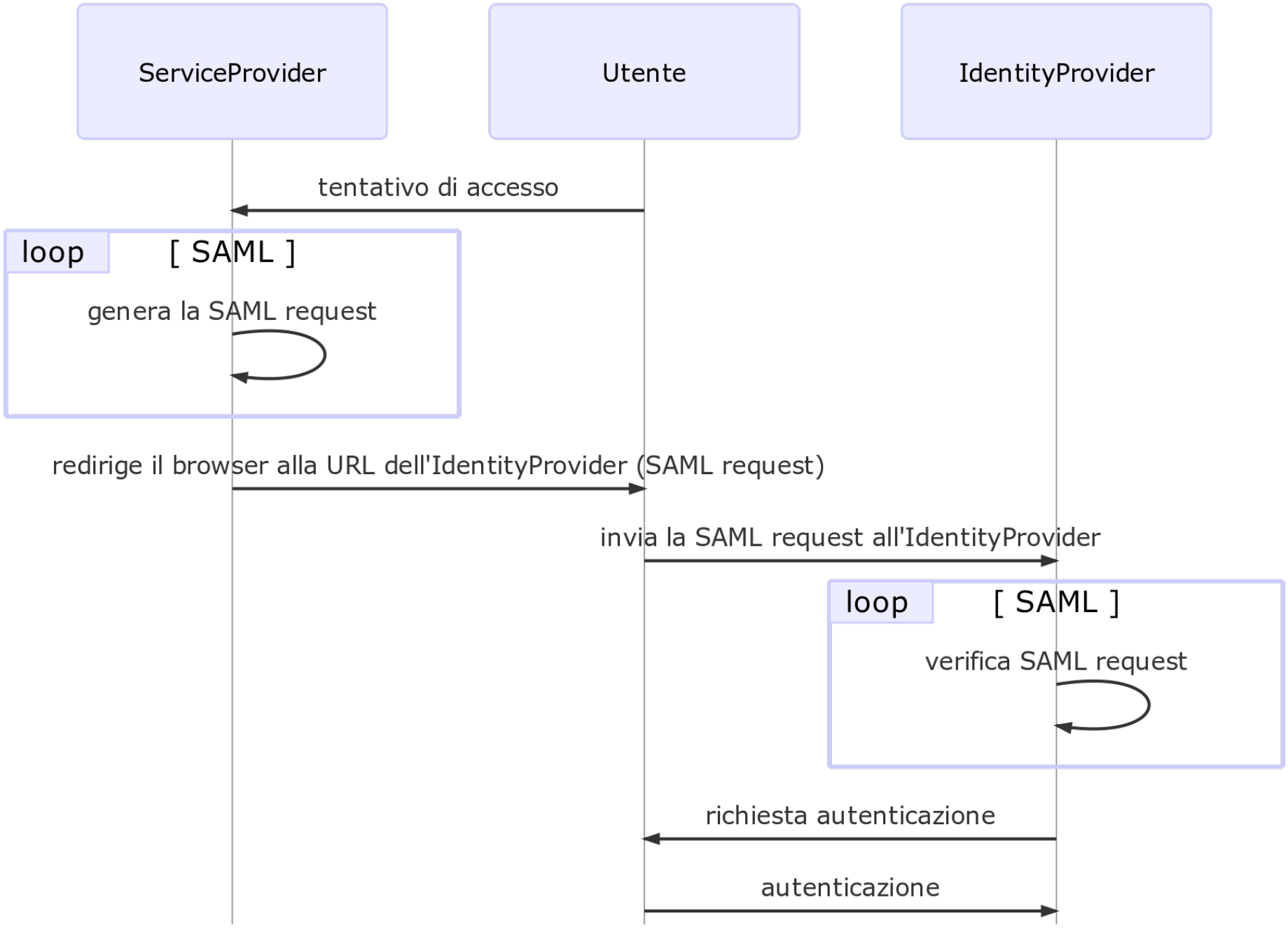
Security Assertion Markup Language

- Standard OASIS
- Regole per lo scambio di dati di **autenticazione** e **autorizzazione**
- Basato su XML
- Web browser SSO (Single Sign On)

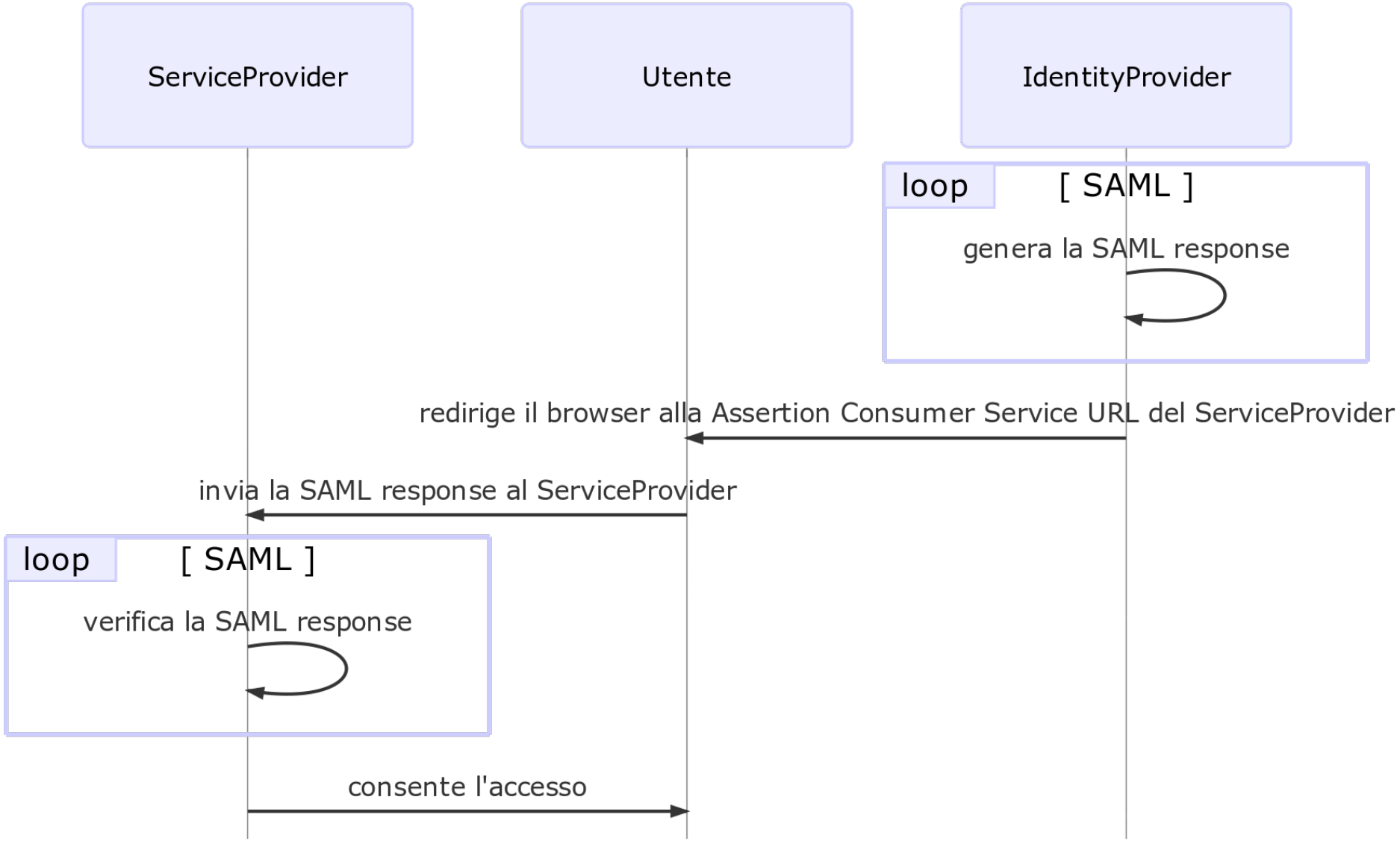
SAML gli attori

- Principal:
  - l’utente
- Identity Provider
  - Collegato a DB utenti (tipicamente una directory)
  - Implementa l’**autenticazione**
  - Rilascia gli attributi
- Service Provider
  - Protegge l’accesso ad un servizio
  - Implementa l’**autorizzazione**
  - Consuma gli attributi

Flusso SAML - 1



Flusso SAML - 2



SAML 2.0 Interoperability Deployment Profile

http://saml2int.org/profile/current/

DEMO

SAML AuthnRequest

```
<samlp:AuthnRequest

xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="aaf23196-1773-2113-474a-fe114412ab72"
    Version="2.0"
    IssueInstant="2004-12-05T09:21:59"
    AssertionConsumerServiceIndex="0"
    AttributeConsumingServiceIndex="0">

<saml:Issuer>https://sp.example.com/SAML2</saml:Issu
er>
  <samlp:NameIDPolicy
      AllowCreate="true"
      Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient"/>
</samlp:AuthnRequest>
```

SAML Assertion

```
<saml:Assertion

xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion
"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance"
    ID="b07b804c-7c29-ea16-7300-4f3d6f7928ac"
    Version="2.0"
    IssueInstant="2004-12-05T09:22:05">

<saml:Issuer>https://idp.example.org/SAML2</saml:
Issuer>
  <ds:Signature

xmlns:ds="http://www.w3.org/2000/09/xmldsig#">...
</ds:Signature>
```

SAML Assertion: Subject

```
  <saml:Subject>
    <saml:NameID
    Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:transient">
      3f7b3dcf-1674-4ecd-92c8-1544f346baf8
    </saml:NameID>
    <saml:SubjectConfirmation

Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
      InResponseTo="aaf23196-1773-2113-474a-
fe114412ab72"

Recipient="https://sp.example.com/SAML2/SSO/POST"
      NotOnOrAfter="2004-12-05T09:27:05"/>
    </saml:SubjectConfirmation>
  </saml:Subject>
```

SAML Assertion: AuthnContext

```
  <saml:Conditions
      NotBefore="2004-12-05T09:17:05"
      NotOnOrAfter="2004-12-05T09:27:05">
    <saml:AudienceRestriction>

<saml:Audience>https://sp.example.com/SAML2</saml:Audience
>
    </saml:AudienceRestriction>
  </saml:Conditions>
  <saml:AuthnStatement
      AuthnInstant="2004-12-05T09:22:00"
      SessionIndex="b07b804c-7c29-ea16-7300-4f3d6f7928ac">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>

urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTr
ansport
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
```

SAML Assertion: AttributeStatement

```
  <saml:AttributeStatement>
    <saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attrib
ute:X500"
    x500:Encoding="LDAP"
    NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:uri"
    Name="urn:oid:1.3.6.1.4.1.5923.1.1.1.1"
    FriendlyName="eduPersonAffiliation">
      <saml:AttributeValue
      xsi:type="xs:string">member</saml:AttributeValue>
      <saml:AttributeValue
      xsi:type="xs:string">staff</saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

solo SAML?

new kids on the block: OpenID Connect

OpenID Foundation

La Federazione IDEM

Federazione IDEM: Attori

La comunita':

- Assemblea dei membri
- Comitato di Indirizzo (CDI)
- Comitato Tecnico Scientifico (CTS)

GARR:

- Servizio GARR IDEM AAI

Chi può aderire ?

- Possono entrare a far parte della Federazione IDEM, in qualità di membri, tutti gli **enti con finalità accademiche, scientifiche e culturali connesse alla Rete Italiana dell'Università e della Ricerca GARR** .
- Possono inoltre partecipare alla Federazione IDEM, in qualità di **partner**, organizzazioni terze (ad esempio editori, fornitori di software o servizi online, ecc), purché forniscano **contenuti o servizi che siano ritenuti utili alla Comunità GARR**. Per tutti la partecipazione è soggetta all'approvazione del Comitato d'Indirizzo della Federazione IDEM.

La Federazione di Test

- L’accesso alla Federazione di Test è garantito dal Servizio IDEM GARR AAI e si può richiedere a idem-help@garr.it.
- **Il passaggio per la Federazione di Test è obbligatorio** prima di poter accedere con il proprio IdP o SP alla Federazione IDEM, per avere la garanzia che il nuovo servizio che entra in federazione sia **aderente ai requisiti**.

La Richiesta di Adesione

- Per partecipare alla Federazione IDEM come Membro o come Partner occorre sottoscrivere rispettivamente la Richiesta di Adesione o l'Accordo di Collaborazione e sottomettere contestualmente la Richiesta di registrazione di un servizio (IdP o SP). Tutta la documentazione compilata deve essere inviata **firmata dal rappresentante legale dell'organizzazione** che chiede di aderire via email a idem@garr.it.

La Procedura di Approvazione

Al ricevimento della richiesta di adesione, il Servizio IDEM GARR AAI provvede ad effettuare i necessari **controlli tecnici e di sicurezza**.

L’Attivazione nella Federazione di produzione

All’avvenuta approvazione della richiesta di adesione del nuovo partecipante, **il Servizio IDEM GARR AAI provvederà ad assistervi nel trasferimento** del vostro servizio dalla Federazione di Test alla Federazione di Produzione.

DOPAU e
Specifiche tecniche attributi