24-25 Novembre 2009
Roma, Sede centrale ENEA

Attori nella Federazione e Profili SAML

Massimiliano Pianciamore
massimiliano.pianciamore@cefriel.it

CEFRIEL
FORGING INNOVATION POLITECNICO DI MILANO

Agenda

- Ruoli e Attori in una infrastruttura federata
  - Service Provider
  - Identity Provider
  - Attribute Authorities
- Lo standard SAML 2.0
  - Asserzioni e Statement
  - Bindings
  - Profiles
- Identity Provider Discovery
- SAML Metadata

massimiliano.pianciamore@cefriel.it

Suddivisione dei ruoli in una infrastruttura federata

- Il paradigma federato costringe a ripensare i ruoli delle organizzazioni nella catena del servizio:
  - Prima fornitori di servizio e di identità erano la stessa organizzazione, ora appartengono a organizzazioni diverse
- I fornitori di servizio ("**Service Provider**", SP) presidiano l'offerta di funzionalità applicative
- I fornitori di identità ("**Identity Provider**", IdP) si specializzano nella gestione delle identità digitali

massimiliano.pianciamore@cefriel.it

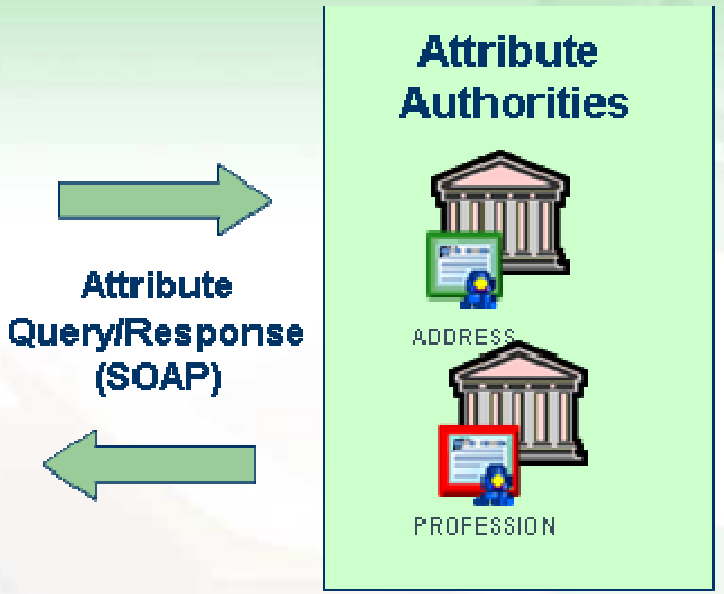
Attori in una Infrastruttura Federata: Identity Provider

- Un **Identity Provider** è un'entità della federazione ICAR in grado di fornire asserzioni sull'identità digitale sugli utenti/subject conosciuti
  - **riceve richieste di autenticazione** con l'indicazione dell'insieme dei metodi di autenticazione ritenuti accettabili dal richiedente
  - **produce token di autenticazione** che certificano l'avvenuto riconoscimento di un subject secondo una specifica modalità (Es. username/pwd, HardwareToken, etc.)
    - Il token di autenticazione prodotto può eventualmente includere anche un insieme di attestazioni del valore degli attributi che caratterizzano il profilo dell'utente mantenuto dal quell'Identity Provider
  - Normalmente un IdP **non è in grado di comportarsi da Attribute Authority**
    - Può produrre attestazioni di attributo soltanto a seguito dell'avvenuta autenticazione di un utente e congiuntamente al token di autenticazione
  - La produzione del token di autenticazione tipicamente prevede l'interazione con il browser utente

massimiliano.pianciamore@cefriel.it

Attori in una Infrastruttura Federata: Attribute Authorities

- Una **Attribute Authority** è in grado di fornire certificazioni di attributo relative ai subject conosciuti
  - Esempi:
    - tutti gli attributi conosciuti di un determinato subject
    - certificazione del valore (o dei valori) di uno o più attributi relativi ad uno specifico subject
- In generale, le Attribute Authorities (AA) **non si comportano come Identity Provider** e non sono in grado di certificare l'identità di un utente/subject
  - Una AA non è in grado di fornire token di autenticazione agli altri componenti della federazione
- Il recupero delle certificazioni di attributo dalle Attribute Authorities tipicamente non prevede l'interazione diretta con l'utente
  - Interazioni M2M
    - Es. SOAP requests/responses



massimiliano.pianciamore@cefriel.it

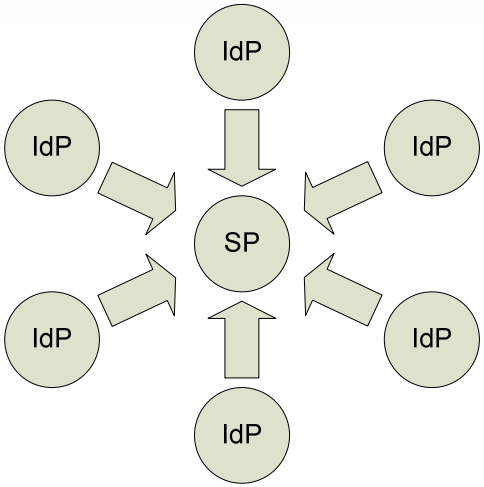
Identità Federata: Considerazioni

- Non esiste una authority 'globale'
  - Le singole (attribute) authorities possono certificare **sottoinsiemi** (in generale distinti) di attributi associati a uno specifico subject
  - Uno stesso attributo per un determinato subject può essere certificato da più authorities (anche con valori diversi tra loro)
    - Esempio: Attributi 'ruolo' o 'professione'
- Servizi distinti possono richiedere sottoinsiemi diversi di attributi di un subject per consentire l'accesso a risorse protette
  - Esempio: dati personali, qualifiche professionali, certificazioni di ruolo

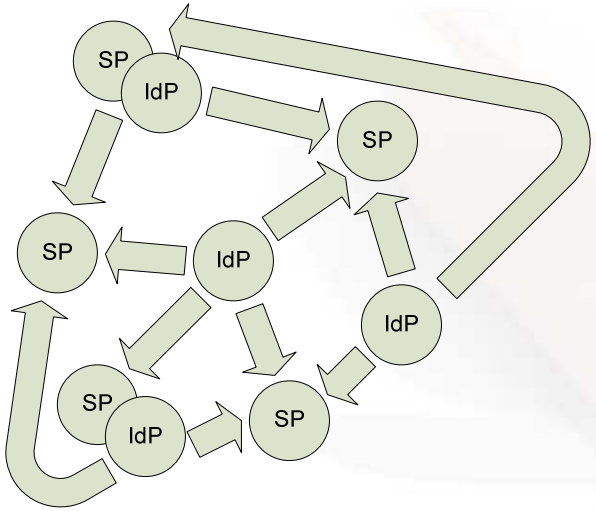
massimiliano.pianciamore@cefriel.it

Suddivisione dei ruoli in una infrastruttura federata

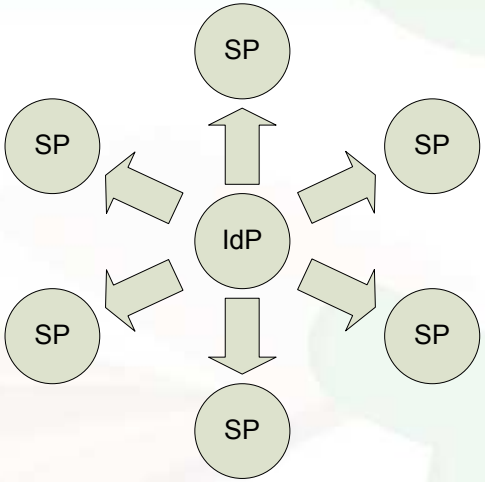
- **Identity Provider** e **Service Provider** possono cooperare secondo diversi "**profili**", ciascuno dei quali definisce l'ambito fiduciario e contrattuale che lega le due tipologie di entità



Profilo "SP Hub"



Profilo "Multi Provider"



Profilo "IdP Hub"

massimiliano.pianciamore@cefriel.it

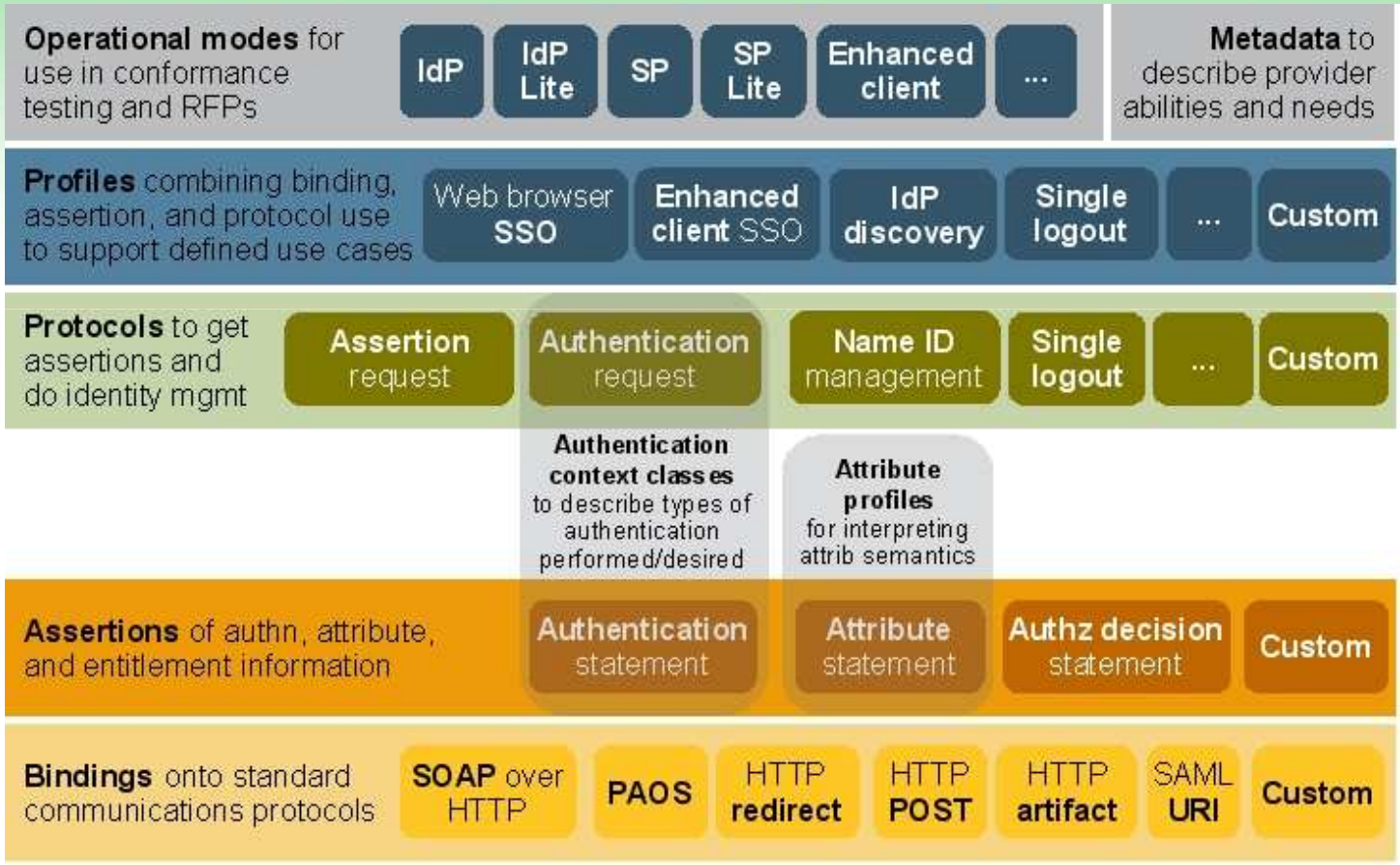
Lo standard SAML

- SAML è un framework per lo scambio di informazioni di sicurezza, dette **asserzioni**, tra business partner via Internet
  - creato nel 2002 dall'ente di standardizzazione OASIS
  - basato su XML
  - indipendente dai singoli vendor
- Principali obiettivi di SAML
  - permettere molta di quella interoperabilità che si è dimostrata assolutamente necessaria tra i prodotti di sicurezza e i sistemi di gestione degli accessi sicuri ai siti Web
  - realizzare un framework unificato che sia in grado di trasmettere le informazioni di sicurezza dell'utente che interagisce con un sistema, in modo da realizzare una "lingua franca" delle credenziali di sicurezza che permetta di scambiare informazioni senza modificare i sistemi di sicurezza esistenti
  - funzionare sui meccanismi di trasporto più comuni (come HTTP, SOAP, ...)

OASIS

massimiliano.pianciamore@cefriel.it

Framework SAML: "the big picture"



Fonte: SUN

massimiliano.pianciamore@cefriel.it

Principali componenti di SAML

- Asserzioni
  - Presenti in tre tipi diversi, sono dichiarazioni di fatti riguardanti l'utente, sia esso una persona fisica o un sistema hardware/software
  - Le **asserzioni di autenticazione** sanciscono il fatto che un utente ha provato la propria identità ad un opportuno **asserting party**
  - Le **asserzioni di attributo** certificano alcuni dati del profilo utente (es., il ruolo assunto in un'organizzazione)
  - I permessi (AuthorizationDecision) identificano invece quali operazioni un utente può compiere (per esempio l'accesso ad una data pagina di un servizio)
- Protocolli
  - Definiscono come si richiedono e ricevono le asserzioni contattando un asserting party
  - Sono costituiti da successioni di messaggi chiamati "SAML request" e "SAML response", codificati in una notazione XML
  - I messaggi di richiesta indicano dati sui soggetti relativamente ai quali viene richiesta un'asserzione
  - Nei messaggi di risposta sono presenti le asserzioni richieste

massimiliano.pianciamore@cefriel.it

Principali componenti di SAML (2)

- Binding
  - I protocolli stabiliscono la struttura delle informazioni che possono essere scambiate ma non determinano le specifiche modalità di trasporto.
  - A tal fine sono stati definiti opportuni 'binding' che indicano come realizzare effettivamente in SAML lo scambio di informazioni di sicurezza attraverso alcuni dei principali protocolli di trasporto (per esempio HTTP o SOAP)
- Profili
  - Corrispondono ad un certo numero di scenari d'uso, nei quali è definito come le asserzioni, i protocolli e i binding vengono utilizzati in modo combinato per raggiungere gli scopi per i quali tali scenari sono stati pensati
  - Esempi di profili sono quelli per effettuare il single sign-on tra vari servizi cross-dominio.

massimiliano.pianciamore@cefriel.it

Versioni dello standard SAML

- SAML 1.0
  - OASIS standard, novembre 2002
- SAML 1.1
  - OASIS standard, settembre 2003
- SAML 2.0
  - OASIS standard, marzo 2005

massimiliano.pianciamore@cefriel.it

SAML 2: Asserzioni e Statement

- Costituiscono il fondamento dello standard SAML
  - Definiscono un insieme di informazioni che esprimono
    - affermazioni (**statement**)
    - emesse da una SAML authority (**asserting party**)
    - a proposito di un soggetto (**subject**).
  - L'entità che riceve e utilizza tali statement è detta SAML requester (o **relying party**).
- La specifica SAML definisce tre diversi tipi di statement che possono essere contenuti in un'asserzione:
  - statement di autenticazione (Authentication Statement)
  - statement di attributo (Attribute Statement)
  - statement di autorizzazione (Authorization Decision Statement)

massimiliano.pianciamore@cefriel.it

SAML 2: Asserzioni (2)

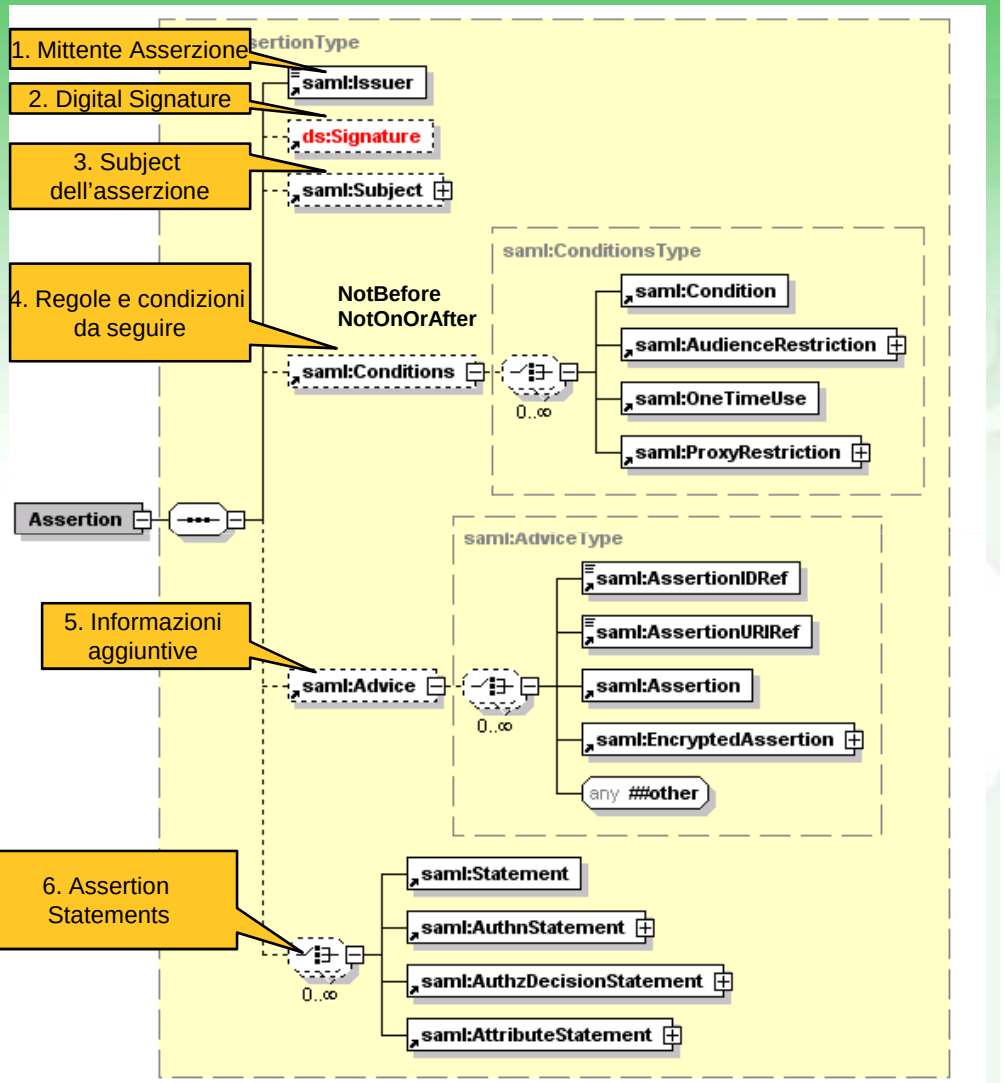
- Un'asserzione contenente statement di autenticazione afferma che
  - un subject si è autenticato,
  - e lo ha fatto in un determinato contesto
    - istante temporale
    - modalità di autenticazione

- Un'asserzione che contiene statement di attributo afferma che
  - un subject è associato a determinate caratteristiche individuali (gli attributi) espresse in generale come coppie nome-valore/i

massimiliano.pianciamore@cefriel.it

Asserzioni SAML: Struttura

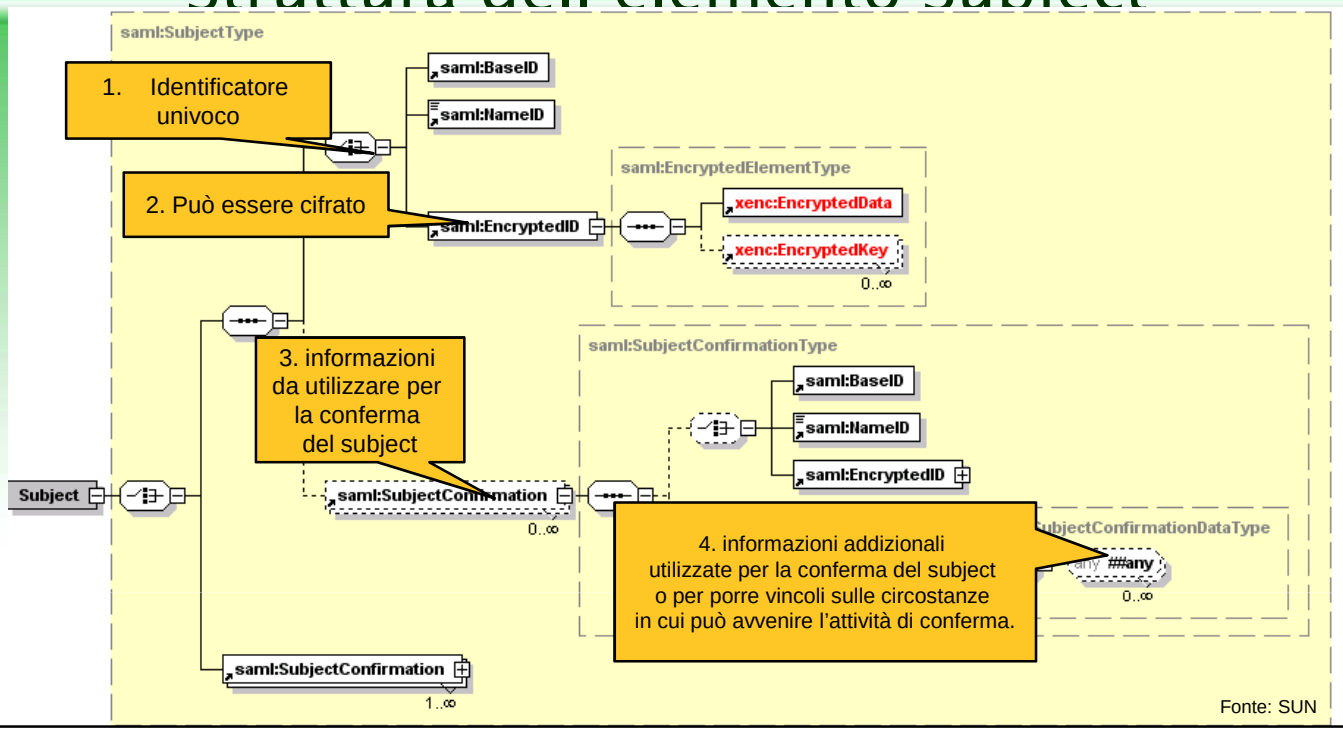
```
<saml:Assertion

xmlns:saml="urn:oasis:names:tc:SAML:2.0:
assertion"
  Version="2.0"
  IssueInstant="2009-10-28T14:01:00Z">
  <saml:Issuer>
    www.identityprovider.com
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID

Format="urn:oasis:names:tc:SAML:1.1:name
id-format:emailAddress">
      J.Handy@emeffgee.com
    </saml:NameID>
  </saml:Subject>
  <saml:Conditions
    NotBefore="2009-10-28T14:00:05Z"
    NotOnOrAfter="2009-10-28T14:05:05Z">
  </saml:Conditions>
    ... Assertion statements...
</saml:Assertion>
```



Fonte: SUN

massimiliano.pianciamore@cefriel.it

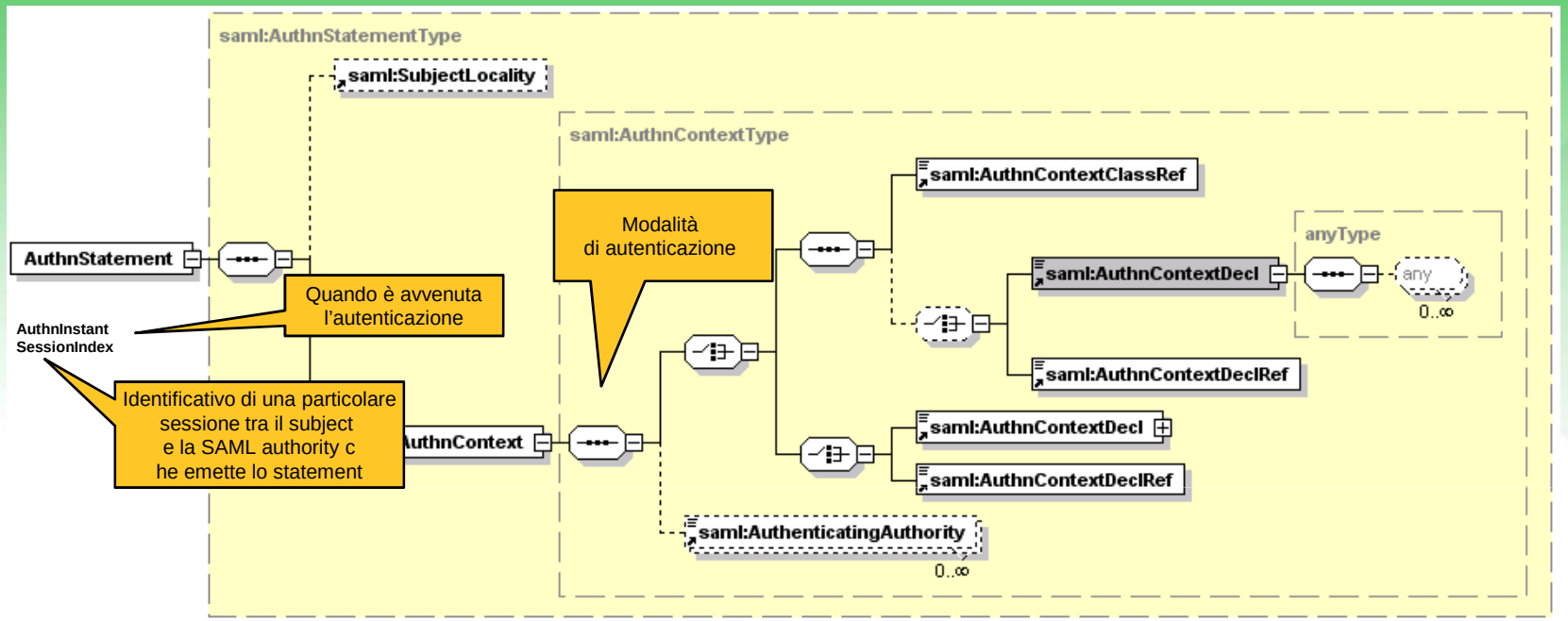
Struttura dell'elemento Subject




```
<saml:Assertion ... elementi comuni ... >
  ... elementi comuni...
 <saml:Subject xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

   <saml:NameID NameQualifier="https://idp.icar.it/icar-idp-test"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">CGNNMO50A01F205J

   </saml:NameID>

   <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer"
        xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">

        <saml:SubjectConfirmationData
        InResponseTo="s25a02bff875afc3e8c1e2eaac72b5fa5cf3df40d3"

        NotOnOrAfter="2008-04-18T10:18:34.876Z"

        Recipient="https://pa.icar.it:3443/icar-pa/AssertionConsumerService" />

   </saml:SubjectConfirmation>

</saml:Subject> </saml:Assertion>
```

massimiliano.pianciamore@cefriel.it

Struttura di un Authentication statement




```
<saml:Assertion ... elementi comuni ... >
  ... elementi comuni...
  <saml:AuthnStatement
    AuthnInstant="2009-10-28T14:00:05Z"
    SessionIndex="0">
    <saml:AuthnContext>
      <saml:AuthnContextClassRef>
urn:oasis:names:tc:SAML:2.0:ac:classes:SmartcardPKI
      </saml:AuthnContextClassRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  ... altri statement...
</saml:Assertion>
```

Fonte: SUN

massimiliano.pianciamore@cefriel.it

Authentication Context

- L'attributo *AuthenticationMethod* usato in SAML 1.1 è sostituito in SAML 2.0 da un *Authentication context*
- SAML 2.0 definisce un insieme di Authentication Context predefiniti per gli scenari di autenticazione più comuni
- E' anche possibile definire un nuovo Authentication context o personalizzare un Authentication Context esistente
  - Attenzione all'interoperabilità!!!

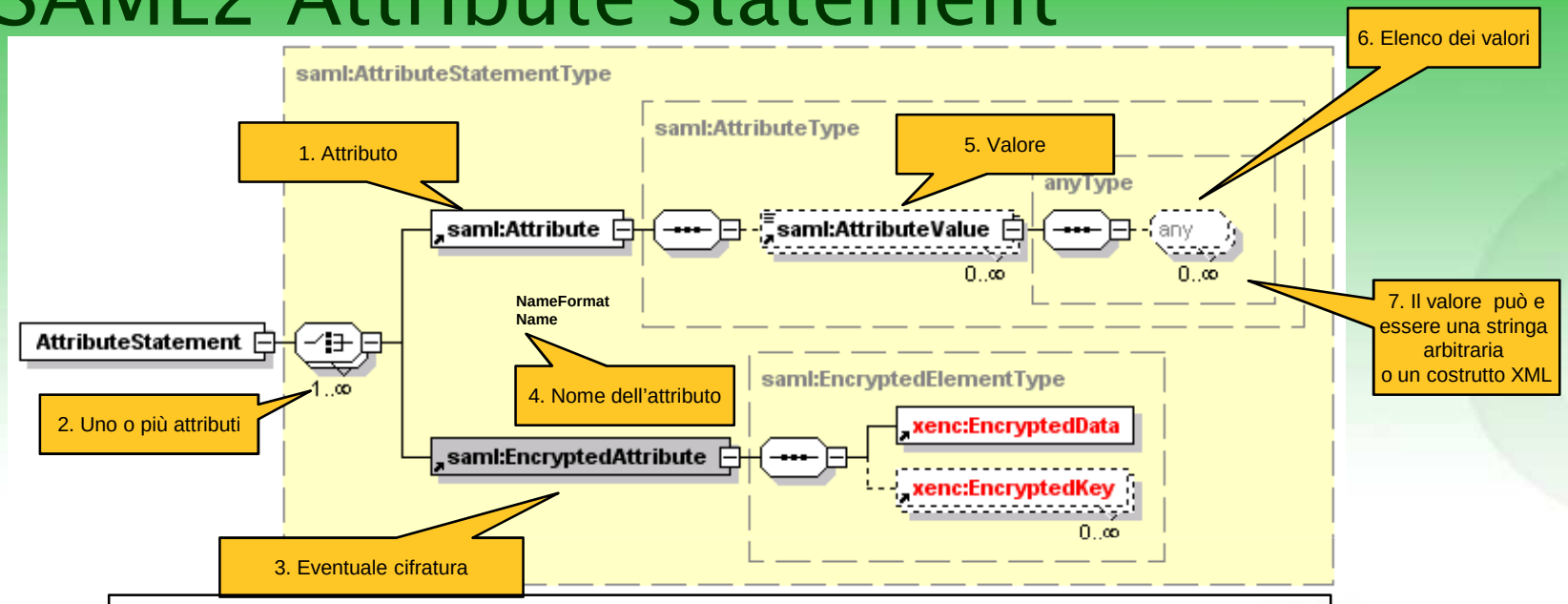
massimiliano.pianciamore@cefriel.it

Authentication Context: Esempi

- **Internet Protocol**
- **Internet Protocol Password**
- Kerberos
- Mobile One Factor Unregistered
- Mobile Two Fa1ctor Unregistered
- Mobile One Factor Contract
- Mobile Two Factor Contract
- **Password**
- **Password Protected Transport**
- Previous Session
- Public Key – X.509
- Public Key – PGP
- Public Key – SPKI
- Public Key – XML Signature
- **Smartcard**
- **Smartcard PKI**
- Software PKI
- Telephony
- Nomadic Telephony
- Personalized Telephony
- Authenticated Telephony
- Secure Remote Password
- **SSL/TLS Cert-Based Client Authentication**
- Time Sync Token

massimiliano.pianciamore@cefriel.it

SAML2 Attribute statement




```
<saml:Assertion ... informazioni comuni ... >
  ... informazioni comuni ...
  <saml:AttributeStatement>
    <saml:Attribute
      NameFormat="http://emeffgee.com" Name="Role" >
      <saml:AttributeValue>repair_tech</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      NameFormat="http://emeffgee.com">
      Name="Certification"
      <saml:AttributeValue xsi:type="emeffgee:type">
        <emeffgee:CertRecord language="EN">
          <Course>
            <Name>Structural Repair</Name>
              <Credits>3</Credits>
          </Course> ...
        </emeffgee:CertRecord>
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Fonte: SUN

SAML2 Bindings

- Un *protocol binding* definisce una modalità di trasporto di SAML Request e Response
  - Stabiliscono come mappare i messaggi di richiesta e risposta SAML su alcuni protocolli standard di comunicazione
- La specifica SAML2 descrive in dettaglio un sottoinsieme di casi significativi al fine di promuovere la conformità allo standard:
  - HTTP Redirect (GET) Binding
  - HTTP POST Binding
  - HTTP Artifact Binding
  - SAML SOAP Binding (SOAP 1.1)
  - Altri
    - Reverse SOAP (PAOS) Binding
    - SAML URI Binding
    - ...

massimiliano.pianciamore@cefriel.it

SAML2 Bindings (2)

- Binding "HTTP POST" e "HTTP Redirect"
  - Supportano i casi in cui l'asserting party (per esempio un certificatore d'identità) e il relying party (per esempio un fornitore di servizi) devono interagire utilizzando uno user agent (per esempio un browser web) che agisce da intermediario.
  - In particolare, l'interazione con lo user agent nei casi in cui sia necessario inoltrare una richiesta di autenticazione a una SAML authority può avvenire rispettivamente:
    - mediante una form HTML che contiene una action di input o submit che si traduce in una HTTP POST verso la SAML authority (è questo il caso della versione "POST->POST binding" del profilo)
    - mediante un messaggio di redirect, con HTTP status code 302 o 303, diretto verso la SAML authority (è questo il caso della versione "Redirect->POST binding" del profilo)

massimiliano.pianciamore@cefriel.it

SAML2 Bindings (3)

- Binding "HTTP POST": Il messaggio SAML viene codificato come un documento XML da inserire nella form HTML restituita all'HTTP client dell'utente (User Agent).
  - Il messaggio SAML viene codificato in formato base-64 e collocato in un campo nascosto (hidden) che deve avere nome SAMLRequest (o SAMLResponse nel caso di risposta)
  - L'attributo action della form deve indicare l'end-point HTTP del ricevente
  - L'attributo method della form dev'essere "POST"
- Binding "HTTP Redirect": La trasmissione del messaggio richiede l'uso di una tecnica di URL encoding
  - L'intero contenuto del messaggio dev'essere collocato nell'URL query string (adottando anche un "deflate" encoding) associato a un parametro di nome SAMLRequest (o SAMLResponse nel caso di risposta) e quindi trasmesso mediante HTTP GET
- Binding "SAML SOAP": La trasmissione di richieste e risposte avviene tramite il protocollo SOAP
  - I messaggi SAML devono essere inclusi nel body del messaggio SOAP
  - In aggiunta è possibile definire header SOAP custom
  - E' il binding utilizzato per le Attribute Query

massimiliano.pianciamore@cefriel.it

Profili SAML2

- SAML supporta un certo numero di *profili*, intesi come specifiche combinazioni di elementi, protocolli e regole di binding
- I più rilevanti rispetto all'interazione tra entità SAML sono
  - SSO Profiles
  - Artifact Resolution Profile
  - Attribute Profiles
  - Assertion Query/Request Profile
  - Name Identifier Mapping Profile

massimiliano.pianciamore@cefriel.it

SAML2 'SSO Profiles'

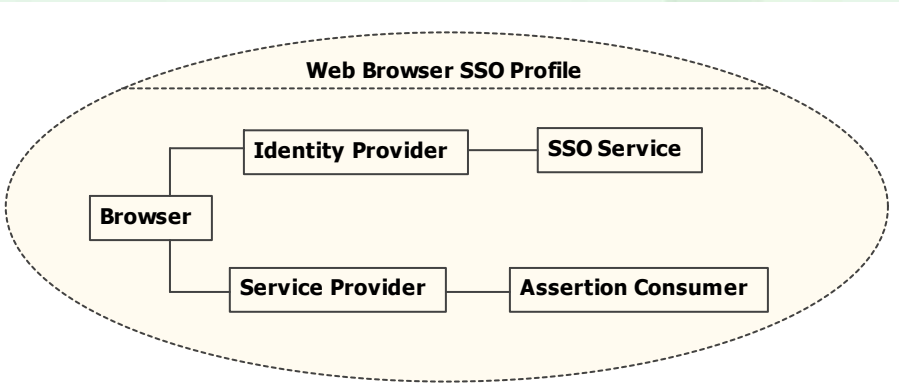
- I Profili SSO S*AML2* includono:
  - Web Browser SSO Profile
  - Identity Provider Discovery Profile
  - Enhanced Client or Proxy (ECP) Profile
  - Single Logout Profile
  - Name Identifier Management Profile

- Il profilo Web Browser SSO è una evoluzione di quello già definito in SAML 1.1
  - Gli altri profili sono stati introdotti nella specifica SAML2

massimiliano.pianciamore@cefriel.it

Web Browser SSO Profile

- Il profilo "Web Browser SSO" descrive l'interazione a fini di autenticazione di
  - Utente (rappresentato dal suo User Agent)
  - Service Provider (che comprende un Assertion Consumer)
  - Identity Provider SAML (che comprende un SSO Service)



massimiliano.pianciamore@cefriel.it

Web Browser SSO Profile (2)

- Il profilo si articola in una serie di sottocasi che nascono dalla combinazione di diverse dimensioni di scelta:
  - Interazione iniziata dal Service Provider o dall'Identity Provider
  - Approccio "push" piuttosto che "pull" per il recupero delle asserzioni emesse dall'Identity Provider.
- Esempi :
  - "SP Initiated: POST->POST Binding"
    - l'interazione è iniziata dal fornitore del servizio e l'interazione tra questo e il certificatore d'identità avviene secondo il binding "HTTP POST"
  - "SP Initiated: Redirect->POST Binding"
    - l'interazione è iniziata dal fornitore del servizio e l'interazione tra questo e il certificatore d'identità avviene secondo il binding "HTTP Redirect".

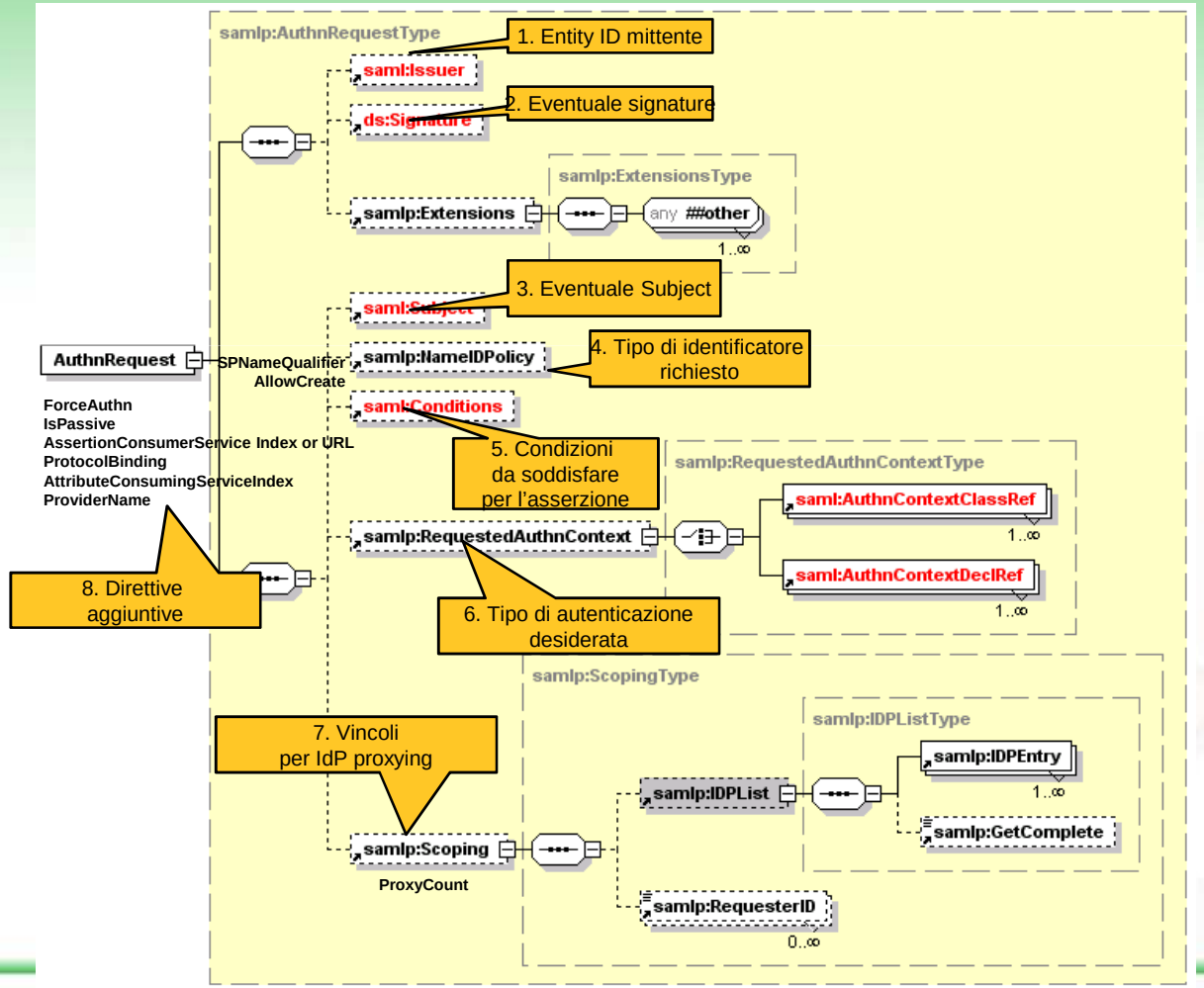
massimiliano.pianciamore@cefriel.it

Web Browser SSO Profile (3)

- Rispetto a quanto definito in SAML1 la specifica SAML2 introduce nel protocollo uno specifico elemento `<samlp:AuthnRequest>`
  - In questo modo è possibile dettagliare completamente una richiesta di autenticazione
- A differenza di quanto definito in SAML1, i profili SAML2 Browser SSO sono di solito SP-Initiated

massimiliano.pianciamore@cefriel.it

Struttura Authentication Request



Fonte: SUN

massimiliano.pianciamore@cefriel.it

SAML2 AuthnRequest: Esempio

```
 <?xml version="1.0" encoding="utf-8"?>

<samlp:AuthnRequest
AssertionConsumerServiceURL="http://sp.icar.it:8080/icar-
sp/AssertionConsumerService"
AttributeConsumingServiceIndex="1"
Destination="https://lp.icar.it:6443/icar-
lp/SSOServiceProxy" ForceAuthn="false"
ID="s231e3a715714745c318cc7ae3525785e87f80bc5b"
IsPassive="false" IssueInstant="2008-04-18T10:00:19.688Z"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
POST" Version="2.0"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

        <saml:Issuer
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">http://s
p.icar.it:8080/icar-sp</saml:Issuer>

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

       ...

        </ds:Signature>

        <samlp:NameIDPolicy AllowCreate="false"
Format="urn:oasis:names:tc:SAML:2.0:nameid-
format:persistent"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol" />

...
```

```
        <samlp:RequestedAuthnContext Comparison="exact"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

                        <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oa
sis:names:tc:SAML:2.0:ac:classes:Password</saml:AuthnCont
extClassRef>

                        <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oa
sis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTranspo
rt</saml:AuthnContextClassRef>

                        <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oa
sis:names:tc:SAML:2.0:ac:classes:SoftwarePKI</saml:AuthnC
ontextClassRef>

                        <saml:AuthnContextClassRef
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">urn:oa
sis:names:tc:SAML:2.0:ac:classes:Smartcard</saml:AuthnCon
textClassRef>

        </samlp:RequestedAuthnContext>

        <samlp:Scoping ProxyCount="2"
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">

                        <samlp:RequesterID
xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol">http:/
/sp.icar.it:8080/icar-sp</samlp:RequesterID>

        </samlp:Scoping>

</samlp:AuthnRequest>
```


massimiliano.pianciamore@cefriel.it

Web Browser SSO Profile: Esempi

- In SAML2, il profilo *Web Browser SSO* è specificato in termini molto generali
- Una implementazione è libera di scegliere una qualsiasi combinazione di *binding*
- Esempi
  - SAML2 Browser/POST
  - SAML2 Browser/Artifact

massimiliano.pianciamore@cefriel.it

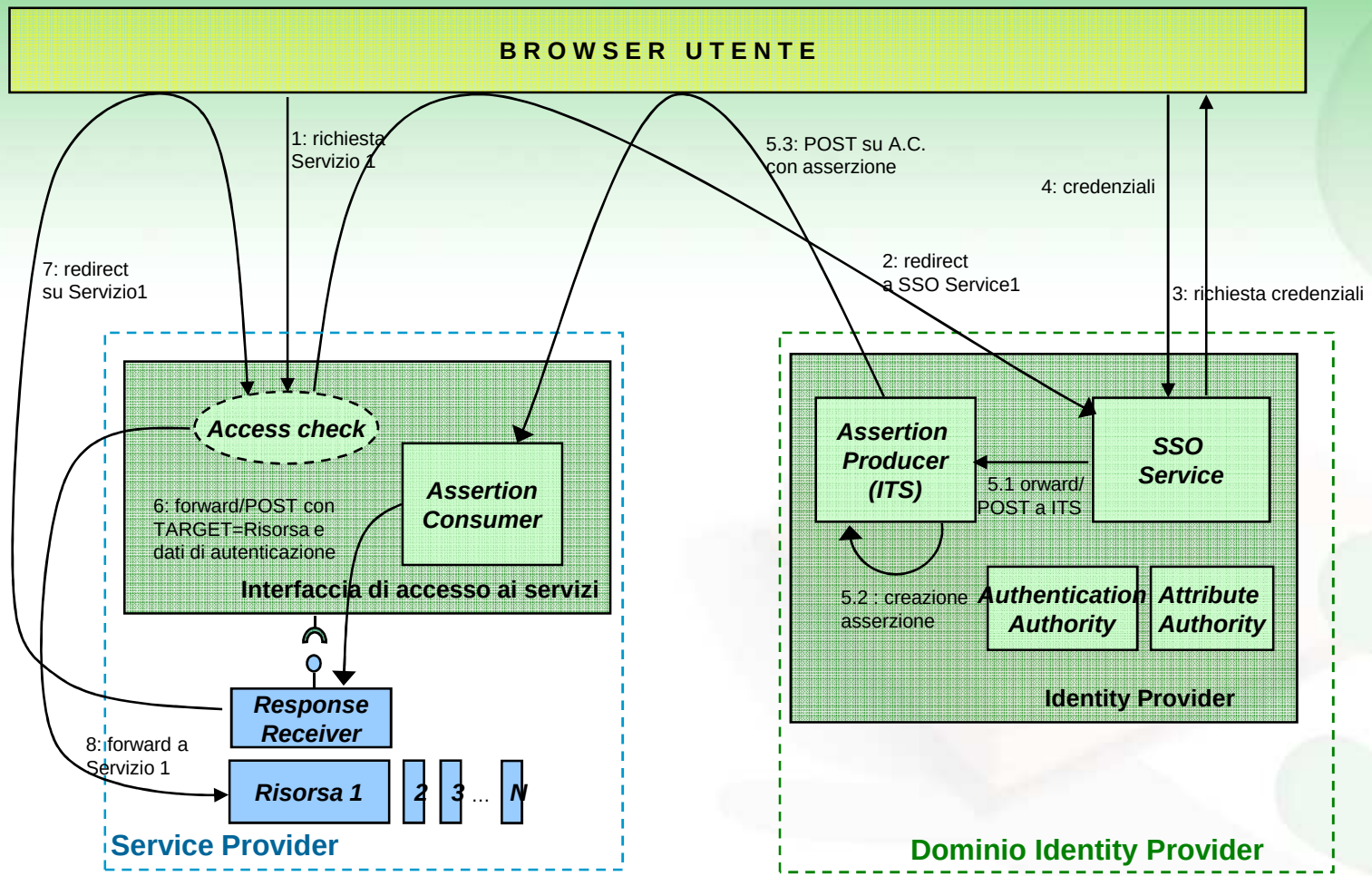
SAML2 Browser/POST Profile

- I passi del profilo *SAML 2.0 Browser/POST* sono i seguenti:

1. Richiesta di accesso alla Risorsa target [SP]
2. Redirect verso il Single Sign-on (SSO) Service [IdP]
3. Richiesta di credenziali [HTML Form]
4. Risposta utente
5. Preparazione Response con Asserzione/i e invio Response ad Assertion Consumer Service
6. Redirect verso risorsa target [SP]
7. Accesso a risorsa target

massimiliano.pianciamore@cefriel.it

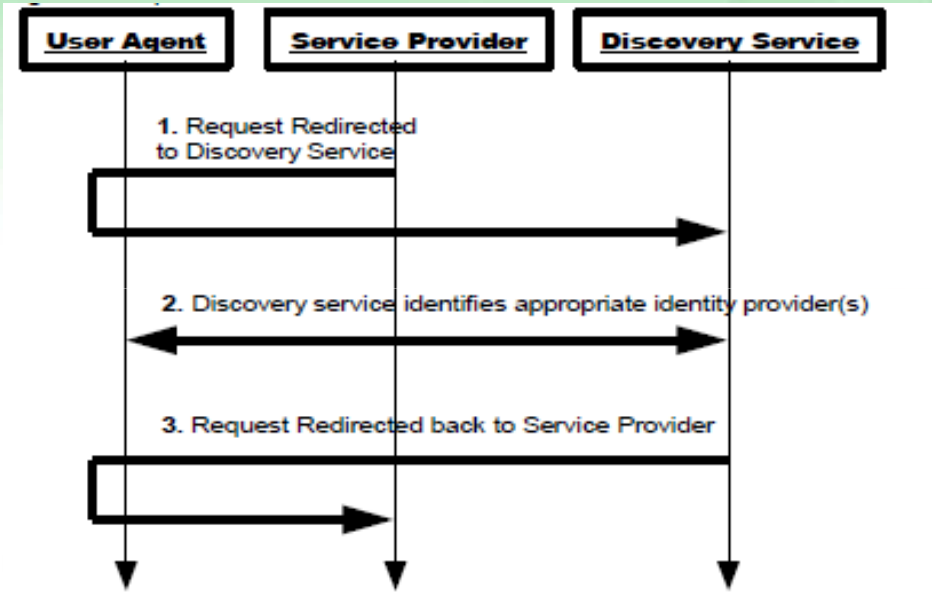
SAML2 Browser/POST Profile (2)



massimiliano.pianciamore@cefriel.it

SAML2 IdP Discovery Profile

- Definisce un protocollo Browser-based attraverso il quale un servizio di discovery centralizzato può fornire a un Service Provider che lo richiede l'identificatore univoco di un Identity Provider a cui inviare l'Authentication Request



Fonte: OASIS

massimiliano.pianciamore@cefriel.it

SAML2 Assertion Query/Request Profile

- Il profilo *Assertion Query/Request* supporta l'esecuzione di diverse tipologie di Query:
  - `<samlp:AttributeQuery>`
  - `<samlp:AssertionIDRequest>`
  - `<samlp:SubjectQuery>`
  - `<samlp:AuthnQuery>`
  - `<samlp:AuthzDecisionQuery>`
- Il binding SOAP è quello più usato

massimiliano.pianciamore@cefriel.it

SAML2 Attribute Query

```
<samlp:AttributeQuery
  ID="..."
  Version="..."
  IssueInstant="..."
  Destination="..."
  Consent="...">
  <saml:Issuer>...</saml:Issuer>
  <ds:Signature>...</ds:Signature>
  <!-- extensions go here -->
  <saml:Subject>...</saml:Subject>
  <saml:Attribute>...</saml:Attribute>
</samlp:AttributeQuery>
```

- Possono essere presenti diversi elementi <saml:Attribute>

massimiliano.pianciamore@cefriel.it

SAML2 Attribute Profiles

- Gli elementi `<saml:Attribute>` devono essere conformi a un *SAML2 Attribute Profile*
- Esempi
  - Basic Attribute Profile
  - X.500/LDAP Attribute Profile
  - UUID Attribute Profile
  - DCE PAC Attribute Profile
  - XACML Attribute Profile

massimiliano.pianciamore@cefriel.it

Esempio: X.500/LDAP Attribute Profile

```
<saml:Attribute

xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500"
  NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:uri"
  Name="urn:oid:2.5.4.42" FriendlyName="givenName">
  <saml:AttributeValue xsi:type="xsd:string"
x500:Encoding="LDAP">
    Steven
  </saml:AttributeValue>
</saml:Attribute>
```

Fonte: SUN

massimiliano.pianciamore@cefriel.it

SAML2 Single Logout Profile

- SAML2 definisce un Profilo *Single Logout* (SLO)
- SLO richiede la gestione delle sessioni
- SLO è complicato e poco supportato nelle implementazioni SAML2 esistenti

massimiliano.pianciamore@cefriel.it

Metadati SAML2

- Durante il funzionamento delle varie entità presenti nell'architettura, si rende necessario conoscere quali sono le modalità secondo cui devono essere svolte alcune attività, sia relativamente al comportamento della singola entità, che in relazione all'interazione con altre entità.
  - Ad esempio, ogni IdP deve essere in grado di decidere se accettare richieste di autenticazione non firmate, se operare una verifica della firma digitale delle stesse e, in caso affermativo, ottenere l'elenco delle chiavi da utilizzare per tale verifica; o ancora, se firmare digitalmente un responso di autenticazione, prima di inviarlo al richiedente.
- Informazioni come quelle appena riportate costituiscono una sorta di meta-informazioni o "**metadati**", diverse rispetto alle informazioni vere e proprie scambiate tra gli attori in gioco ma funzionali allo scenario nel suo complesso.

massimiliano.pianciamore@cefriel.it

Metadati SAML2 (2)

- La specifica SAML 2.0 prevede la possibilità di dichiarare, per i vari tipi di entità coinvolte nei suoi profili, quali sono i metadati associati
- A tal fine, la specifica definisce alcuni schemi XML corrispondenti alle varie tipologie di descrittori di entità esistenti
  - Esistono così descrittori di entità di tipo Service Provider, entità di tipo Identity Provider ed entità di tipo Attribute Authority.
- Per poter essere recuperati, i metadati devono poter essere letti
  - sia localmente da parte della stessa entità a cui sono riferiti,
  - sia remotamente, da parte di entità terze.
    - A questo proposito, la specifica SAML 2.0 si limita a manifestare l'esigenza di disporre di un sistema per la pubblicazione dei metadati, senza scendere nei dettagli di come ciò debba essere fatto

massimiliano.pianciamore@cefriel.it