New Metada Extensions

come rendere più facile la vita all'utente Federato

Massimo Benini

DSET (Dipartimento sistemi e tecnologie)

m.benini@cineca.it

- Alcune cosiderazioni iniziali
- Nuovi flussi di Login
- Customizzare la Login page
- TagLibraries
- Metadata Extensions
- Utilizzare i metadata extensions nella Login page
- DS user interface

Argomenti della presentazione

Il problema

Come si potrebbe fare in modo che i Service Provider siano indipendenti dai Discovery Service delle federazioni a cui appartengono?

NB: non stiamo discutendo dell'utilità delle Federazioni, ma vogliamo trovare un modo per poterci svincolare dai loro Discovery Service

Esempio:

- Servizio di Libreria online che ha dei contratti solo su una parte degli IDP presenti in IDEM.
Come fare per mostrare solo gli IDP abilitati?

- Oppure come VCONF che oltre agli utenti di IDEM ha un suo bacino utenti.

CINECA

1) In molti casi utenti Federati coesistono con utenti propri del SP (chiamiamoli username/password user). Di solito, per il servizio, questi ultimi sono utenti “più importanti”.
E' verosimile che questo accada per ancora un po' di tempo, anche di fronte a BIG IDP (identity provider con molti utenti di tipo diverso).

→ Non possiamo proporre una modalità di login “più complicato” per questo tipo di utenti solo per il fatto che al servizio possono accedere degli utenti Federati.

2) E 'da sperare che i Service Provider siano in grado di conservare una storia di scelte login precedenti (compreso se precedentemente effettuato l'accesso con username / password) → **“Previous Selections cookies”**

Alcune considerazioni-assunzioni

3) Ogni Service Provider dovrebbe far parte al massimo di una federazione o comunque poche (meno di 10) federazioni → non sarebbe altrimenti fattibile fare del clien-side aggragation of identity providers.

4) Ai Service Provider interessa limitare la scelta degli IDP ai loro clienti?
→ ad alcuni interessa veramente mentre per altri l'approccio è: “se sono nella federazione IDEM a noi va bene..”

5) Dovremmo assumere che ogni SP può avere uno o più IDP “preferiti”;

Alcune considerazioni-assunzioni

Flussi e landing points

- **Existing user**
- **First time user**

Gli “existing user” si aspettano di passare velocemente e più facilmente la fase di login.

Per i “first time user” non è sbagliato mostrare delle viste più lunghe e complicate.

Dobbiamo quindi progettare due flussi distinti.

I nostri utenti (in genere studenti e academici) sono differenti rispetto ad utenti di applicazioni e-commerce.

→**internet banking login** – molteplici pagine, non c’è coerenza tra i vari vendor, ma agli utenti non interessa perché c’è un valore economico dietro, sono disposti a farlo.

→ **kiosks, shared machines, SP indifference** - dovremmo pensare a dei modi per velocizzare il loro flusso di login.

I "landing points" o punti iniziali idividuati sono 3:

- **L’home page ha un frame fisso dedicato alla login;**
- **Lazy session initiator "You need to log in to get to where you want“;**
- **Pagina di login dedicata;**

Tutti i “landing points” devono avere lo stesso flusso e gli stessi “suggerimenti visivi”.

Come ottenere questi suggerimenti visivi?

→ **Estensioni dei metadati** per contenere icone e altre informazioni riguardanti IDP e SP per fornire scorciatoie agli utenti abituali e non.

CINECA

Landing points

Home Page - returning users

Caso di un utente già loggato su un altro IDP della Federazione che accede a un SP federato.

In caso di login Federato, dovremmo essere in grado di trattare chiunque si sia loggato da qualsiasi altro IDP federato come returning user.

Welcome back to MY_SP, Rod. Not Rod? Click _here_

Ad un returning user dovrebbe essere mostrato il nome e l'icona dell'istituzione nel quale ha fatto login precedentemente:

You have previously logged in using the _IdP_ [Button]

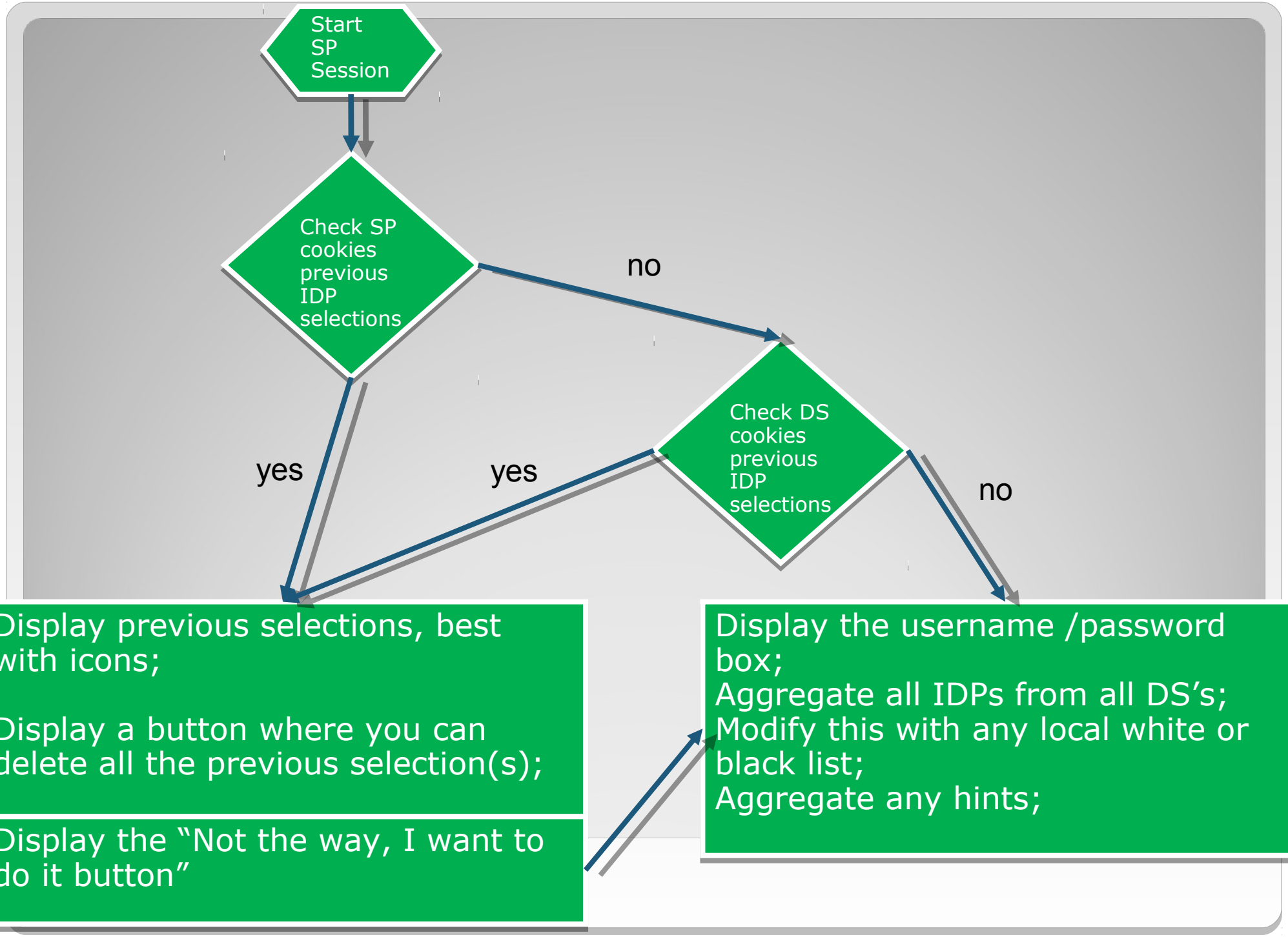
Alcune possibili implementazioni dei flussi di login

In ogni caso abbiamo bisogno del seguente link:

I do not want to login like this. Take me to the _main login_ page

Cliccando sul link si dovrebbero ripulire tutti i cookie SP locali (traccia di quali IDP sono stati scelti precedentemente) ma non i cookie settati dai DS sulle precedenti scelte degli IDP (vedi meglio fra qualche slides..) e si viene rediretti sulla pagina di login principale.

Ridisegnamo il flusso di Login con le assunzioni appena fatte



Modificare la login.jsp:
1) Editare il file src/main/webapp/login.jsp nel IdP distribution package.
2) Ri-esegui lo script di installazione dell'IDP.
3) Restart del Servlet container.

Required Parts:
Alcuni elementi devono essere presenti mentre il resto può avere il massimo grado di customizzazione:
La form deve avere questo action obbligatoriamente:
• <%=request.getAttribute("actionUrl")%>
•The j_username input field must be used for the username.
•The j_password input field must be used for the user's password.

Supporto alle TAGLIB:
Dalla versione dell'IDP 2.3.0 è disponibile una taglib che mette facilmente a disposizione della jsp alcuni tag specifici.
Alcuni di questi tag hanno lo scopo di semplificare l'estrazione delle informazioni contenute nelle estensioni dei metadati <mdui:UIInfo>

Finding, Updating and Deploying the login page

•Le Tag Libraries consentono di semplificare lo sviluppo di siti attivi e di distribuire il codice in maniera semplice da utilizzare e riutilizzare.

•Per definire una tag library occorre definire due cose:

1.Un file TLD (Tag Lib Definition) che specifica i singoli Tag ed a quale "classe" corrispondono;
2.Le classi che effettivamente gestiscono i tag;

Il file TLD (e' un file XML), specifica i singoli tag, quali sono i loro parametri (se ne hanno), quale e' il "body" (se esiste) e quale classe Java si occupa di gestirlo, le singole classi poi devono essere sviluppate per gestirsi ogni tag.

•Una singola Tag Lib puo' contenere centinaia di tag o uno solo.

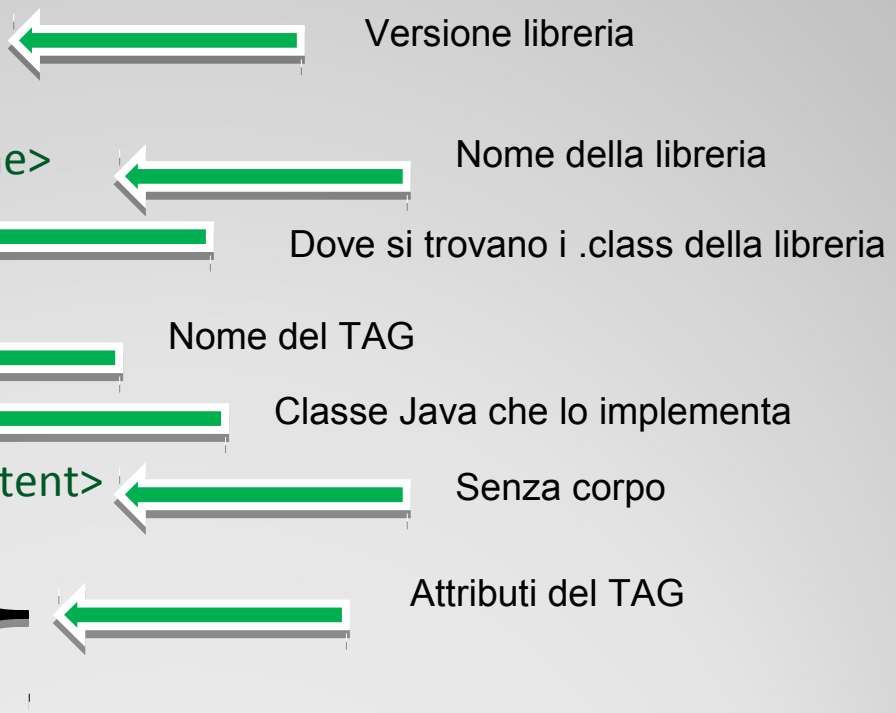
Tag Libraries

```
?xml version="1.0" encoding="ISO-8859-1" standalone="no" ?>
<!DOCTYPE taglib
   PUBLIC "-//Sun Microsystems, Inc.//DTD JSP Tag Library 1.1//EN"
   "http://java.sun.com/j2ee/dtds/web-jsptaglibrary_1_1.dtd">

<taglib>

 <tlibversion>1.0</tlibversion>
 <jspversion>1.1</jspversion>
 <shortname>mytaglib</shortname>
 <uri>taglib</uri>

 <tag>
  <name>test</name>
  <tagclass>test</tagclass>
  <bodycontent>emtpy</bodycontent>
  <attribute>
   <name>first</name>
   <required>true</required>
  </attribute>
 </tag>
</taglib>
```



Esempio file TLD, descrittore del TAG

•Dichiarare nella jsp login.jsp l'uso della taglibrary definita precedentemente:

```
<%@ taglib uri="taglib.tld" prefix="mtl" %>
```

•Il prefix viene usato per distinguere i tag di una libreria dall'altra, in questo modo e' possibile avere lo stesso tag in diverse librerie senza pero' confonderle tra di loro.

•Una volta inserito il richiamo della libreria, possiamo usare i tag con:

```
<mtl:test first="primo_parametro">
```

Utilizzare le taglibraries 1/3

• Occorre scrivere una apposita classe Java che estenda TagSupport (questo per i tag "semplici", per tag piu' complessi sono disponibili classi-base piu' complete).

• La classe deve implementare i metodi: doStartTag() e doEndTag().

• Se il tag non ha nessun "body", la StartTag deve ritornare come valore SKIP_BODY, altrimenti si generera' un errore di runtime.

• Se abbiamo definito uno o piu' parametri nel tag, per ogni parametro occorrera' definire la coppia di metodi setparamname() e getparamname(), per permettere di impostare e recuperare il valore dei vari parametri.

•Una volta definita la classe il nostro tag e' pronto a funzionare.

CINECA

Utilizzare le taglibraries 1/3

Codice classe java che implementa il TAG:

```
import javax.servlet.*;
import javax.servlet.jsp.*;
import javax.servlet.jsp.tagext.*;

public class taglib
  extends TagSupport
{
  private String first;

  public int doStartTag()
    throws JspException
  {
    try
    {
      pageContext.getOut().println("Questo e' il tag!<br>");
      pageContext.getOut().println( first );
    }
    catch( Exception e )
    {
      throw new JspException( "taglib:" + e.getMessage() );
    }

    return SKIP_BODY;
  }

  public int doEndTag()
  {
    return EVAL_PAGE;
  }

  public void setfirst( String first )
  {
    this.first = first;
  }

  public String getfirst()
  {
    return first;
  }
}
```

```
<?xml version="1.0" encoding="ISO-8859-1"
standalone="no" ?>
<!DOCTYPE taglib PUBLIC "-//Sun Microsystems,
Inc.//DTD JSP Tag Library 1.1//EN"
 "http://java.sun.com/j2ee/dtds/web-
jsptaglibrary_1_1.dtd">

<taglib>
 <tlibversion>1.0</tlibversion>
 <jspversion>1.1</jspversion>
 <shortname>mytaglib</shortname>
 <uri>taglib</uri>

 <tag>
  <name>query</name>
  <tagclass>query</tagclass>
  <bodycontent>emtpy</bodycontent>

  <attribute>
   <name>sql</name>
   <required>true</required>
  </attribute>

  <attribute>
   <name>dsn</name>
   <required>true</required>
  </attribute>

  <attribute>
   <name>user</name>
   <required>true</required>
  </attribute>
  <attribute>
   <name>password</name>
   <required>true</required>
  </attribute>
  <attribute>
   <name>fields</name>
   <required>true</required>
  </attribute>
 </tag>
</taglib>
```

TAG query <mlt:query>

```
import …

public class query
  extends TagSupport
{
  /* SQL String used to query the database */
  private String sql;

  /* user name */
  private String user;

  /* password */
  private String password;

  /* DSN */
  private String dsn;

  /* fields list */
  private String fields;

  /* start the tag and perform the work */
  public int doStartTag()
    throws JspException
        ……
{   /* used to parse the fields list */
    StringTokenizer t;
    String connString;
    int fieldnum;

    /* try to connect to the database */
    try
    {
}
    catch( Exception e )
    {
      /* any exception */
      throw new JspException( "query:" +
e.getMessage() );
    }

    return SKIP_BODY;
  }

  /* close the tag */
  public int doEndTag()
  {
    return EVAL_PAGE;
  }

//Metodi getter e setter dei fields    ….. }
```

CINECA

query.java

Per utilizzare il nostro TAG e' sufficiente mettere in una pagina JSP i seguenti tag:

```
<%@ taglib uri="taglib.tld" prefix="mtl" %>
<html>
<head>
<title>TagLib Test</title>
</head>

<h1>Tabella</h1>
<mtl:query
  sql="SELECT FirstName,LastName FROM PERSONS"
  dsn="SOFT"
  user="MBENINI"
  password="XL0-M3Lo--"
  fields="FirstName,LastName"
/>
</body>
</html>
```

TAG query <mlt:query>

Metadata Extensions

•I metadati definiti da SAML 2.0 forniscono un meccanismo per esprimere e comunicare informazioni riguardanti le varie entità SAML coinvolte.
Nel processo di autenticazione è però di solito coinvolto un utente umano, user-agent, che partecipa in modo attivo allo scambio di messaggi.

•Di seguito definiremo un insieme di estensioni per i metadati esistenti che forniscono le informazioni necessarie per migliorare la presentazione delle interfacce utenti e, nel caso di discovery di Identiy Provider, forniscono utili consigli e raccomandazioni per aiutare durante la scelta.

•Il TAG <mdui:UIInfo> DEVE essere contenuto all'interno del TAG <md:Extensions> che a sua volta è contenuto dentro il TAG <md:IDPSSODescriptor> oppure <md:SPSSPDescriptor>.

<mdui:UIInfo> element

•L'elemento **<mdui:UIInfo>** contiene le informazioni pertinenti alla creazione di interfacce utenti per identity provider selection/discovery, user authentication, attribute release consent, etc.

•Questo elemento contiene al suo interno un numero arbitrario di questi altri TAG in qualsiasi ordine:

<mdui:DisplayName>
Localized names for the entity operating in the containing role.

<mdui:Description>
Localized descriptions of the entity operating in the containing role.

<mdui:Keywords>
Localized search keywords, tags, categories, or labels for the containing role.

<mdui:Logo>
Localized logo graphic for the entity operating in the containing role.

<mdui:InformationURL>
URLs to localized information about the entity operating in the containing role.

<mdui:PrivacyStatementURL>
URLs to localized information about the privacy practices of the entity operating in the containing role.

•Questo elemento invece fornisce informazioni per dare dei suggerimenti all'utente durante la fase di discovery, sulla scelta dell'IDP.

•Un meccanismo di selezione server-side insieme alle informazioni client-supplied potrebbero influenzare positivamente in modo da portare alle scelte più probabili.

•Le informazioni presenti in questi TAG servono solo per aiutare l'utente proponendoli gli IDP che più probabilmente sceglierebbe e non per scegliere un IDP in modo definitivo.

•L'elemento `<mdui:DiscoHints>` deve essere contenuto all'interno del TAG `<md:Extensions>` a sua volta contenuto all'interno del TAG `<md:IDPSSODescriptor>`

•L'elemento `<mdui:DiscoHints>` può essere presente al massimo UNA VOLTA dentro il TAG `<md:Extensions>`

CINECA

<mdui:DiscoHints> Discovery Hinting Information

<mdui:DiscoHints> element

L'elemento **<mdui:DiscoHints>** contiene informazioni che possono essere usate durante il processo di selezione discovery come suggerimenti per proporre all'utente uno o più identity provider associati all'utente.

Il TAG, al suo interno, contiene qualsiasi numero dei seguenti elementi in qualsiasi ordine:

<mdui:IPHint>

IP address blocks associated with, or serviced by, the entity operating in the containing role.

<mdui:DomainHint>

DNS domain names associated with, or serviced by, the entity operating in the containing role.

<mdui:GeolocationHint>

Geographic coordinates associated with, or serviced by, the entity operating in the containing role.

Security considerations

• Tutte le URL devono essere controllati contro attacchi di XSS e e relative vulnerabilità.
Only HTTP, HTTPS o DATA, meglio https.
• Il controllo delle URL deve essere fatto da chi pubblica i metadati che contengono le extensions.

Relationship with Existing Metadata Element

La maggior parte delle Identity provider interfaces si basano su <md:OrganizationDisplayName>:

<md:Organization>
<md:OrganizationName xml:lang="en">Example Organization, Ltd.</md:OrganizationName>
<md:OrganizationDisplayName xml:lang="en">Example Organization</md:OrganizationDisplayName>

L'uso si basa su due assunzioni:
1.il nome dell'organizzazione e il contesto è riconoscibile dall'utente;
•l'organizzazione ha un unica entity operante in un particolare ruolo in un determinato periodo;

Suggested Precedence

•<mdui:DisplayName>;
• <md:ServiceName> (se applicabile <md:AttributeConsumingService>);
• entityID o hostname associato all'endpoint del servizio;

CINECA

```
<EntityDescriptor entityID="https://idp.switch.ch/idp/shibboleth"
  xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
xmlns:mdui="urn:oasis:names:tc:SAML:metadata:ui">

  <IDPSSODescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">

    <Extensions>
      <mdui:UIInfo>

        <mdui:DisplayName xml:lang="en">SWITCH</mdui:DisplayName>
        <mdui:DisplayName xml:lang="de">SWITCH</mdui:DisplayName>

        <mdui:Description xml:lang="en">
           Switzerland's national research and eduction network.
        </mdui:Description>
        <mdui:Description xml:lang="de">
           Das schweizerische Hochschul- und Forschungsnetzwerk.
        </mdui:Description>

        <mdui:Logo height="16" width="16">
            https://switch.ch/resources/images/smalllogo.png
        </mdui:Logo>
        <mdui:Logo height="97" width="172">
            https://switch.ch/resources/images/logo.png
        </mdui:Logo>
```

Esempio metadata extensions

```
<mdui:InformationURL xml:lang="en“>http://switch.ch</mdui:InformationURL>
<mdui:InformationURL xml:lang="de“>http://switch.ch/de</mdui:InformationURL>

</mdui:UIInfo>


  <mdui:DiscoHints>

            <mdui:IPHint>130.59.0.0/16</mdui:IPHint>
        <mdui:IPHint> 2001:620::0/96</mdui:IPHint>

        <mdui:DomainHint>switch.ch</mdui:DomainHint>

        <mdui:GeolocationHint>geo:47.37328,8.531126</mdui:GeolocationHint>

  </mdui:DiscoHints>

</Extensions>

    <!-- other role-level elements -->
  </IDPSSODescriptor>
</EntityDescriptor>
```

Esempio metadata extensions

Dalla versione 2.3.0 è disponibile l'uso della taglib "idpui".

Nella login.jsp dichiarare la taglib:

```
<%@ taglib uri="urn:mace:shibboleth:2.0:idp:ui" prefix="idpui" %>
```

Service Provider Name

Tag Format: <idpui:serviceName/>
Typical Outputs: "sp.example.org" or "The Example SP" or "urn:foo:bar:1:24"
Fornisce un nome user-friendly per il service provider. Non viene applicato nessun altro tag HTML.

Comportamento:

1 Cerca l'elemento <mdui:DisplayName> nel linguaggio del browser preferibilmente dentro <md:UIInfo/> all'interno di <md:SPSSODescriptor>.
2 Se non c'è cerca <md:ServiceName> nell'elemento <md:AttributeConsumingService> nei metadati del SP.
3 In assenza di questi, se l' EntityID è un URL allora viene presa la parte relativa all'hostname.
4 In assenza di un entityID, viene usato il body del TAG.

Personalizzare la pagina di login

Service Provider Description

Tag Format: <idpui:serviceDescription>Default Value</idpui:serviceDescription>

Typical Outputs: "An example SP, used for something exciting" or "Default Value"

Fornisce una descrizione user-friendly per il service provider. Non viene applicato nessun altro tag HTML.

Comportamento:

1 Cerca l'elemento <mdui:Description> nella lingua del Browser preferibilmentedentro al TAG <mdui:UIInfo/> all'interno del TAG <md:SPSSODescriptor>.

2 Se non esiste cerca <md:ServiceDescription> all'interno di <md:AttributeConsumingService> nei metadati del Service Provider.

3 In assenza di questi viene usato il body del TAG.

Service Provider Logos

Tag Format: <idpui:serviceLogo cssId="Id" cssClass="class" cssStyle="style" minWidth="integer" maxWidth="integer" minHeight="integer" maxHeight="integer">default</idpui:serviceLogo>

Typical Output:

Attributi:

Name	Default value	Controls
alt	same as <idpui:serviceName/>	The text to associate with the alt attribute
minHeight	0	The minimum height of any returned logo
maxHeight	MaxInt	The maximum height of any returned logo
minWidth	0	The minimum width of any returned logo
maxWidth	MaxWidth	The maximum width of any returned logo
cssId	<none>	If present, the value is included as the id for the image (id="value")
cssClass	<none>	If present, the value is included as the class for the image (class="value")
cssStyle	<none>	If present, the value is included as the style for the image (style="value")

Comportamento:

Cerca il logo contenuto dell'elemento <mdui:Logo> all'interno di <mdui:UIInfo> contenuto dentro <md:SPSSODescriptor> opportunamente vincolato dagli attributi specificati nel TAG <idpui:serviceLogo>.

Se è presente nei metadati il risultato è del tipo:

Se non è presente viene utilizzato il contenuto del di <idpui:serviceLogo> (se presente, esempio icona di default)

Per l'utilizzo degli altri TAG:

"https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAuthUserPassLoginPage"

Personalizzare la pagina di login

- JSP file wayf.jsp

- Come si accede alle estensioni dei metadati per il login e il discovery?

- Importare le seguenti librerie:

```
<%@ page language="java"
import="java.util.*,
edu.internet2.middleware.shibboleth.wayf.*,
java.lang.*, org.opensaml.xml.*,
org.opensaml.saml2.common.*,
org.opensaml.saml2.metadata.*,
org.opensaml.samlext.saml2mdui.*,
javax.servlet.http.*,
java.net.*"%>
```

```
<%
  String spName = null;
  String spLogo = null;
  EntityDescriptor sp = (EntityDescriptor)
request.getAttribute("providerObject");
  if (null != sp) {
    List<RoleDescriptor> roles = sp.getRoleDescriptors();
    for (RoleDescriptor r:roles) {
      Extensions ex = r.getExtensions();
      if (null == ex) {
        continue;
      }
      List<XMLObject> splist = ex.getOrderedChildren();
      for (XMLObject o:splist) {
        if (o instanceof UIInfo) {
          UIInfo info=null;
          info = (UIInfo) o;
          if (info.getLogos() != null) {
            for (Logo logo : info.getLogos()) {
              if (logo.getHeight() <= 16 && logo.getWidth()
<= 16) continue;
              if (null == spLogo) spLogo = logo.getURL();
              break;
            }
            for (DisplayName dn : info.getDisplayNames()) {
              if (null == spName) spName =
dn.getName().getLocalString();
              break;
            }       }       }     }   }
 if (spName == null) {
      try {
        URI uriId = new URI(sp.getEntityID());
        String scheme = uriId.getScheme();

        if ("http".equals(scheme) ||
"https".equals(scheme)) {
          spName = uriId.getHost();
        } else {
          spName = sp.getEntityID();
        }
      } catch (URISyntaxException e) {
        //
        // It wasn't an URI.  return full entityId.
        //
        spName = sp.getEntityID();
      }
    }
  } else {
    spName = "Unknown Service Provider";
  }
%>
```

CINECA

DSUI Discovery Service User Interface

```
<%
  double bestRatio = Math.log(80.0/60.0);
  sites = (TreeSet<IdPSite>) request.getAttribute("sites");
%>

<script type="text/javascript">
  var theIcons =[];
  var theLogos=[];
<%
  for (IdPSite site:sites) {
    if (null == site.getExtensions()) { continue; }
    List<XMLObject> list =
site.getExtensions().getOrderedChildren();
    UIInfo info=null;
    for (XMLObject o:list) {
      if (o instanceof UIInfo) {
        info = (UIInfo) o;
        break;
      }
    }
    if (info == null) { continue;}
    if (null == info.getLogos() || 0 == info.getLogos().size())
{ continue;}
    String logoUrl = null;
    String iconUrl = null;
    double curRatio = 0;
    for (Logo logo : info.getLogos()) {
      if (logo.getHeight() <= 16 && logo.getWidth() <= 16) {
          iconUrl = logo.getURL();
        continue;
      }
        if (logoUrl == null) {
            logoUrl = logo.getURL();
          curRatio =
Math.log(logo.getWidth()/logo.getHeight());
          continue;
        }
        double ratio =
Math.log(logo.getWidth()/logo.getHeight());
        double him = Math.abs(bestRatio - curRatio);
        double me = Math.abs(bestRatio - curRatio);
        if (him > me) {
            logoUrl = logo.getURL();
          curRatio = ratio;
        }
    }
    if (logoUrl != null) {
     %> theLogos['<%=site.getName()%>']='<
%=logoUrl%>'; <%
    }
    if (iconUrl != null) {
     %> theIcons['<%=site.getName()%>']='<
%=iconUrl%>'; <%
    }
  }
%>
</script>
```

DSUI Discovery Service User Interface

- http://www.soft-land.org/articoli/taglib
- http://www.niso.org/workrooms/sso
- https://spaces.internet2.edu/display/~rdw@iay.org.uk/Home
- https://spaces.internet2.edu/display/~rdw@iay.org.uk/SPDiscoveryObservationsRequirements
- https://target.iay.org.uk/
- https://refeds.org/meetings/sep11/slides/nicole-refedsREF2-fall2011.pdf
- https://sh2testsp1.iay.org.uk/
- http://wiki.oasis-open.org/security/SAML2MetadataUI
- https://wiki.shibboleth.net/confluence/display/SHIB2/IdPAuthUserPassLoginPage
- https://wiki.shibboleth.net/confluence/display/SHIB2/DSUIEdit

CINECA

Bibliografia