Roma, 2-3 Dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

Capire il Single Logout

Maria Laura Mantovani
GARR e Università di Modena e Reggio Emilia

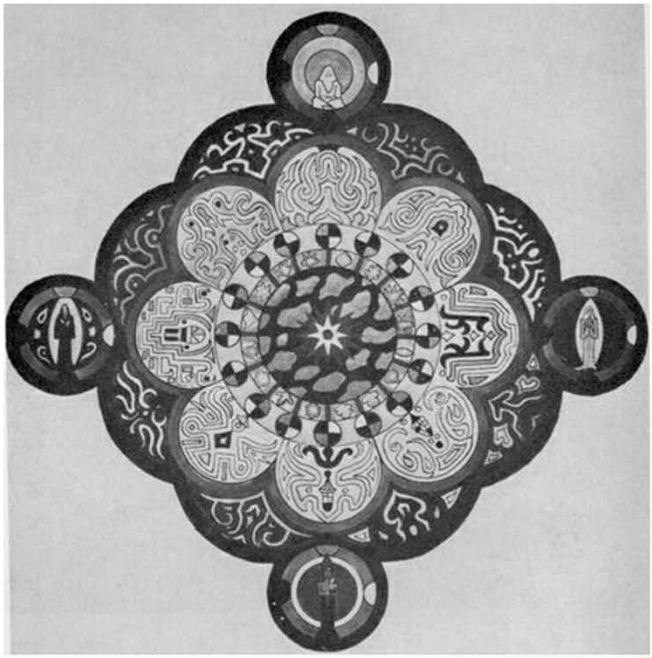
marialaura.mantovani@garr.it

Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca

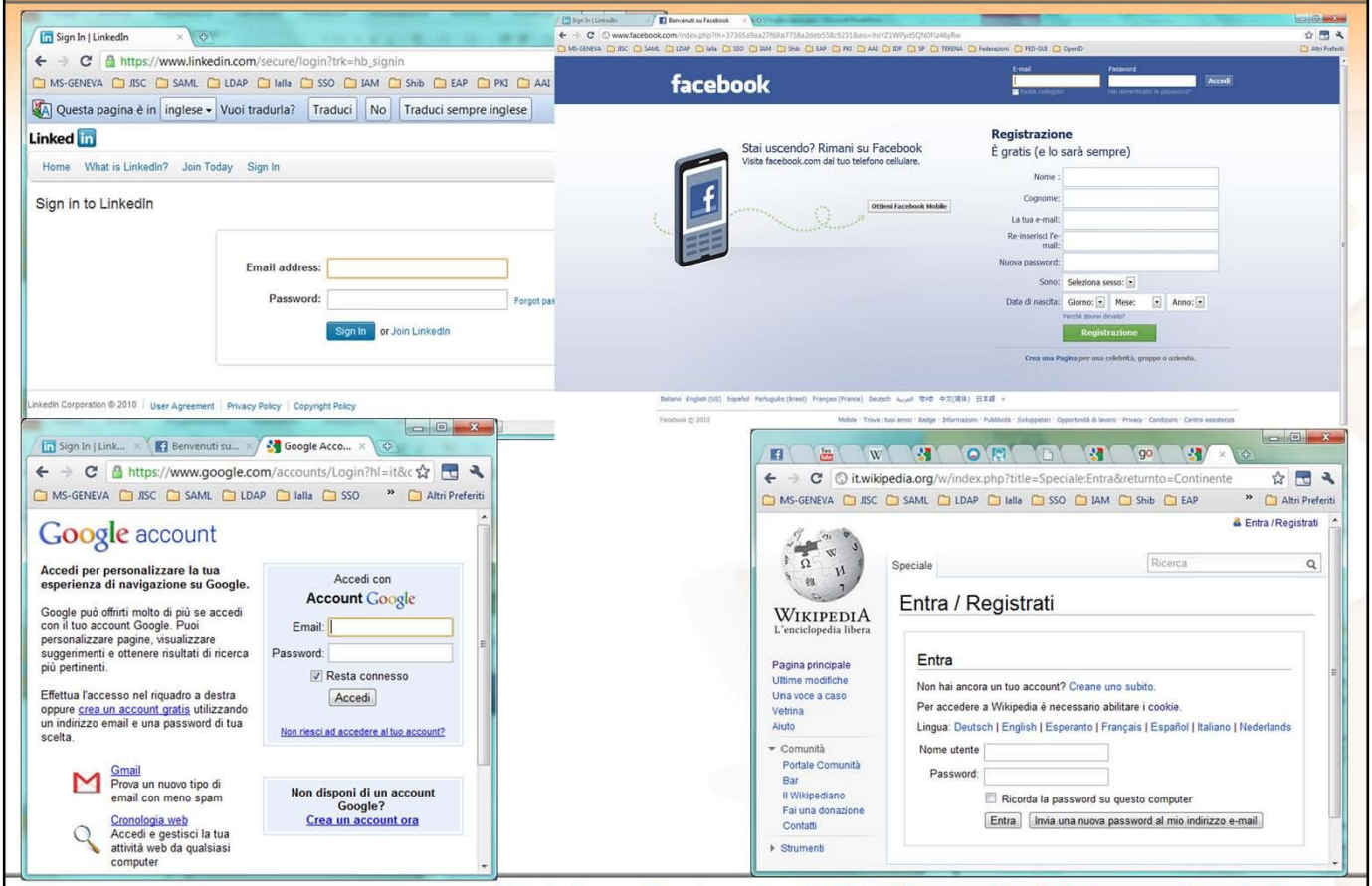
AGENDA:

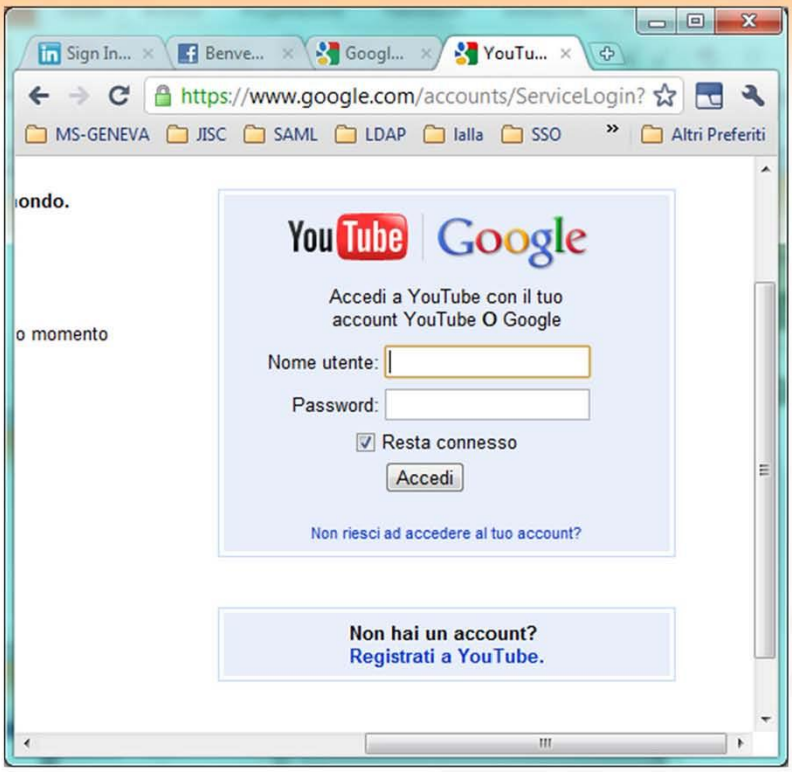
- Sessione SSO
- Logout
- SAML2 SLO Profile
- Problemi
- Consigli

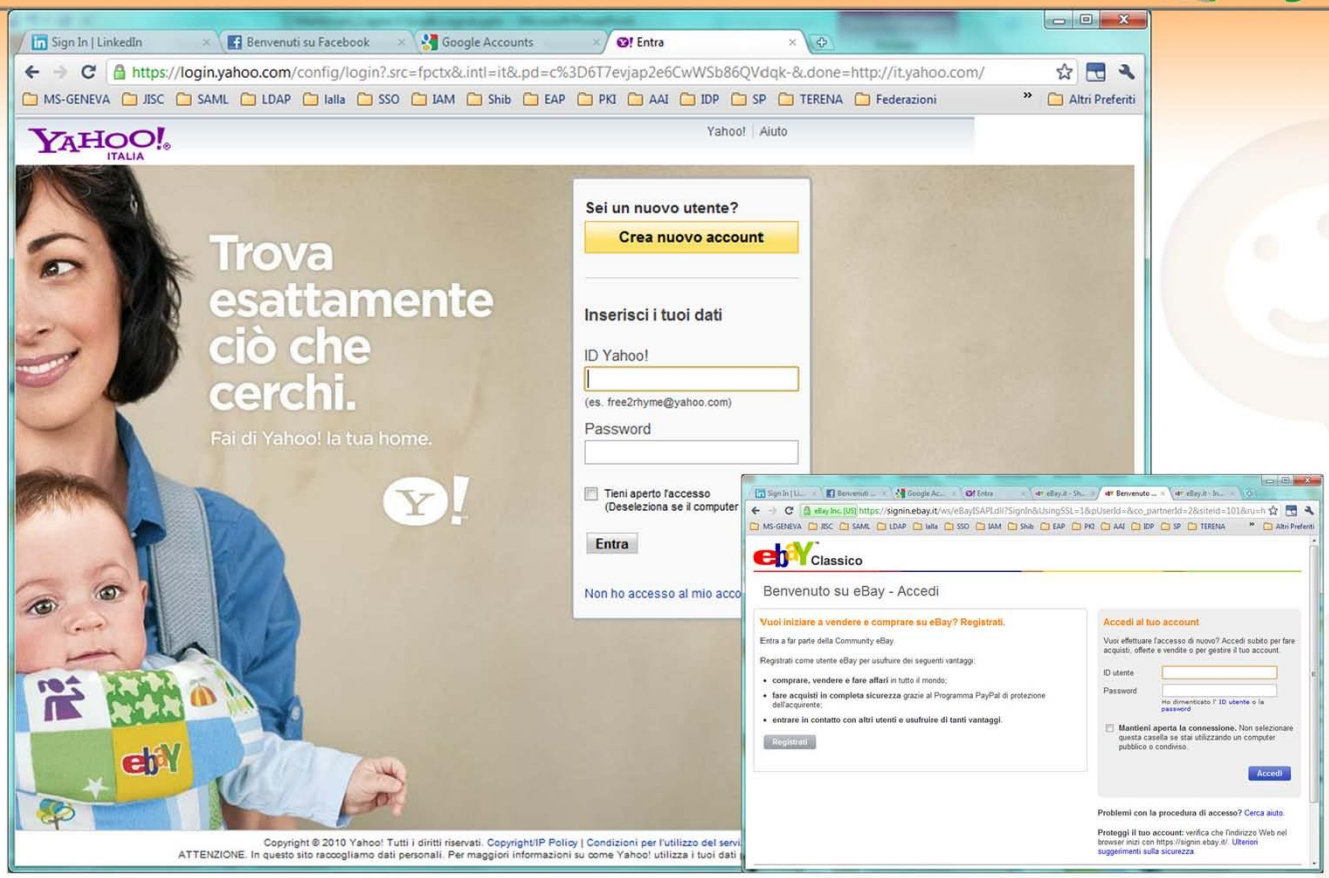
SESSIONE: semplice o complessa?

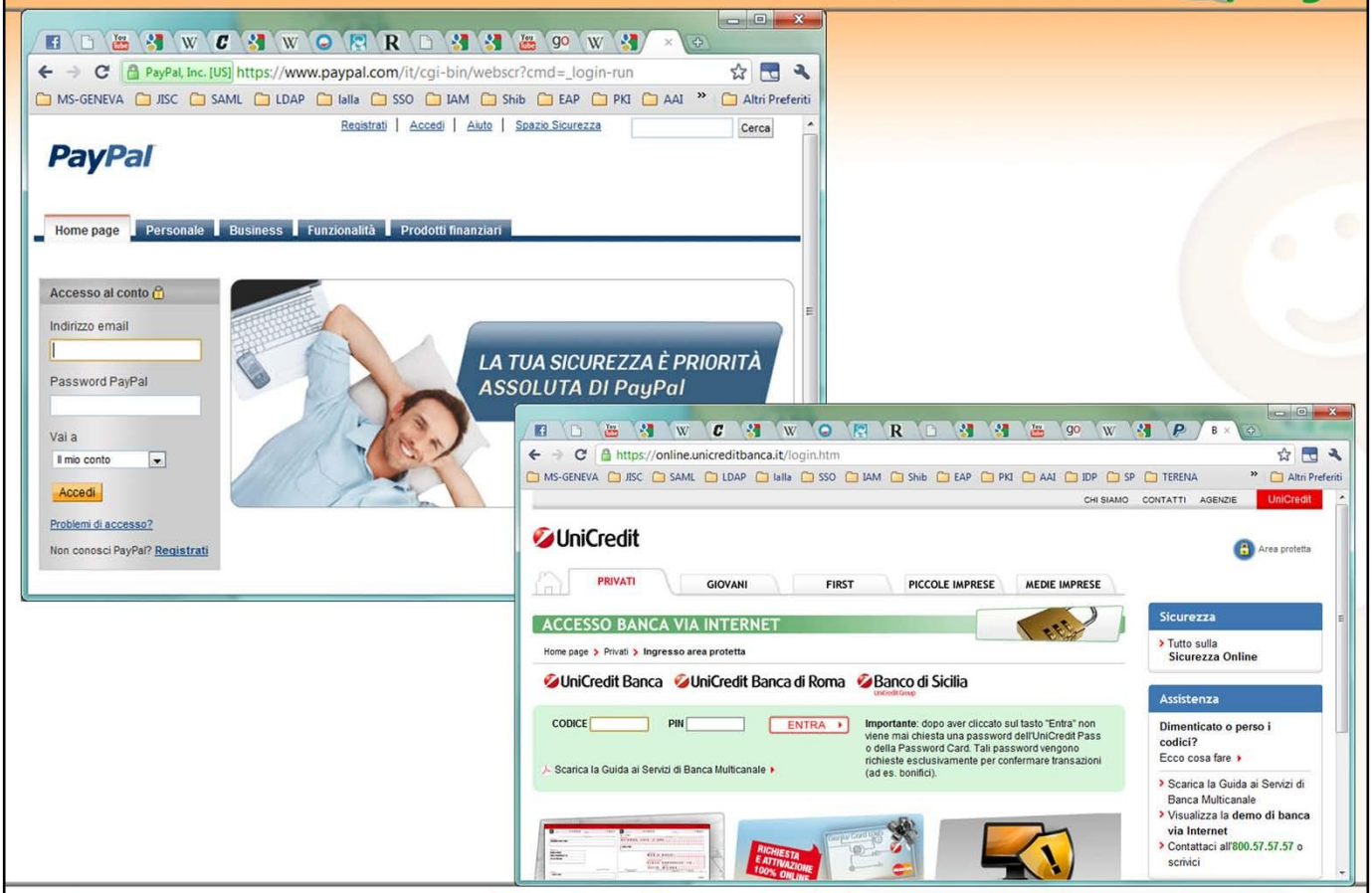


Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day

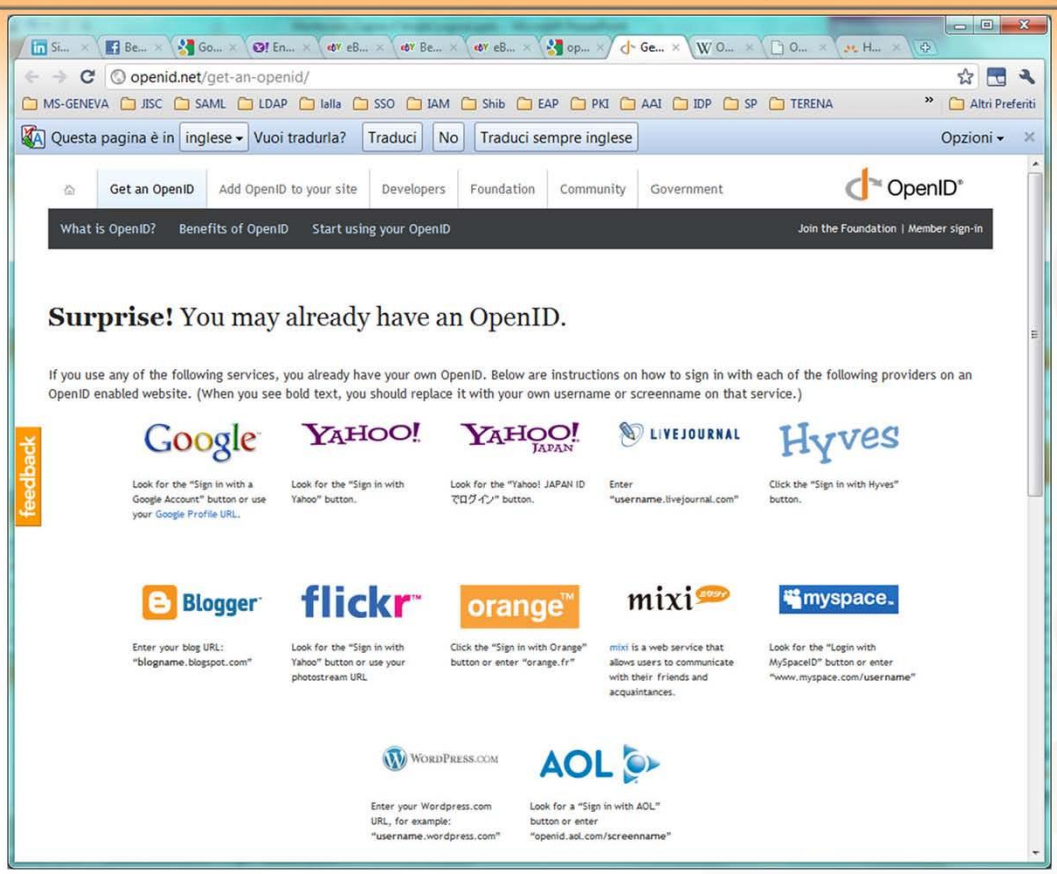


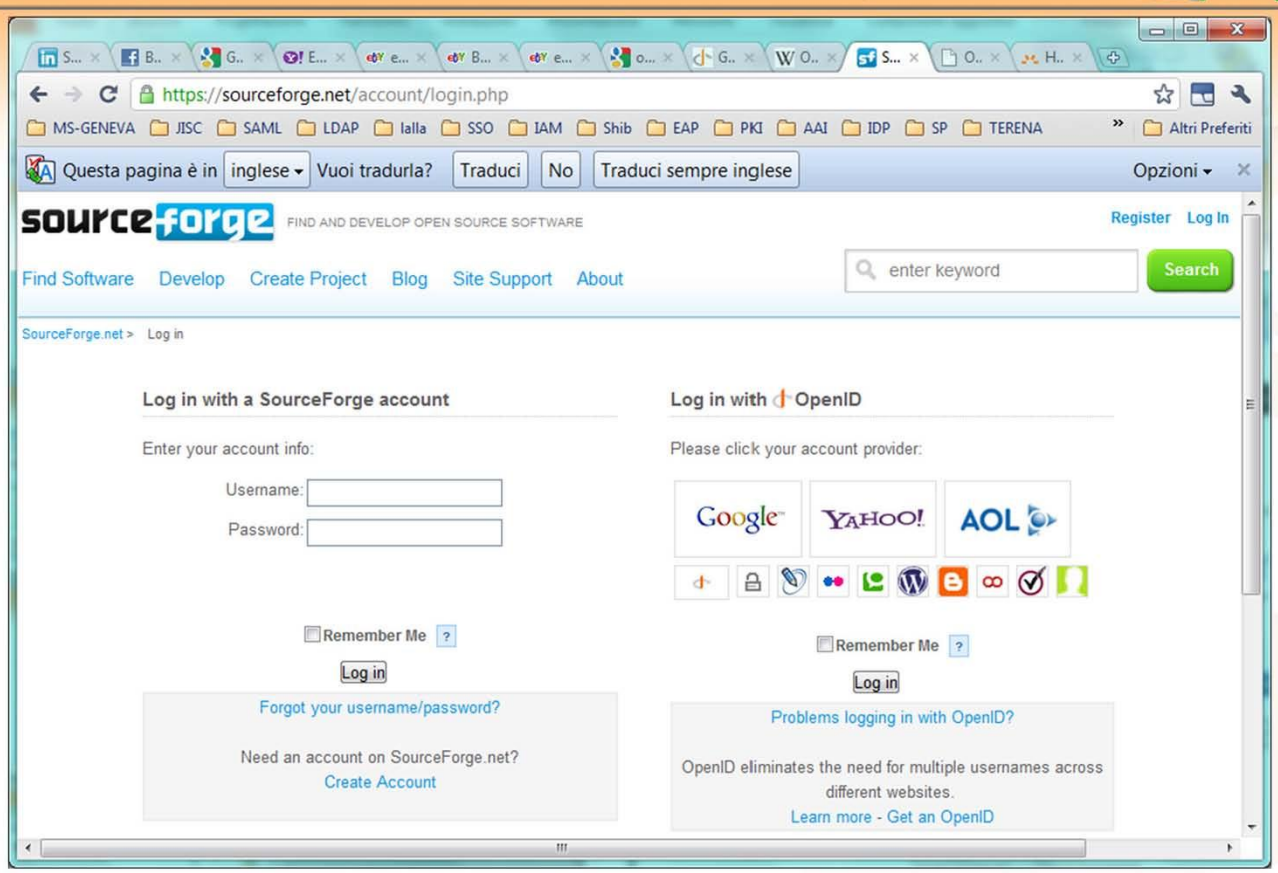

Sign In...
Benve...
Googl...
YouTu...
https://www.google.com/accounts/ServiceLogin?
MS-GENEVA
JISC
SAML
LDAP
lalla
SSO
Altri Preferiti
ondo.
o momento
YouTube
Google
Accedi a YouTube con il tuo account YouTube O Google
Nome utente:
Password:
Resta connesso
Accedi
Non riesci ad accedere al tuo account?
Non hai un account?
Registrati a YouTube.

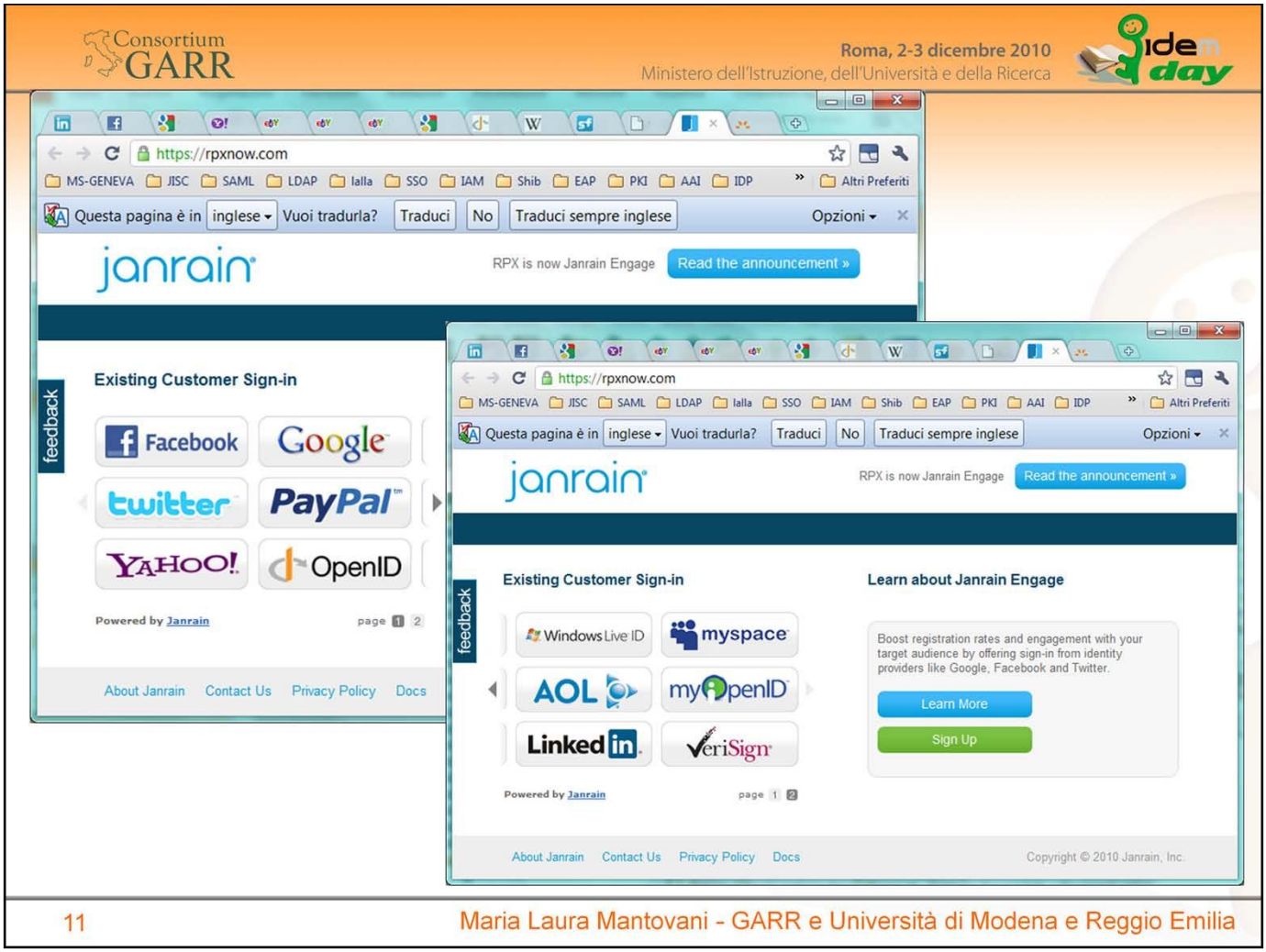

Sign In | LinkedIn
Benvenuti su Facebook
Google Accounts
Entra
https://login.yahoo.com/config/login?.src=fpctx&.intl=it&.pd=c%3D6T7evjap2e6CwWSb86QVdqk-&.done=http://it.yahoo.com/
YAHOO! ITALIA
Yahoo! Aiuto
Trova esattamente ciò che cerchi.
Fai di Yahoo! la tua home.
Sei un nuovo utente?
Crea nuovo account
Inserisci i tuoi dati
ID Yahoo!
Password
Tieni aperto l'accesso
Entra
ebay Classico
Benvenuto su eBay - Accedi


PayPal
Home page
Personale
Business
Funzionalità
Prodotti finanziari
Accesso al conto
Indirizzo email
Password PayPal
Vai a
Il mio conto
Accedi
Problemi di accesso?
Non conosci PayPal? Registrati
LA TUA SICUREZZA È PRIORITÀ ASSOLUTA DI PayPal
UniCredit
PRIVATI
GIOVANI
FIRST
PICCOLE IMPRESE
MEDIE IMPRESE
ACCESSO BANCA VIA INTERNET
UniCredit Banca
UniCredit Banca di Roma
Banco di Sicilia
CODICE
PIN
ENTRA
Sicurezza
Assistenza


openid.virgilio.it
VIRGILIO OpenID BETA
Cerca nel Web
CERCA
COS'È OPENID | DOVE | IMPOSTAZIONI PERSONALI | BLOG
Apri il tuo OpenID
accedi con OpenID
Entra con Facebook
e-mail
password
password dimenticata
ENTRA
Cos'è Virgilio OpenID
Dove lo utilizzo
Una sola registrazione per tutto il web in totale sicurezza!
Cosa
Dove
Non hai ancora un OpenID?
Iscriviti adesso
Per saperne di più
Wikipedia
L'enciclopedia online
OpenID Europe Foundation
Progetto Open Source per OpenID in Europa
OpenID Foundation
La Fondazione di OpenID
Planet OpenID
Il mondo OpenID
Myblog
OpenID visto da Myblog
Technorati
Il punto di vista dei blogger
Blog OpenID
Il blog italiano di OpenID
Virgilio OpenID
OpenID è la nuova tecnologia che ti permette di avere un solo username e una sola password da utilizzare su centinaia di siti web.
Una volta attivato il tuo Virgilio OpenID per accedere ad un sito che supporta OpenID sarà sufficiente inserire gli stessi dati di accesso che usi su Virgilio: potrai dire addio alle numerose registrazioni utilizzate fino ad oggi!
avanti

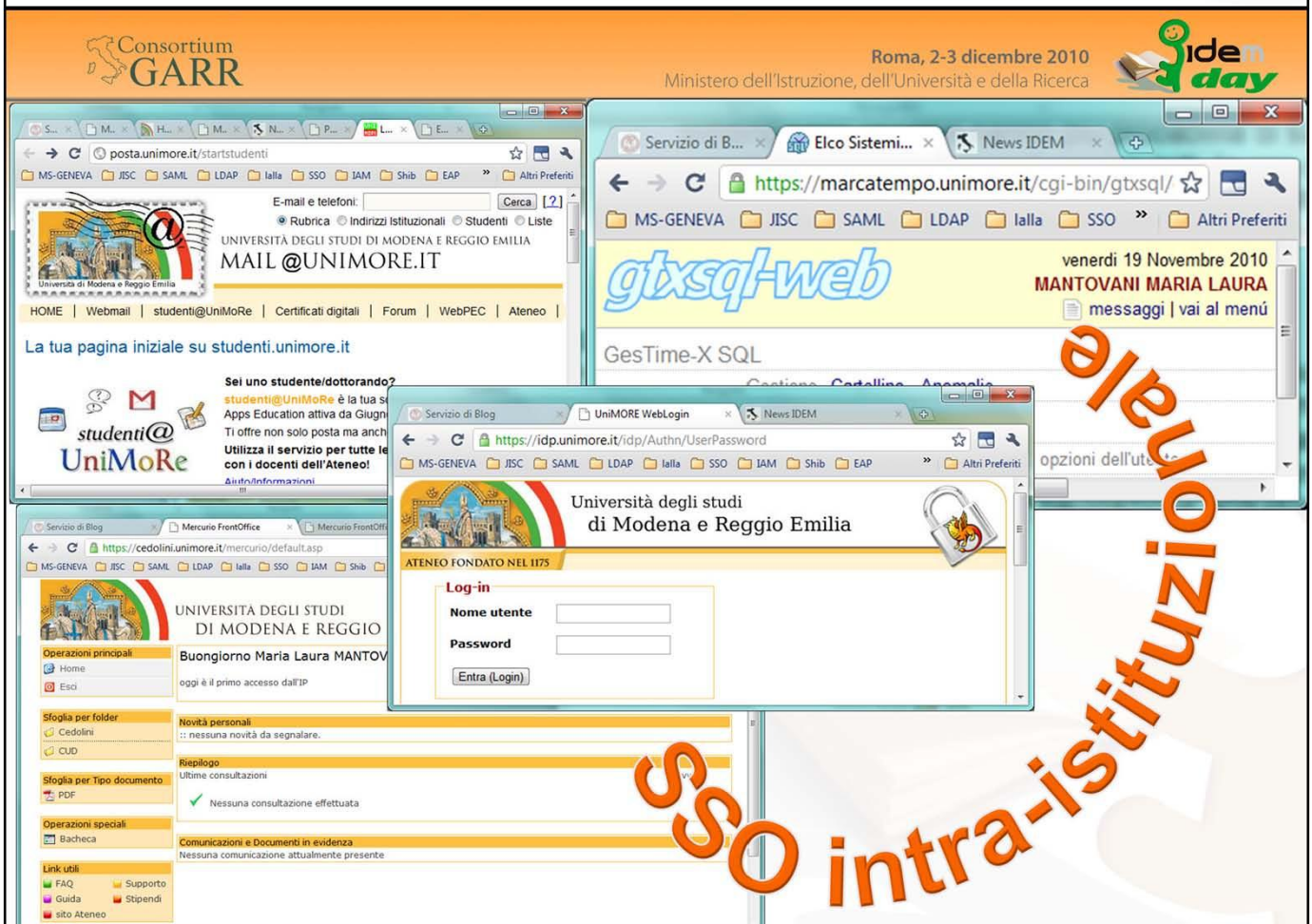

openid.net/get-an-openid/
Get an OpenID
Add OpenID to your site
Developers
Foundation
Community
Government
OpenID
What is OpenID?
Benefits of OpenID
Start using your OpenID
Join the Foundation | Member sign-in
Surprise! You may already have an OpenID.
If you use any of the following services, you already have your own OpenID. Below are instructions on how to sign in with each of the following providers on an OpenID enabled website. (When you see bold text, you should replace it with your own username or screenname on that service.)
Google
YAHOO!
YAHOO! JAPAN
LIVEJOURNAL
Hyves
Blogger
flickr
orange
mixi
myspace.
WordPress.com
AOL
feedback


https://sourceforge.net/account/login.php
sourceforge
FIND AND DEVELOP OPEN SOURCE SOFTWARE
Register
Log In
Find Software
Develop
Create Project
Blog
Site Support
About
enter keyword
Search
SourceForge.net > Log in
Log in with a SourceForge account
Enter your account info:
Username:
Password:
Remember Me
Log in
Forgot your username/password?
Need an account on SourceForge.net?
Create Account
Log in with OpenID
Please click your account provider:
Google
YAHOO!
AOL
Remember Me
Log in
Problems logging in with OpenID?
OpenID eliminates the need for multiple usernames across different websites.
Learn more - Get an OpenID



Janrain Engage helps connect your site to the social web through a robust set of APIs and social widget interfaces. Ultimately, a Janrain Engage solution accelerates your user registration and sign-in process by quickly and easily converting anonymous site visitors into active registered users. In addition, Janrain Engage enables you to import a rich set of profile data and social graphs from your users' social networks allowing you to gain both deeper insight into your users, keep their profiles up to date, and transform your site into a more social destination.


Roma, 2-3 dicembre 2010
Istruzione, dell'Università e della Ricerca
idem day
Cilea Digital Library
Un servizio di biblioteca digitale
Atlases - PATHOLOGY IMAGES
Collection of high resolution histological images
Hypertext atlas of Dermatopathology
https://wayf.idem.garr.it/WAYF/?entityID=ht
YouBlog
SSO nella Federazione IDEM
È necessario autenticarsi per pot
GARR
Seleziona
Consiglio nazionale delle Ricerche
GARR
ISTAT
Politecnico di Milano
Università Ca Foscari di Venezia
Università IUAV di Venezia
Main Page
Progetto biblioMIME
Benvenuti in NILDE
Certificati personali TCS
Emeroteca Virtuale
SERVIZIO DI ACCESSO REMOTO
per i soli utenti registrati
SERVIZIO DI ACCESSO REMOTO
per gli utenti IDEM


Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day
posta.unimore.it/startstudenti
MAIL @UNIMORE.IT
HOME | Webmail | studenti@UniMoRe | Certificati digitali | Forum | WebPEC | Ateneo |
La tua pagina iniziale su studenti.unimore.it
https://marcatempo.unimore.it/cgi-bin/gtxsql/
gtxsql-web
venerdi 19 Novembre 2010
MANTOVANI MARIA LAURA
messaggi | vai al menù
GesTime-X SQL
https://idp.unimore.it/idp/Authn/UserPassword
Università degli studi
di Modena e Reggio Emilia
ATENEO FONDATO NEL 1175
Log-in
Nome utente
Password
Entra (Login)
https://cedolini.unimore.it/mercurio/default.asp
UNIVERSITÀ DEGLI STUDI
DI MODENA E REGGIO
Buongiorno Maria Laura MANTOV
SSO intra-istituzionale

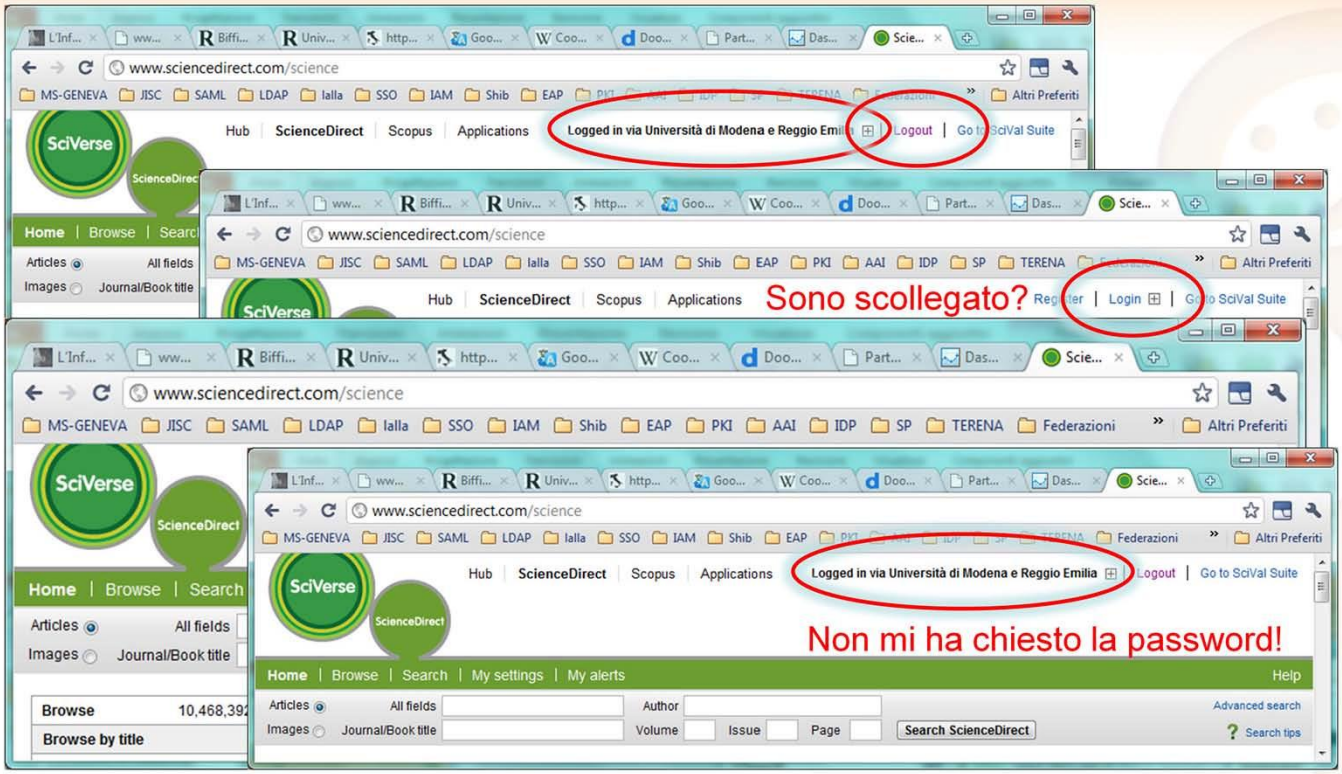
Single Sign On & User experience

- Durante la navigazione acquisiamo diverse sessioni autenticate: quella intra-istituzionale, oltre a IDEM, OpenID, FB, PayPal… alcune di esse sono sessioni SSO.
- Dopo un certo periodo di navigazione, l'utente è consapevole di quali siano le risorse sulle quali è collegato e a quali sessioni, SSO o meno, appartenga ciascuna risorsa acceduta?

Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day

LOGOUT: sai cosa mangi?

Cosa intende l'utente con Logout?

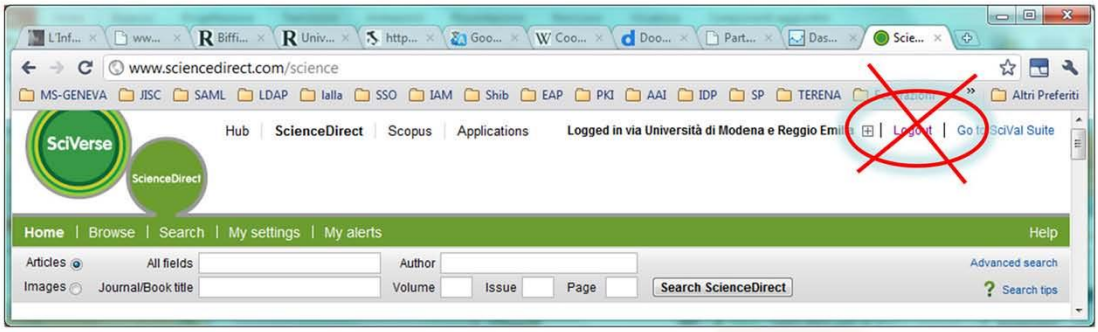


Che significa Logout?

- Uscire dall'applicazione corrente …
  - Quanto abbiamo visto prima non è Logout
- … rimanendo collegato nelle altre.
- Cosa vuol dire uscire dall'applicazione corrente se questa appartiene ad una sessione SSO?
  - Local Logout?
    - Come lo chiamiamo?
    - Come spiegarlo all'utente?
- Che cos'è il Single Logout?
  - SLO significa scollegare tutte le applicazioni che appartengono ad una sessione SSO.
  - Le applicazioni che non appartengono a questa sessione SSO rimangono collegate, finché non le si scollega esplicitamente.

Riesco ad individuare la sessione SSO e tutte le applicazioni che ne fanno parte?

Non dare all'utente un falso senso di sicurezza



Affinché la procedura di Logout sia efficace e non crei un falso di senso sicurezza, l'utente deve capire che ha attiva una certa sessione SSO e deve poter prevedere che cosa succederà cliccando sul bottone Logout.

Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day

Abbiamo un problema di comunicazione con l'utente

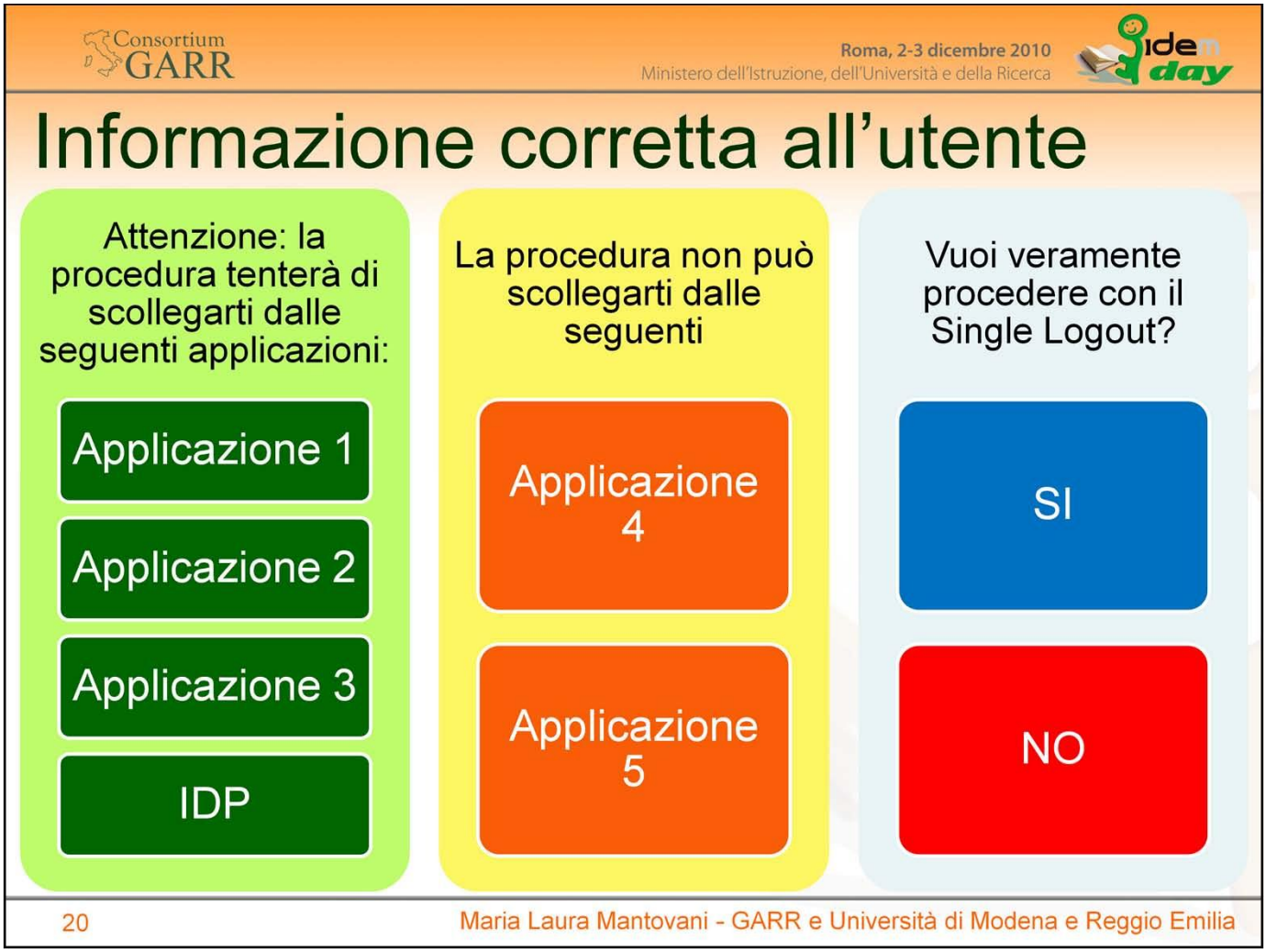
Coinvolgere tutti gli SP su una grafica comune?

Spiegare che ci sono 3 diversi concetti di logout:

Rendere graficamente evidente all'immaginazione dell'utente che cosa succederà se si clicca su:

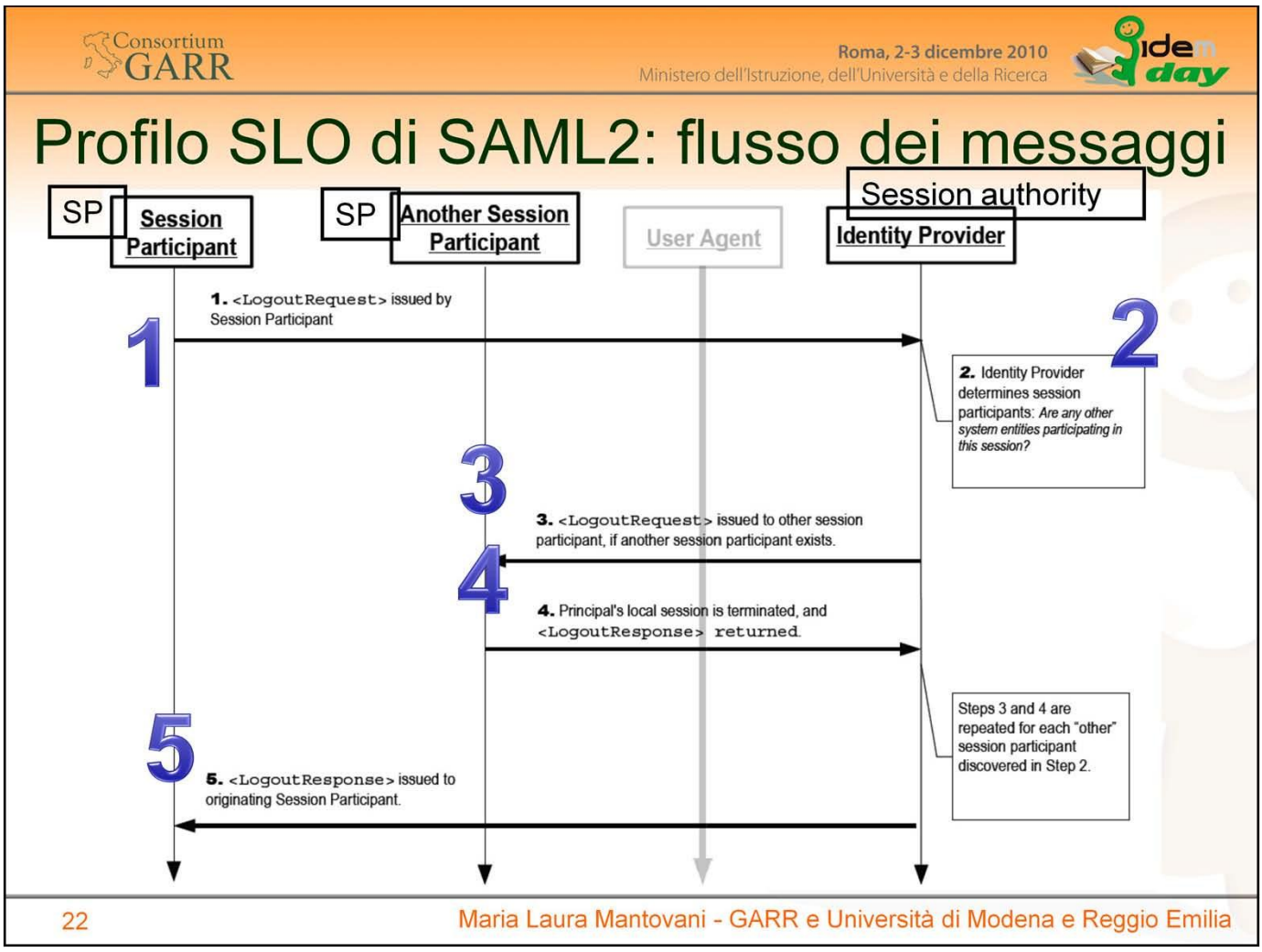
POSSIAMO INVESTIRE SU QUESTI FRONTI?

Logout	Local Logout	Single Logout	Logout	Local Logout	Single Logout



Affinché la procedura di Logout sia efficace e non crei un senso di falsa sicurezza, l'utente deve capire che ha attiva una certa sessione SSO e deve poter prevedere che cosa succederà cliccando sul bottone Logout.

SAML2 SLO: interoperabilità ridotta



Profilo SLO di SAML2: flusso dei messaggi

Il profilo SLO di SAML2 prevede una serie di messaggi che devono essere scambiati tra un Partecipante, l'IDP e altri partecipanti, eventualmente passando per lo User Agent dell'utente.
Il SAML 2 SLO può iniziare sia dall'SP (1) che dall'IDP (2).

Nel caso inizi dall'SP il flusso dei messaggi parte dal punto 1 e termina al punto 5.
Nel caso inizi dall'IDP il flusso inizia al punto 2 e termina alla conclusione del punto 4 ossia al ricevimento del messaggio da parte dell'IDP.
Colui che inizia il SLO ha la responsabilità di fornire all'utente l'informazione relativa al successo o al fallimento.

1. (Se inizia l'SP) SP manda la <LogoutRequest> all'IDP.
2. L'IDP recupera l'elenco di tutti gli SP per cui ha autenticato l'utente, che quindi fanno parte della sessione SSO, e per ciascuno ripete i passi 3 e 4.
3. L'IDP manda la <LogoutRequest> all'SP.
4. L'SP tenta di distruggere la sua sessione con l'utente, e manda indietro la <LogoutResponse> che indica il successo o meno dell'operazione.

   4end. L'IDP distrugge la sua sessione con l'utente.

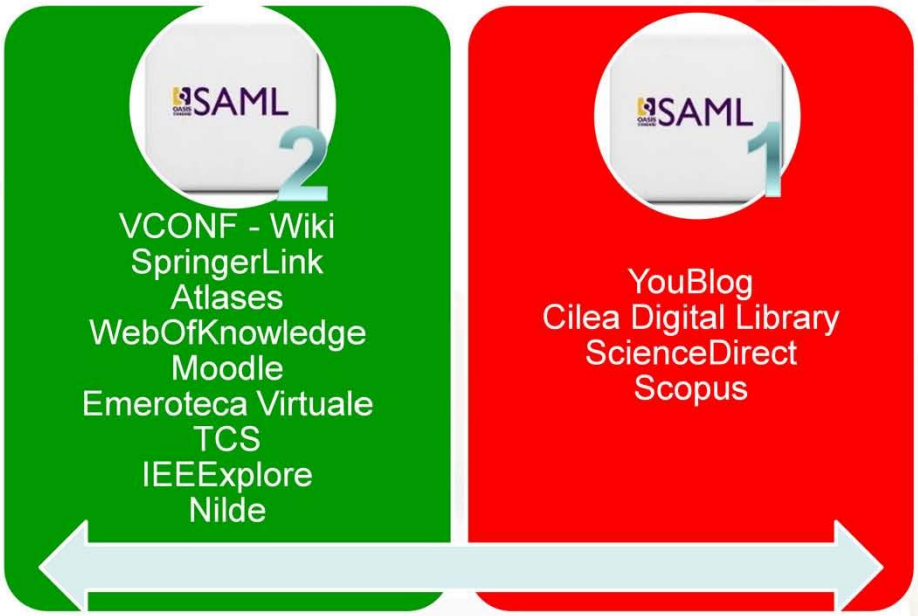
5. (Se aveva iniziato l'SP) L'IDP manda la <LogoutResponse> all'SP che aveva iniziato il SLO il quale distrugge la sua sessione con l'utente.

Profilo SLO di SAML2

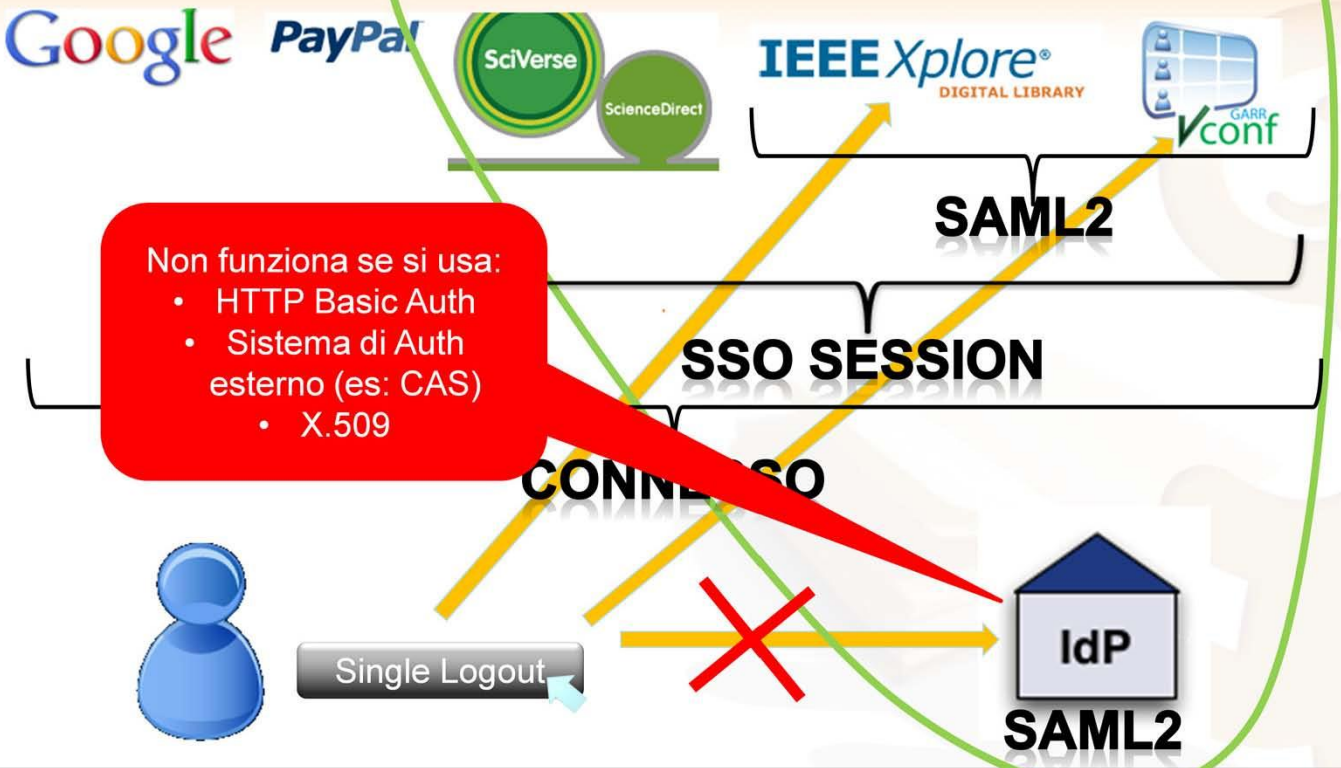
Premessa

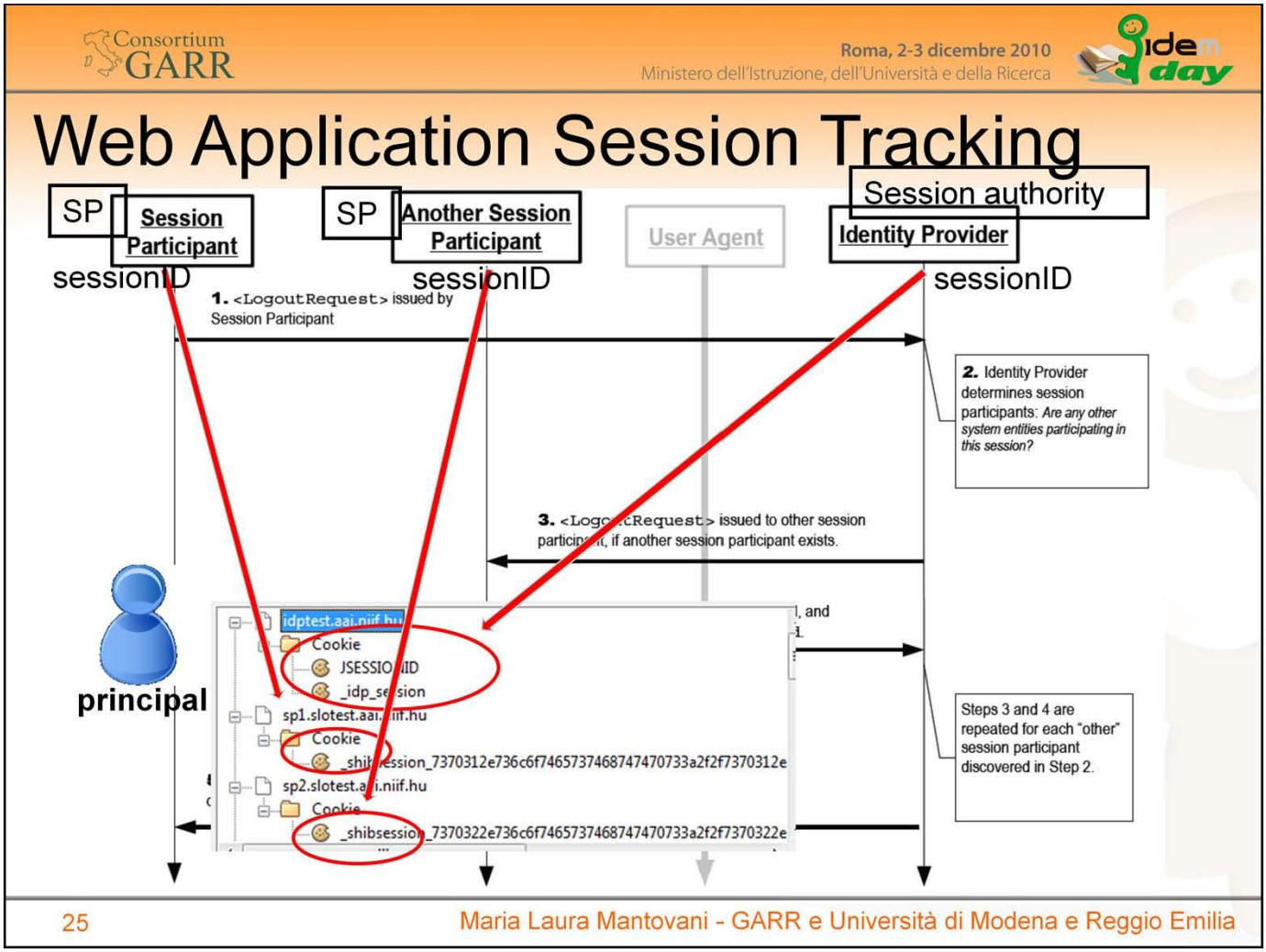
- Vale per applicazioni SAML2
  - Non vale per applicazioni SAML1

Nella Federazione IDEM



Single Logout secondo SAML2 profile





Web Application Session Tracking

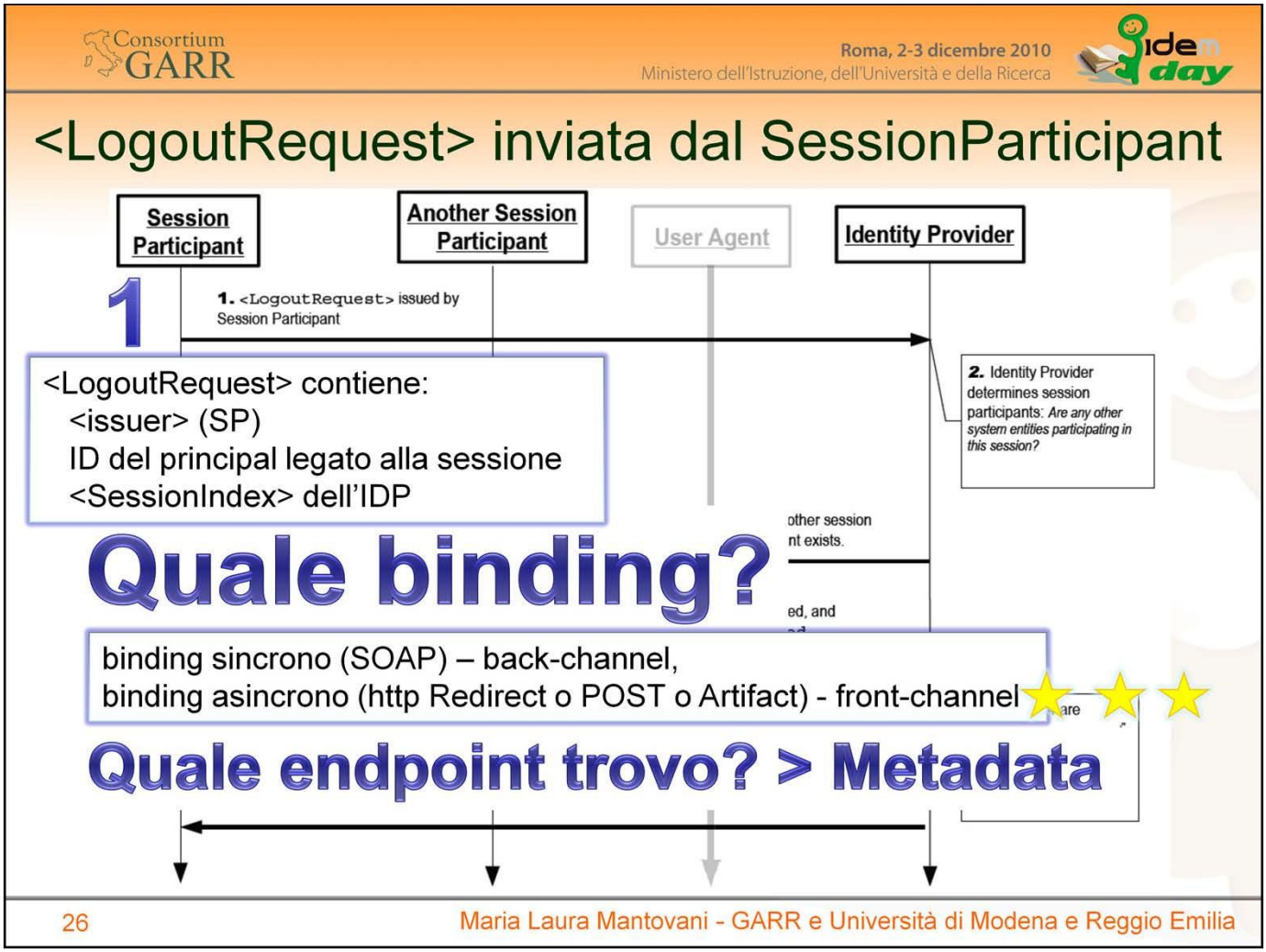
La maggiorparte delle applicazioni web registrano in memoria l'informazione relativa agli utenti correntemente attivi e indicizzano ciascuna sessione con un numero generato casualmente: il sessionID.

Questo sessionID viene anche registrato in un cookie del browser, così che ogni volta che l'utente ritorna all'applicazione, il cookie viene ripresentato e l'applicazione può ritrovare la sessione dell'utente.

Anziché la tecnica dei cookie, è possibile usare altre tecniche, tipo un URL re-writing o un altro sistema.

Il valore di sessionID registrato nel cookie viene quindi utilizzato per stabilire la sessione SSO tra il principal e l'IDP. In questa fase anche l'IDP può registrare il proprio cookie nel PC dell'utente.

I successivi relying party della session SSO ricevono anch'essi lo stesso sessionID, lo utilizzano internamente e registrano il proprio cookie nel PC dell'utente.



Vincoli del Binding:

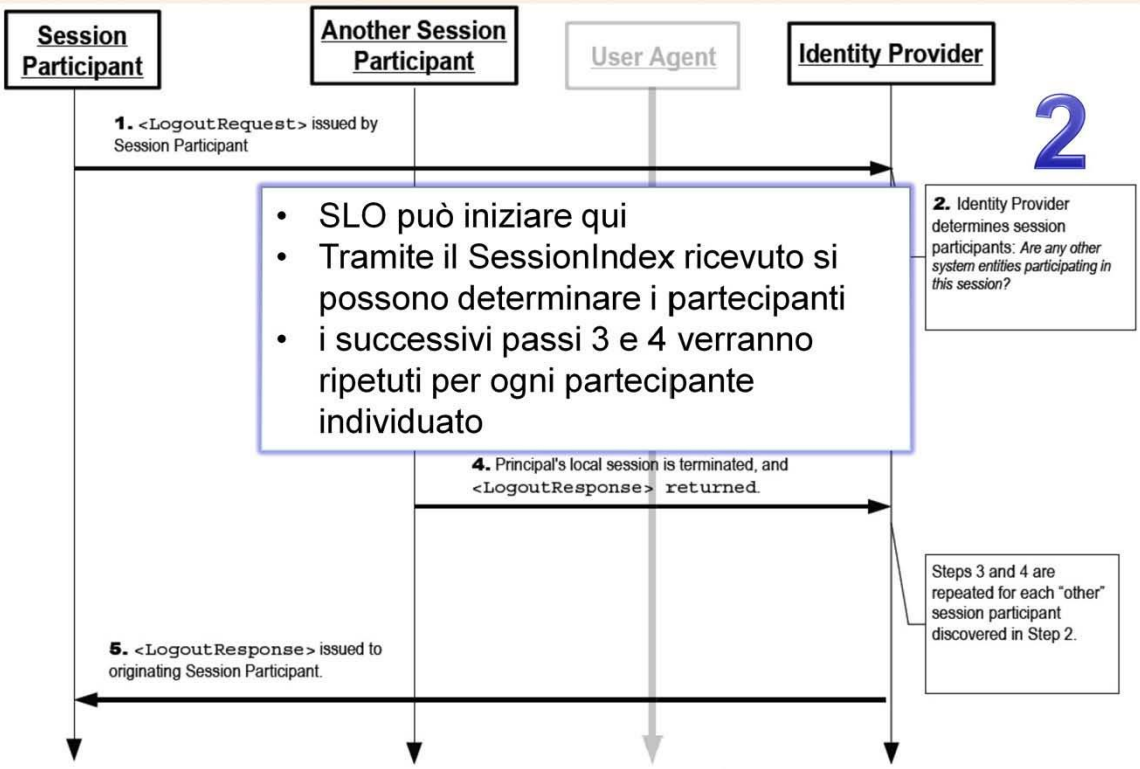
A) Se viene utilizzato un binding back-channel, tutti i successivi messaggi nel profilo devono usare il binding back-channel. Se uno partecipanti alla sessione non implementa il binding back-channel, il profilo si interrompe.

B) Se viene usato un binding front-channel, il successivo messaggio nel profilo può usare binding front-channel oppure back-channel. In questo modo la scelta del binding può essere operata in base alle esigenze del ricevente il messaggio.

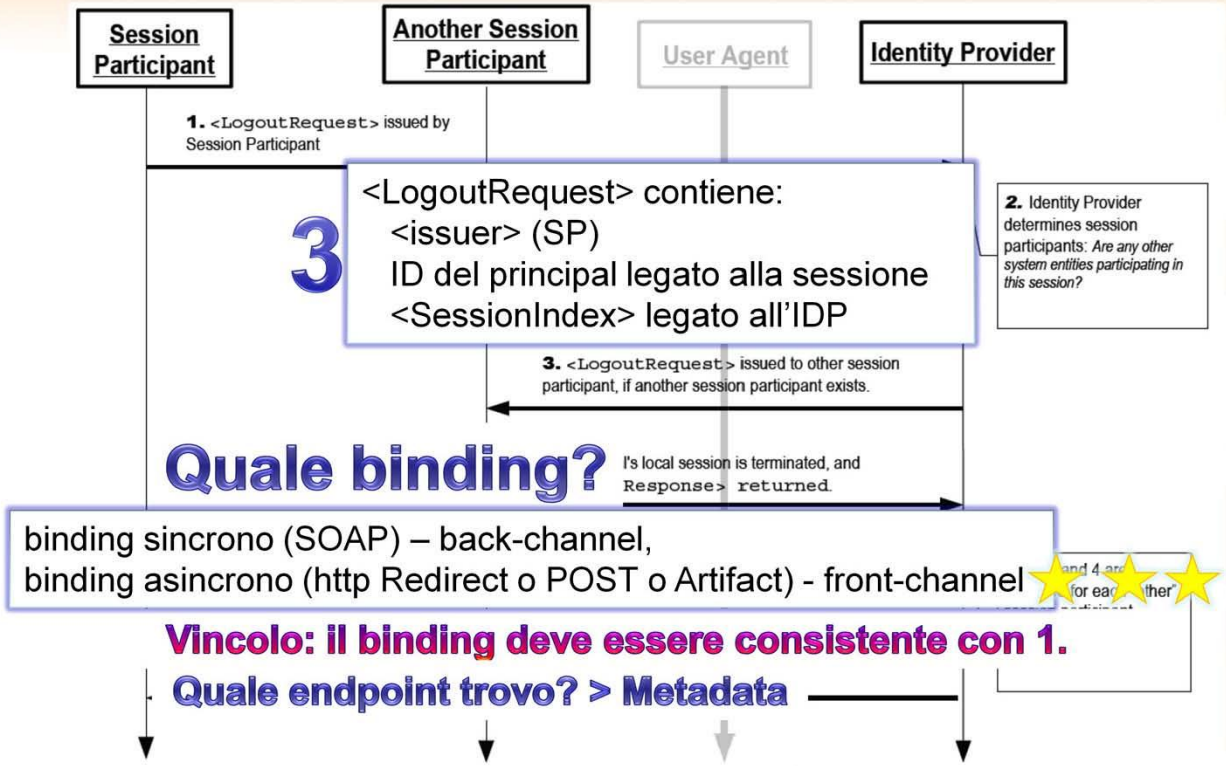
SAML2 consiglia di implementare il profilo SLO in modo che i partecipanti alla sessione usino, se possibile, un binding "front-channel" per massimizzare la probabilità che l'autorità di sessione possa propagare il logout con successo a tutti i partecipanti.

Tuttavia il binding front-channel è soggetto a maggiori problemi di comunicazione.

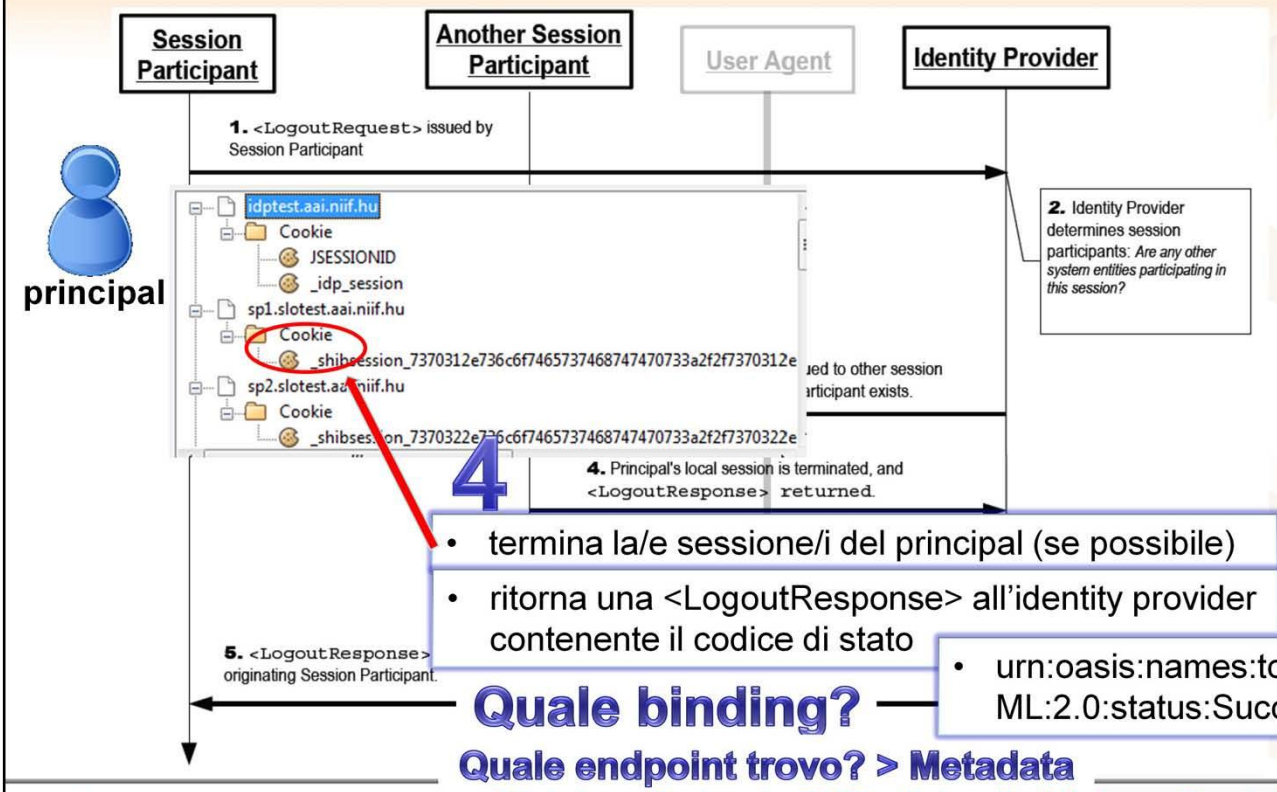
IdentityProvider determina gli altri SessionParticipant



<LogoutRequest> inviata agli altri SessionParticipant



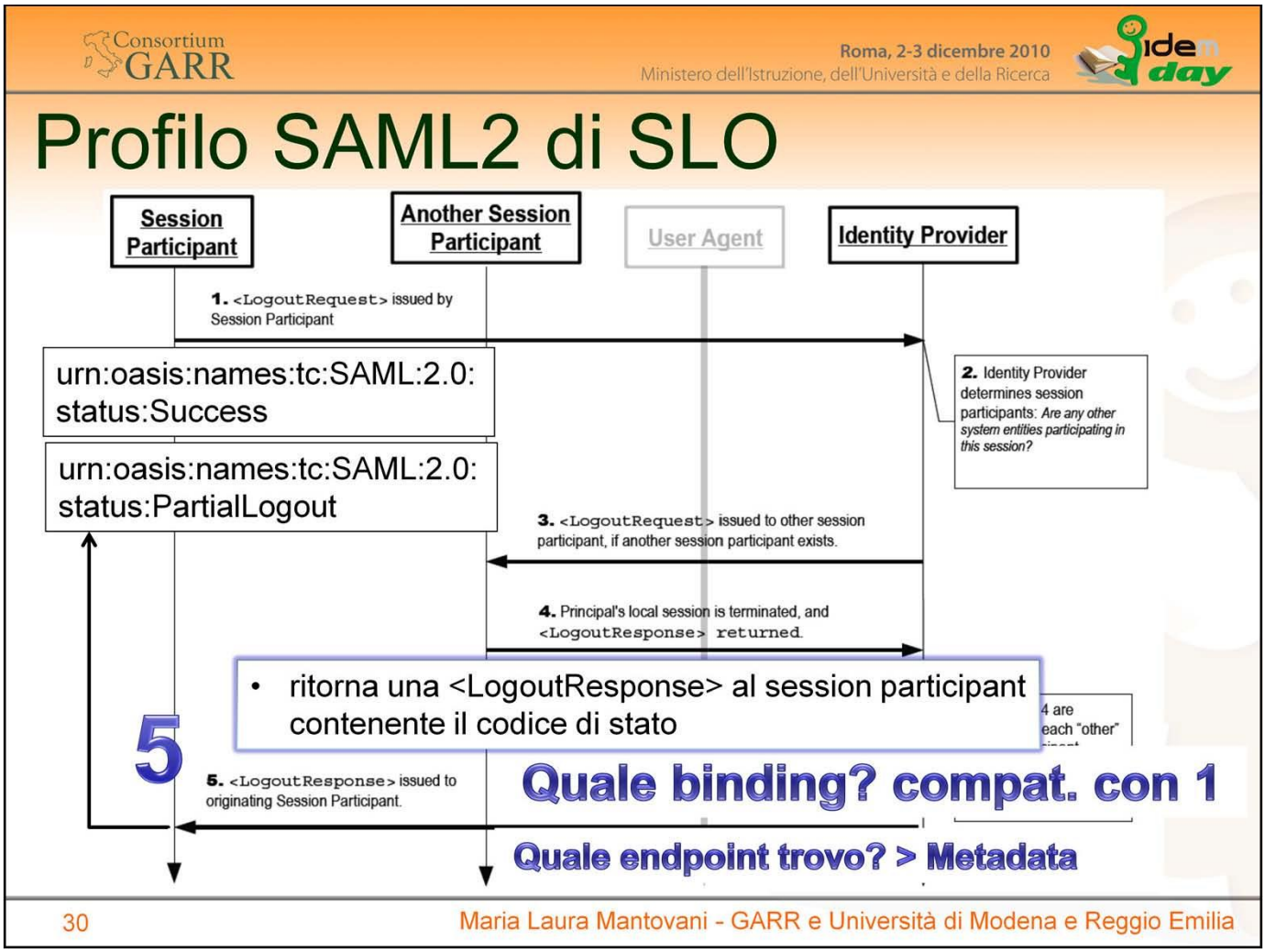
Sessione locale del Principal è terminata, <LogoutResponse>



- termina la/e sessione/i del principal (se possibile)
- ritorna una <LogoutResponse> all'identity provider contenente il codice di stato
- urn:oasis:names:tc:SAML:2.0:status:Success

Quale binding?

Quale endpoint trovo? > Metadata



Comunicare il Successo o il Fallimento del SLO

Abbiamo un altro problema con l'interfaccia utente quando siamo nel caso di uno SLO iniziato dall'SP. In questo caso infatti è responsabilità dell'SP fornire all'utente l'indicazione finale riguardante il successo o il fallimento dello SLO. Tuttavia le informazioni che l'SP riceve dall'IDP sono molto ridotte: una URI che indica il successo oppure un'altra che dice che c'è stato qualche problema. Non vengono indicate, in nessuno dei due casi, per quali partecipanti alla sessione lo SLO ha avuto successo e per quali è eventualmente fallito. Nel caso di fallimento non è possibile indicare all'utente la causa del fallimento. In caso di fallimento è importante dire all'utente di chiudere il browser.

Problema Binding: Back-channel

- Se non è supportato da tutti i Partecipanti alla Sessione SSO, lo SLO fallisce.
- Se supportato da tutti, ma anche uno solo degli SP o IDP partecipanti alla sessione SSO non è responsivo, lo SLO fallisce.
- Service Providers must have configured <Notify>
  - To inform application of logout via back-channel
- Adapted web applications via back-channel requests
  - This involves some work on your side …
- **Adapted Applications:**
  - Worldwide there are less than 10 applications that already are ready to support SAML 2 logout (incl. Moodle, ILIAS, Resource Registry)

Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day

Problema Binding: Front-channel

- Se si procede iterativamente (Daisy-Chain), nel caso un SP non risponda, all'utente viene presentato un http-error, la procedura di SLO si interrompe e non è possibile dare un risultato all'utente.
  - => Evitare Daisy-Chain
- IFRAMES? È un tentativo per ridurre il problema
  - Rimane una soluzione parziale perché non compatibile con i requisiti di accessibilità e quindi non supportata da tutti i browser
  - Browser bloccano i third party cookies
- Non è possibile SLO amministrativo

the session cookie of the SP software in a foreign domain is third party cookie when it is sent in an IFrame.

HAI DEI PROBLEMI?

Problemi:

user experience is the key to success
Vale anche per SLO!

- Problemi con l'utente:
  - Comunicare all'utente che cosa succederà quando darà il comando di SLO
  - Comunicare all'utente il successo o il fallimento del SLO quando questo è iniziato dall'SP
  - Problemi di accessibilità

Immagine e iframe

- Problemi tecnici e di interoperabilità:
  - Problemi di binding
    - Front-channel: alta probabilità di interruzione
    - Back-channel: alta probabilità di trovare qualche partecipante che non lo implementa (simpleSAMLphp)

*** http error**
*** nella Richiesta**

  - IDP SAML2 con auth esterna: non supportato
  - SAML1 non supportato
  - È difficile implementare il SLO amministrativo
  - SLO richiede un intervento/policy su tutti gli SP in Federazione
- Problemi di policy con i Partner
  - Quale SP partecipante può iniziare l'SSO?

Una non soluzione

Quando si presentano questi problemi molti chiedono perché non ci sia un protocollo in cui ci sia comunicazione solo tra l'SP che inizia il Logout e l'IdP.

L'obiettivo sarebbe quello di distruggere la sessione tra SP e IDP in modo che gli utenti debbano ri-autenticarsi se visitano di nuovo quello specifico SP.

Questo approccio lascia attive tutte le altre sessioni SP e comunicare agli utenti esattamente ciò che hanno, e non hanno, disconnesso non è probabilmente possibile

Pertanto, questo approccio aumenta il rischio che un utente possa abbandonare un computer con sessioni attive e permettere un non intenzionale, e forse dannoso, accesso di altri utenti a tali servizi.

Per dirla in modo conciso, qualsiasi applicazione che tenti questo approccio sta guardando solo a se stessa a costo di compromettere la sicurezza di ogni altra applicazione che partecipa al sistema di SSO.

Esempio di una applicazione resa Shibboleth compliant, ma gli sviluppatori hanno dimenticato di rimuovere o aggiustare la procedura di logout.
Il logout è stato demandato all'implementazione SLO di Shibboleth SP, che cancella correttamente il cookie da esso impostato.

Tuttavia l'applicazione ha impostato un proprio session cookie, e questo non viene cancellato né da Shib (non è suo compito), né dalla applicazione.
Il risultato è che se un utente che ha attiva una sessione SSO esegue il logout e se ne va lasciando il browser aperto, l'utente successivo, anche se si ricollega con una diversa sessione SSO, viene riassociato dentro l'applicazione allo stesso utente attivo precedentemente. Si verifica pertanto, accidentalmente, nell'applicazione una impersonificazione di un altro utente.

Questo bug di Drupal attualmente è stato corretto, ma è possibile che siano incorsi un questo errore di programmazione anche altri sviluppatori per altre applicazioni di cui non siamo a conoscenza.

Questo esempio dovrebbe allertare gli amministratori di sistemi riguardo alle possibili minacce introdotte da uno SLO implementato senza regole precise.

Shibboleth.

- **Shibboleth Service Provider 2.1**
  - Supports local and global logout
- **Shibboleth Identity Provider 2.1/2.2**
  - Support neither local nor global logout
- Plugin ungherese SLO per Shib IDP 2.1.5

https://wiki.aai.niif.hu/index.php/SLODemo

SimpleSAMLphp

- Non implementa binding SOAP (back-channel) perché troppo difficile
- Non firma i messaggi
  - Contro lo standard
  - Insicuro a meno che l'endpoint sia HTTPS
- Consiglia a tutti la sua proposta di Single Logout Deployment Profile
  - The <samlp:LogoutRequest> issued by a requester MUST be sent to the responder using the HTTP-REDIRECT binding.
  - The <samlp:LogoutResponse> issued by a responder MUST be sent to the requester using the HTTP-REDIRECT binding.
  - If the Service Provider receives LogoutRequest with IsPassive="True" it MUST be able to terminate the session without interacting with the user.

Interoperability Profiles

- Profilo SAML2 SLO (in generale tutti i profili SAML2) ha troppe variabili opzionali. Attenendosi solo a questo si rischia il fallimento del profilo.
- È necessario, per poter interoperare in una Federazione, o in una inter-Federazione, accettare di attenersi ad un Profilo di Interoperabilità
- Single Logout Deployment Profile
- Kantara Initiative eGovernment Implementation Profile

Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day

Kantara Initiative eGovernment Implementation Profile

an implementation profile of the SAML V2.0 Single Logout Profile

- require initiation of logout by a Service Provider using either the front- or back-channel, and initiation/propagation of logout by an Identity Provider using the back-channel.
- IDP and SP implementations MUST support the SAML SOAP binding (back-channel).
- IDP MUST support the HTTP-Redirect bindings for the reception of messages (front-channel)

Identity Provider 3.0 Single Logout Details

29 NOV 2010

https://spaces.internet2.edu/display/SHIB2/IdPSLODetails

Current Thinking

- As discussed on the SLO Issues page there are many problems associated with Single Logout. All of the especially difficult problems revolve around the propagation of the SLO request from the IdP to SPs (excluding the initiating SP).
- Therefore, the plan for the initial support of SLO will be to allow an SP to initiate an SLO request either via the front-channel or back-channel but the propagation of that request to other SPs will be exclusively via the back-channel. By allowing the front-channel delivery of the initiating SLO request SPs can avoid the need for an SLO UI.
- This solution will require SP-protected applications to either use the SP session exclusively or properly tie the application session to the SP-session.

Work for domesticating applications

Conclusioni

SLO ?

Perché tutti vogliono fare logout?

- Se il PC, notebook, smartphone, … è usato in modo esclusivo solo dal proprietario il logout è superfluo
- Il logout serve per poter lasciare la postazione ad un'altra persona
- Per lasciare la postazione si ottiene sicurezza maggiore facendo logout dal S.O. (l'utente e l'amministratore della postazione può verificare l'effettivo logout)
- **SLO completo, indipendentemente dal numero di sessioni SSO attive, da versione SAML2/1 e ogni implementazione di applicazione «non SAML», si ottiene in modo sicuro chiudendo il browser**
- Il LOCAL logout è inutile o dannoso
  - LE APPLICAZIONI CHE DEVONO OBBLIGATORIAMENTE PERMETTERE IL LOGOUT DEVONO STARE FUORI DALLA FEDERAZIONE? QUALI SONO?

Consortium GARR
Roma, 2-3 dicembre 2010
Ministero dell'Istruzione, dell'Università e della Ricerca
idem day

1-DIC-2010

> Do you consider that we should give up the SLO goal?

- I would prefer to view SLO as a way of making the Logout function of apps actually do *something* useful and basically just try to clear the IdP session.
- At that point if you add an optional user-initiated action to send some SOAP messages out and clear as many apps as you happen to be able to hit, I have no objection.
- But at the end, you have to stick up a message saying to close the browser, and that's where we were before SLO.

Scott Cantor

Riferimenti

- **Profiles for the OASIS Security Assertion Markup Language (SAML) V2.0**
  4.4 Single Logout Profile
  http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf
- **SLOIssues**
  https://spaces.internet2.edu/display/SHIB2/SLOIssues
- **SLO: Single Log-out**
  Inedible cookies, sticky sessions and false hopes
  http://www.switch.ch/export/sites/default/uni/security/aai/event/aai-info-day-2009/slides/AAI-ID09-51-SLO.pdf
- **Single Logout all'ungherese**
  http://www.terena.org/activities/tf-emc2/meetings/15/emc2_2010_slo.pdf
- **Plugin ungherese per Shibboleth**
  https://wiki.aai.niif.hu/index.php/ShibIdpSLO
- **SLODemo**
  https://wiki.aai.niif.hu/index.php/SLODemo
- **SLO per SimpleSAMLphp**
  https://rnd.feide.no/2008/08/25/how_to_create_a_fancy_iframe_logout_demo_-_from_a_to_z/
- **Front-Channel Single Logout Deployment Profile (per interop. con SimpleSAMLphp**
  https://rnd.feide.no/2009/07/09/front-channel_single_logout_deployment_profile/
- **Kantara Initiative eGovernment Implementation Profile of SAML V2.0**
  http://kantarainitiative.org/confluence/download/attachments/38929505/draft-kantara-egov-saml2-profile-2.0-03.pdf