GARR

The Italian Academic & Research Network

www.garr.it

La Federazione IDEM

IDEntity Management per l'accesso federato

Maria Laura Mantovani

marialaura.mantovani@garr.it

9° WORKSHOP GARR
Al servizio degli utenti

Consortium GARR

A che punto siamo?

www.garr.it

- Il "Progetto IDEM", iniziato nell'Aprile 2007, si è concluso il 31 Marzo 2009
- dal 1 Aprile 2009 è attiva la "Federazione IDEM" e il ***Servizio IDEM GARR AAI***

  Staff: *Maria Laura Mantovani*
  Barbara Monticini
  Simona Venuti

- Primo Convegno IDEM, 30-31 Marzo 2009, Roma presso l'Università di RomaTRE
- On-line http://www.garr.it/eventiGARR/idem09//programma.html le registrazioni delle relazioni e le presentazioni

2

Consortium GARR | 15-18 GIUGNO 2009 | 9° WORKSHOP GARR Al servizio degli utenti | Maria Laura Mantovani marialaura.mantovani@garr.it

Chi era presente l'anno scorso al WS8 di Milano forse ricorderà che si è parlato di IDEM in termini di progetto con il forte desiderio di passare presto alla operatività completa della Federazione.

Il Progetto si è concluso il 31 Marzo 2009 e dal 1 Aprile 2009 è attiva la Federazione IDEM con il Servizio IDEM GARR AAI ossia il pieno supporto della Direzione GARR alle necessità della comunità delle Organizzazioni GARR per facilitare il loro ingresso nella Federazione.

Questo inizio è stato inaugurato con i 2 giorni del Primo Convegno IDEM del 30-31 Marzo scorsi, tenutosi a Roma presso l'Università di RomaTRE.

Partecipanti al Progetto IDEM

www.garr.it

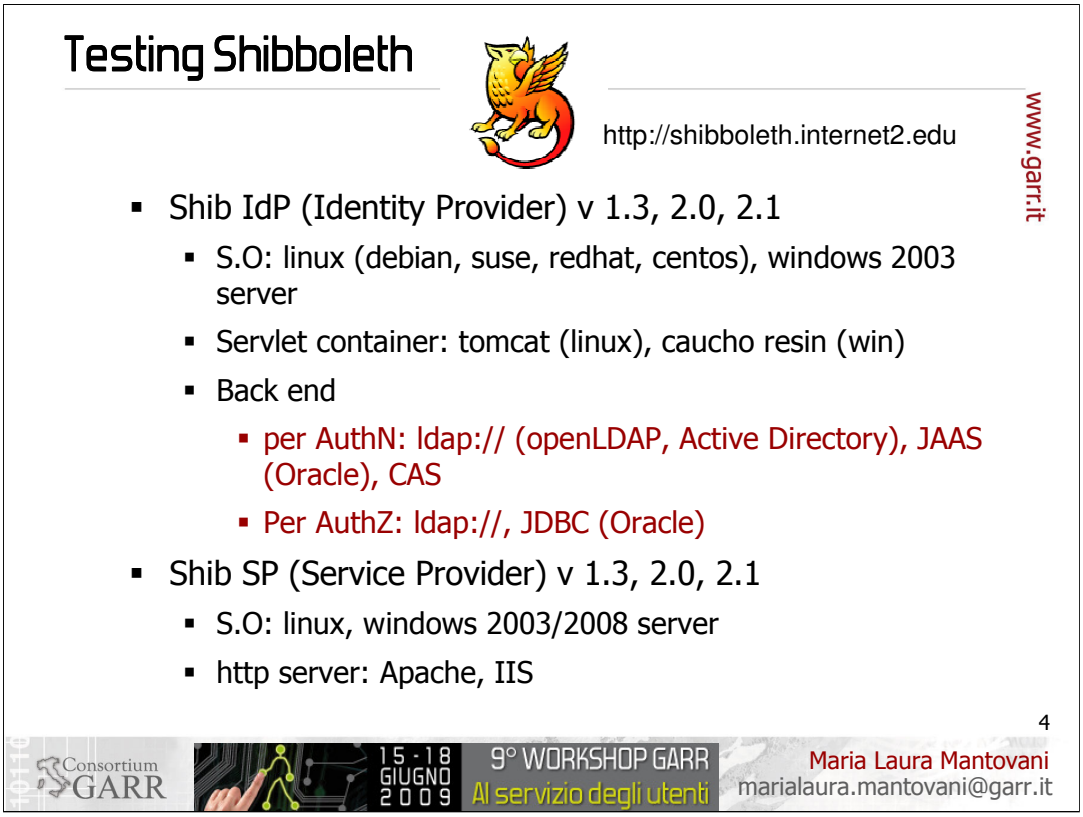
Università Partecipanti	Enti di Ricerca, Consorzi
Politecnico di Bari	CASPUR
Politecnico di Milano	CILEA
Univ. dell'Aquila	CNR AdR Bologna
Univ. di Cagliari	CNR Ceris Torino
Univ. di Genova	CNR IBIMET Firenze
Univ. di Modena e Reggio Emilia	CNR IFC Pisa
Univ. di Padova	CNR IIT Pisa
Univ. di Parma	CNR IFC Pisa
Univ. di Roma3	CNR ISSIA Bari
Univ. di Torino	CNR IVV Torino
Univ. di Urbino	GARR
Univ. di Venezia	INAF IASF Bologna
	ISTAT

http://www.idem.garr.it/partecipanti.php

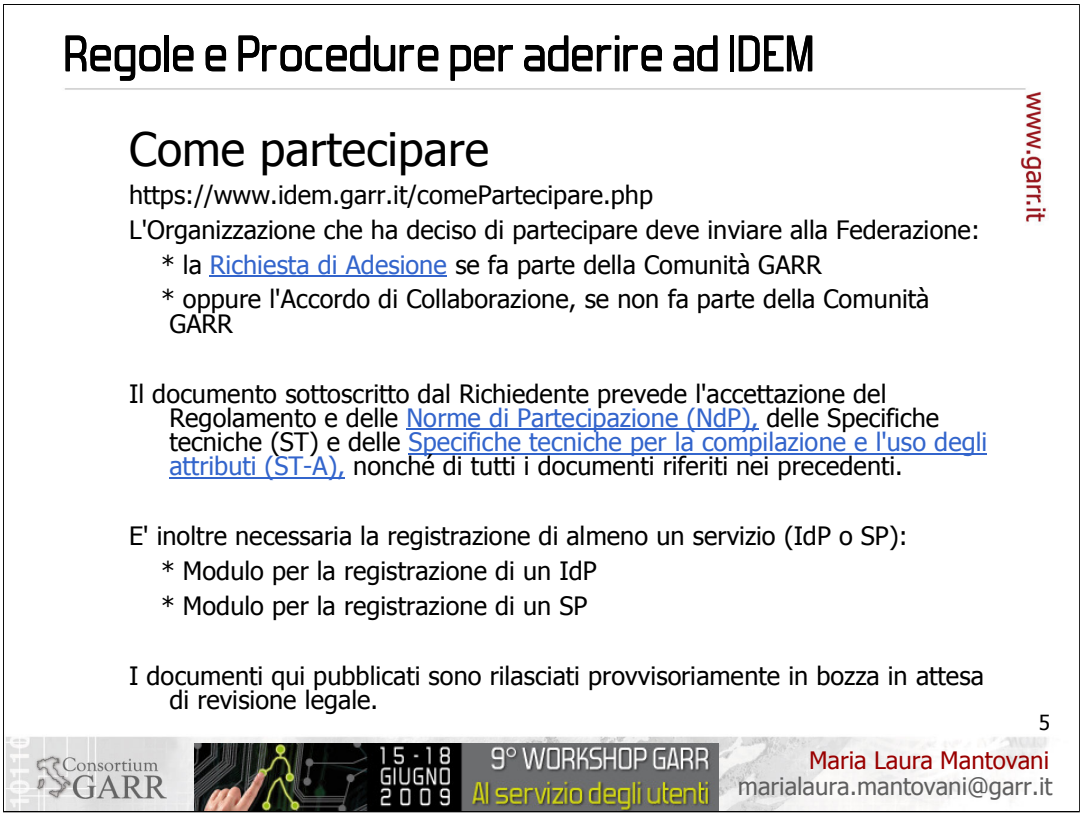
3

Maria Laura Mantovani
marialaura.mantovani@garr.it

Il progetto, realizzato per capire il funzionamento e dimostrare la fattibilità e la funzionalità della Federazione, è stato condotto da una ventina di organizzazioni Partecipanti che avevano dichiarato la loro disponibilità nel 2007 ad affrontare l'incognita .



Nel corso del progetto sono state provate le versioni di Shibboleth (il frame work scelto per l'operatività della Federazione) IdP e SP 1.3 e 2.0 e 2.1, con diverse configurazioni architetturali (Servlet container (non solo tomcat ma anche caucho resin), S.O. ospitante (linux debian, suse, redhat, …, Windows 2003 server, windows 2007 server), DB Backend (OpenLDAP, Active Directory, Oracle), http server (Apache, IIS);



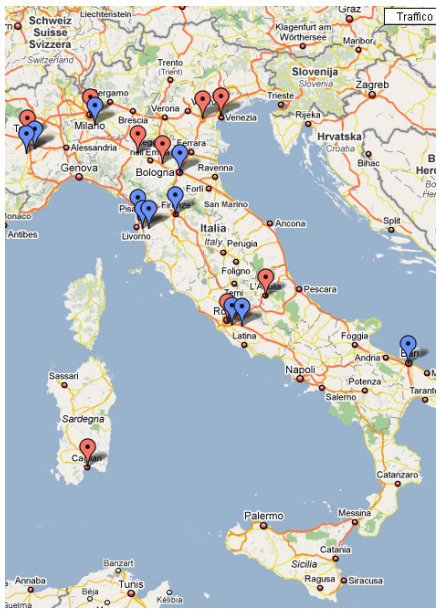
sono state studiate le caratteristiche che accomunano le utenze dei nostri enti ed è stato prodotto il Documento Attributi, che è la base che serve per normalizzare la definizione degli utenti delle organizzazioni partecipanti.

Sono poi state redatte le Specifiche Tecniche a cui è necessario attenersi per aderire alla Federazione e la Documentazione Normativa che ci vogliamo dare all'interno della Federazione nonché i moduli di adesione.

Identity Provider attivi

Università Partecipanti		
Politecnico di Bari	✔	
Politecnico di Milano	✔	IdP
Scuola Normale Superiore		
Univ. dell'Aquila	✔	IdP
Univ. di Cagliari	✔	IdP
Univ. di Genova	✔	
Univ. di Modena e Reggio Emilia	✔	IdP
Univ. di Padova	✔	IdP
Univ. di Parma	✔	IdP
Univ. di Roma3	✔	IdP
Univ. di Torino	✔	IdP
Univ. di Urbino	✔	
Univ. di Venezia	✔	IdP

Enti di Ricerca, Consorzi		
CASPUR Roma	✔	IdP
CILEA	✔	IdP
CNR AdR Bologna	✔	IdP
CNR AdR Pisa	✔	
CNR Ceris Torino	✔	IdP
CNR IBIMET Firenze	✔	
CNR IFC Pisa	✔	IdP
CNR IIT Pisa	✔	IdP
CNR ILC Pisa	✔	IdP
CNR ISSIA Bari	✔	IdP
CNR IVV Torino	✔	IdP
GARR	✔	IdP
ICTP Trieste		
INAF	✔	
INAF IASF Bologna	✔	
ISTAT	✔	IdP

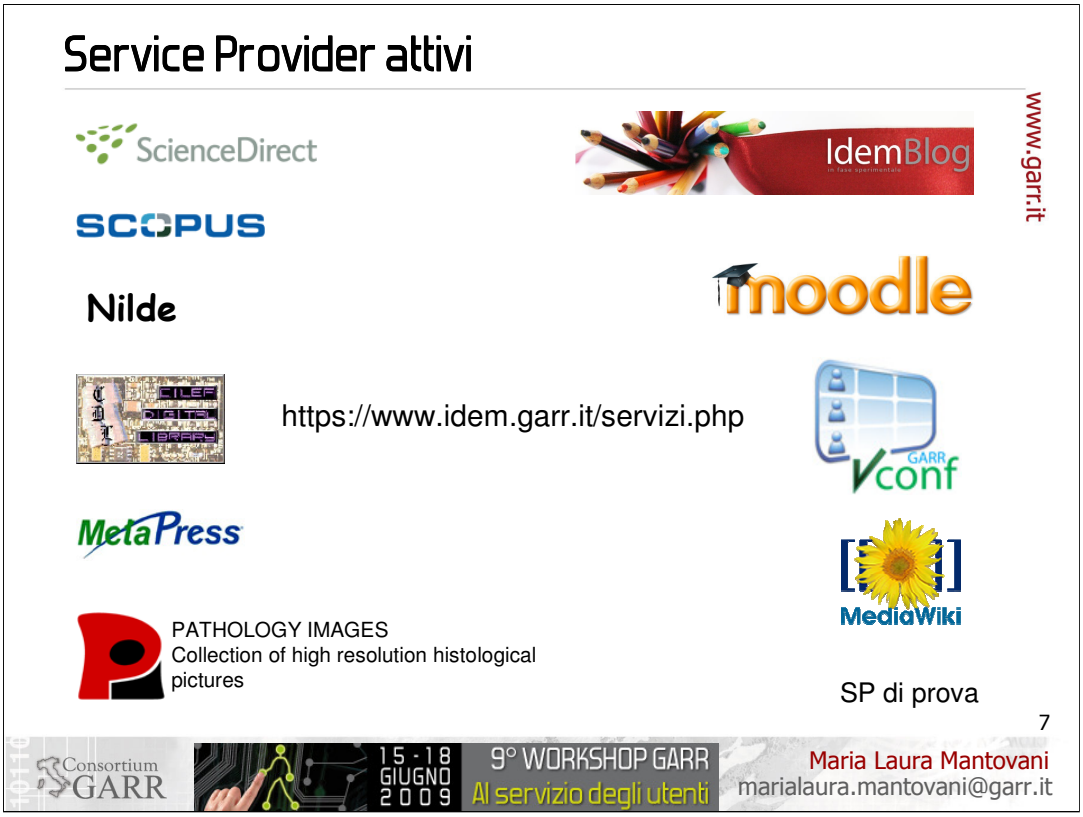


www.garr.it

http://www.idem.garr.it/partecipanti.php

6

Sono stati messi in opera una ventina di IdP che sono tuttora funzionati e forniscono l'accesso alle RISORSE federate a circa 1 milione di utenti.

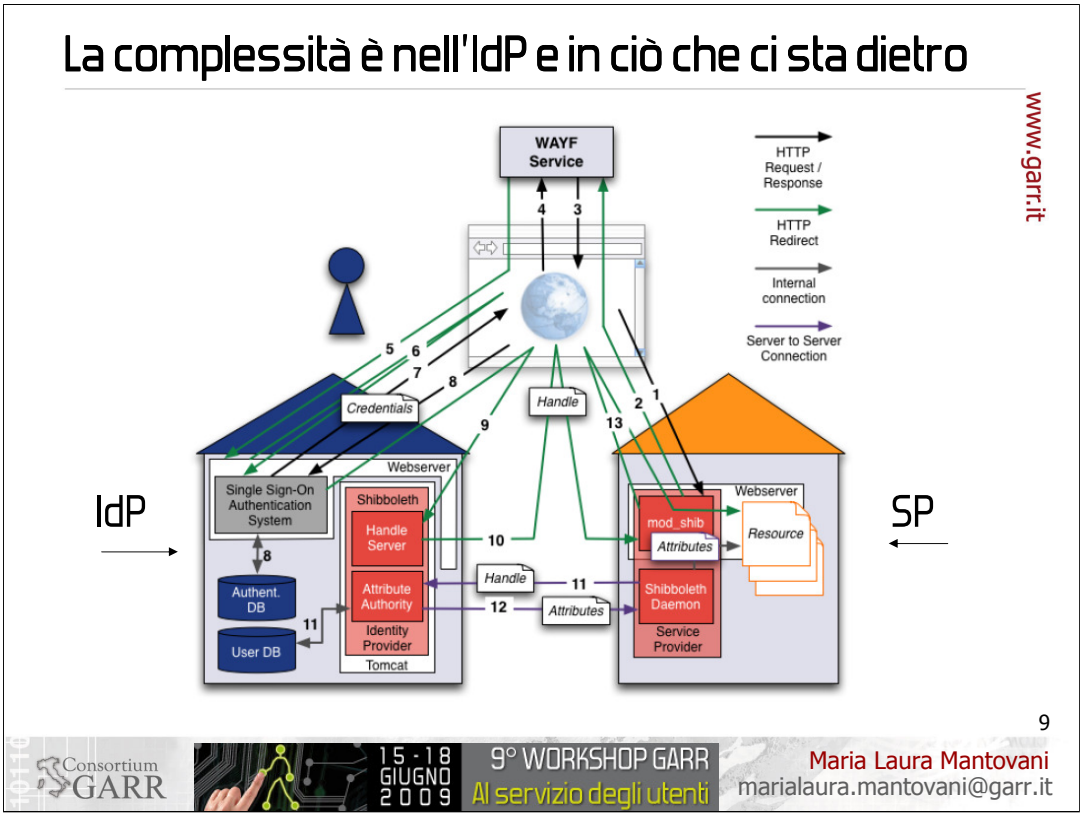


Sono stati messi in opera una decina di risorse a cui gli utenti finali degli enti partecipanti possono accedere mediante l'uso delle proprie credenziali istituzionali.

ScienceDirect	Elsevier
Scopus	Elsevier
GARR VCONF	GARR
Pathology Atlases	Masaryk University
Metapress	Springer Science+Business Media
CILEA Digital Library	CILEA
NILDE	CNR BO
idemblog	Università di Torino
LMS Moodle	Università di Modena e Reggio Emilia
IDEM wiki	CASPUR
SP di Prova	GARR

Il titolo di questo workshop "Al Servizio degli utenti: quando tecnologie complesse incontrano la semplicità di utilizzo" si addice perfettamente al lavoro da fare e al risultato che si ottiene mettendo in opera la Federazione. L'obiettivo della federazione è quello di SEMPLIFICARE la vita agli utenti. In che modo?

1. Eliminando la molteplicità di credenziali che ciascuno di noi deve possedere, e che sono poi da conservare, da ritrovare, per accedere ai molti servizi protetti di cui ciascuno di noi fa quotidiano uso;
2. Eliminando la richiesta di introduzione successiva delle credenziali da parte dei servizi (Single Sign On);
3. Proteggendo opportunamente le credenziali e i dati personali degli utenti.



Che cosa è necessario fare per essere “adeguati” a fornire questo servizio ai nostri utenti, cioè a rendere loro la vita più facile, garantendo comunque la sicurezza, nell’accesso alle risorse?

L’IdP (Identity Provider) di ciascuna organizzazione è l’unico “consumatore” delle credenziali del proprio utente per tutti i servizi federati.

Come conseguenza le Risorse (SP) non posseggono più le credenziali e non sono oberate dal lavoro di operare in sicurezza la gestione di queste credenziali.

Dov’è quindi la complessità tecnologica? E’ principalmente nell’IdP (e in ciò che ci sta intorno). Ed è una complessità gestionale oltre che tecnologica. Vediamo perché:

1. gli attori in gioco nella Federazione (IdP e SP) si scambiano asserzioni in tutta sicurezza facendo uso del protocollo SAML (Security Assertion Markup Language). Prossimamente un tutorial su SAML. In questo modo si proteggono le credenziali e anche lo scambio di altre informazioni riguardanti gli utenti
2. La Federazione si basa sulla fiducia reciproca:
   - IdP passa a SP asserzioni SAML vere e aggiornate
   - Diversi IdP in situazioni analoghe si comportano allo stesso modo: accettano di attenersi alla stesse policy

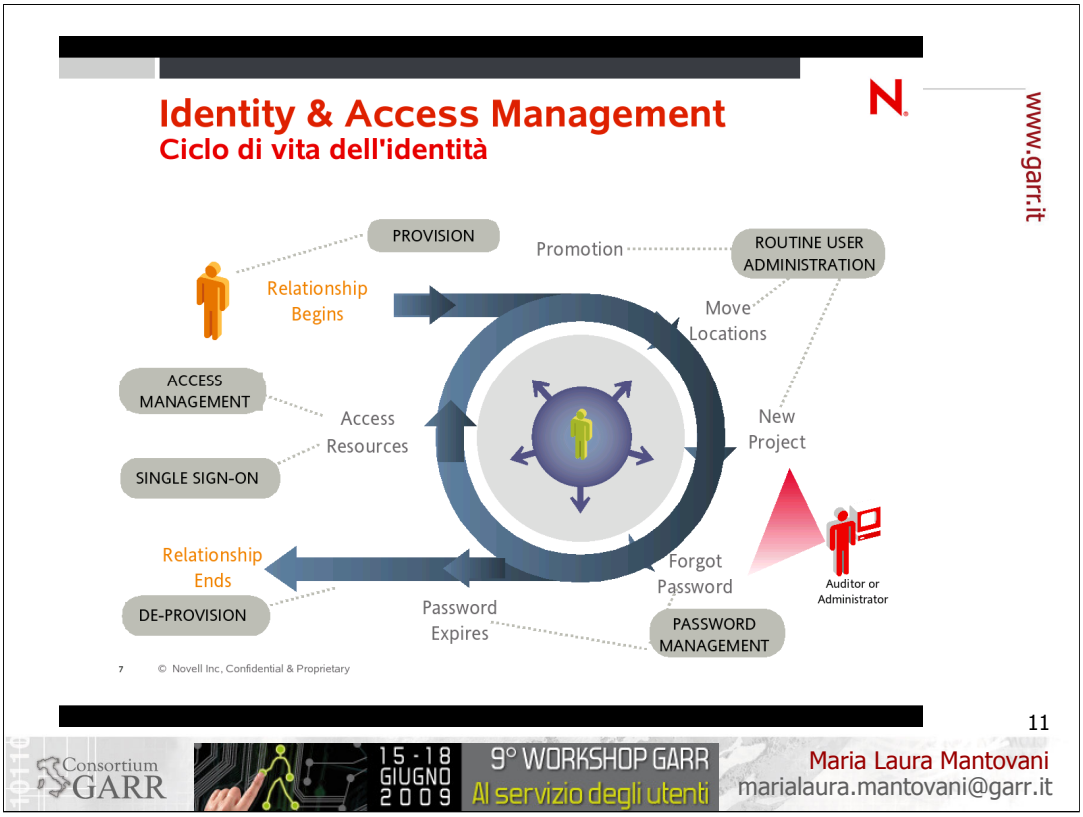
Le basi della fiducia reciproca

- Persone Reali
- Account Tracciabili
- Profilatura condivisa
  - eduPersonAffiliation
  - eduPersonEntitlement

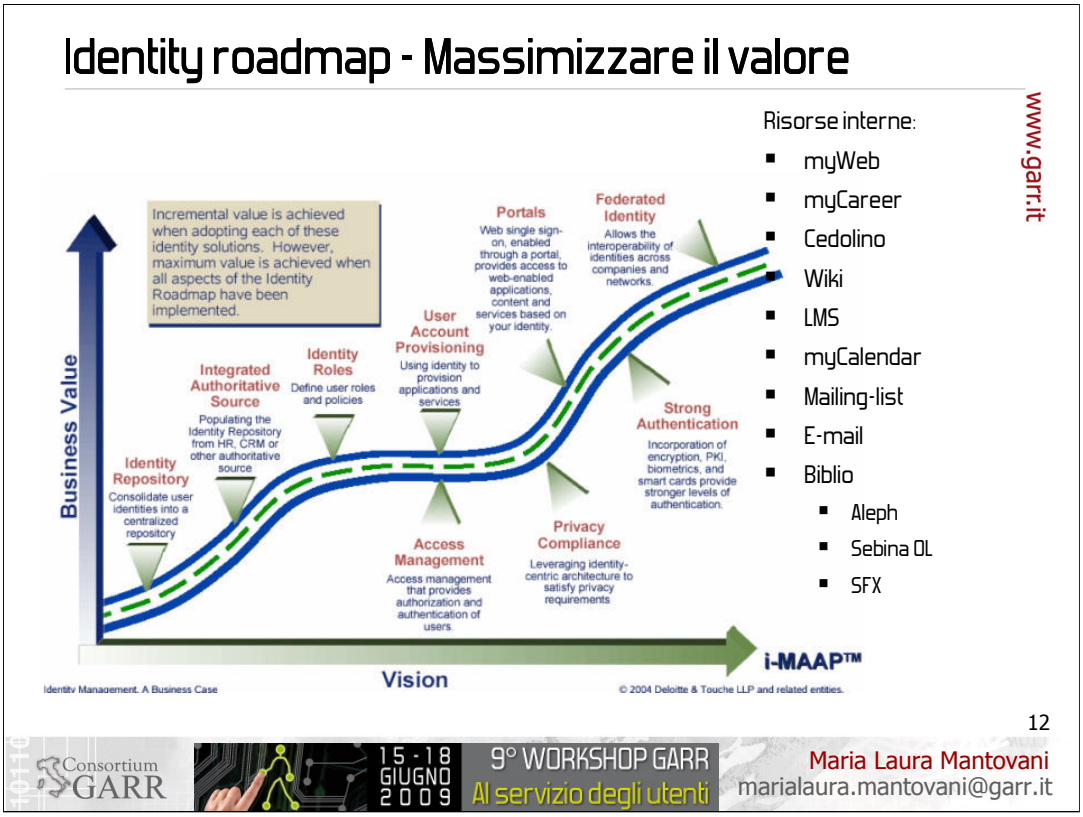
https://www.idem.garr.it/docs/AAI_attributi.pdf
https://www.idem.garr.it/docs/NormePartecipazione_V0.9.5W.pdf

10

Per questo l'organizzazione che implementa l'IdP deve assicurare agli altri partecipanti che le identità digitali che essa certifica mediante il proprio IdP corrispondano a persone reali, sempre tracciabili nella propria organizzazione, profilate con correttezza e cura nell'aggiornamento degli attributi: in particolare attualmente la Federazione richiede correttezza, tempestività e cura per quanto riguarda l'affiliazione e il ruolo (affiliation), e i diritti di accesso (entitlement).



L'organizzazione partecipante che registra il proprio IdP nella Federazione può fornire questa assicurazione agli altri Partecipanti solo se ha in opera delle procedure di gestione dei propri utenti precise e affidabili. L'insieme di queste regole e procedure che l'organizzazione si dà per la gestione della propria utenza si chiama "Identity Management" e comprende la gestione del ciclo di vita dell'identità digitale sulla base di documentazione reale, l'aggiornamento continuo di una base di dati delle identità digitali, la messa in opera di procedure di gestione, interne all'organizzazione, che possono coinvolgere maggiormente il personale amministrativo di segreteria, piuttosto che quello tecnico.

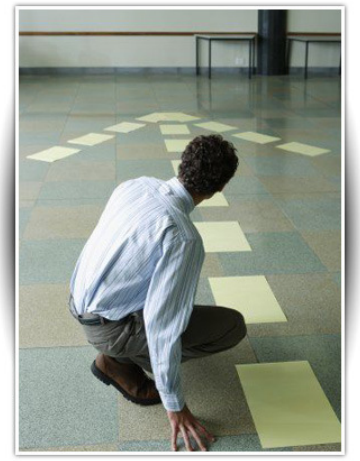


Implementare un IdP Shibboleth (o da altro Framework analogo) con l'obiettivo di ottenere un sistema per l'Autenticazione, il Single Sign On e l'Autorizzazione all'accesso alle Risorse comporta uno sforzo organizzativo e gestionale che verrà ripagato in un tempo più breve se l'organizzazione utilizzerà lo stesso sistema anche per l'accesso alle proprie risorse interne (ad esempio la sezione personale sul sito istituzionale, servizi riservati: visualizzazione carriera, stipendio, …, wiki, LMS, l'accesso all'aggiornamento di agende e calendari, l'accesso a sistemi collaborativi, apps, mailing-list, posta elettronica, servizi bibliotecari intra-istituzionali quali il prestito bibliotecario (Aleph e tutti prodotti di Ex-Libris sono già shib compliant, Sebina lo sarà a breve perché come Federazione lo abbiamo esplicitamente chiesto a Data Management).

Ma il Servizio IDEM GARR AAI cosa fa?

www.garr.it

1. Aiuto alle Organizzazioni della Community GARR che vogliono partecipare alla Federazione IDEM



Contattateci:
idem@garr.it

13

Consortium GARR | 15-18 GIUGNO 2009 | 9° WORKSHOP GARR Al servizio degli utenti | Maria Laura Mantovani marialaura.mantovani@garr.it

Nel frattempo cosa farà il Servizio IDEM GARR AAI?

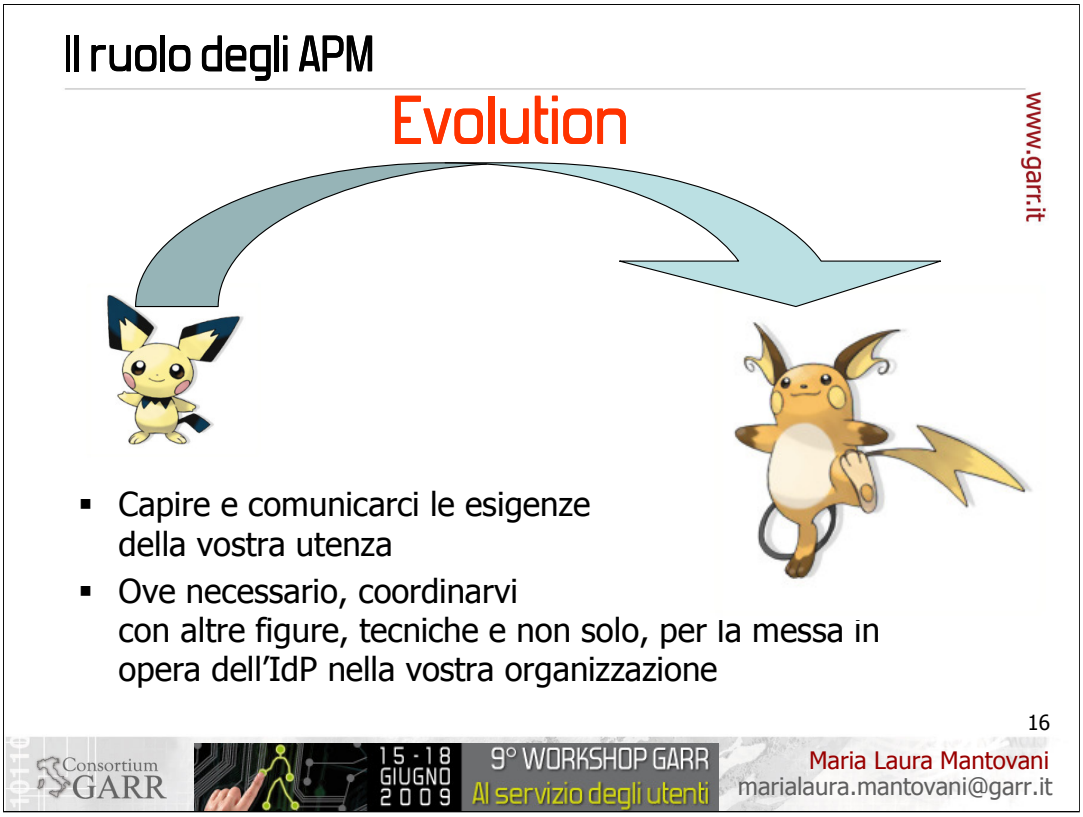
1. E' disponibile per qualsiasi richiesta di aiuto e di consulenza nell'implementazione dell'IdP della propria organizzazione, in una qualsiasi fase del processo, anche se volete per quanto riguarda l'organizzazione del sistema di Identity Management. Siete invitati a contattarci! idem@garr.it

1. Stipulerà accordi con il maggior numero possibile di fornitori di Risorse, affinché gli utenti della Federazione abbiano agevolmente accesso ai servizi di cui hanno bisogno.
   Attività in corso:
   - con il maggior numero possibile di editori che forniscono i loro servizi on-line. Ci sono contatti in corso con Refworks, con American Chemical Society, con OVID, …
   - con CINECA per rendere accessibili tramite l'accesso federato tutti i loro servizi: in particolare la suite U-GOV e il sito DOCENTE del MIUR
   - con CILEA e con CASPUR per l'accesso ai rispettivi servizi on-line per l'utenza.
   - con Microsoft per i programmi DreamSpark e MSDN Academic Alliance
   E' importante la vostra segnalazione di servizi rispetto ai quali i vostri utenti trarrebbero giovamento dall'accesso federato. Conoscendo le vostre necessità possiamo prendere contatti con i fornitori di risorse e coinvolgerli nella federazione.

- 3. Continuerà nello sviluppo del sito web della Federazione www.idem.garr.it dove troverete la documentazione sempre più arricchita e le novità sull'evoluzione della Federazione

- 4. Garantirà il funzionamento dei Partecipanti nella Federazione IDEM, grazie alla manutenzione continua e alla custodia del file metadata.xml e alla gestione del WAYF server (o della sua evoluzione: il Discovery Service)

- 5. Studio e sperimentazione di nuove funzionalità per l'interoperabilità ad esempio con il servizio di Federazione di Microsoft, oppure altro esempio per l'accesso a Grid.



Cosa chiediamo a voi APM?

Abbiamo ricordato che abbiamo inaugurato la Federazione 2 mesi fa il 30-31 marzo scorsi con il Primo Convegno IDEM a cui hanno partecipato circa 200 persone. Abbiamo constatato che oggi qui presenti ci sono oltre 200 convenuti, ma l'intersezione tra i 2 gruppi è solo del 10%. Ciò potrebbe far pensare che non sono gli APM le figure tecniche direttamente coinvolte nella realizzazione dei sistemi che servono a comporre la Federazione. Oppure, come recita la presentazione di questo workshop, è necessaria una evoluzione del ruolo degli APM in risposta alle nuove necessità degli utenti: oltre la fornitura di connettività a larga banda ed alta affidabilità, è necessario orientarsi a soddisfare l'utente finale nella sua esigenza di accesso ad una vasta gamma di servizi avanzati che siano il più possibile trasparenti e fruibili in modo immediato.

Perciò a voi APM chiediamo:

di informarvi, capire e farci sapere quali sono le risorse protette utilizza te dalla vostra utenza (ferroviedellostato.it?)
Noi cercheremo di attivarci per rendere accessibili tramite l'accesso federato le risorse che ci segnalerete.

di informarvi, capire, coordinarvi con il personale all'interno della vostra organizzazione che può essere maggiormente coinvolto e farci sapere se possiamo esservi utili per il completamento del sistema di Identity Management della vostra organizzazione e per la messa in opera dell'IdP

Concludo preannunciandovi che vorremmo organizzare un IDEM-DAY (novembre?): una giornata dedicata a tutorial specificamente tecnici per approfondire la conoscenza su SAML, sulla installazione e configurazione di Shibboleth IdP e SP, sugli aspetti tecnici dell'Identity Management.