GARR

The Italian Academic & Research Network

www.garr.it

# Federazione IDEM

## Servizio GARR-AAI

Maria Laura Mantovani

GARR-CTS, Roma, 21.05.2009

Consortium GARR

# Fase Pre-Progetto – Mag05-Ago07

www.garr.it

- Promozione, Formazione e Reclutamento
  - 13-05-2005 BoF: "Realizzazione di un'AAI per la rete GARR" alla Conferenza "GARR 05" - Pisa (primo incontro pubblico) 1
  - 16-02-2006 I giornata GARR sull'Authentication & Authorization Infrastructure 2 - Roma
  - 06-03-2007 II giornata GARR sull'Authentication & Authorization Infrastructure: "Autenticazione federata e biblioteche digitali"3 - Roma (consolidamento del gruppo di lavoro)
  - 02-04-2007 Kick off meeting per la creazione di una Federazione GARR delle AAI italiane4 - Bologna, nasce il Progetto Pilota Nazionale per lo studio, realizzazione e test di una Federazione di AAI.
  - 12-06-2007 Il progetto pilota è "battezzato" IDEM (IDentity Management federato per l'accesso ai servizi)
  - 02-08-2007 Il Direttore del GARR invia le lettere di nomina per formare il Comitato Tecnico di Gestione (CdG) del Progetto Pilota IDEM

1http://www.garr.it/conf_05/programma.htm
2http://www.garr.it/aai/programma.html
3http://www.garr.it/aai2
4http://www.garr.it/meeting_aai

# Risultato Reclutamento Volontari (2007)

www.garr.it

- Università
- Altri enti

# Fase Progetto: Ago07-Mar09



## Roadmap

- *Ago 07-Dic 07:* Attività dei Gruppi di Lavoro: Studio e Stesura Doc. Attributi e prime Specifiche Tecniche
- *Gennaio 2008:* vengono inviate le lettere d'invito alle organizzazioni che hanno mostrato interesse.
- *Marzo 2008*: è il termine per rispondere all'invito e aderire al progetto.
- *31 Marzo 2008:* prima riunione del Comitato di Gestione.
- *30 Giugno 2008:* data entro la quale i partecipanti devono predisporre un IdP attivo e funzionante secondo le specifiche richieste.
- *31 Dicembre 2008:* è richiesto ai partecipanti di inviare al Comitato di Gestione un documento in cui vengono descritte le proprie procedure per l'accreditamento degli utenti.
- *Ott 08-Mar 09:* Redazione Regolamento e Norme di Partecipazione

# Fase Progetto: Ago07-Mar09



- Gruppi di Lavoro (e di Studio) per la redazione della Documentazione:
  - Tecnico (Specifiche Tecniche e Documento Attributi)
    - Molte ore di lavoro in videoconferenza
- Promozione e Formazione
- Realizzazione infrastruttura (Metadata, WAYF, Web, HelpDesk, IdP e SP di test)
- Comitato di Gestione (CdG) – Governo della Federazione
  - Legale (Regolamento, Norme di Partecipazione, Modulistica per l'Adesione, DOPAU)
    - Molte ore di lavoro in videoconferenza e de visu
- Inviti a Organizzazioni
  - Adesione di IdP
  - Adesione di SP

# Fase Progetto: Ago07-Mar09

www.garr.it

- Promozione e Formazione
  - Presentazione: "Gestire" le identità per "gestire" la sicurezza dei dati (R. Conte (IFC-CNR)) al convegno: IRCCS Conference "Health Science Community: la medicina nelle arterie della rete GARR", 12 Dicembre 2007, Roma
  - Presentazione: Il progetto IDEM(R. Cecchini (GARR)) al convegno: Workshop GARR 08: GARR-X, il Futuro della Rete (1--4-04-2008)
  - Presentazione: IDEM: IDEntity Management federato per l'accesso ai servizi (M. L. Mantovani (UniMoRe)) al convegno: Workshop GARR 08: GARR-X, il Futuro della Rete (1--4-04-2008)
  - Tutorial: Costruire uno Shibboleth IdP per IDEM (F. Malvezzi (UniMoRe)) al convegno: Workshop GARR 08: GARR-X, il Futuro della Rete (1--4-04-2008)
  - Tutorial: Shibboleth SP per IDEM con Debian (F. Malvezzi (UniMoRe)) al convegno: Workshop GARR 08: GARR-X, il Futuro della Rete (1--4-04-2008)
  - Tutorial: Shibboleth SP per IDEM con Windows 2003 Server(D. Crecchia (UniMoRe)) al convegno: Workshop GARR 08: GARR-X, il Futuro della Rete (1--4-04-2008)
  - Presentazione: IDEM: affidabilità e riservatezza nella gestione delle identità per l'accesso a servizi remoti (R. Conte (IFC-CNR) al convegno: V convegno Internet Document Delivery e cooperazione inter-bibliotecaria "Tools, best practices and copyright", 21-22-23 Maggio 2008, Libera Università di Bolzano
  - Presentazione: Le Infrastrutture di Autenticazione e Autorizzazione (AAI) e IDEM (V. Calabritto (CASPUR)) al convegno: CIBER: seminario primaverile 2008 (11-13 Giugno)
  - "Incontro con il gruppo di lavoro IDEM GARR-AAI" 13 Ottobre 2008 Sala Pentagono-CNR - Roma

# Promozione e Formazione

(alcuni interventi)

- Francesco Malvezzi e Danilo Crecchia
  **Shibboleth e IDEM 2.x**
- Raffaele Conte
  **IDEM: Specifiche Tecniche e Attributi**
- Claudio Marotta
  **Auditing nella Federazione**
- Virginia Calabritto - CASPUR
  **Le Federazioni AAI: cosa e perchè**
- Maria Laura Mantovani - GARR
  **La Federazione IDEM**
- **Use Case UniTo e UniMoRe**
- Angelo Saccà - Università di Torino
  **Linee guida per un DOPAU (DOcumento Processo Accreditamento Utenti)**


www.garr.it

# Partecipanti al Progetto 31-03-2009

- IdP Università (9)
- IdP Altri (11)
- SP (13)

- Utenti totali (sottostima)
  870.000 (10/20 risp.)
  865.000 (5 risp)


www.garr.it

# Risorse attive: SP-test (1/13)

www.garr.it

**Organizzazione** GARR

**Contatti** B. Monticini (monticini@fi.infn.it)

**Descrizione** Web per il test degli IdP che entrano nella Federazione del Progetto

**Data di attivazione** Maggio 2008

**Stato** operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti di tutte le OA della Federazione del Progetto

**Uso** Servizio di test ad uso degli idp della federazione

**Note e problemi incontrati** Nessuno

**Piattaforma usata** Debian Etch a 64bit su server xen

# Risorse attive: Wiki (2/13)



**Organizzazione** CASPUR

**Contatti** I. De Marinis (ilaria.demarinis@caspur.it), V. Calabritto (Virginia.Calabritto@caspur.it)

**Descrizione** **Wiki** del Progetto Pilota IDEM (mediawiki) per produzione e condivisione di documentazione

**Data di attivazione** Aprile 2008

**Stato** operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti di tutte le OA della Federazione del Progetto

eduPersonPrincipalName

**Uso** Regolarmente usato da tutti i membri del Comitato di Gestione e dei gruppi di lavoro. Oltre 170 utenti: il Comitato di Gestione del progetto, i partecipanti al progetto ed il resto della comunità accedono con le utenze delle organizzazioni di appartenenza, con ruoli ed autorizzazioni differenziate, alla documentazione del progetto

**Note e problemi incontrati**

**Piattaforma usata** Debian; Shibboleth 1.3

# Risorse attive: LMS Moodle (3/13)

www.garr.it

**Organizzazione** Università degli Studi di Modena e Reggio Emilia

**Contatti** M. L. Mantovani (marialaura.mantovani@unimo.it), F. Malvezzi(francesco.malvezzi@unimore.it)

**Descrizione** **Moodle-Idem:** Piattaforma e-learning

**Data di attivazione** Maggio 2008

**Stato** Operativa

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti di tutte le OA della Federazione

eduPersonPrincipalName, sn, givenName, mail

**Uso** prova di fattibilita', provato da circa 60 utenti

**Note e problemi incontrati** nessuno

**Piattaforma usata** Debian etch, shibboleth-sp 2.0

# Risorse attive: IdemBlog (4/13)

www.garr.it

**Organizzazione** Università degli Studi di Torino

**Contatti** P. Laguzzi (paola.laguzzi@unito.it)

**Descrizione** **IdemBlog -** Creando un blog si possono condividere immagini, foto, audio, video, pensieri, documenti con lo scopo di favorire la diffusione di una cultura che vede nella condivisione e nella relazione tra persone un elemento primario di crescita e innovazione, per esplorare originali forme e fenomeni di aggregazione e di community

**Data di attivazione** Maggio 2008

**Stato** operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti di tutte le OA della Federazione

sn, givenName, mail

**Uso** Si contano più di 4000 login provenienti da tutti gli IdP della Federazione Pilota

**Note e problemi incontrati**

**Piattaforma usata** RedHat, Shibboleth 1.3

# Risorse attive: GARR VCONF (10/13)

www.garr.it

**Organizzazione** GARR

**Contatti** vconf-service@garr.it.

**Descrizione** GARR VCONF – servizio di videoconferenza

**Data di attivazione** Giugno 2008

**Stato** operativo

**URLs** http://vconf.garr.it/

**Policy e attributi richiesti** Aperto a tutti gli utenti di tutte le OA della Federazione del Progetto. Attributi richiesti sn, givenName, mail.

**Uso** Comunicazione audio-video tra sedi diverse (videoconferenza)

**Note e problemi incontrati** --

**Piattaforma usata** --

# Risorse attive: Metapress (6/13)



**Organizzazione** SPRINGER L.t.d.

**Contatti** H. Klusendorf (HeatherKlusendorf@Metapress.COM) - tecnico

U. Lengwenat (Ulrike.Lengwenat@springer.com), A. Gallo (Alessandro.Gallo@springer.com)

support@metapress.com

**Descrizione** **Metapress**

**Data di attivazione** Ottobre 2008

**Stato** Operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti delle O.A. che hanno sottoscritto il controtto

Attributi richiesti: eduPersonScopedAffiliation

**Uso** nd

**Note e problemi incontrati** L'interazione è stata rapida ed efficente

Le feature di personalizzazione sono disponibile solo per gli accessi con le utenze locali alla piattaforma

Variazioni nei metadata degli IdP devono essere comunicate a support@metapress.com

Per I nuovi IdP il contatto tecnico deve inviare un mail a:

con oggetto: "Shibboleth: Add my IdP <institution name>"

corpo: MetaPress Ids, Nome dell'Organizzazione, URL dell' IdP e indirizo e-mail del contatto tecnico

**Piattaforma usata**

# Risorse attive: ScienceDirect (7/13)

www.garr.it

**Organizzazione** Elsevier

**Contatti** A. De Vrie (ale@elsevier.com)

**Descrizione** **ScienceDirect –** piattaforma per la fruizione di periodici elettronici in abbonamento

**Data di attivazione** Ottobre 2008

**Stato** Operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti delle O.A. che hanno sottoscritto il controtto

eduPersonEntitlement con il valore di

urn:mace:dir:entitlement:common-lib-terms;

il Virtual Host dell'IdP deve avere la direttiva SSLVerifyClient impostata al valore optional_no_ca

**Uso** nd

**Note e problemi incontrati** Interazione un po' lenta.

**Piattaforma usata**

# Risorse attive: Scopus (8/13)



**Organizzazione** Elsevier

**Contatti** A. De Vrie (ale@elsevier.com)

**Descrizione** **SCOPUS**

**Data di attivazione** Ottobre 2008

**Stato** Operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti delle O.A. che hanno sottoscritto il controtto

eduPersonEntitlement con il valore di

urn:mace:dir:entitlement:common-lib-terms;

il Virtual Host dell'IdP deve avere la direttiva SSLVerifyClient impostata al valore optional_no_ca

**Uso** nd

**Note e problemi incontrati** Interazione lenta.

**Piattaforma usata**

# Risorse attive: Atlases (9/13)



**Organizzazione** Masaryk University

**Contatti** M. Prochazka (michalp@ics.muni.cz)

**Descrizione** **Atlases** - Atlante di imaggini di immagini (risonanze magnetiche, tomografie computerizzate, immagini da microscopio.....) di dermatologia, patologia fetale, neonatale e patologia degli organi per il cui accesso è disponibile per il cui accesso è disponibile una iterfaccia di microscopio virtuale

**Data di attivazione** Novembre 2008

**Stato** Operativo

**URLs** https://atlases.muni.cz/

**Policy e attributi richiesti** Il servizio è gratuito aperto a tutti gli utenti di tutte le OA della Federazione del Progetto, previa accettazione delle policy del servizio per ciascuna sua sezione.

eduPersonPrincipalName

**Uso** nd

**Note e problemi incontrati** L'interazione è stata rapida ed efficente

I metadata della risorsa sono firmati con un certificato di una CA non riconosciuta dai principali browser

**Piattaforma usata** nd

# Risorse attive: Science Direct On Site (5/13)



**Organizzazione** CILEA

**Contatti** R. Gibellini (gibellini@cilea.it)

**Descrizione** **Science Direct On Site** – Piattaforma per la gestione e visualizzazione dei periodici elettronici sottoscritti

**Data di attivazione** Dicembre 2008

**Stato** operativo

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti delle O.A. che hanno sottoscritto il contratto CDL e hanno contattato staff_sdos@cilea.it tramite il proprio referente CDL

eduPersonScopedAffiliation

**Uso** nd

**Note e problemi incontrati**

**Piattaforma usata** nd

# Risorse in attivazione: ISI Web Of Knowledge (11/13)



**Organizzazione** Thomson Reuter

**Contatti** M. Plebani () - comerciale

C. Ireland (chris.ireland@thomsonreuters.com) – help desk II livello

ts.websetups@thomson.com

**Descrizione** ISI Web Of Knowledge

**Data di attivazione** Non è stato possible attivarlo

**Stato** test

**URLs**

**Policy e attributi richiesti** Aperto a tutti gli utenti delle O.A. che hanno sottoscritto il controtto

eduPersonScopedAffiliation

**Uso** --

**Note e problemi incontrati** Interazione lentissima e faticosa

I nuovi IdP che aderciscono alla Federzione devono compilare lo ShibbolethSetupForm ed inviarlo al supporto di primo livello per l'abilitazione all'accesso.

eduPersonScopedAffiliation

**Piattaforma usata** nd

# Risorse in attivazione: Nilde (12/13)



**Organizzazione** CNR Area di Ricerca di Bologna

**Contatti** S. Mangiaracina, A. Tugnoli (mangiaracina@area.bo.cnr.it, a.tugnoli@area.bo.cnr.it )

**Descrizione** **NILDE-Utenti**. Permette agli utenti delle biblioteche aderenti al network NILDE (http://nilde.bo.cnr.it/index.php?st=2) di richiedere copie di articoli scientifici non posseduti presso le stesse biblioteche. Il servizio puo' essere richiamato a partire dalle principali banche dati bibliografiche scientifiche.

**Data di attivazione** ---

**Stato** test

**URLs** http://nilde.bo.cnr.it/utenti-sso

**Policy e attributi richiesti** Aperto a tutti gli utenti delle biblioteche aderenti a NILDE e appartenenti ad un ente che partecipa alla Federazione.

eduPersonTargetedID

**Uso** >Gli utenti attualmente iscritti al servizio NILDE-Utenti sono circa 10.000. Attraverso una procedura di "recupero account" e' possibile che gli utenti possano migrare dall'autenticazione precedente, con username e password locali a NILDE, all'autenticazione istituzionale attraverso IDEM, senza perdere i dati bibliografici legati al loro precedente account.

**Note e problemi incontrati** ---

**Piattaforma usata** Debian; Shibboleth 1.3

# Risorse in attivazione: Cont@ct Centre (13/13)



**Organizzazione** ISTAT

**Contatti** C. Catalano (cecilia.catalano@istat.it), A. Cardacino (alessio.cardacino@istat.it)

**Descrizione** **Cont@ct Centre**. Server web per la richiesta e l'acquisizione di dati e informazioni statistiche prodotte dall'Istat

**Data di attivazione** Non è stato possible attivarlo

**Stato** test

**URLs** https://contact.istat.it/

**Policy e attributi richiesti**

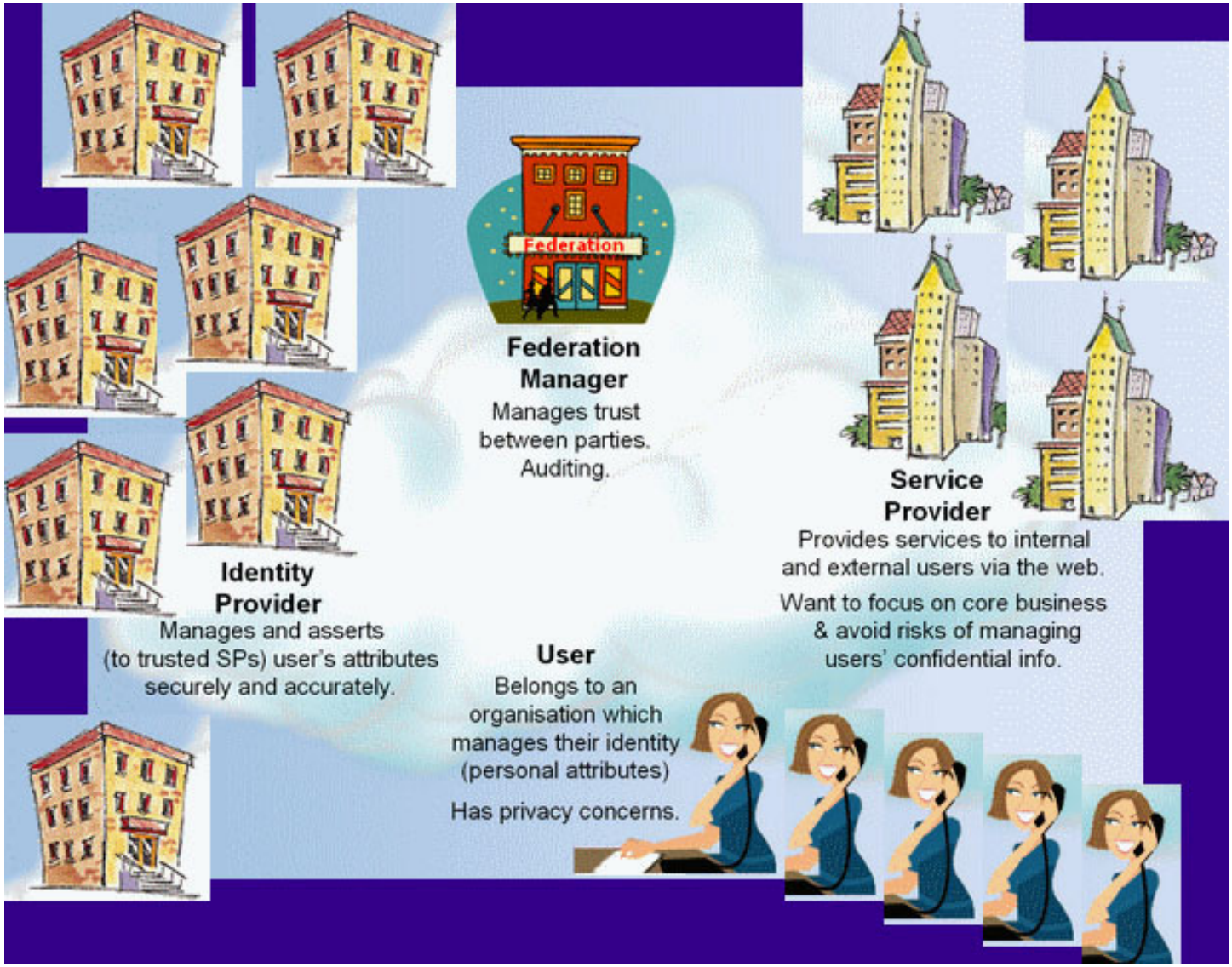
eduPersonTargetedID, eduPersonScopedAffiliation, givenName, sn, mail

**Uso** --

**Note e problemi incontrati** Per gli attributi richiesti, senza possibilità dell'utente di dare la libertatioria, si pongono dei problemi da discutere

**Piattaforma usata** Redhat 4 - Shibboleth v. 2

# La Federazione: Problematiche



# Problematiche per gli Utenti



- L'Utente appartiene ad una Organizzazione che gestisce la sua Identità Digitale
  - Possiede caratteristiche (Attributi)
  - Ha diritto ad un trattamento dei propri dati personali conforme alla normativa privacy
  - Pretende sicurezza nell'uso delle risorse (non vorrebbe avere problemi di password)

# Problematiche per le Organizzazioni (IdP)



- Gestiscono i dati personali dei propri utente (conformemente a normativa privacy)
- Asseriscono agli SP fidati gli Attributi degli Utenti
- Vogliono garantire sicurezza all'Utente/Trasmettono in un canale sicuro
- Trasmettono informazioni accurate
- Vogliono dare ai propri utenti un metodo di accesso facilitato (SSO), per risorse interne ed esterne
- Realizzano un sistema di Identity & Access Management

# Problematiche per le Risorse (SP)



- Forniscono Servizi agli utenti della propria organizzazione, ma anche di altre organizzazioni
- Preferiscono focalizzarsi sul loro business
- Preferiscono evitare di dover gestire informazioni confidenziali degli utenti
- Vogliono ricevere Asserzioni veritiere sulle quali basare le politiche di Autorizzazione

# Problematiche per il Gestore della Federazione



- Gestisce la fiducia tra i Partecipanti (IdP e SP)
  - Concorda e definisce regole comuni
  - Favorisce la standardizzazione sulla valorizzazione di alcuni Attributi per gli IdP
  - Favorisce la standardizzazione sull'uso di alcuni attributi per gli SP
- Per garantire la Fiducia reciproca controlla i partecipanti (Audit)
- Diffonde la cultura per un corretto utilizzo delle identità digitali e delle tecnologie correlate
- Help Desk

# Attività del Servizio IDEM-AAI 2009-2010

# Attività del Servizio IDEM-AAI 2009-2010



- Organizzazione e Documentazione
  - Supporto al CdG per la redazione del Regolamento
  - Supporto al CdG per la redazione delle Norme di Partecipazione
  - Supporto al CdG per la redazione della modulistica per l'Adesione
  - Supporto al CdG per la redazione del Report 2008
  - Supporto al CdG per la redazione delle Specifiche Tecniche
  - Razionalizzazione di schema di DOPAU e DOPAR
  - Coordinamento con attività e servizi GARR (DB, IAM, SSO, …)
  - Registrazione e aggiornamento periodico di IDEM in REFEDS
  - Coordinamento con TERENA
  - Sito web www.idem.garr.it (restiling sito statico, copywriting nuovi contenuti - manca tutta la documentazione tecnica, CMS-Drupal)
  - Traduzione in inglese di tutta la documentazione cartacea e on-line utile per Confederazioni e SP all'estero
  - Ricerca, redazione e pubblicazione di Use Cases e di Best Practices
  - Relazioni con IdP e SP per individuare le loro necessità, ad esempio sul tema "attributi", e proporre direttive e modi di operare

(attività già iniziate)

# Attività del Servizio IDEM-AAI 2009-2010



- Supporto Tecnico
  - Formazione del personale dedicato al supporto tecnico (ST)
  - Definizione delle procedure operative del ST (ticketing, flussi, supporto telefonico, SLA)
  - Servizio WAYF/Discovery Service di produzione e server WAYF/Discovery Service di prova
  - Servizio IdP di produzione per Direzione GARR
  - Server IdP di prova su varie piattaforme
  - Server SP di prova su varie piattaforme
  - Procedure automatizzate di controllo dei Metadati (sicurezza dei certificati utilizzati dai partecipanti)
  - Procedura di accompagnamento per l'ingesso di un nuovo IdP nella Federazione - comprende tutta la fase di test della funzionalità dell'IdP
  - Procedura di accompagnamento per l'ingesso di un nuovo SP nella Federazione - comprende tutta la fase di test della funzionalità dell'SP e dell'interoperabilità con la federazione
  - Transizione da Shibboleth 1.3 a Shibboleth 2.1
  - Test di eventuali nuove versioni di Shibboleth
  - Redazione e aggiornamento  delle guide di installazione per IdP e SP.- FAQ

(attività già iniziate)

# Attività del Servizio IDEM-AAI 2009-2010



- Promozione e Formazione (1/2)
  - Lettere ufficiali ai firmatari degli aderenti al progetto per dire che il progetto e' finito ed occorre sottoscrivere la richiesta di Adesione alla Federazione e soddisfare i requisiti
  - Lettere ufficiali a tutti gli enti GARR per invitarli ad aderire alla Federazione
  - Email personalizzate ai partecipanti al Convegno per capire ognuno come intende proseguire nei confronti di IDEM
  - Diffusione di cultura e competenze riguardo l'Identity and Access Management presso i partecipanti e gli interessati (gestione delle identità digitali da parte dei soggetti che ne hanno l'autorità) (al fine di ampliare il numero di IdP nella Federazione)
  - Diffusione di standard riguardo il Processo di accreditamento degli utenti
  - Diffusione della cultura dell'Attribute Based Access Control (gestione dei ruoli e degli attributi da parte dei soggetti che ne hanno l'autorità)
  - Promozione delle enterprise directory sincronizzate con i sistemi informativi aziendali
  - Diffusione della cultura della fiducia interna alla federazione: la fiducia ci puo' essere se le regole sono uguali per tutti

# Attività del Servizio IDEM-AAI 2009-2010



- Promozione e Formazione (2/2)
  - Seminari, corsi, workshop, incontri nelle varie sedi degli interessati per valutare ed affrontare con gli interessati le problematiche specifiche ed indirizzarli ed aiutarli nella progettazione e nella realizzazione del sistema di Identity & Access Management della loro istituzione
  - Seminari e tutorial "Shibboleth install fest" (al fine di ampliare il numero di IdP e di SP nella Federazione)
  - "Individuazione da parte della federazione tutti gli SP di interesse (es: editori scientifici, con contratti nelle università e negli EPR per l'accesso alle loro risorse), scaletta di priorità, avvio e conduzione delle relazioni per concordare l'ingresso nella federazione
  - Quali servizi il Partecipante può condividere nella Federazione? Promozione culturale rivolta ai partecipanti
  - Definizione di un piano di promozione della rete delle identità e dei servizi federati rivolto a consorzi (standardizzazione dei servizi di accesso ai sistemi) ed enti (pubbliche amministrazioni per servizi ai cittadini, ausl per servizi ai malati, ai medici, in generale alle comunità di interesse, camere di commercio, …)
  - Raccordo con altre Federazioni Nazionali
  - Aiuto all'Organizzazione Evento annuale IDEM – IDEM DAY (Nov 2009)
  - Relazioni con operatori telefonici per l'accesso ad Internet (ADSL/Wireless) tramite Federazione

(attività già iniziate)

# Attività del Servizio IDEM-AAI 2009-2010



- Progettazione e studio
  - Rilascio degli attributi da parte dell'utente finale in modalità consapevole e informata (uApprove, ArpView, PERMIS o altri strumenti)
  - Level of Assurance
  - Uso dell'autenticazione federata per accesso alla rete in modalità wireless
  - Interoperabilità con altre implementazioni di SAML2.0 (SimpleSAMLphp, Microsoft 'Geneva' Framework, Progetto ICAR, …)

(attività già iniziate)

GARR

The Italian Academic & Research Network

www.garr.it

# Federazione IDEM

## Servizio GARR-AAI

Maria Laura Mantovani

GARR-CTS, Roma, 21.05.2009

Consortium GARR