



# La Federazione IDEM

Maria Laura Mantovani

GARR

idem@garr.it

Primo Convegno IDEM

Roma, 30-31 marzo 2009

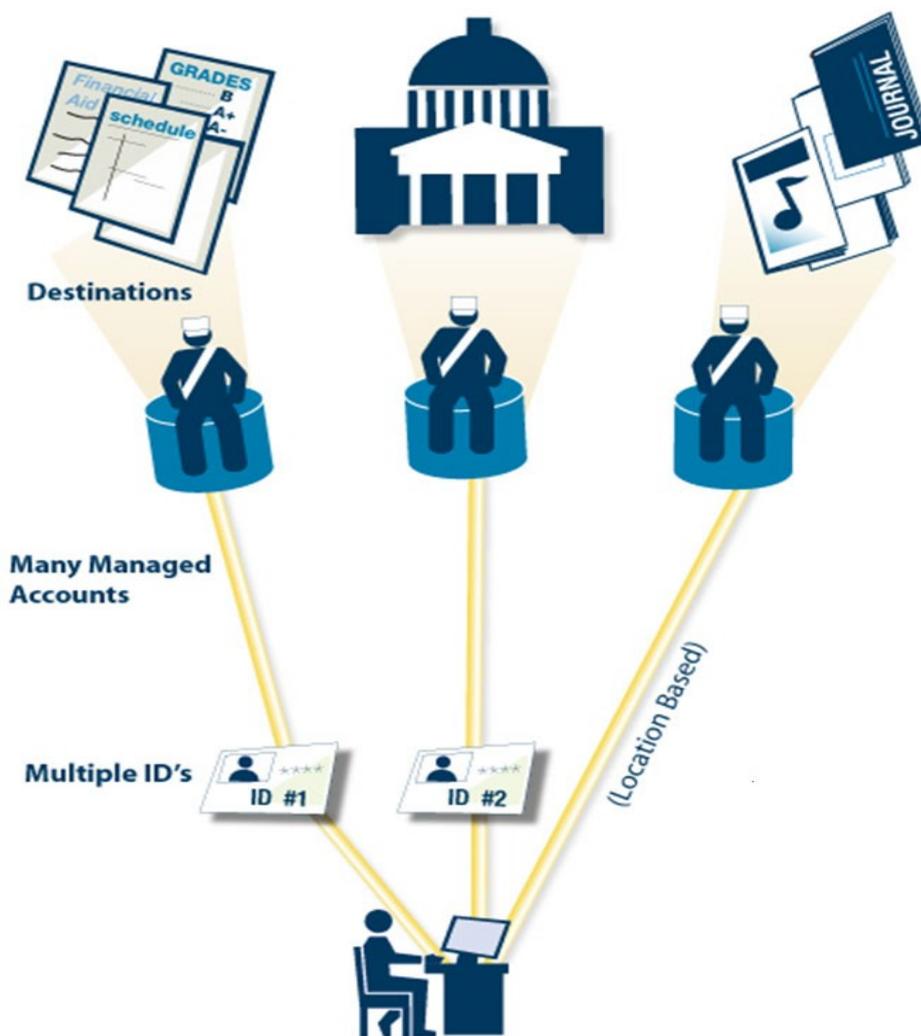
Dalle password all'identità digitale federata



# SENZA IDEM



- L'utente ha molte credenziali per accedere a diversi servizi
- L'accesso può essere basato sulle credenziali, ma anche sull'IP di provenienza
- Viene sprecato tempo nella gestione degli account anziché nella gestione delle risorse
- Manca uno standard che accomuna i Partecipanti
- Non c'è collaborazione perché la condivisione risulta difficile o insicura
- L'aggiunta di nuove risorse o nuovi utenti può richiedere un ulteriore lavoro significativo



Primo Convegno IDEM

Roma, 30-31 marzo 2009

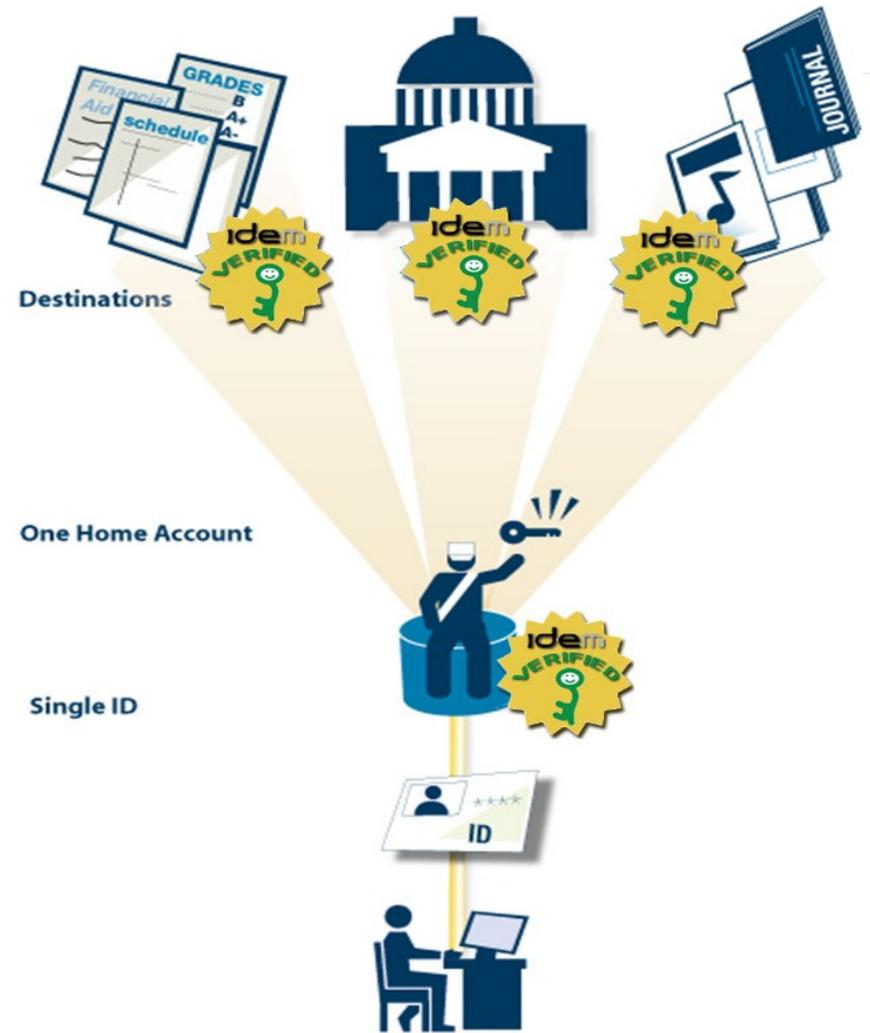
Dalle password all'identità digitale federata



# CON IDEM



- Gli utenti si registrano in un unico punto (la propria home organization) e accedono facilmente a molte risorse che la federazione mette loro a disposizione
- Gli utenti devono gestire meno credenziali
- C'è un controllo fine riguardo il rilascio di informazioni che riguardano l'utente
- L'accesso è basato su standard e prodotti open source
- Nuove risorse e nuovi utenti possono essere aggiunti velocemente
- Il diritto di accesso è regolato dagli attributi, non dalle credenziali o dall'IP



Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



# CHI PUÒ PARTECIPARE AD IDEM?



IDEM è:

- una federazione di organizzazioni che creano un ambiente comune di identità verificate per supportare la ricerca e la didattica
- il cui intento è di facilitare la collaborazione attraverso la condivisione di risorse protette per mezzo di un circolo di fiducia comunemente condiviso.

i PARTECIPANTI si suddividono in:

- MEMBRI: le organizzazioni afferenti alla comunità GARR
- PARTNER: tutte le altre organizzazioni interessate

**Primo Convegno IDEM**

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



# CHI PUÒ PARTECIPARE AD IDEM?



## MEMBRI: le organizzazioni afferenti alla comunità GARR

1. gli Enti fondatori del Consortium GARR (CNR, ENEA, INFN e la Fondazione CRUI in rappresentanza delle Università italiane);
2. gli organismi di ricerca vigilati dal MIUR, tra cui ASI, INAF, INGV e altri;
3. i Consorzi Interuniversitari per il Calcolo (CASPUR, CILEA, CINECA);
4. le università e istituzioni culturali e/o scientifiche straniere con sede in Italia e per le quali esistono accordi con il Governo italiano;
5. organismi culturali e di ricerca afferenti ad altri Ministeri, quali MiBAC e Salute;
6. associazioni o consorzi tra organismi di cui alle categorie 1 e 2;
7. centri di ricerca e istituzioni culturali e/o scientifiche italiane di rilevante interesse per la comunità scientifica nazionale e centri di ricerca.

**Primo Convegno IDEM**

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



# CHI PUÒ PARTECIPARE AD IDEM?



## PARTNER: tutte le altre organizzazioni interessate

1. Fornitori di informazioni e di contenuti anche multimediali, Editori (Elsevier, Springer, Thomson Reuters, ... ), altri anche in Italia
2. Fornitori di Servizi on line (Download di software, musica, ... , Acquisto biglietti per viaggi, spettacoli, ... , Servizi Ricerca/Offerita Lavoro, Accesso a dati scientifici di laboratori non statali (ed es. all'estero)
3. Fornitori di servizi per i cittadini: servizi anagrafici, servizi sanitari, pagamenti ...
4. ...

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata

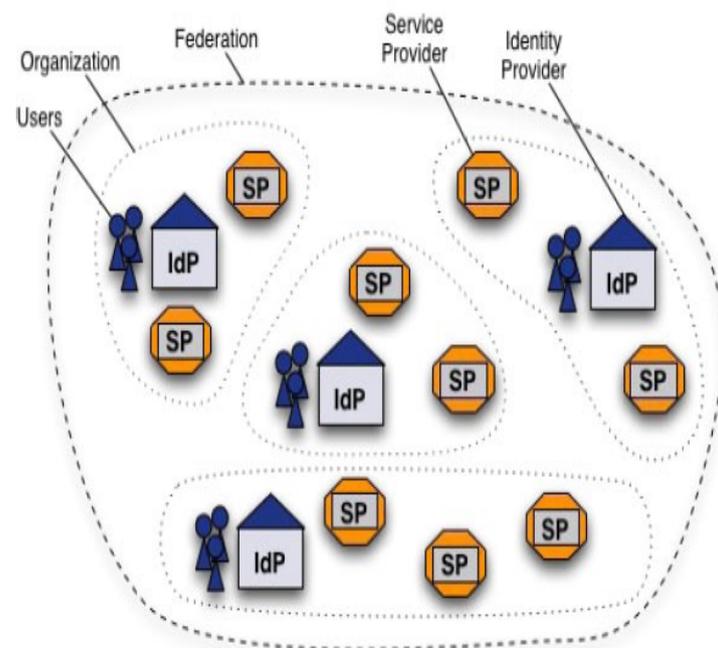


# PER PARTECIPARE



i Partecipanti (Membri e Partner)  
PARTECIPANO ad IDEM e REGISTRANDO  
SERVIZI

- Servizio di gestione e verifica delle identità (Identity Provider (IdP))
- Risorsa accessibile in rete a seguito di una procedura di identificazione e autorizzazione (Service Provider (SP))



Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



# PER PARTECIPARE

---



- I Membri partecipano ad IDEM registrando principalmente il servizio di gestione delle identità (Identity Provider), ma anche con risorse
- I Partner partecipano ad IDEM registrando principalmente risorse



# REGISTRARE SERVIZI



Il Membro può registrare nella Federazione uno ed un solo IdP relativo al sistema di Identity Management della propria Organizzazione.

(eccetto il CNR la cui peculiare organizzazione fatta da istituti con autonomia organizzativa, geograficamente distribuiti sul territorio Nazionale, può registrare più IdP, facendosi carico di garantire l'univocità della registrazione dell'utente finale)

Oltre all'IdP, il Membro può registrare una o più risorse ulteriori.



# REGISTRARE SERVIZI

---



Il Partner registra nella Federazione una o più Risorse.

A fronte di richiesta accuratamente motivata, gli organi di governo della Federazione possono consentire al Partner anche la registrazione dell'IdP dell'Organizzazione.



# REQUISITI PER LA REGISTRAZIONE DI UN IDP



- impegno istituzionale nella gestione degli utenti (IAM & directory enhancement)
- l'IdP è un sistema/servizio aggiuntivo da gestire
- gli attributi relativi agli utenti devono essere resi disponibili ed utilizzati nel rispetto della privacy dell'utente e della legislazione vigente e in modo conforme a denominazione, sintassi e semantica indicate in ST-A (Specifiche Tecniche – Attributi, <http://idem.garr.it>)
- deve essere reso disponibile agli altri Partecipanti un documento contenente i dati salienti riguardanti il sistema di identity management secondo lo schema DOPAU (DOcumento Processo Accreditamento Utenti) predisposto dalla Federazione; i fornitori di risorse potranno utilizzare le informazioni relative alle procedure operative di gestione degli utenti per determinare il livello di fiducia delle asserzioni per ogni Partecipante.



# REQUISITI PER LA REGISTRAZIONE DI UNA RISORSA



- deve essere reso disponibile agli altri Partecipanti un documento contenente i dati salienti riguardanti il sistema di accesso alle risorse secondo lo schema DOPAR (DOcumento Processo Accreditamento Risorsa) predisposto dalla Federazione



# REQUISITI LA REGISTRAZIONE DI SERVIZI (IDP E DI RISORSE)



- i servizi da registrare devono essere conformi alle specifiche tecniche (ST) (documentazione <http://idem.garr.it>)
- i servizi devono essere sotto la completa responsabilità del Partecipante che li registra anche quando gestiti tramite contratti di outsourcing
- il Partecipante deve fornire alla Federazione i propri Metadati aggiornati e mantenere i Metadati sui servizi di propria competenza secondo le indicazioni della Federazione rispettando la procedura e i tempi indicati in ST
- il Partecipante deve comunicare alla Federazione il nominativo del Contatto Tecnico e comunicare tempestivamente ogni variazione
- il Partecipante deve realizzare un pagina web secondo il modello descritto in ST e provvedere all'aggiornamento delle informazioni in essa contenute



# RICHIESTA DI ADESIONE



Al fine di aderire alla Federazione, l'Organizzazione

- prende visione di tutta la documentazione legale (Regolamento e Accordo di Partecipazione) e tecnica messa a disposizione dalla Federazione e valuta la fattibilità della propria partecipazione con uno o più servizi, IdP e/o SP;
- compila in duplice copia il Contratto di Adesione e lo invia al Comitato di Indirizzo, completo degli allegati e firmato dal Legale Rappresentante; tramite il Contratto di Adesione l'Organizzazione accetta le regole derivanti dalla partecipazione alla Federazione e nomina il Referente Organizzativo e il Referente Tecnico;
- Per la Federazione IDEM il Contratto viene controfirmato dal Consortium GARR;
- contestualmente al Contratto di Adesione, invia la richiesta di registrazione di IdP e/o di una o più Risorse; ulteriori richieste di registrazione servizi potranno essere presentate in seguito all'adesione.

Contratti, documentazione e modulistica: <http://idem.garr.it>

**Primo Convegno IDEM**

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



# SERVIZI DELLA FEDERAZIONE



## SERVIZIO IDEM-AAI

al fine avviare una federazione “solida”, cioè con presupposti organizzativi stabili e durevoli e garantire ai fornitori di servizi “federabili” un contesto nel quale condurre investimenti su base pluriennale

1. servizio di promozione e formazione.
2. servizio di supporto tecnico;
3. servizio di supporto per organizzazione e documentazione;
4. servizio progettazione e studio;

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



- Diffusione di competenze IAM (al fine di ampliare il numero di IdP nella Federazione)
- Diffusione di standard riguardo il Processo di accreditamento degli utenti
- Seminari e tutorial (al fine di ampliare il numeri di IdP e di SP nella Federazione)
- Quali servizi il Partecipante può condividere nella Federazione?  
Promozione culturale rivolta ai partecipanti
- Individuazione da parte della federazione tutti gli SP di interesse
- Definizione di un piano di promozione della rete delle identità e dei servizi federati rivolto a enti (pubbliche amministrazioni per servizi ai cittadini, ausl per servizi ai malati, ai medici, in generale alle comunità di interesse, camere di commercio, ...)
- Relazioni con operatori telefonici per l'accesso ad Internet (ADSL/Wireless) tramite Federazione



- Definizione e messa in opera delle procedure operative del Servizio Tecnico (ticketing, flussi, supporto telefonico, SLA)
- Servizio WAYF, Discovery Service
- Servizio di condivisione dei Metadati e Procedure automatizzate di controllo dei Metadati (sicurezza dei certificati utilizzati dai partecipanti)
- Testing di piattaforme e versioni al fine di individuare le eventuali problematiche dei partecipanti
- Procedura di accompagnamento per l'ingresso di un nuovo IdP nella Federazione - comprende tutta la fase di test della funzionalità dell'IdP
- Procedura di accompagnamento per l'ingresso di un nuovo SP nella Federazione - comprende tutta la fase di test della funzionalità dell'SP e dell'interoperabilità con la federazione
- Monitoraggio e auditing
- Servizio IdP per gli Homeless (in valutazione)





# SERVIZIO DI SUPPORTO PER ORGANIZZAZIONE E DOCUMENTAZIONE



- Redazione e aggiornamento delle guide di installazione per IdP e SP
- Un sito web dove si trovino tutte le informazioni
- Raccolta di Use Cases e di Best Practices da pubblicare sul sito web che siano utili ai partecipanti ai fini della adesione e del mantenimento dei loro servizi nella federazione
- Documentazione in lingua inglese per facilitare l'attivazione di SP all'estero e relazioni con le Federazioni all'estero
- Coordinamento con attività e servizi GARR
- Coordinamento con altri progetti di identità federata a livello nazionale
- Coordinamento con le altre federazioni Europee
- Supporto agli organi di governo della Federazione per la redazione dei documenti legali, della documentazione tecnica, dei report annuali.

**Primo Convegno IDEM**

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



La Federazione ha bisogno di evolvere, di stare al passo con le altre Federazioni analoghe nel resto del mondo

Alcune tematiche in corso di studio:

- **Attributi e Privacy:** come può fare l'utente finale a conferire il consenso informato e puntuale sul rilascio degli attributi che lo riguardano
- **Sistemi di identificazione e livello di certezza dell'identità (Level of Assurance)**
- **Uso dell'autenticazione federata per accesso anche a servizi non web (es alla rete in modalità wireless)**
- ...





## Chi è?

3 FTE:

Maria Laura Mantovani (100%)

Barbara Monticini (50%)

Simona Venuti (50%)

...

con il Contributo **INDISPENSABILE** del Comitato Tecnico-Scientifico  
(l'attuale Comitato di Gestione del Progetto IDEM)

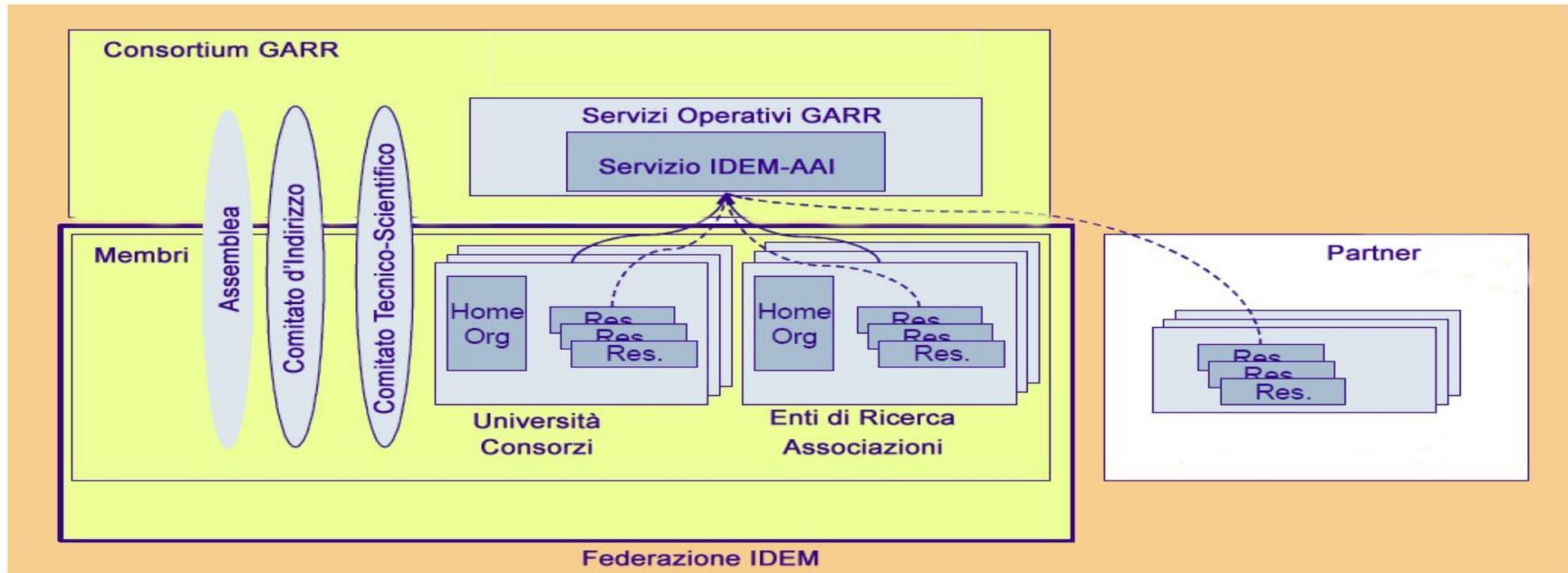
Il Servizio Tecnico IDEM-AAI si raccorda con gli organi di Governo della  
Federazione



# IL FUTURO GOVERNO DI IDEM



I Partecipanti alla Federazione IDEM si esprimeranno nei seguenti organi  
Assemblea dei Membri, Comitato d'Indirizzo, Comitato Tecnico-Scientifico



I comitati danno le linee guida, il Servizio le mette in opera insieme al contributo indispensabile ed effettivo del Comitato Tecnico-scientifico

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



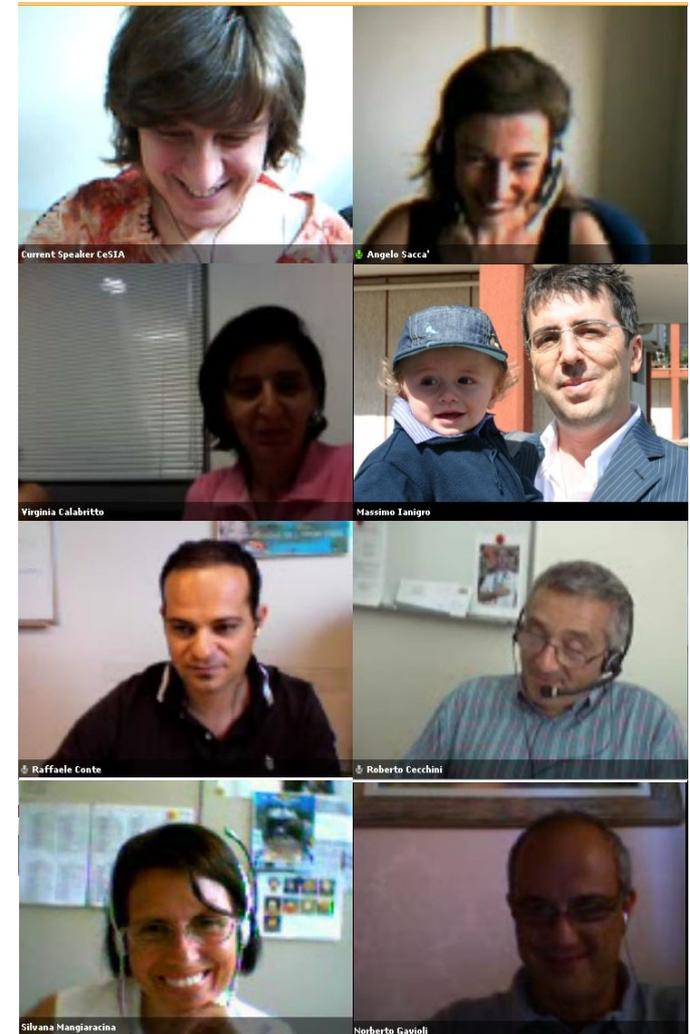
# IL COMITATO DI GESTIONE



(finisce 12/2009)

- \* Virginia Calabritto, CASPUR Roma
- \* Roberto Cecchini, GARR Firenze
- \* Raffaele Conte, CNR IFC Pisa
- \* Roberto Gaffuri, Politecnico di Milano
- \* Norberto Gavioli, Univ. dell'Aquila
- \* Valentino Gratton, Politecnico di Bari
- \* Massimo Ianigro, CNR ISSIA Bari
- \* Silvana Mangiaracina, CNR AdR Bologna
- \* Maria Laura Mantovani, Univ. di Modena e Reggio Emilia
- \* Tiziana Podesta', Univ. di Genova
- \* Angelo Sacca', Univ. di Torino
- \* Stefano Zanmarchi, Univ. di Padova

Call for new members



Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata

