

Primo Convegno IDEM

Roma, 30-31 marzo 2009



Dalle password all'identità digitale federata

Le Federazioni AAI: cosa e perché

Virginia Calabritto
idem@garr.it



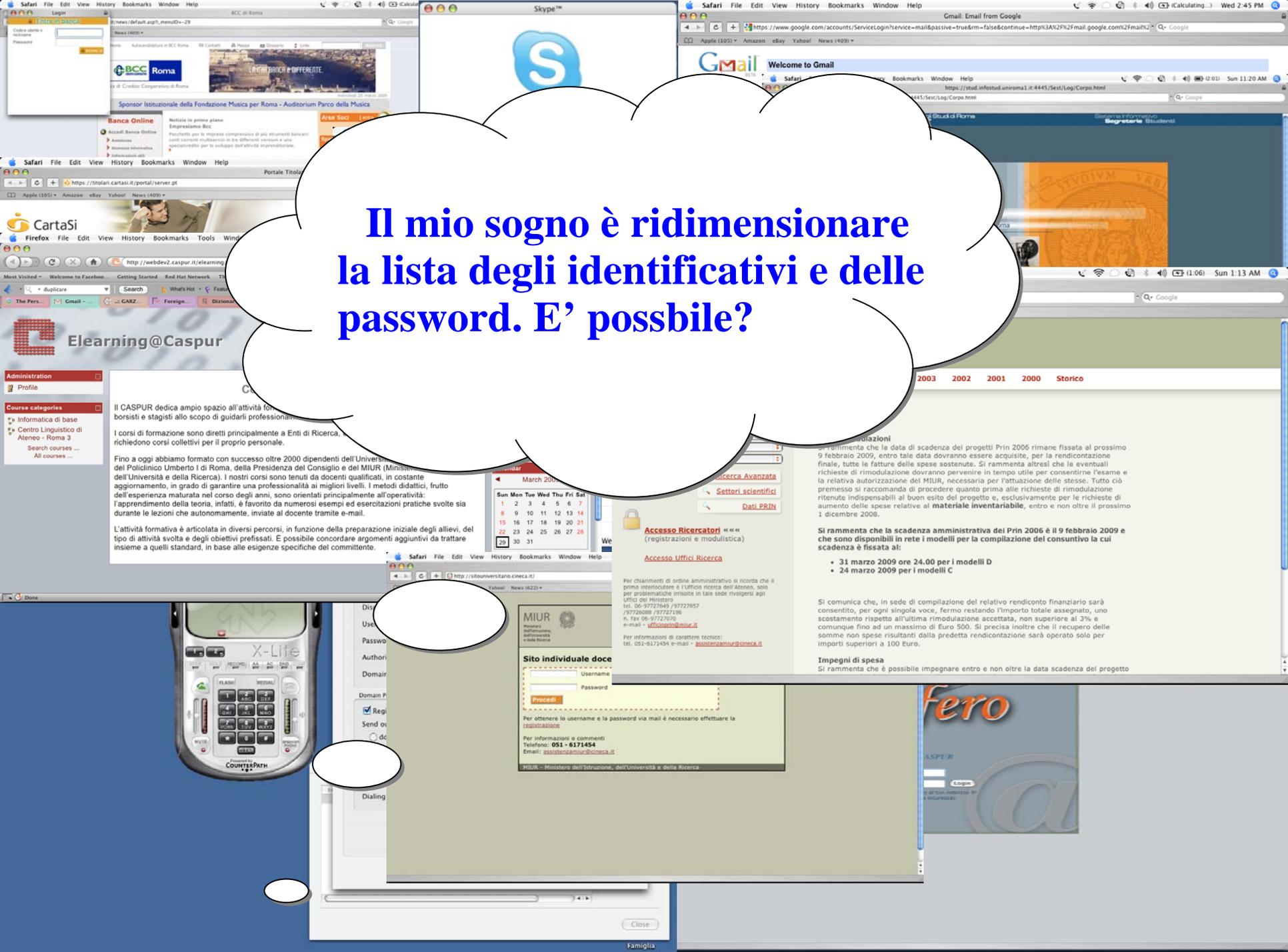


I have a dream....

Essere una Pop Star



Il mio sogno è ridimensionare la lista degli identificativi e delle password. E' possibile?



Il CASPUR dedica ampio spazio all'attività formativa per i borsisti e stagisti allo scopo di guidarli professionalmente. I corsi di formazione sono diretti principalmente a Enti di Ricerca, richiedono corsi collettivi per il proprio personale. Fino a oggi abbiamo formato con successo oltre 2000 dipendenti dell'Università del Policlinico Umberto I di Roma, della Presidenza del Consiglio e del MIUR (Ministero dell'Università e della Ricerca). I nostri corsi sono tenuti da docenti qualificati, in costante aggiornamento, in grado di garantire una professionalità ai migliori livelli. I metodi didattici, frutto dell'esperienza maturata nel corso degli anni, sono orientati principalmente all'operatività: l'apprendimento della teoria, infatti, è favorito da numerosi esempi ed esercitazioni pratiche svolte sia durante le lezioni che autonomamente, inviate al docente tramite e-mail. L'attività formativa è articolata in diversi percorsi, in funzione della preparazione iniziale degli allievi, del tipo di attività svolta e degli obiettivi prefissati. È possibile concordare argomenti aggiuntivi da trattare insieme a quelli standard, in base alle esigenze specifiche del committente.

March 2009

Sun	Mon	Tue	Wed	Thu	Fri	Sat
1	2	3	4	5	6	7
8	9	10	11	12	13	14
15	16	17	18	19	20	21
22	23	24	25	26	27	28
29	30	31				

Accesso Ricercatori (registrazioni e modulistica)
Accesso Uffici Ricerca

Si rammenta che la scadenza amministrativa del Prin 2006 è il 9 febbraio 2009 e che sono disponibili in rete i modelli per la compilazione del consuntivo la cui scadenza è fissata al:

- 31 marzo 2009 ore 24.00 per i modelli D
- 24 marzo 2009 per i modelli C

Si comunica che, in sede di compilazione del relativo rendiconto finanziario sarà consentito, per ogni singola voce, fermo restando l'importo totale assegnato, uno scostamento rispetto all'ultima rimodulazione accettata, non superiore al 3% e comunque fino ad un massimo di Euro 500. Si precisa inoltre che il recupero delle somme non spese risultanti dalla predetta rendicontazione sarà operato solo per importi superiori a 100 Euro.

Impegni di spesa
Si rammenta che è possibile impegnare entro e non oltre la data scadenza del progetto

MIUR
Ministero dell'Istruzione, dell'Università e della Ricerca

Sito individuale doce

Username:
Password:

Per ottenere lo username e la password via mail è necessario effettuare la registrazione.

Per informazioni e commenti
Telefono: **051 - 6171454**
Email: gaia@caspcasur@ciencia.it

MIUR - Ministero dell'Istruzione, dell'Università e della Ricerca



Si, è possibile.

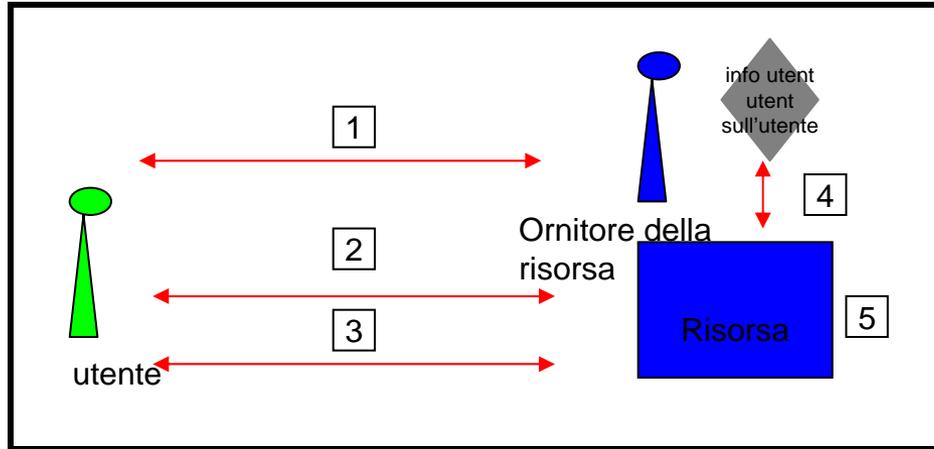
Nelle nostre organizzazioni e nelle comunità a cui esse appartengono. **“Yes, we can”**.

Come?

Razionalizzando le proprie infrastrutture di autenticazione e autorizzazione e partecipando ad una Federazione AAI

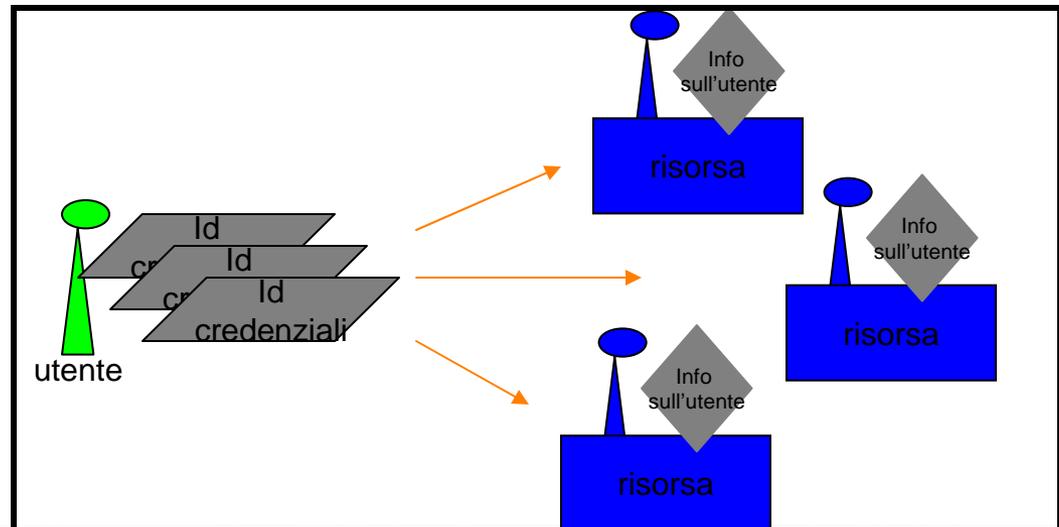


Accesso ad una risorsa



Autenticazione è il processo che verifica l'*identità* ovvero risponde alla domanda: "l'utente è chi dice di essere?"

Autorizzazione è il processo che consente l'accesso alle risorse solamente a coloro che hanno i *diritti* di usarle

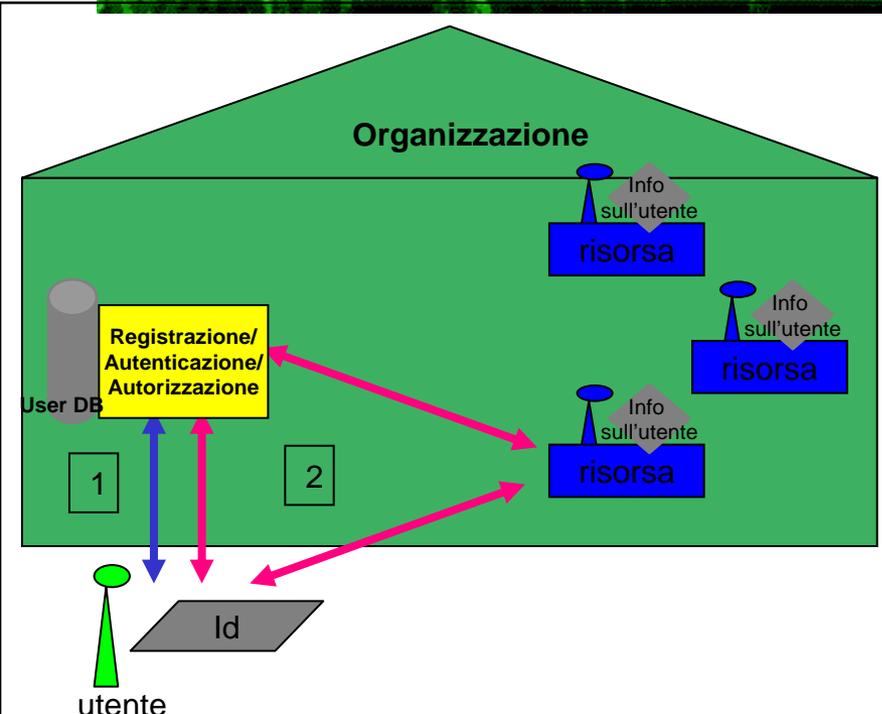


Problematiche

- ◆ Gli utenti sono frustrati dal ricordare molti codici d'accesso
- ◆ L'utente fornisce dati personali in diversi siti
- ◆ Aumenta il rischio potenziale di furto e scambio non autorizzato delle credenziali
- ◆ I dati dell'utente ed il lavoro della loro gestione sono duplicati

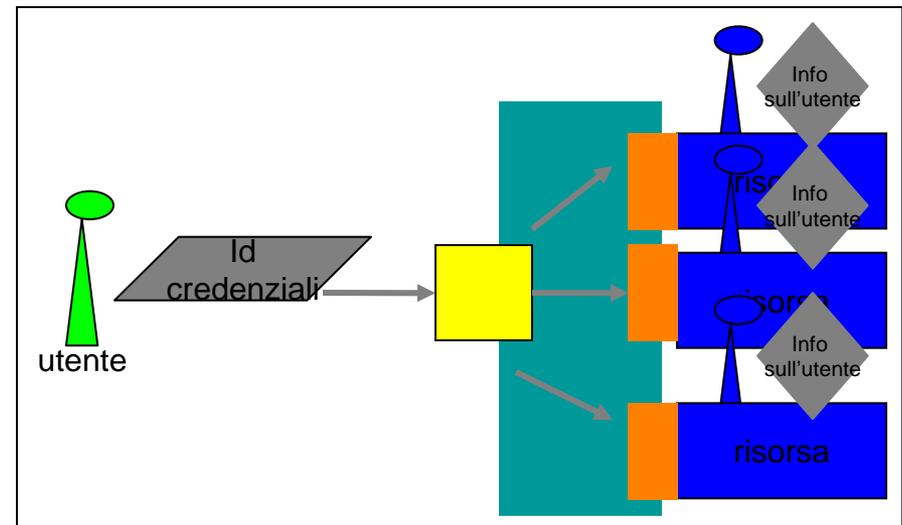


IdM/IAM



Identità digitale - Insieme delle caratteristiche essenziali e uniche di un soggetto che sono in grado di identificarlo

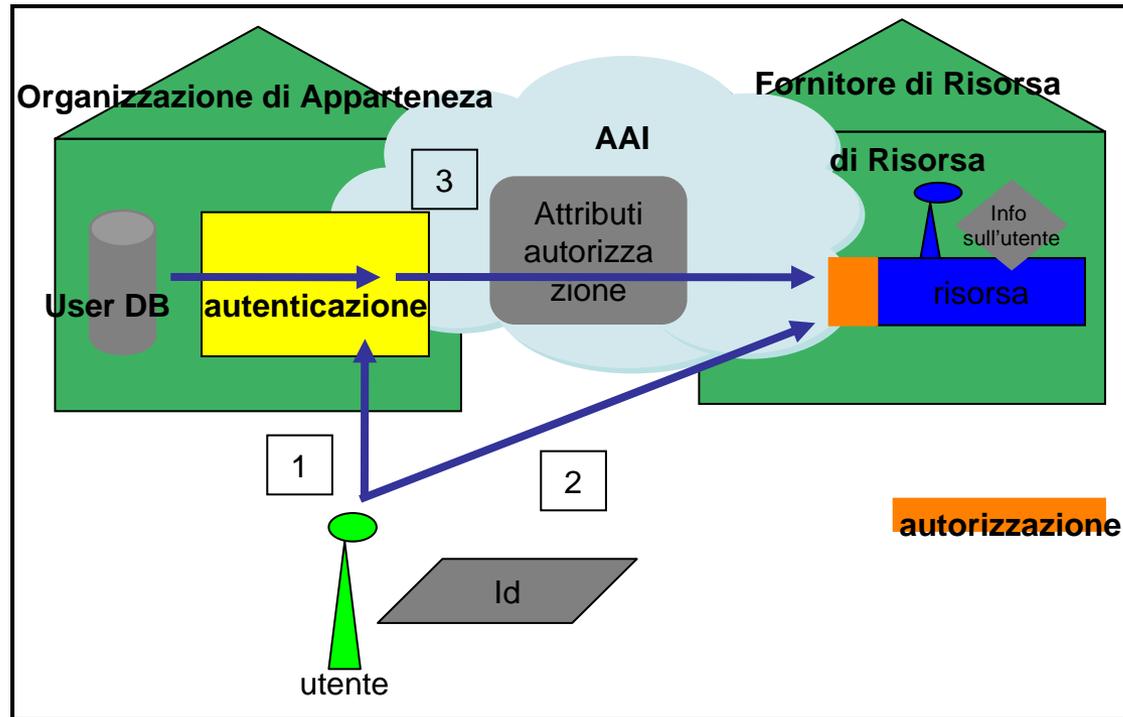
Attributi - elementi che esprimono le caratteristiche di un identità



IdM = Identity Management
IAM = Identity & Access Management



Accesso federato ad una risorsa



La Federazione AAI



La **Federazione** è un accordo, tra organizzazioni e fornitori di risorse, con il quale i partecipanti decidono di fidarsi reciprocamente, delle informazioni che si scambiano nei processi di AA, sulla base di regole e linee di condotta stabilite per gestire le relazioni di fiducia.

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



La Federazione AAI: privacy



- ◆ Le informazioni scambiate, tra fornitore di identità e fornitore di risorsa, non riguardano i dati dell'autenticazione ma solo gli attributi, per i quali c'è stato già un accordo, che servono ad assegnare il diritto di accesso alla risorsa.
- ◆ I fornitori di risorse devono fidarsi della dichiarazione dell'organizzazione di appartenenza sull'identità dell'utente.
- ◆ Le organizzazioni di appartenenza devono accordarsi sulla rappresentazione delle identità (schema degli attributi)



Vantaggi: utente

- ◆ Riduzione del numero di credenziali da ricordare
- ◆ Utilizzo delle credenziali ufficiali della propria organizzazione
- ◆ Maggior sicurezza sulla privacy e maggior controllo sui propri dati personali
- ◆ Scambio informazioni e contenuti tra i “soci” più facile
- ◆ Accesso alle risorse online con un’unica password ed un unico metodo



Vantaggi: Organizzazione dell'utente

- ◆ Policy e procedure si applicano e si modificano in un solo punto
- ◆ Maggior controllo dei processi di autenticazione e autorizzazione
- ◆ Economia di scala nell'implementazione e gestione di nuovi e vecchi servizi
- ◆ Utenti più soddisfatti ==> “ritorno di immagine”
- ◆ Meno richieste all'help desk
- ◆ Maggiore aderenza ai requisiti di legge sulla gestione, conservazione e protezione dei dati personali



Vantaggi: fornitore di risorse

- ◆ Riduzione del carico amministrativo per la gestione di identità e credenziali
- ◆ Maggiore flessibilità di autorizzazione (istituzione, ruolo etc...)
- ◆ Bacino d'utenza



Ancora vantaggi per tutti



- ◆ Informazioni aggiornate ed affidabili
- ◆ Miglioramento della sicurezza dei dati e dei sistemi

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



Nel mondo



TECNOLOGIA	PAESE	NOME
Shibboleth	Svizzera	SWITCHaai
	Regno Unito	UK Federation
	Germania	DFN-AAI
	Francia	CRU Federation
	Finlandia	HAKA
	Australia	AAF
	USA	InCommon
PAPI	Spagna	PAPI
A-select	Olanda	A-SELECT

<https://refeds.terena.org/index.php/Federations>

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



Shibboleth



- ◆ E' la tecnologia scelta per la Federazione Pilota IDEM
- ◆ E' un package opensource per il SSO federato e non, basato su standard SAML, nato da un progetto di Internet2
- ◆ Per Shibboleth:
 - ◆ Un Organizzazione di Appartenenza fornisce identità e gestisce un servizio di Identity Provider (IdP)
 - ◆ Un Fornitore di Risorse gestisce un servizio di Service Provider (SP)
 - ◆ All'interno della Federazione esiste un servizio di discovery chiamato Where Are You From (WAYF)



Progetto Pilota IDEM



Kick-start: 2/04/2007

Durata: 1 anno (2008)

Coordinamento: GARR e CdG

Tecnologia: Shibboleth

Organizzazioni: invitate 29 - hanno risposto: 27 - hanno finalizzato: 21

Identity Provider: 21 per un totale di ca. 700.000 utenti

Risorse: 8 + 1test SP + 2 solo in test

Operatività: 30/6/2008-31/12/2008

<http://idem.garr.it> ==> <http://progettoIDEM.garr.it>

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



Risultati



- ◆ Abbiamo raccolto specifiche e risultati del progetto in un report che verrà pubblicato a breve
 - ◆ Abbiamo acquisito esperienza utile a predisporre l'infrastruttura tecnico-amministrativa per avviare la Federazione di produzione
 - ◆ Abbiamo dimostrato la fattibilità, l'operatività, l'utilità e l'usabilità di una federazione AAI.
- La Federazione Pilota IDEM ne è la prova.



Domande



Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata



Grazie

Primo Convegno IDEM

Roma, 30-31 marzo 2009

Dalle password all'identità digitale federata

