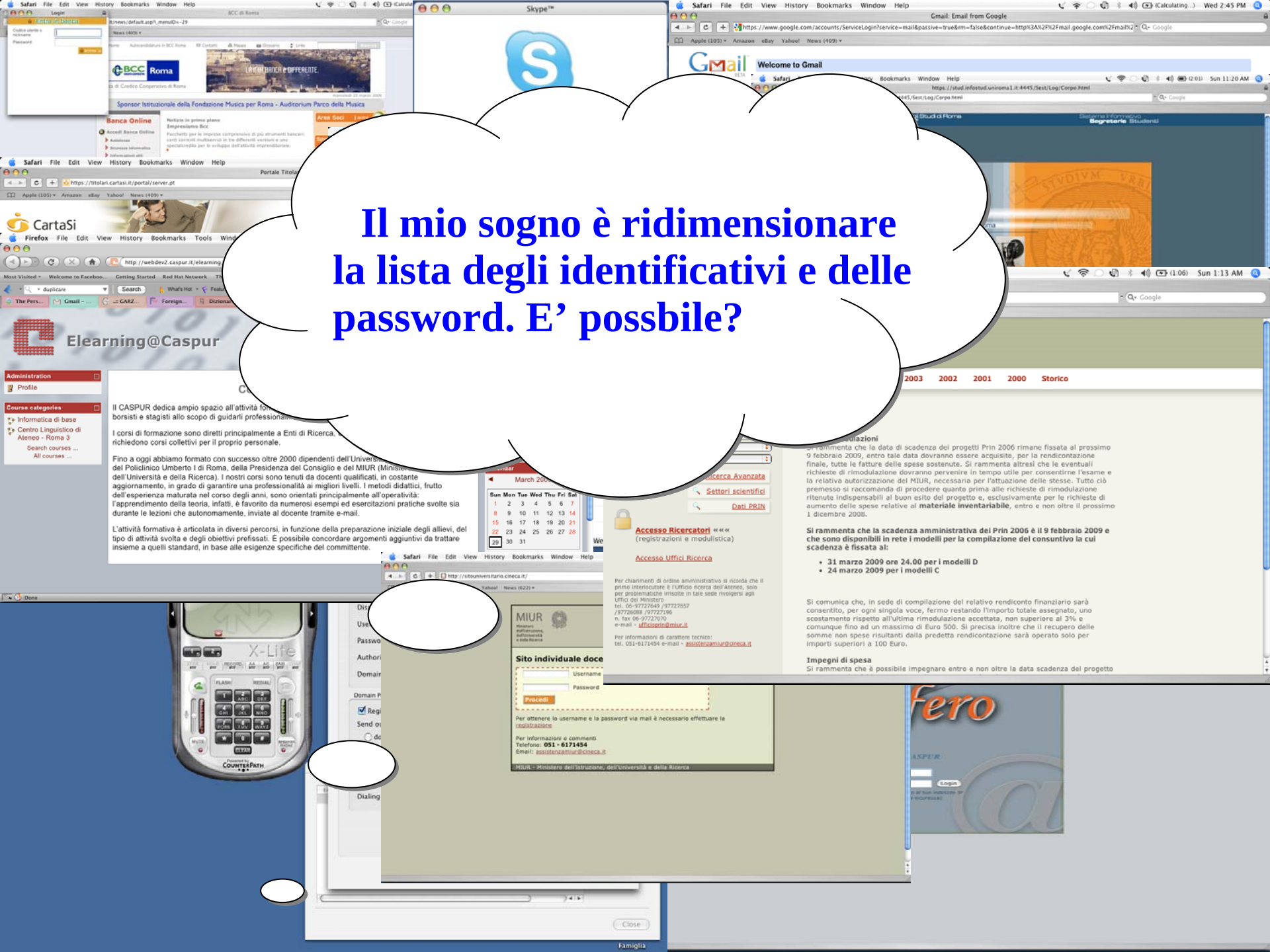
Primo Convegno IDEM
Roma, 30-31 marzo 2009
Dalle password all'identità digitale federata

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' possbile?

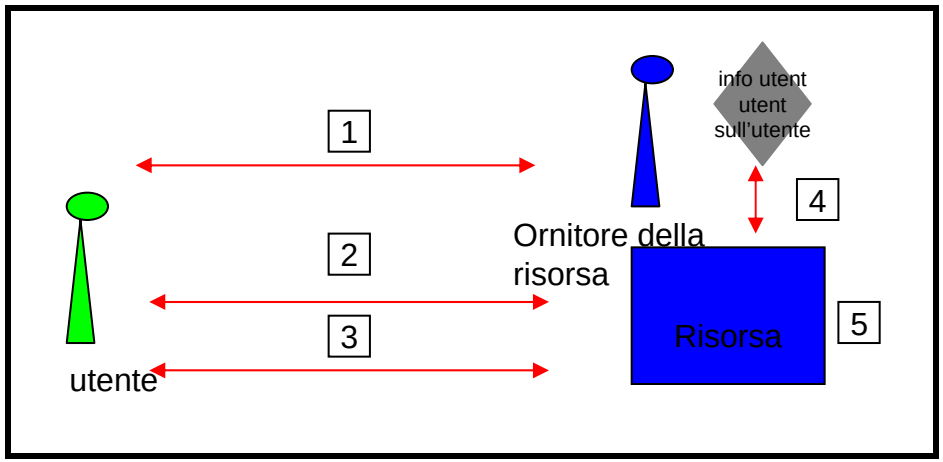
Si, è possibile.

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

Come?

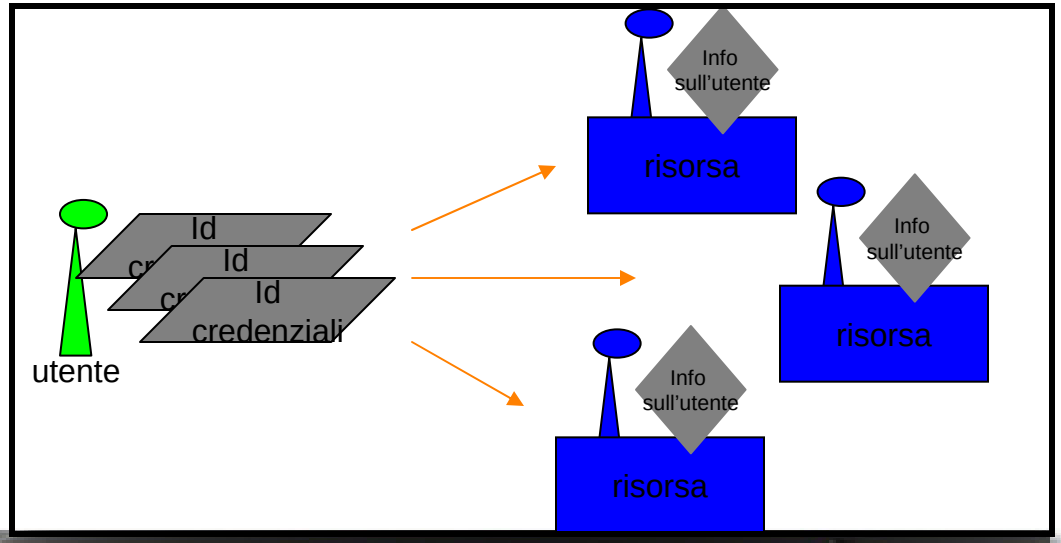
Razionalizzando le proprie infrastrutture di autenticazione e autorizzazione e partecipando ad una Federazione AAI

Accesso ad una risorsa



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

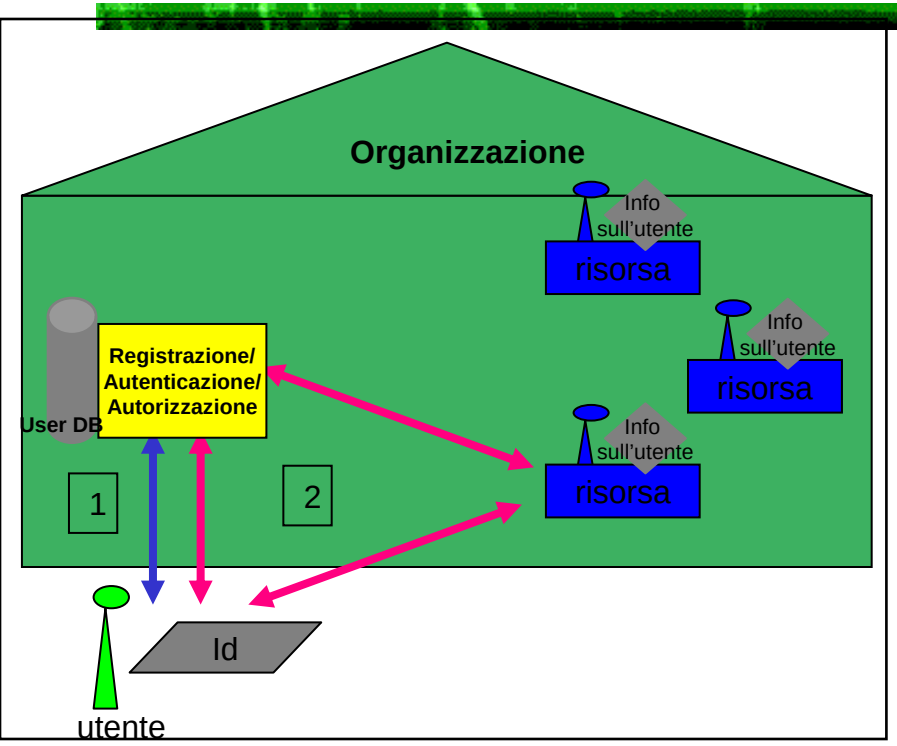
Autorizzazione è il processo che consente l'accesso alle risorse solamente a coloro che hanno i *diritti* di usarle



Problematiche

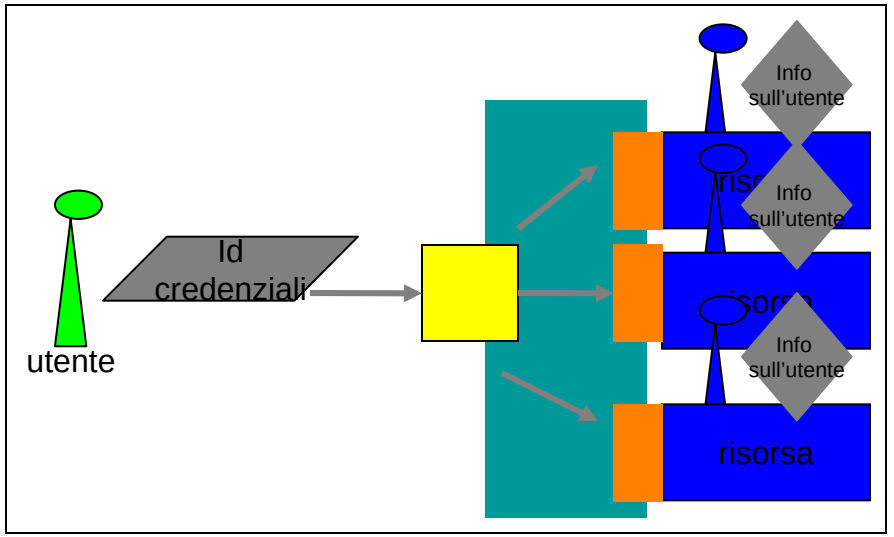
- Gli utenti sono frustati dal ricordare molti codici d'accesso
- L'utente fornisce dati personali in diversi siti
- Aumenta il rischio potenziale di furto e scambio non autorizzato delle credenziali
- I dati dell'utente ed il lavoro della loro gestione sono duplicati

IdM/IAM



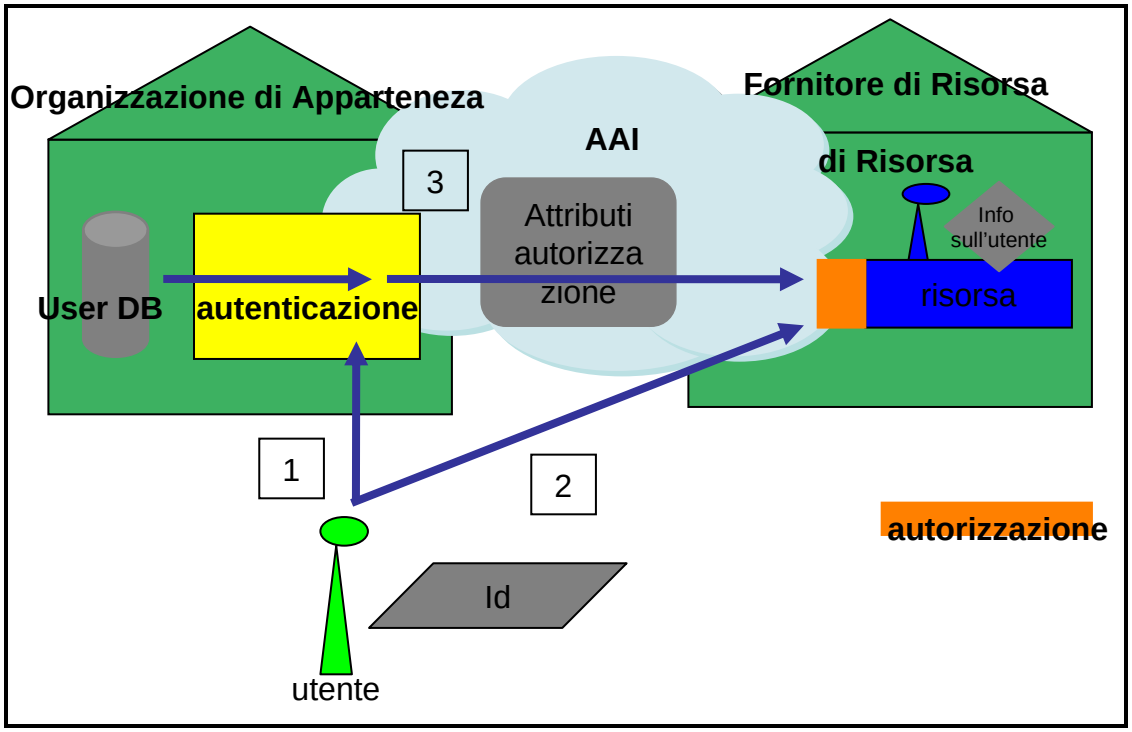
Identità digitale - Insieme delle caratteristiche essenziali e uniche di un soggetto che sono in grado di identificarlo

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.

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

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

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

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

?

Grazie