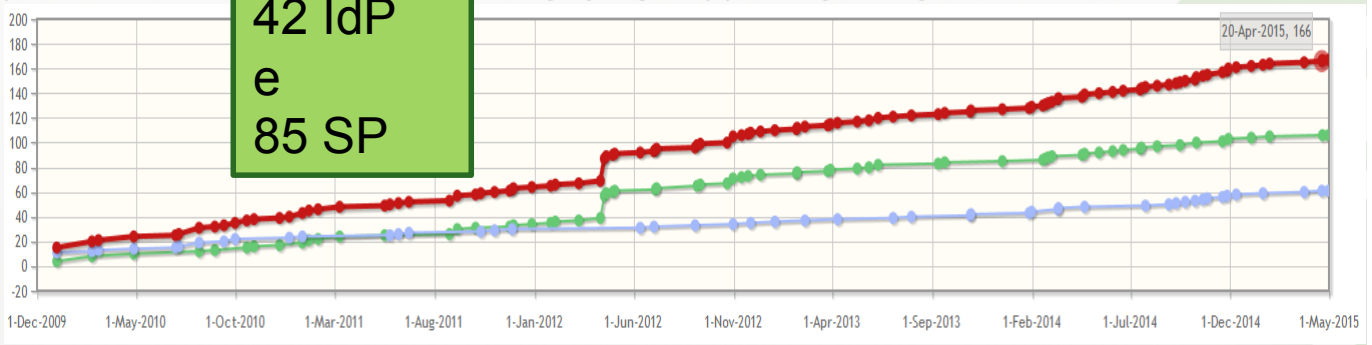
10 anni di infrastrutture di autenticazione e autorizzazione

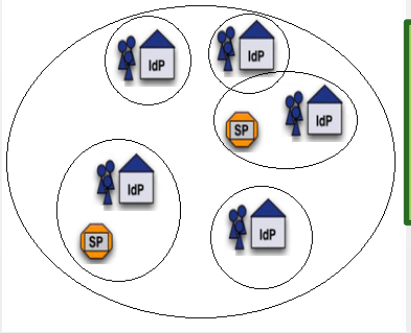
- 2005-2006
  a chi interessa

- 2009-2013
  Federazione IDEM

42 IdP
e
85 SP

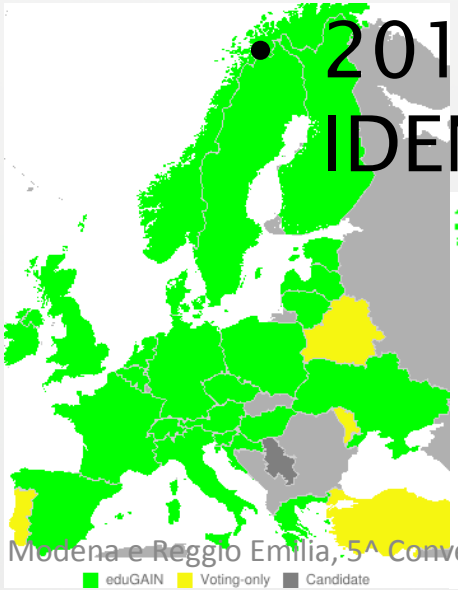


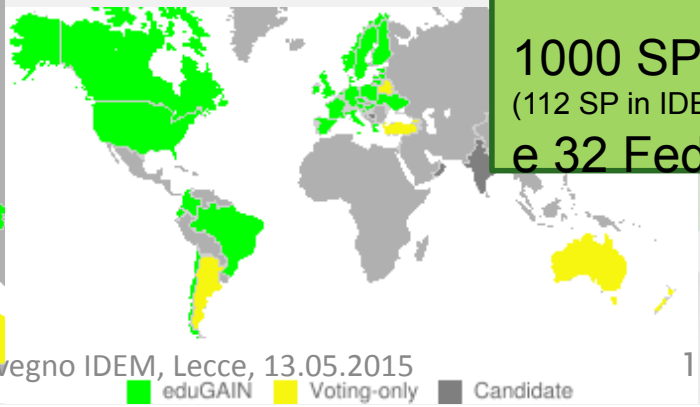
- 2007-2008
  Progetto IDEM



20 IdP
e
10 SP

- 2014-2015
  IDEM + eduGAIN

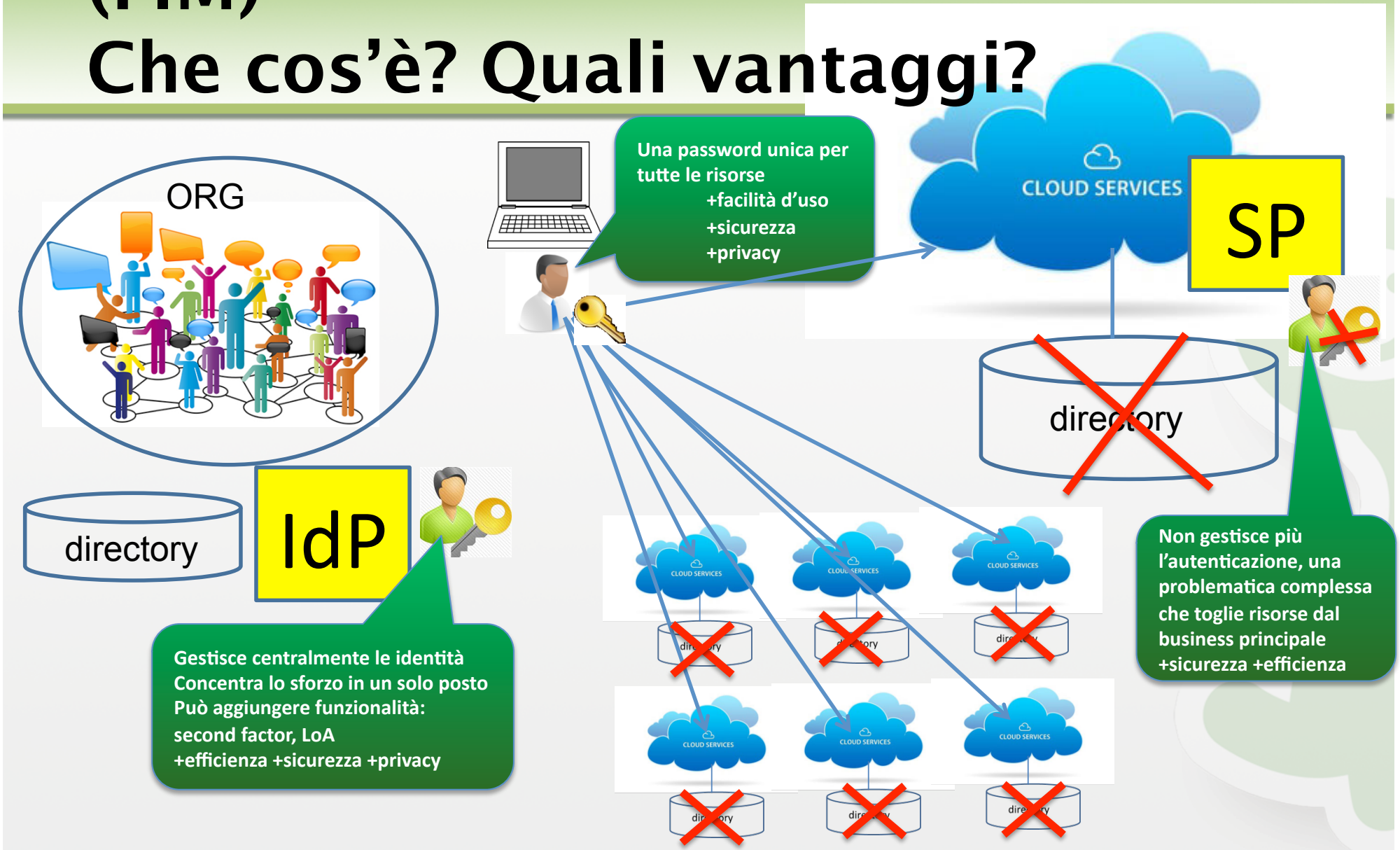




61 IdP
1200 IdP in eduGAIN

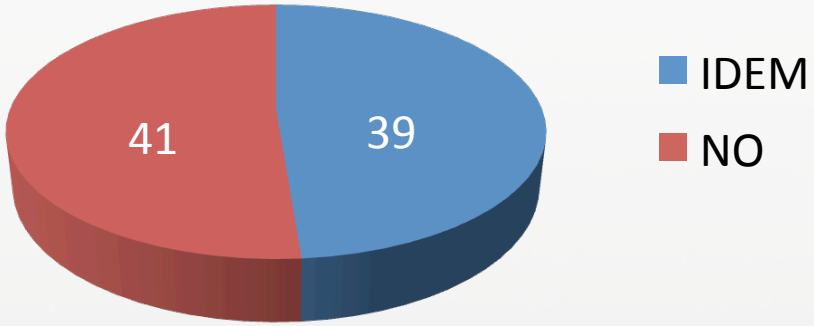
1000 SP
(112 SP in IDEM)
e 32 Fed

Gestione Federata di Identità (FIM)
Che cos'è? Quali vantaggi?

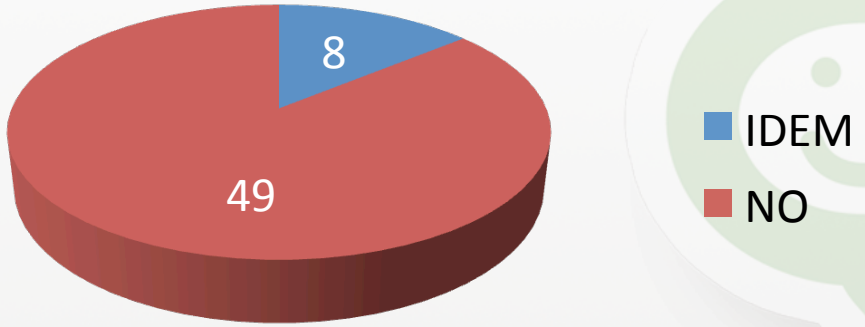


Adesione a IDEM con IdP da Organizzazioni R&E inferiore al 50%

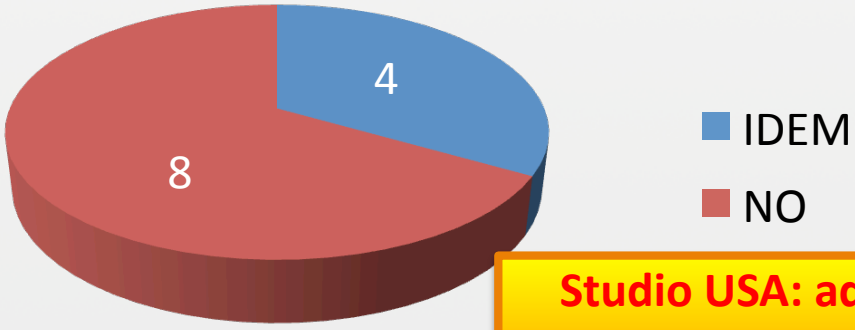
Università



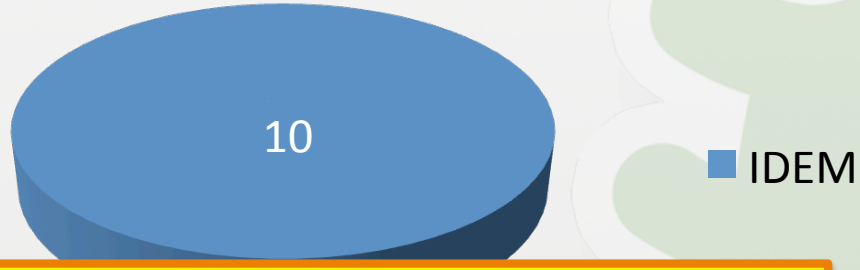
IRCCS+IZS



Enti di ricerca MIUR



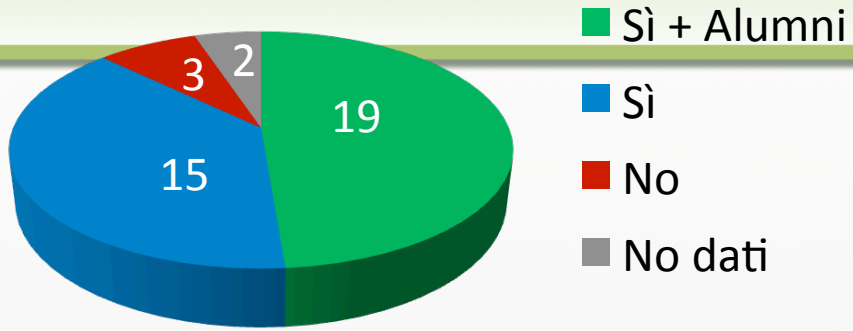
Altri



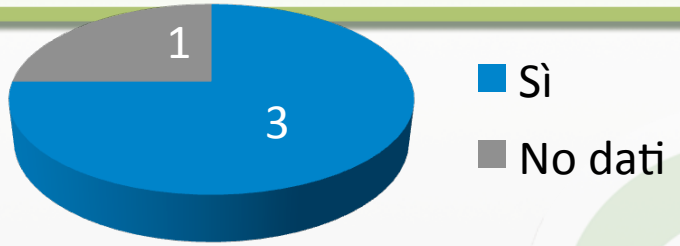
Studio USA: adoption of federated identity management systems has been slow

L'IdP gestisce tutte le identità?

Università in IDEM

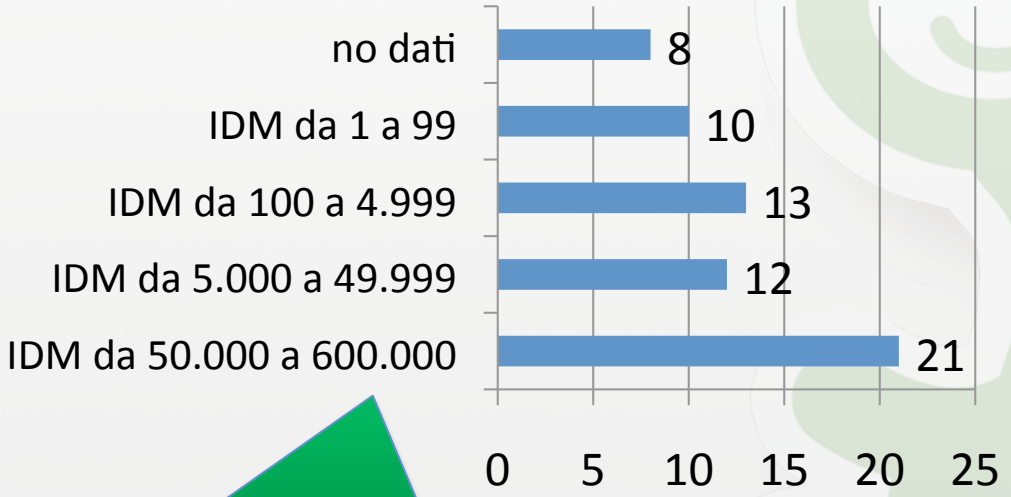


Enti di Ricerca MIUR in IDEM



IDENTITÀ DIGITALI in IDEM TOTALI

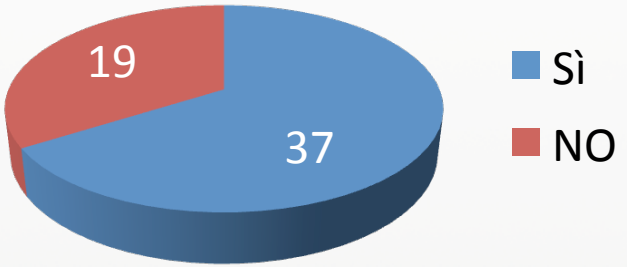
4.004.745 identità digitali	1.660.212 Member
1.575.188 Student	144.715 Staff
1.267.810 Alumni	896.284 Senza affiliazione



Una volta decisa l'adesione, l'IdP viene popolato
È anche un requisito di IDEM

Utilizzo dell'IdP: poco SSO?

L'IDP autentica servizi interni (locali) all'Organizzazione?



Numero LOGIN/mese
in totale circa 13.202.627

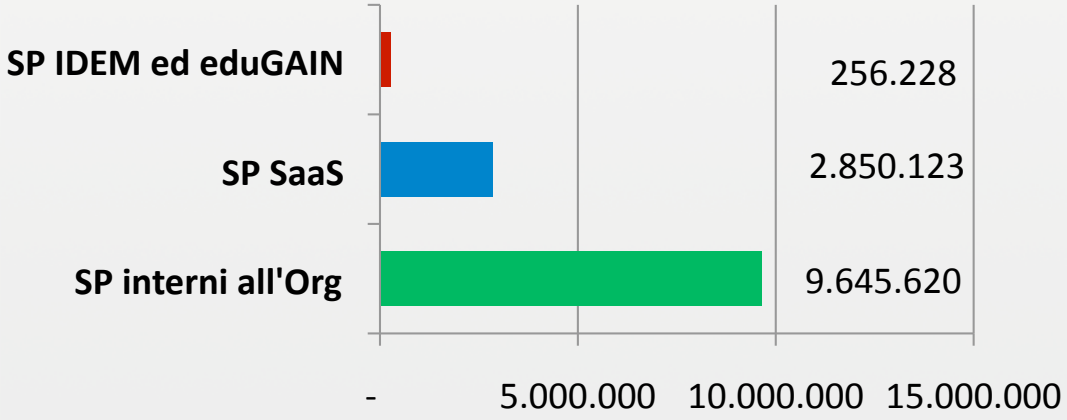
N.Login interni per mese/Member		
Organizz	Orgs.	Freq. %
> 50	2	**4%**
5 - 50	7	**13%**
1 - 5	5	**9%**
0,01 - 1	13	24%
0	21	38%
na	7	13%

26%

N.Login SaaS per mese/Member		
Risposte	Orgs.	Freq. %
> 5	5	**9%**
1 - 5	6	**11%**
0,01 - 1	7	13%
0	37	67%

20%

Numero LOGIN verso:



N.Login IDEM per mese/Member		
Risposte	Orgs.	Freq. %
> 1	3	**5%**
0,1 - 1	9	**16%**
< 0,1	39	71%
na	4	7%

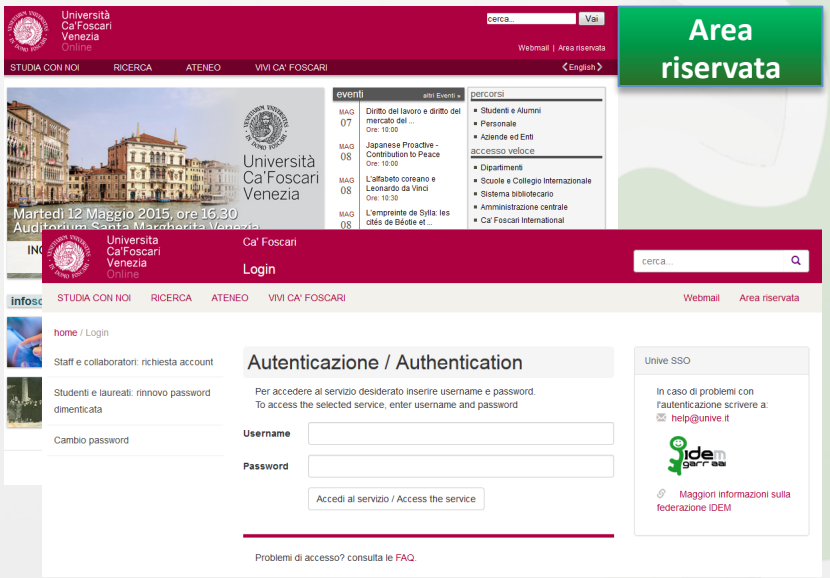
21%

TOP FIVE!

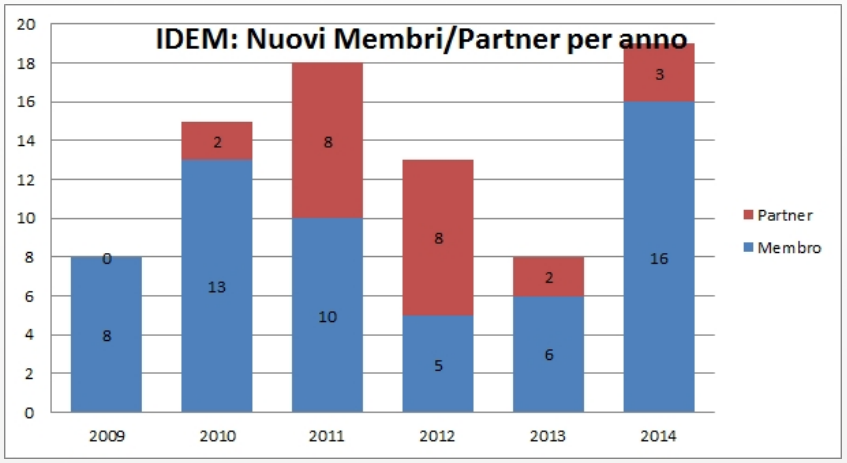
Sede dell'IDP	N.Login interni per mese/Member
Università Bocconi	113,16
Politecnico di Milano	60,64
Università "CA' Foscari" Venezia	13,60
Università degli Studi di Padova	12,32
Università degli Studi di Trento	11,02

Sede dell'IDP	N.Login SaaS per mese/Member
Università degli Studi di Trento	10,34
Politecnico di Milano	10,04
Università degli Studi di Parma	6,55
Università degli Studi di Milano-Bicocca	6,50
Università degli Studi di Padova	6,06

Sede dell'IDP	N.Login IDEM per mese/Member
Università "CA' Foscari" Venezia	4,15
Università degli Studi di Milano-Bicocca	0,23
Università degli Studi di Torino	0,15
Università degli Studi di Parma	0,09
Università degli studi del Piemonte Orientale	0,09
Università degli Studi di Trieste	0,09



Incrementi 2014-2015 e Proiezioni



	identità digitali	login/mese	login risorse IDEM/mese
2014	2.962.940	8.304.335	87.105
2015	4.004.745	13.202.627	256.228
incremento	**35%**	**59%**	**194%**

Potenziale numeri ID Federazione IDEM

- Potenziale ID Member 2.500.000
- Potenziale ID Alumni 5.500.000 – 7.500.000

	login/mese	login risorse IDEM/mese
top 11 (su 56)	12.730.887	238.354
	96%	93%
proiezione attuali membri IDEM	42.822.074	801.736
potenziale Federazione IDEM	85.644.149	1.603.472

IDEM: Successo o …?

ELEMENTI POSITIVI	ELEMENTI NEGATIVI
4 MILIONI DI IDENTITÀ DIGITALI ASSEGNATE	ADESIONI TOT < 50% DEL POTENZIALE
IDP POPOLATI CON TUTTE LE IDENTITÀ	POCO UTILIZZO SINGLE SIGN ON
BEST SCORE INCREMENTO MEMBRI 2014	
ACCESSO A RISORSE IDEM QUADRUPLICATO	

CAUSE	
CONCORRENZA DI ALTRO SSO (ADFS, CAS, Altro)	RETICENZA FORNITORI ESTERNI
ORGANI DI GOVERNO NON SENSIBILI	COSTO INTEGRAZONE SP
	RISCHIO DISSERVIZIO/RESPONSABILITÀ

CRITICITÀ SUPERABILI-SUPERATE	
SINGLE LOGOUT (IN SHIB 3)	POCHE RISORSE BIBLIOGRAFICHE -> MOLTE
ALTA AFFIDABILITÀ (IN SHIB 3)	FORMAZIONE (LEGACY, NON-WEB)
FACILITÀ AGGIORNAMENTO (IN SHIB 3)	

Gestione Federata di Identità (FIM)
Quali cause dell'adozione lenta?

Management delle organizzazioni poco sensibile alla tutela della privacy delle ID di personale/studenti

Domanda: L'IDP ha attivato un meccanismo per chiedere il consenso all'utente riguardo la trasmissione degli attributi?

Risposta	Freq.	Freq. %
No	37	67%
Sì, uApprove	17	31%
Sì, altro	2	4%

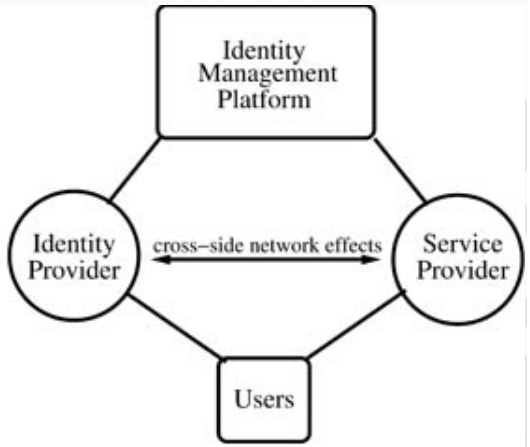
Motivazione risposta No	
si sta pianificando	7
mancanza risorse	7
non necessario	8

È riconosciuto che la richiesta di soddisfare la normativa Privacy è uno dei fattori trainanti per la realizzazione dell'IdP

In Germania l'attenzione alla privacy degli utenti è altissima e il numero degli IdP nella Federazione DFN-AAI è 188!

Logica vincente in un sistema economico a 2 facce *(two-side market)*

- Gestire centralmente le identità:
  - è più economico,
  - dà più potere di controllo,
  - dà gli strumenti per fare rispettare la legge privacy,
  - dà un servizio migliore agli utenti
- Ma chi vince e chi perde dentro l'organizzazione?
  - Il management dell'organizzazione è consapevole e di conseguenza dà incentivi per la realizzazione?
- Le 10-15 organizzazioni più virtuose possono aiutare le altre R&E a fare sistema?
  - Per quale vantaggio? In un contesto federato, un maggior numero di IdP è più incisivo nel richiedere ai SP l'adeguamento
- I SP non devono essere penalizzati, devono beneficiare anche loro



Conclusioni Landau-Moore

Fattori di successo

- Ogni caso d'uso ha il suo
- Non è mai la tecnologia

Quando gli incentivi delle parti interessate (IdP e SP) controbilanciano le contese, allora il sistema di gestione delle identità federato (FIM) ha possibilità di successo. Quando prevalgono le contese, allora il fallimento del FIM è più probabile.

Fattori di contesa

- Sempre gli stessi
- 4 fattori economici:
  1. Chi guadagna nel collezionare i dati personali?
  2. Chi definisce le regole per l'autenticazione?
  3. Chi ha la responsabilità quando le cose vanno male?
  4. Chi guadagna e chi perde dall'interoperabilità?

1. Chi guadagna nel collezionare i dati personali?

- Il fatto che le parti (IdP e SP) possano accedere ai dati personali può essere determinante per il successo di FIM
- La legge garantisce esplicitamente all'utente il controllo sui propri dati personali (EU, FERPA, NSTIC)
- Le aziende private fanno meno attenzione alla privacy ma dovrebbero stare più attente
- Principio di necessità del trattamento: SP dovrebbe trattare solo i dati personali necessari ad erogare il servizio
- IdP e SP, grazie alla tecnologia SAML possono aiutarsi a vicenda nel soddisfare i requisiti di legge.

2. Chi definisce le regole per l'autenticazione?

- Giocare il ruolo di IdP significa dettare le regole dell'autenticazione
- Gli IdP hanno il vantaggio della prima mossa e possono guadagnare più alte quote mercato abbassando la robustezza dei sistemi di autenticazione
- Una volta che il sistema è radicato i costi di migrazione ad un LoA maggiore possono essere alti e l'IdP potrebbe essere tentato di cambiare le regole per allontanare la responsabilità di disservizio
- Gli SP potrebbero non essere contenti di livelli di sicurezza troppo bassi e potrebbero volere LoA più alti

3. Chi ha la responsabilità quando le cose vanno male?

- Se l'IdP che deve autenticare l'utente non è disponibile , questo causa anche problemi di affidabilità all'SP: un utente che ha diritto di accesso non riesce ad entrare
- Se l'IdP sbaglia a fare l'autenticazione (tipicamente problemi di sicurezza) anche un utente non autorizzato potrebbe accedere al SP
- Il livello di rischio accettabile dal SP è importante. Quanto costa al SP un errore di autenticazione da parte dell'IdP?

4. Chi guadagna e chi perde dall'interoperabilità?

- Interoperabilità può essere dannosa per il SP se questo deve trattare dati molto riservati
- Interoperabilità può essere poco importante per il SP se il numero di utenti che si guadagnerebbero è irrisorio

Conclusione

- Solo nei casi in cui IdP e SP raggiungono un equilibrio in ciascuna di queste 4 contese, ed entrambe le parti ci guadagnano, allora il sistema FIM può avere probabilità di successo.
- Al contrario qualcuno potrebbe non vedere incentivi per partecipare
- Un utente guadagna attraverso la facilità d'uso, l'accesso a molteplici servizi, maggiore privacy, sicurezza incrementata.
- Il SP guadagna acquisendo più dati utente, raggiungendo una fetta più larga di mercato, eliminando la responsabilità per gli errori di autenticazione.
- L'IdP guadagna dal controllo sui dati utente

Complessivamente tutte le parti devono guadagnare

Caso d'uso EDITORI: può diventare un successo anche in Italia e in Europa

- Ha portato al successo le federazioni in USA e UK
  - Tecnologia SAML ha messo al centro la privacy
  - Bibliotecari hanno considerato la privacy come parte della mission della biblioteca
- Ha superato le criticità dell'autenticazione per IP
  - Auth IP = No controllo, errori, no mobilità
- Gli editori hanno visto vantaggi anche per loro nell'avere un riconoscimento puntuale dell'utente
- Tutte le risorse (a parte quelle italiane – serve massa critica)
- Statistiche e Accounting (JUSP)
- Può essere un esempio per le scuole nell'adozione dei libri digitali

InCommon and the National Institutes of Health (NIH): un altro caso di successo

- I ricercatori del NIH spesso collaborano con i ricercatori universitari e dei laboratori nazionali sia in U.S.A. che all'estero.
- NIH si fida di InCommon per l'identificazione nelle organizzazioni partecipanti
- InCommon adotta una identificazione più fine nei dipartimenti delle organizzazioni (se privacy e possibilità di controllo sono importanti per la home organization, allora si accetta di fare + lavoro)
- Il ricercatore si focalizza sulla ricerca e le risorse del laboratorio non vengono impiegate nell'identificazione degli utenti; l'IdP identifica i propri utenti, e gli SP possono fidarsi di tale identificazione

Caso d'uso: eLearning

- Ha portato al successo la federazione Svizzera
- Per IDEM:

Caso d'uso: Portali

Qual è il nostro H2020? (Obiettivi)

- Top Membri IDEM collaborano al superamento del *divide* nell'uso degli IdP -> vantaggio: una maggiore massa critica è più incisiva nel mercato degli SP
- Potenziale della Federazione IDEM da colmare: Nella mia organizzazione come si risponde alle richieste di: Sicurezza, Privacy, Controllo degli utenti, Servizio agli utenti?
- Casi d'uso di nuove Risorse da trovare nella logica economica del *two-side market*, affinché tutti ne abbiano vantaggio.

Ringraziamenti

- Daniele Ripanti, Università Politecnica delle Marche, per la predisposizione e l'elaborazione del sondaggio "Raccolta di informazioni dai Contatti Tecnici degli IDP", 2014 e 2015
- I risultati completi del sondaggio gireranno come slideshow durante i break.

Q&A

Bibliografia

- Federazione IDEM, https://www.idem.garr.it/
- eduGAIN Status, https://technical.edugain.org/
- Risultati del sondaggio “Raccolta di informazioni dai Contatti Tecnici degli IDP”, 2014 e 2015
- S. Landau, T. Moore, Economic tussles in federated identity management, 2012 http://journals.uic.edu/ojs/index.php/fm/article/view/4254/3340#p5