SCIRES-IT
SCIentific RESearch and Information Technology
Ricerca Scientifica e Tecnologie dell'Informazione
Vol 2, Issue 1 (2012), 43-58
e-ISSN 2239-4303, DOI 10.2423/i22394303v2n1p43

IDENTITY AND ACCESS MANAGEMENT E FEDERAZIONE

Virginia Calabritto[*]

[*]CASPUR – Roma, ITALIA

Abstract

La rete telematica è in costante crescita e così i servizi online che, in modo sempre più penetrante, rappresentano un aspetto della nostra quotidianità. I servizi in rete si distinguono in servizi ad accesso libero e servizi ad accesso controllato. Ogni giorno studenti, ricercatori e docenti accedono a contenuti e servizi (risorse[1]) ad accesso controllato con modalità diverse, la più diffusa è l'utilizzo dell'informazione utenza/password, informazione diversa per ciascuna risorsa. Da questo punto di vista l'ampia disponibilità di risorse in rete crea all'utente, ma non solo a lui, diversi problemi, non ultimo quello della memorizzazione di un numero sempre più ampio di coppie utenza/password.

L'articolo è teso ad illustrare, nel dettaglio, scenario e problematiche per passare quindi ad accennare alle tecnologie che possono costituire una soluzione, ovvero, l'Identity Management, il Single Sign On e le federazioni di infrastrutture di autenticazione e autorizzazione e, quindi, a degli esempi tra cui IDEM, la prima federazione italiana di Infrastrutture di Autenticazione e Autorizzazione, che coinvolge gli enti della comunità scientifica ed accademica e i fornitori di servizi.

Keywords

IAM, identità, SSO, beni culturali.

1. Lo scenario

La rete telematica è in costante crescita e così i servizi on line che, in modo sempre più penetrante, rappresentano un aspetto della nostra quotidianità. I servizi in rete si distinguono fra quelli ad accesso libero e quelli ad accesso controllato. Ogni giorno studenti, ricercatori e docenti accedono a contenuti e servizi ad accesso controllato con modalità diverse. Pensiamo ad esempio ai servizi di una biblioteca: dall'ingresso fisico in biblioteca, per il quale generalmente si esibisce un badge, al collegamento in rete da postazione fissa o mediante WiFi, quindi attraverso l'utilizzo di un certificato digitale o di utenza/password; dall'accesso a banche dati bibliografiche al download del full-text di riviste elettroniche; dall'utilizzo dell'OPAC a quello dei discovery tool. Pensiamo poi a servizi più generici come la posta elettronica, le piattaforme collaborative o le piattaforme e-learning utilizzate, a seconda dell'utente, per caricare corsi, svolgere prove o fruire lezioni. Ed infine, come ultimi esempi, ma non certo con minor potenziale in quest'ambito, pensiamo ai sempre più numerosi portali

[1]In rete l'utente trova disponibili contenuti, dati, piattaforme e applicazioni, con il termine risorsa sinteticamente ci si riferisce ad uno di questi servizi e li si distingue dai servizi fornitori e gestori di identità

per la comunità che si occupa dei beni culturali o ai servizi dei musei virtuali (di gestione: prenotazione visite, acquisto biglietti; di collaborazione e promozione: wiki, forum, blog; di informazione e formazione differenziati per tipologia di utente ...).

L'utilizzo delle *risorse* ad accesso controllato, come quelle degli esempi riportati, avviene a seguito di processi di autenticazione e autorizzazione e, a tutt'oggi, le modalità prevalentemente utilizzate sono: l'uso di utenza/password e, nel mondo delle biblioteche digitali, l'uso dell'indirizzo IP. Tali modalità, nei più comuni scenari del momento, presentano limitazioni e problematiche.

Possiamo chiamare la coppia utenza/password: "credenziali"; queste si possono distinguere in "locali", rilasciate dalla piattaforma di una singola risorsa e in "istituzionali", rilasciate dall'organizzazione a cui l'utente appartiene (di seguito: l'Organizzazione). Utilizzare credenziali locali per l'utente significa dover ricordare coppie utenza/password diverse per ogni risorsa cui si ha diritto di accesso, e a ciò si deve aggiungere che, quasi sempre, per ottenere le credenziali è necessario compilare un modulo di registrazione (processo più o meno rapido ed intuitivo); inoltre, nel caso di smarrimento delle credenziali, l'utente deve conoscere le procedure di recupero delle sue credenziali specifiche per ogni risorsa. Con le credenziali istituzionali, nei casi migliori, l'utente è avvantaggiato perché, con le stesse, può accedere a più servizi della propria Organizzazione ricordando una sola coppia utenza/password che deve però continuare a digitare per l'accesso ad altre *risorse*.

L'accesso via indirizzo IP si basa sulla verifica, appunto, dell'indirizzo IP di provenienza della richiesta di accesso; gli indirizzi IP riconosciuti, e quindi autorizzati, sono quelli associati all'Organizzazione dell'utente e comunicati da questa al fornitore della risorsa. Questa modalità, tipicamente, lega l'utente alla postazione di lavoro all'interno della propria Organizzazione.

Con il panorama offerto da queste due modalità di accesso quando l'utente si trova al di fuori della propria Organizzazione e, quindi, utilizza un'altra rete con altri indirizzi IP, egli continuerà a poter usare alcune *risorse*, quelle con accesso tramite credenziali, ma non potrà utilizzare quelle il cui accesso si basa sul riconoscimento dell'indirizzo IP. In questi casi potrà ovviare al problema se la sua Organizzazione offre servizi di proxy o VPN[2], tecnologie che, sostanzialmente, consentono al dispositivo utilizzato (personal computer, tablet, smartphone....) di "presentarsi" alle *risorse* con un indirizzo IP dell'Organizzazione.

[2] Virtual Private Network , rete di telecomunicazioni privata, instaurata tra soggetti che utilizzano un sistema di trasmissione pubblico e condiviso

Utilizzare proxy o VPN implica configurare opportunamente la propria postazione di lavoro, attività non sempre immediata per tutti gli utenti e che richiede ancora una volta l'uso di credenziali.

Questo è uno scenario decisamente disorientante, che richiede conoscenza e consapevolezza da parte dell'utente per capire dove e come poter usare una risorsa e per gestire e custodire le numerose credenziali che possiede.

L'elevato numero di credenziali e la problematica della loro custodia espongono al potenziale rischio di smarrimento, furto e scambio non autorizzato delle credenziali, fattori che oltre ad abbassare il livello di sicurezza dei sistemi aumentano la frustrazione da parte dell'utente. Inoltre, la distribuzione dei dati personali dell'utente, in repository di soggetti diversi, si ripercuote anche sulla privacy e sull'accuratezza dei dati.

Se per l'utente lo scenario è disorientante, per i fornitori di *risorse* e le Organizzazioni il carico di gestione è notevole.

I fornitori di *risorse* devono offrire e sottoporre a manutenzione diverse metodologie di accesso in relazione alle esigenze degli utenti e delle Organizzazioni, nonché gestire credenziali con relativi diritti e profili associati alle policy delle diverse Organizzazioni e alle legislazioni dei diversi Paesi. Inoltre, di grande importanza per particolari gruppi di utenti, come gli operatori delle biblioteche, la possibilità di generare statistiche d'uso dettagliate e affidabili è decisamente limitata non potendo ad esempio utilizzare un'autorizzazione basata sul ruolo dell'utente.

Le Organizzazioni devono gestire credenziali istituzionali e locali, per le *risorse* specifiche, con conseguente duplicazione dei dati e della gestione, per non parlare delle attività legate all'erogazione del servizio di proxy (supporto all'utenza, gestioni di lunghi elenchi degli indirizzi di siti web ai quali il proxy deve consentire l'accesso) e di quelle legate alla gestione delle liste degli indirizzi IP. In questo scenario, per ogni nuova risorsa offerta, deve essere aggiunta un'intera infrastruttura di identificazione, con conseguente replica delle credenziali e gestione della sicurezza su più sistemi.

Una soluzione a queste molteplici problematiche si ottiene consentendo all'utente di utilizzare le medesime credenziali per l'accesso a tutte le *risorse* a cui ha diritto, implementando sistemi di Single Sign On (SSO) e partecipando a federazioni di autenticazione e autorizzazione.

2. La Soluzione

Abbiamo detto che l'accesso ad un servizio online controllato genericamente avviene per effetto dei seguenti passi:

- l'utente si identifica, nei casi più comuni, compilando un modulo presso il fornitore di servizio;
- il fornitore registra l'utente e gli fornisce delle credenziali;
- l'utente utilizza le credenziali per accedere al servizio, operazione che passa attraverso l'autenticazione e l'autorizzazione.

L'*autenticazione* è il processo che verifica l'identità ovvero risponde alla domanda: "l'utente è chi dice di essere?"
L'*autorizzazione* è il processo che consente l'accesso alle *risorse* solamente a coloro che hanno i diritti di usarle.
Il *Single Sign On,* traducibile come *autenticazione unica* o *identificazione unica,* consente all'utente di utilizzare le medesime credenziali per accedere a tutte le *risorse* cui ha diritto, autenticandosi una sola volta per sessione di lavoro. Il Single Sign On può estendersi oltre il dominio dell'Organizzazione dell'utente con accordi bilaterali tra gli enti e con la partecipazione a federazioni di autenticazione e autorizzazione, arrivando a consentire all'utente di accedere ad un sempre maggior numero di *risorse*, cui ha diritto, con le medesime credenziali ed un'unica autenticazione per sessione di lavoro. In pratica, con la soluzione qui riportata, si passa dallo scenario descritto ed illustrato in figura 1 allo scenario illustrato in figura 2.

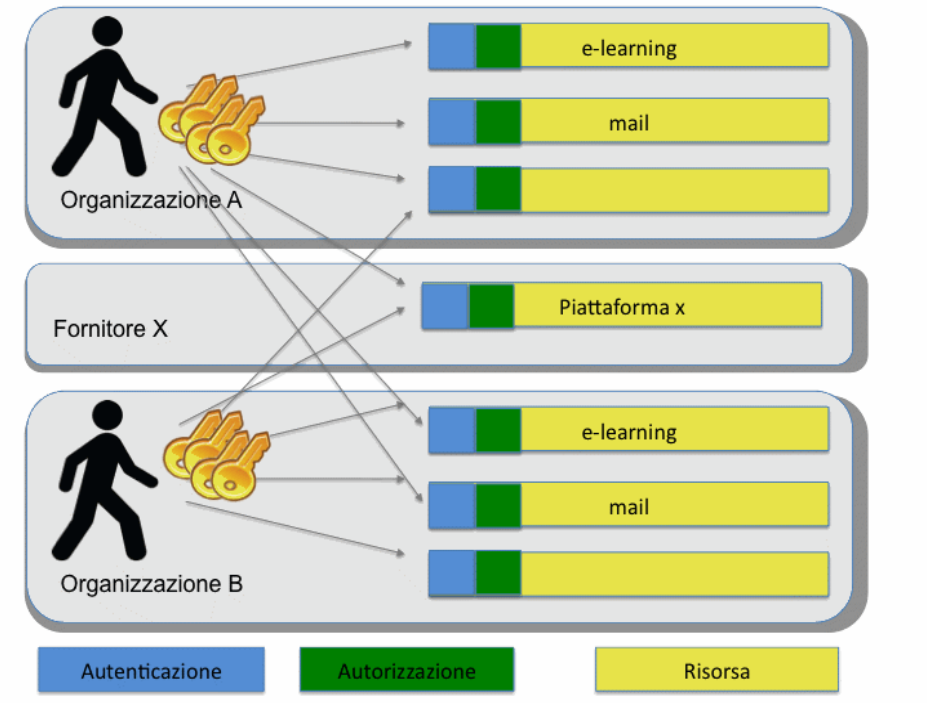

Fig. 1: scenario "a" senza SSO

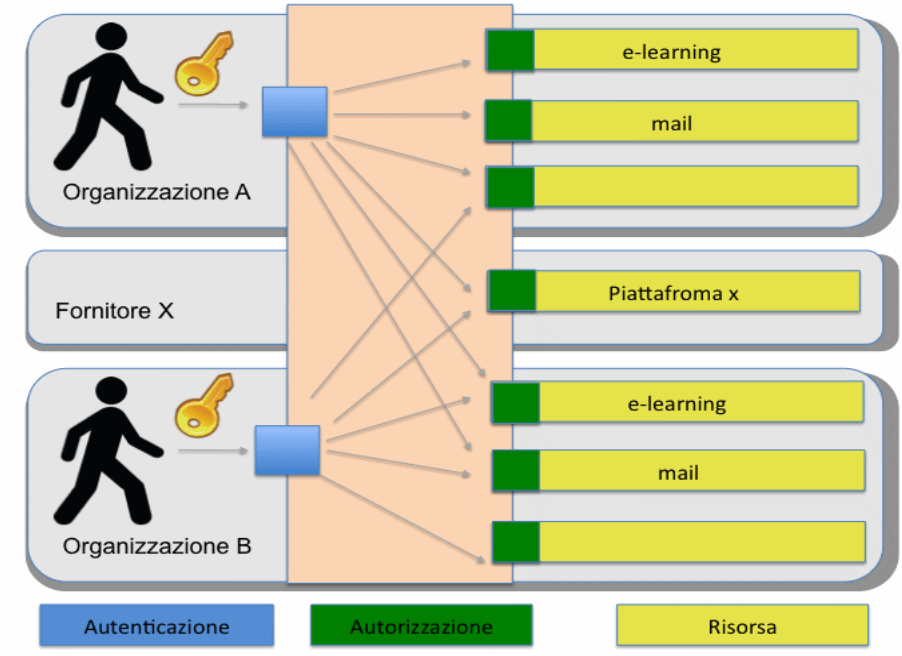

Fig. 2: scenario "b" con SSO

Le figure evidenziano gli elementi base degli scenari: gli *utenti*, le *Organizzazioni*, le *risorse* ed i *Fornitori di risorse*, ruolo svolto, a seconda del caso, da terze parti o dalle Organizzazioni stesse. Dalle illustrazioni notiamo che passando dallo scenario "a" allo

scenario “b”, oltre alla riduzione del numero di credenziali in circolazione, la funzionalità di autenticazione si sposta dalla risorsa all'infrastruttura dell'Organizzazione. I *vantaggi*, che derivano da questo nuovo scenario, sono evidenti:

- l'utente non deve più gestire numerose credenziali, ma utilizza solo quelle istituzionali, che hanno la caratteristica di essere gestite e utilizzate sempre all'interno della propria Organizzazione, soggetto che gode della fiducia dell'utente ed è titolato a trattare i dati dell'utente in sicurezza e nel rispetto della privacy;
- aumenta il livello di sicurezza delle credenziali, per cui l'utente potrà prestare più cura all'uso, alla conservazione ed alla generazione della propria password (sarà meno propenso a cederla a terzi e farà più attenzione a non perderla, essendo questa utilizzata anche per *risorse* più sensibili; non avrà il problema di generare password simili e facilmente memorizzabili);
- i fornitori di *risorse* non hanno più il carico di gestire le credenziali;
- le Organizzazioni hanno un maggior controllo sulle credenziali nonché sulla privacy, sulla sicurezza dei dati e dei sistemi con una notevole riduzione dei relativi costi di gestione.

3. L’identity and access management e le federazione di AAI

In termini un po' più sistematici, per consentire all'utente di accedere a tutte le *risorse* a cui ha diritto, in modo semplice, è necessario che l'Organizzazione disponga di un adeguato sistema di “*Identity and Access Management*” (IAM) ovvero un sistema di gestione delle *identità digitali*[3] e degli accessi che consente a chi ne ha diritto di accedere alle *risorse* dell'organizzazione, in modo semplice e razionale, così da aumentare la produttività ed il livello generale della sicurezza e diminuire i costi di gestione degli utenti.

Con un tale sistema ad ogni persona identificata nell'Organizzazione è assegnata da un'identità digitale descritta da un insieme ben definito di attributi opportunamente valorizzati; l'Organizzazione ha un maggior controllo dei processi di autenticazione, autorizzazione e auditing; pertanto si possono applicare regole di privacy, controllare la sicurezza e fare report; le decisioni di cambiamenti quali diversi privilegi di accesso, nuove

[3] “Insieme delle caratteristiche essenziali ed uniche di un soggetto che permettono di identificarlo” - H. Abelson e L. Lessig

strategie e nuovi servizi possono essere attivati più velocemente, tra questi, l'adozione del Single Sign On e la partecipazioni a federazioni di AAI[4].

Una f*ederazione di AAI* (in seguito Federazione) è un accordo tra Organizzazioni, con il quale i partecipanti decidono di fidarsi reciprocamente delle informazioni che si scambiano su utenti e *risorse*, nei processi di autenticazione e autorizzazione, sulla base di regole e linee di condotta stabilite per gestire le relazioni di fiducia. In sintesi, si costituisce un "circolo di fiducia" in cui i partecipanti concordano il protocollo per lo scambio di informazione nei processi di AA, lo schema degli attributi, i requisiti di partecipazione e funzionamento della federazione. Le organizzazioni aderiscono alle Federazioni partecipando con servizi di gestione di identità (IdP[5]) o con risorse (SP[6]).

Partecipare ad una Federazione consente di:

- facilitare la collaborazione e la mobilità degli utenti;
- fornire più servizi agli utenti;
- facilitare l'accesso a servizi;
- ridurre il numero delle credenziali ed il numero dei relativi moduli richiesta da compilare
- offrire i propri servizi ad altri utenti della federazione;
- diminuire il carico amministrativo generato dagli accordi bilaterali tra IdP e SP;
- ridurre i costi di gestione.

4. Le Federazioni concretamente

Nell'ultimo decennio le Federazioni si sono andate via via diffondendo e, attualmente, in Italia e nel mondo esistono diverse realtà ed esempi sia nel settore della Ricerca e della Formazione che, più in generale, in quello della Pubblica Amministrazione. Numerose sono e sono state le iniziative ed i progetti nazionali ed internazionali in merito alle identità digitali e alle Federazioni, esperienze spesso calate in ambiti più ampi quali sicurezza e mobilità. In questo senso, consistenti sono stati gli interventi previsti, a livello europeo, nel settimo Programma quadro R&S (FP7) e nel Programma quadro per la competitività (CIP), a

[4]Federazione di Infrastrutture di Autenticazione e Autorizzazione (dall'inglese Authentication and Authorization Infrastructure).
[5]Identity Provider
[6]Service Provider

titolo di esempio citiamo il progetto STORK (Secure idenTity acrOss boRders linKed) concluso a giugno 2011, il cui l'obiettivo è stato la realizzazione di un sistema europeo di riconoscimento dell'identità elettronica che potesse operare insieme con quelli nazionali.

Quali esempi di Federazioni nel settore Ricerca e Formazione, in tabella 1, riportiamo, dall'elenco, nella sezione REFEDs[7], del wiki[8] di TERENA[9], quelle attualmente in produzione.

Tabella 1: Federazioni internazionali

PAESE	NOME	Dal
Austria	ACOnet Identity Federation	2008
Australia	Australian Access Federation - AAF	2009
Belgio	Belnet R&E Federation	2010
Brasile	Comunidade Acadêmia Federada - CAFe	2010
Canada	Canadian Access Federation - CAF	--
Svizzera	SWITCHaai	2005
Cina	CERNET Authentication and Resource Sharing Infrastructure - CARSI	2006
Rep. Ceca	eduID.cz	---
Germania	DFN-AAI	2007
Danimarca	WAYF	2008
Spagna	SIR	2008
Finlandia	Haka	2005
Francia	Fédération Éducation-Recherche	2006
Grecia	GRNET	2007
Croazia	AAI@EduHr	--
Ungheria	eduID.hu	2010
Italia	IDEM	2009
Irlanda	Edugate	--
Giappone	GakuNin	2010
Paesi Bassi	SURFnet	2007
Norvegia	FEIDE	2003
Portogallo	RCTSaai	--
Svezia	SWAMID	2007
Slovenia	ArnesAAI Slovenska izobraževalno raziskovalna federacija	2009

[7]Research and Education FEDerations, organizzazione con la mission di dare voce e rappresentare i bisogni delle Federazioni della ricerca e della formazione di tutto il mondo formazione (https://refeds.org)
[8]https://refeds.terena.org/index.php/Federations
[9]Trans-European Research and Education Networking Association (http://www.terena.org)

Regno Unito	UK Access Management Federation for Education and Research	2006
USA	InCommon	--

Un'altra realtà che si va diffondendo sono le cooperazioni tra Federazioni, in Europa KALMAR210 ed eduGAIN11 ne costituiscono due esempi nel settore della Ricerca e Formazione.

KALMAR2 è una confederazione12 alla quale partecipano le Federazioni nazionali dei Paesi scandinavi, della Danimarca e dell'Islanda. EduGAIN, di più recente costituzione, è un'interfederazione13 alla quale, attualmente, partecipano 11 Federazioni nazionali, tra cui IDEM, con un totale di 21 servizi di gestione e verifica delle identità (IdP) e 25 *risorse* (SP). Al momento sono ancora allo studio codici di condotta che possano così consentire completa operatività a IdP ed SP, nel pieno rispetto delle normative europee; anche sul versante tecnico c'è ancora qualche problematica14 da approfondire.

In Italia, nella Pubblica Amministrazione, tra Federazioni, studi e progetti pre e post Codice dell'Amministrazione Digitale (CAD) e Sistema di Connettività Pubblico (D. Lgs.. 82/05), pre e post Sistema Pubblico per la Cooperazione applicativa (SPCoop), "Regole tecniche e di sicurezza per il funzionamento del Sistema Pubblico di Connettività" (DPCM 1-3-08) e "Modello di gestione federata delle identità digitali" (GFID - dicembre 2008), troviamo un certo numero di esperienze, tra le quali citiamo:

- il *progetto PEOPLE*[15], ufficialmente concluso a ottobre 2006, ha portato all'esercizio di una comunità di portali[16] erogatori di servizi di e-government e sopratutto, di grande rilevanza per quanto descritto in questo articolo, ha costruito un circolo fiduciario tra un numeroso gruppo di Comuni italiani; circolo di fiducia basato sul framework SiRAC[17] che implementa un sistema di identità federate indipendente dal gestore dell'identità e dagli schemi di autenticazione;

[10]https://www.kalmar2.org
[11]http://www.edugain.org
[12]Insieme di Federazioni che cooperano, "federazione di Federazioni", con un comune modello di fiducia, standard e policy, definite da un organizzazione di indirizzo, alle quali le Federazioni membre normalmente si allineano;
[13]Insieme di Federazioni che cooperano con un insieme minimo di accordi mantenendo le proprie policy e standard
[14]Ad esempio la normalizzazione dei metadati
[15]http://www.progettopeople.it/ e
[16] Portali della Pubblica Amministrazione per offrire sia servizi per il pubblico che di back-office, la maggior parte dei quali richiedono l'autenticazione dell'utente
[17] Servizi Infrastrutturali di Registrazione, Autenticazione e Comunicazione – http://riuso.cnipa.gov.it/soluzioni/anteprima.bfr?id=368

- il *progetto FedERa*[18] promosso dalla Regione Emilia-Romagna per consentire a cittadini e imprese di disporre di un'autenticazione federata, tramite la quale accedere ai servizi online forniti da tutti gli enti locali dell'Emilia-Romagna. Dal progetto, iniziato nel 2007, è nato il sistema FedERa messo in produzione a gennaio 2010; sistema pensato e sviluppato con il fondamento dell'interoperabilità tra i servizi del progetto PEOPLE e quelli del progetto ICAR[19];
- il *progetto ICAR* realizzato, con il coordinamento del CISIS, dalle Regioni e le Province Autonome fra il 2006 e il 2009, in risposta all'avviso del CNIPA per la selezione di progetti per "lo sviluppo dei servizi infrastrutturali e SPCoop", tra l'altro, ha affrontato il tema dell'identità digitale federata.

L'attività del progetto è stata proseguita da CISIS e da alcune Regioni con la sottoscrizione di un accordo quadro[20]. L'aggiornamento 2010, circa il dispiegamento infrastrutturale, riporta che 3 regioni (Emilia Romagna, Toscana e Campania) avevano già realizzato la Gestione delle Identità Digitali Federate, 18 Regioni intendevano realizzarla e tra queste 10 avrebbero adottato il modello ICAR;

- il servizio di Single Sign On federato tra INPS[21] e INPDAP[22], realizzato secondo il modello di Gestione Federata delle Identità Digitali (GFID)[23]

Nonostante l'attenzione e l'interesse in Italia, l'esperienza Federativa in ambito di Pubblica Amministrazione è ancora limitata e non sono molti i riscontri tangibili per l'utente finale.

[18]Federazione degli Enti dell'Emilia-Romagna per l'Autenticazione
[19]Interoperabilità e Cooperazione Applicativa in rete tra le Regioni
[20]Accordo Quadro di cooperazione interregionale permanente per lo sviluppo delle iniziative volte al potenziamento della società dell'informazione e dell'e-government
[21]Istituto Nazionale di Previdenza Sociale
[22]Istituto Nazionale di Previdenza per i Dipendenti dell'Amministrazione Pubblica
[23]http://www.openspcoop.org/openspcoop_v3//doc/spcoop/SPCoop-ModelloGFID_V1.5.pdf

5. La Federazioni IDEM

IDEM è la prima federazione italiana d'Infrastrutture di Autenticazione e Autorizzazione della comunità degli enti di Ricerca e Formazione.
Sinteticamente:

Nome	IDEM - Identity Management per l'accesso federato
Partecipanti	Organizzazioni - fornitori di servizi di identità o di risorse della comunità GARR[24] (Membri) o esterne alla comunità (Partner)
Operatore	GARR[25]
Protocollo	SAML
Schema attributi[26]	Selezione minimale dagli schemi LDAPv3, eduPerson, SCHAC, descritta nel documento: Specifiche Tecniche Attributi (ST-A)
Regole e requisiti	Descritte nei documenti:Regolamento Federazione IDEM (RFI), Norme di Partecipazione (NdP), Specifiche Tecniche (ST), Accordo di collaborazione, Richiesta di Adesione
Architettura di riferimento	Shibboleth

Fondamento del circolo di fiducia di IDEM è l'assicurazione da parte delle Organizzazioni che forniscono identità che corrispondono a persone reali, ad utenze tracciabili e sono correttamente descritte secondo lo schema condiviso. Inoltre, le organizzazioni che forniscono le *risorse* richiedono ed accettano solo gli attributi giudicati essenziali alla decisione di autorizzazione.
Ad Ottobre 2011, la Federazione IDEM contava[27] un totale di 2.976.105 utenti; attualmente[28] è costituita da 44 Partecipanti[29] di cui 33 Membri e 11 Partner ed ha all'attivo 39 Servizi di gestione e verifica delle identità e 46 *Risorse*[30], tra queste, molte nel settore dell'editoria

[24]http://www.garr.it/a/utenti/comunita-garr
[25]Consortium GARR, associazione senza fini di lucro fondata con il patrocinio del Ministero dell'Istruzione, dell'Università e della Ricerca e con l'obiettivo di gestire e far crescere la rete italiana delle Università e della Ricerca (http://www.garr.it)
[26]Prodotto dello studio delle caratteristiche che accomunano le utenze degli enti della comunità GARR
[27]Statische sono disponibili: https://www.idem.garr.it/it/fatti-e-cifre/raccolta-dati-federazione e https://www.idem.garr.it/it/documenti/doc_details/150-raccolta-dati-federazione-ottobre-2010-pdf
[28]Dati dalla relazione "attività 2011" all'Assemblea dei Membri di IDEM 17.4.2012
[29]Lista completa: https://www.idem.garr.it/en/participants-idem
[30]Lista completa: https://www.idem.garr.it/index.php/en/services/sp

digitale, altre sono captive portal[31] per l'accesso a reti WiFi; ci sono poi FileSender[32], e-Science Gateway[33], blog, wiki e piattaforme e-learning.

6. Nel mondo dei beni culturali

In che modo le Federazioni possono essere utili nel mondo dei beni culturali, una comunità che, tra gli obbiettivi principali, ha quello della diffusione libera e la condivisione del patrimonio culturale tangibile e digitale e che, quindi, non vedrebbe apparentemente la necessità di controllare l'accesso alle *risorse* digitali online?

Come prima cosa occorre ricordare che in questo, come in altri ambiti, servizi ed utenza sono diversificati: si va dal mero amatore di opere, allo studioso, al ricercatore e all'operatore di settore.

Per la prima tipologia di utenti, i portali di Europeana[34] e Google Art Project[35] si prestano a mostrare degli esempi immediati; entrambi consentono agli utenti di accedere ad opere d'arte digitali senza nessun controllo mentre, a seguito di autenticazione, offrono la possibilità di salvare ricerche, creare gallerie personali, annotare e modificare commenti alle proprie selezioni, condividere con altri la propria attività. A questo punto, è evidente che se questi portali o un insieme di portali simili facessero parte di una Federazione, gli utenti di quest'ultima potrebbero utilizzarli avvantaggiandosi delle proprie credenziali istituzionali senza doversene procurare delle altre.

La produzione di materiale per piattaforme simili a quelle appena discusse o la realizzazione stessa di queste piattaforme o la riproduzione e l'elaborazione di dati a livello scientifico richiedono collaborazione fra ricercatori e utilizzo di risorse pregiate quali strumentazioni, applicazioni, risorse di calcolo e di memorizzazione, quasi sempre, necessariamente collegate alla rete. L'accesso a queste risorse, proprio perché pregiate, non può che essere di tipo controllato. Inoltre, nel settore dei beni culturali, la domanda di *risorse* pregiate si unisce alla

[31]Portale web per effettuare l'autenticazione prima di poter accedere alla rete

[32]Applicazione web che permette agli utenti di inviare a qualsiasi destinatario file molto grandi ovviando ai limiti solitamente imposti alla posta elettronica

[33]Insieme di applicazioni e tool sviluppati da una comunità ed integrati attraverso un portale o una suite di applicazioni con un'interfaccia utente grafica configurabile, così da poter rispondere alle esigenze di una specifica comunità

[34]Nato nel 2008, Europeana consente alle persone di esplorae le risorse digitali di musei, biblioteche, archivi e collezioni audio-video d'Europa (33 paesi, 2200 istituzioni, 23 milioni di oggetti) - http://europeana.eu/

[35]Lanciato nel 2011, Google Art Project è una raccolta online di immagini in alta risoluzione (gigapixel, miliardi di pixel) di opere di musei tra i più importanti del mondo (17 musei, 155 collezioni, oltre 32000 opere) - http://www.googleartproject.com

richiesta di alta qualità delle stesse (prestazioni, sicurezza, affidabilità, disponibilità, capacità di conservazione a lungo termine), interoperabilità (tra i differenti dati che descrivono un bene, ad esempio immagini, analisi chimiche, analisi fisiche) e strumenti d'accesso a più livelli. Queste esigenze generalmente trovano risposta in sistemi distribuiti geograficamente (i quali, se opportunamente organizzati, oggi vengono indicati con il nome di e-infrastructure[36]) e nelle Federazioni che offrono un controllo granulare sui diritti di accesso alle *risorse* online.

Nella federazione IDEM è disponibile una *risorsa* che possiamo considerare la sintesi di quanto esposto finora, si tratta dello Science Gateway (piattaforme che usano le e-infrastructure) INDICATE[37], ovvero un portale dove risiede un'applicazione che consente la ricerca semantica negli archivi messi a disposizione dal progetto MICHAEL[38] ed un'applicazione che mette a disposizione tre archivi digitali: il De Roberto DR[39], quello archeologico dell'area del Mediterraneo (MED Repo[40]) e il China Relics DR[41].

Una risorsa cui, al momento, l'utente accede solo dopo i seguenti passi:

- richiesta di registrazione, operazione che richiede all'utente l'immissione di dati disponibili negli IdP;
- conferma della richiesta di registrazione;
- ricezione dell'email di accettazione della registrazione.

Di fatto, un ottimo esempio ma con un'esperienza d'uso, per l'utente, decisamente onerosa, venendo meno alcuni dei vantaggi che una Federazione dovrebbe offrire; da questo punto di vista, si tratta di una risorsa evidentemente ancora in fase sperimentale che richiede ulteriori investimenti.

[36]Infrastruttura digitale, termine utilizzato per indicare un insieme di risorse di calcolo, risorse di memorizzazione e applicazioni interconnessi da reti ad altissima capacità - http://cordis.europa.eu/fp7/ict/e-infrastructure/ - Glossario di e-infrastructure - http://www.dc-net.org/getFile.php?id=366

[37] International Network for a Digital Cultural Heritage e-Infrastructure: progetto - http://www.indicate-project.eu/ ; risorsa - https://indicate-gw.consorzio-cometa.it/

[38]Multilingual Inventory of Cultural Heritage in Europe - http://michael-culture.it

[39]Federico De Roberto Digital Repository, collezione di circa 8000 pagine diditalizzate dello scrittore italiano Federico De Roberto

[40]Digital Repository of the architectural and archaeological heritage in the MEDiterranean area

[41]Digital Repository of cultural heritage Relics on the ancient China

7. Conclusioni

Le Federazioni offrono vantaggi innegabili per utenti finali, fornitori di risorse e fornitori di identità e pertanto la loro diffusione e affermazione va sostenuta, ma all'attuale stato dell'arte, tecnologico e culturale, anche esse non sono indenni da problematiche (ad esempio, non tutte le implementazioni di Single Sign On dispongono di adeguate e sicure funzionalità di logout[42]; il furto di credenziali, in questo ambito, è ancora più rischioso); sarebbe ingenuo e pericoloso non tenerne conto nell'utilizzo e nella promozione delle Federazioni. Inoltre, come in ogni ambito è importante la formazione e l'informazione, quando è in gioco la sicurezza dei dati e delle informazioni. E' poi fondamentali una chiara comprensione di cosa significhi e comporti l'autenticazione Federata allo stato attuale.

L'esigenza di Federazioni e di un unico sistema di identificazione, pur con tutte le problematiche e le sfide che pongono, è reale ed imminente, pertanto è importante non disperdere le energie, raccogliere i feedback da tutte le realtà, fare tesoro delle sperimentazioni più significative, ed imporre un'accelerazione in questa direzione, così da arrivare a dei risultati tangibili per un sempre più cospicuo numero di utenti.

[42]E' importante ricordare che i browser hanno "memoria", non è infrequente avviare un browser in un terminale pubblico ed avere accesso, ad esempio, alla posta elettronica di qualche sconosciuto. Va chiusa l'applicazione (logout) ed il browser.

REFERENCES

ABELSON, H., LESSIG, L. (1998). *Digital Identity in Cyberspace*, Rif.: http://groups.csail.mit.edu/mac/classes/6.805/student-papers/fall98-papers/identity/white-paper.html

BIANCU, B. (2012). *Un(')utente/una password per l'accesso alle risorse e ai servizi online*, Bibliostar 2012, Rif.: https://www.idem.garr.it/it/documenti/doc_download/199-articolo-biancu - https://www.idem.garr.it/it/documenti/doc_download/198-presentazione-biancu

CHONG, F. (2004). *Identity and Access Management*, Rif.: http://msdn.microsoft.com/en-us/library/aa480030.aspx

DAVIES, C. SHREEVE, M. (2007). F*ederated access management: inernational aspects*, Rif.: http://www.jisc.ac.uk/media/documents/themes/accessmanagement/cc253d018-1.0%20international%20aspects.pdf

LINARE, M. (2005). Identity and Access Management Solution, Rif.: http://www.sans.org/reading_room/whitepapers/services/identity-access-management-solution_1640

SANTAMICONE, M. (2010). Museo & Web: il sito internet, la comunicazione online, il museo 2.0, Rif.: http://www.sideshare.net/azel1974/MUSEO-WEB

STROZZI, S. (2008). *Musei online: Gli strumenti 2.0 al servizio del dibattito culturale*, Lavoro di tesi relatore: E. Esposito, Rif: http://www.slideshare.net/fucktory/musei-online-e-web-20 - http://www.lulu.com/shop/simone-strozzi/musei-online-gli-strumenti-20-al-servizio-del-dibattito-culturale/ebook/product-4293235.html