Rosita Ingrosso[1], Marisol Occioni[2], Vincenzo Praturlon[3]

Identità federata e biblioteche: binomio ideale per i servizi per la didattica e la ricerca.

Buone prassi e casi d'uso

Cenni generali e l'esperienza dell'Università del Salento

I servizi digitali, che i Sistemi bibliotecari mettono a disposizione della comunità scientifica di riferimento, in questi ultimi anni sono cresciuti enormemente e di pari passo è cresciuta l'esigenza di migliorare e semplificarne le modalità di accesso.

In quest'ottica alcuni Sistemi bibliotecari hanno sviluppato una collaborazione con IDEM *(*IDEntity Management per l'accesso federato*)* offrendo l'accesso federato ai servizi messi a disposizione.

La Federazione IDEM[4] nasce da un progetto pilota del GARR del 2007 ed è la prima Federazione italiana di infrastrutture di autenticazione e autorizzazione della comunità dell'istruzione e della ricerca.

L'accesso federato si basa sulla 'cooperazione all'interno della federazione' tra un gruppo di istituzioni (*IDentity Provider* -

[1] CTS IDEM-GdL Biblioteche (Coordinatore). Università del Salento, Studium 2000 Via di Valesio, 24 73100 Lecce Italia, Email: rosita.ingrosso@unisalento.it.
[2] CTS IDEM-GdL Biblioteche. Università Ca' Foscari, San Sebastiano, Dorsoduro 1686, 30123 Venezia Italia, Email: occioni@unive.it.
[3] CTS IDEM-GdL Biblioteche. Ufficio coordinamento per le biblioteche, Università degli studi Roma Tre, Via Ostiense 139 00154 Roma Italia, Email: vincenzo.praturlon@uniroma3.it.
[4] Informazioni, sugli enti aderenti e su come aderire ad IDEM , sono disponibili su <https://www.idem.garr.it> (ultimo accesso 26.04.2017).

IDP), che gestiscono le identità dei propri utenti, e i fornitori di contenuti (*Content Provider-CP*) o fornitori di servizi (*Service Provider-SP*) che offrono l'accesso controllato alle loro risorse.

Ad oggi fanno parte di *IDEM* 71 *Identity Providers* e ben 120 *Service Providers*[5].

Solitamente l'accesso ai servizi e alle risorse, soprattutto quelle a pagamento, utilizzate dagli utenti di un'istituzione (studenti, docenti, ricercatori e anche gli stessi bibliotecari) avviene o tramite *username* e *password* oppure tramite il riconoscimento di IP. Ogni utente è quindi costretto a ricordare un certo numero di *username* e *password* oppure può accedere a determinate risorse solo dalla rete di Ateneo.

Con l'accesso federato, invece, l'*Identity Provider* mantiene le informazioni dei propri utenti, cioè gli attributi utente (ad es.: ruolo, affiliazione, nome o identificativo), e scambia alcuni di questi con il *Service Provider* che riconoscerà e abiliterà l'utente all'accesso.

La privacy dei dati dell'utente sarà quindi mantenuta e garantita dall'*Identity Provider* che non li cede a terzi.

Queste caratteristiche rendono importante l'utilizzo dell'accesso federato nell'ambito dei servizi bibliotecari perché consentono:

1. l'autenticazione e l'autorizzazione a lungo termine;
2. la gestione unificata delle credenziali per i diversi servizi;
3. il *remote consultation,* consentendo alle stesse biblioteche di essere dei *Service Provider* (SP) o *Content Provider* (CP) che mettono a disposizione degli utenti autorizzati le proprie collezioni e i servizi sviluppati all'interno o in *hosting*;
4. un maggiore 'ruolo visibile' dell'utente rispetto all'accesso tramite IP. È infatti possibile abilitare i servizi in base alle caratteristiche dell'utente e non in modo in

[5] Lista delle risorse della Federazione IDEM <https://www.idem.garr.it/servizi/sp> (ultimo accesso 26.04.2017).

differenziato così come avviene attraverso l'abilitazione degli indirizzi IP;
5. maggiori opportunità di integrazione, accessibilità e interoperabilità dei servizi erogati agli utenti;
6. statistiche dettagliate di accesso alle risorse sottoscritte al fine di fornire maggiori elementi di analisi utili in fase di pianificazione strategica dei rinnovi e di sviluppo delle collezioni.

L'accesso federato fornisce dei vantaggi anche all'utente:
1. un unico set di credenziali (*username*/*password*) per accedere a tutte le risorse e ai servizi messi a disposizione;
2. sicurezza e protezione dei dati personali, perché solo gli attributi essenziali sono comunicati all'esterno ai fornitori dei servizi;
3. accessibilità, perché non sono richieste specifiche tecnologiche particolari per l'accesso;
4. mobilità, perché l'accesso ai servizi è flessibile e indipendente dal posto fisico da cui viene effettuato.

IDEM, da ottobre 2011, ha inoltre aderito ad eduGAIN[6], un servizio di 'interfederazione internazionale' che interconnette le federazioni di identità della ricerca e dell'istruzione.

eduGAIN abilita lo scambio sicuro di informazioni relative all'identità, all'autenticazione e all'autorizzazione tra le federazioni partecipanti e quindi permette agli utenti di accedere ai servizi in rete tramite un sistema di *Single Sign On* su scala internazionale usando l'unica *password* data dalla propria organizzazione di appartenenza.

Per aderire a eduGAIN non servono procedure particolari, perché per le organizzazioni che aderiscono ad IDEM i loro Identity Provider vengono automaticamente registrati in eduGAIN. Attualmente eduGAIN conta 2053 *Identity Providers* e 1230 *Service Providers* aderenti.

[6] Informazioni ed enti aderenti sono disponibili su <http://services.geant.net/edugain/> (ultimo accesso 26.04.2017).

Per quanto riguarda l'aspetto relativo alle infrastrutture di ricerca, nel 2015 è stato avviato il progetto AARC[7], finanziato dall'UE, che riunisce 20 differenti partner tra centri nazionali di ricerca e istituzioni accademiche, infrastrutture e fornitori di servizi e biblioteche al fine di creare un'interoperabilità dei sistemi di accesso e autenticazione esistenti. Il Consorzio GARR è uno dei partner di progetto.

AARC ha lo scopo di colmare le lacune tecniche e funzionali che ostacolano l'interoperabilità delle attuali infrastrutture di autenticazione e autorizzazione e per definire delle *policy* comuni.

L'obiettivo di AARC è quindi quello di fornire alla comunità della ricerca e dell'istruzione un set di credenziali uniche per ogni utente che garantisca l'accesso ad una vasta gamma di servizi, a prescindere dall'infrastruttura digitale di appartenenza e le biblioteche, per esempio, hanno da questo progetto tutto il supporto tecnico necessario per dare piena applicazione alle potenzialità dell'accesso federato nel modo più semplice e lineare possibile.

L'esperienza dell'Università del Salento all'interno della comunità IDEM è iniziata nel maggio 2011 con l'adesione in qualità di *Identity Provider* e fornendo, tramite il *Single Sign On*, l'accesso alla banca dati *Web of Science* di Thomson Reuters. In seguito, è stato aggiunto in via sperimentale l'accesso alle *Google Apps* e, nel 2013, l'accesso federato a Scopus e ScienceDirect di Elsevier.

Con il passare degli anni si è notato un importante incremento nell'utilizzo dell'accesso federato ai servizi resi disponibili tramite IDEM, che dimostra come l'utente preferisca questo tipo di autenticazione perché recepita come estremamente semplice.

[7] Authentication and Authorisation for Research and Collaboration. Informazioni sono disponibili su <https://aarc-project.eu> (ultimo accesso 26.04.2017).

L'esperienza dell'Università Ca' Foscari di Venezia

Il cammino di Ca' Foscari come membro della comunità GARR inizia a luglio 2010 con l'adesione a IDEM in qualità di *Identity Provider*. I benefici principali per il Sistema bibliotecario riguardano soprattutto la possibilità per gli utenti di utilizzare da fuori rete le credenziali di Ateneo come unica chiave di accesso alle risorse elettroniche, in questo modo favorendone l'utilizzo.

Un monitoraggio effettuato nel 2013 dalla Biblioteca digitale (in seguito BDA), aveva invece evidenziato che questo servizio veniva sottoutilizzato. Gli utenti ricorrevano a IDEM in modo disomogeneo e solo per pochi prodotti dell'editoria elettronica sottoscritta o acquistata da Ca' Foscari.

I motivi principali erano dovuti a:

a) poca conoscenza del servizio da parte degli utenti;
b) assenza dal sito GARR di documentazione chiara, esaustiva e pronta all'uso per le biblioteche;
c) poco coordinamento tra Area Servizi Informatici di Ateneo (in seguito ASIT) e Sistema bibliotecario;
d) scarsa corrispondenza tra le risorse digitali sottoscritte da Ca' Foscari e quelle effettivamente partner di IDEM.

L'obiettivo 2014: attivazione degli accessi alle risorse elettroniche attraverso autenticazione federata

Per facilitare l'accesso alle piattaforme editoriali e implementarne l'utilizzo, la Biblioteca digitale ha incluso tra gli obiettivi di struttura 2014 l'attivazione degli accessi attraverso l'autenticazione federata e l'incremento del 10% delle risorse in IDEM.

Attorno a questo obiettivo si è costituito un gruppo di lavoro composto da personale bibliotecario BDA con diverse competenze: Chiara Da Villa (corsi di formazione, metadati, piattaforme e editoria digitale), Rossana Giaffreda (DD-ILL, OPAC), Emanuela Molinaro

(corsi di formazione, *back* e *front office* della Biblioteca digitale), Marisol Occioni (contrattazione delle risorse elettroniche).

Le attività

Il gruppo ha iniziato i lavori a febbraio 2014 e pianificato le attività necessarie a raggiungere l'obiettivo, che possono essere così suddivise:

1. verifica delle risorse elettroniche e degli editori federati inclusi nell'elenco dei partner IDEM (non tutte le risorse digitali dello stesso editore erano accessibili con autenticazione federata, quindi si è proceduto a spuntarle titolo per titolo);
2. comparazione tra le risorse di Ca' Foscari e l'elenco IDEM con evidenza di quelle mancanti;
3. contatto diretto con gli editori partner IDEM per:
   a) includere l'Ateneo tra gli enti che utilizzano Shibboleth [8];
   b) attivare le risorse dell'Ateneo al momento non accessibili;
4. vincolare le nuove proposte degli editori alla loro compatibilità con l'autenticazione federata (si è approfittato per spiegare inoltre che l'utilizzo dell'identità digitale scongiura l'accesso improprio da parte di utenti non autorizzati);
5. invio di segnalazioni allo staff IDEM per attivare un maggior numero di prodotti ed editori di interesse per Ca' Foscari.

I risultati

A dicembre 2014 il lavoro del gruppo si è concluso con una serie di dati positivi:

[8] Il sistema per l'accesso federato ad IDEM è basato sul *software open source* Shibboleth.

1. possibilità di utilizzare Shibboleth per 12 risorse di Ateneo, prima accessibili solo via IP;
2. incremento del 14% delle risorse editoriali di interesse per Ca' Foscari, incluse dell'elenco IDEM;
3. aumento del 32% nell'utilizzo delle risorse elettroniche rispetto all'anno precedente;
4. a marzo 2015, Ca' Foscari risultava l'Ateneo italiano con il maggior utilizzo delle credenziali di Ateneo per accedere alle risorse elettroniche.

Un ulteriore risultato, non numerico ma non meno importante, è stata la collaborazione tra lo staff di IDEM e il gruppo di lavoro, che nel corso dell'anno è stato coinvolto in due interviste.

La collaborazione: i questionari

Nel corso del 2014, lo staff di IDEM ha somministrato al gruppo due questionari, tesi a valutare l'utilizzo dell'identificazione federata da parte dei servizi bibliotecari.

La prima rilevazione, fatta da IDEM all'inizio del 2014, aveva come obiettivo mappare l'espansione dell'accesso federato a Ca' Foscari: poiché riguardava anche aspetti legati ai servizi informatici, è stata redatta in collaborazione con Alberto Piotto, direttore dell'Ufficio Applicativi di ASIT.

Il secondo questionario, che ha coinvolto il gruppo in fase di collaborazione già avanzata, era orientato a focalizzare su quali servizi bibliotecari estendere l'autenticazione, oltre l'accesso alle risorse elettroniche. Questa seconda proposta di fatto faceva diventare il gruppo di lavoro un *case study* all'interno del progetto europeo AARC di cui la federazione italiana è partner.

Punti di forza, problemi e sviluppi futuri

Lavorare con IDEM e i colleghi dell'area servizi informatici di Ca' Foscari è stato sicuramente uno degli elementi che non solo ha contribuito al raggiungimento dell'obiettivo, ma anche a creare una filiera di conoscenza e relazioni tra settori coinvolti nel processo, prima poco coordinati.

Purtroppo però l'utilizzo di IDEM è tuttora sottodimensionato rispetto alle aspettative: attualmente riguarda solo il 30% delle piattaforme editoriali dell'Ateneo, la maggioranza delle quali rimane sempre accessibile via IP. L'editoria nazionale continua ad essere la grande assente rispetto a quella internazionale: a marzo 2016 il Mulino[9] è diventato il primo editore italiano ad usare l'identità digitale[10], a fronte di partner storici come ACM, ACS, Elsevier, IEEE, Nature, Springer, Thomson, Wiley, etc.

Per quanto riguarda Ca' Foscari, le risorse elettroniche con il maggior numero di accessi via IDEM sono state nel 2016: ScienceDirect (1.377), Wiley (427), ProQuest Dissertations & Theses Global (382), Emerald Insight (241)[11]. Questi dati, se paragonati in generale con i numeri annuali di consultazione delle risorse digitali, sono estremamente contenuti: probabilmente il sistema di autenticazione tramite le diverse piattaforme editoriali è poco amichevole e spesso disomogeneo.

Per ovviare a questo problema, si sta valutando per il futuro l'opportunità di utilizzare Primo come possibile unica piattaforma di identificazione: ExLibris[12] è tra i produttori partner di IDEM. Ma perché questo avvenga, il numero di editori e risorse

[9] I prodotti editoriali interessati sono Rivisteweb <https://www.rivisteweb.it> (ultimo accesso 26.04-2017) e Darwinbooks <https://www.darwinbooks.it> (ultimo accesso 26.04-2017)

[10] Vd. <https://www.idem.garr.it/news-idem/568-il-mulino-primo-editore-italiano-ad-usare-l-identita-digitale-idem-della-%20comunita-garr> (ultimo accesso 26.04-2017)

[11] I dati riguardano gennaio-maggio 2016. Si ringrazia Alberto Piotto, Direttore Ufficio Applicativi di ASIT per i numeri forniti.

[12] Il Sistema Bibliotecario di Ateneo utilizza Primo di ExLibris per l'accesso integrato alle risorse documentali, cartacee e digitali.

elettroniche deve essere significativo, altrimenti l'utente non ne avrebbe un beneficio.

I risultati fino ad oggi raggiunti confermano che la strada intrapresa è corretta, avvalorati anche dal recente protocollo di intesa con la CRUI.

L'esperienza dell'Università Roma Tre

Roma Tre è tra i fondatori del progetto IDEM. Nel 2006 abbiamo cominciato a collaborare con altre Università ed enti di ricerca per poi aderire formalmente al progetto pilota IDEM.

Da quella esperienza è scaturita una sequenza di attività, sia interne, a livello organizzativo e di processi, sia verso l'esterno in coordinamento con altre realtà (federazione e *Service Provider* in primis):

- 2006: sperimentazione IdP in collaborazione con l'Università MoRe ed il CERIS;
- 2007: adesione progetto pilota IDEM;
- 2008: migrazione IdP SAML 2 ed inserimento nella Federazione di Test;
- 2009: adesione Federazione GARR IDEM;
- 2009: integrazione *certificate authority* TCS per il rilascio *self-service* di certificati digitali;
- 2009: Roma Tre ospita la I° Assemblea della Federazione e l'annuale IDEM Day;
- 2010: autenticazione federata per le risorse bibliotecarie (Metalib, SFX);
- 2010: autenticazione federata per il *web proxy* del Sistema bibliotecario di Ateneo (EZproxy);
- 2010: autenticazione federata per l'Emeroteca Virtuale CASPUR;
- 2011: autenticazione federata per ArcAdia (DSpace);
- 2011: autenticazione federata per il dominio personale. uniroma3.it (Google Apps);

2011: implementazione consenso informato (uApprove);
2011: autenticazione federata per il portale applicativo (U-GOV);
2012: adesione eduGAIN;
2012: realizzazione SP *wifi* federato ed inserimento nella Federazione di Test;
2013: autenticazione federata per il servizio WiFi (ZeroShell);
2013: Roma Tre ospita la IV° Assemblea della Federazione e l'annuale Idem Day;
2014: autenticazione federata per il portale del Sistema bibliotecario di Ateneo (Joomla);
2014: autenticazione federata per il *Discovery* del Sistema bibliotecario di Ateneo (VuFind);
2014: ridondanza *Identity Provider*;
2015: sperimentazione GARRbox, OwnCloud, SeaFile;
2016: Roma Tre ospita il workshop di formazione e l'annuale IDEM Day.

Un approccio bottom-up

A Roma Tre il servizio è stato inizialmente testato più come dimostratore tecnologico che come 'soluzione'.

L'adozione e l'implementazione delle varie componenti è stata quindi promossa dalle strutture tecniche (Area Telecomunicazioni), non dalle biblioteche.

Solo successivamente è stato 'adottato' dalle biblioteche, che stavano cercando una soluzione per l'accesso remoto.

A livello organizzativo, l'integrazione si è realizzata con il trasferimento di una unità dalla struttura tecnica al Sistema bibliotecario.

Questa modalità di sviluppo del servizio ha comportato vantaggi, in alcuni casi anche oltre le aspettative.

Una prima ricaduta positiva è stata che la gestione del servizio, non essendo focalizzata sulle risorse per le biblioteche,

ha 'costretto' ad una implementazione senza scorciatoie, sia a livello di standard che di integrazione con i preesistenti servizi di autenticazione interni. Questo ha portato ad una infrastruttura modulare e flessibile, che ha successivamente facilitato l'adozione del servizio per i servizi più disparati.

In particolare alcuni importanti servizi interni (per esempio U-GOV) sono stati integrati nei nostri sistemi informativi in modo molto semplice grazie alla autenticazione federata.

Un'altra ricaduta significativa della implementazione 'trasversale' del servizio è stata l'esigenza che ne è derivata di formalizzare e 'normalizzare' l'*Identity Management*.

Infatti è stata fatta la scelta di utilizzare un unico connettore LDAP verso le directory (AD) del dominio Microsoft, invece di interrogare direttamente le fonti autoritative (in particolare i db degli applicativi gestionali).

Questo, a fronte della creazione di un punto di *single point of failure*, ha costretto tutti gli attori interessati (che inevitabilmente sono molti in una Università) a cooperare per veicolare nei campi LDAP tutti gli attributi necessari (prelevati dalle varie fonti autoritative) ed in particolare a confrontarsi sulla semantica associata.

Alcune ricadute negative invece sono derivate dalla mancata 'presa in carico' del servizio da parte della comunità bibliotecaria, che ne ha 'semplicemente' subito le criticità e la complessità associata.

In particolare, il servizio continua ad essere percepito come un puro servizio di autenticazione remota, non mettendo a frutto tutte le potenzialità collegate alle identità digitali.

Allo stesso modo, poiché il servizio è 'di Ateneo' e non 'delle biblioteche', non è stato mai formalizzato un budget per la sua gestione, creando una situazione a volte difficile da gestire, in cui i gestori e gli utilizzatori principali afferiscono alle biblioteche, mentre il servizio viene pagato nel 'calderone' dei sistemi informativi.

Un ambiente ibrido

Quando Roma TRE ha cominciato a lavorare con l'autenticazione federata le risorse (SP) disponibili erano limitate a pochissimi editori.

Per fornire una soluzione di accesso remoto, e contemporaneamente continuare a supportare gli editori che autorizzavano solo per IP, è stato implementato un *reverse proxy*.

Parlare del *proxy*, un servizio ormai 'anacronistico' ma molto diffuso in ambito bibliotecario, può sembrare incongruo in questo contesto, ma in realtà l'utilizzo da subito della autenticazione federata sul *proxy* ha permesso di raggiungere contemporaneamente vari obiettivi.

Infatti oltre al consueto obiettivo di mantenere una 'compatibilità' con i sistemi di autorizzazione per IP degli editori, questa strategia ci ha permesso, non solo di mettere molto facilmente in *Single Sign On* le risorse degli editori con i nostri applicativi interni, ma anche di raggiungere finalmente un livello maggiore di granularità sui permessi (ruoli) da lungo desiderato.

Come contropartita, è stato aumentato il carico di gestione della infrastruttura: ogni nuova risorsa va configurata.

Inoltre, a causa di limitazioni in alcuni servizi, è stato necessario dirottare sul *proxy* tutto il traffico di ricerca (non solo quello remoto) creando, da una parte una ulteriore criticità *single point failure*, dall'altro alcune difficoltà con risorse 'restie' ad essere 'proxate' (ssl, Java, procedure 'preistoriche'…).

Un ambiente eterogeneo

Quando abbiamo cominciato a lavorare con l'autenticazione federata l'unico sistema SSO nel mondo bibliotecario era il sistema proprietario Patron Directory Service di ExLibris, che integra Aleph, MetaLib, SFX.

Piuttosto che 'shibbolettizzare' i singoli applicativi, è stato deciso di sfruttare una API del PDS verso SAML.

Anche in questo caso, può sembrare strano fare leva su un sistema di *Single Sign On* proprietario (e concorrente), ma in realtà è proprio questa architettura 'ibrida' che ha permesso, appoggiandosi al PDS nativo, di mettere in *Single Sign On* i servizi ExLibris, usando SAML come 'lingua franca', con una operazione molto poco 'invasiva' sia per il fornitore che per gli utenti.

Abbiamo infatti ottenuto l'autenticazione federata (quindi disaccoppiata e trasparente all'applicativo SOA), e come 'sottoprodotto gratuito' abbiamo messo in SSO il *proxy*.

Questa architettura, che potenzialmente avrebbe in quel momento coperto gran parte dei servizi offerti (tutti infatti ExLibris), ha poi mostrato alcune debolezze: non tutti gli applicativi erano infatti configurati per il PDS.

In particolare per Aleph (che si è preferito lasciare fuori, visto che si stava per migrare ad Alma) questo ha comportato alcuni anni di 'segregazione sso', con gli utenti obbligati ad usare per alcune cose (p.e. le prenotazioni) la pw nativa ExLibris e per altre quella federata.

Un ambiente (troppo?) complesso

Con l'adozione della autenticazione federata si è passato da un modello monolitico, verticale, di autenticazione a livello applicativo, ad uno distribuito e trasversale.

Gli utenti hanno infatti adesso a disposizione quattro canali di accesso principali:

- accesso diretto dal campus via autorizzazione per IP;
- accesso diretto da remoto via autenticazione sulla risorsa;
- accesso via Discovery autenticato;
- accesso via *web proxy* autenticato (di solito a valle del *Discovery*).

Gli utenti più *smart* hanno immediatamente apprezzato e sfruttato, oltre la comodità della *password* unica, la flessibilità dell'architettura nell'accedere alle risorse, modulando secondo le proprie esigenze il tipo di percorso utilizzato.

Così se l'utente più 'fidelizzato' all'editore ha potuto finalmente accedere direttamente al portale commerciale con le proprie credenziali istituzionali, utenti più smaliziati hanno potuto più facilmente integrare le proprie sessioni di ricerca bibliografica 'strutturate' con l'accesso immediato al *full-text*.

Inoltre la presenza di più canali viene percepita come una preziosa 'ancora di salvezza' quando uno dei percorsi abituali non è accessibile (malfunzionamenti).

Bisogna però considerare che, per le stesse ragioni, alcuni utenti più ' tradizionalisti' possono essere disorientati.

Inoltre la complessità infrastrutturale generale aumenta, e con questa le difficoltà e le criticità nella relativa gestione.

Risultati

- Eliminazione degli accessi via VPN e *proxy* lato client;
- eliminazione delle pw dedicate;
- unificazione del punto di autenticazione (IdP);
- adozione per tutti i servizi delle stesse credenziali dell'amministrazione (dominio Microsoft).

Aspettative

- Aumento dei *download* delle risorse…. SI
- aumento degli accessi diretti sulle risorse… SI
- quindi diminuzione degli accessi per IP?… NO!

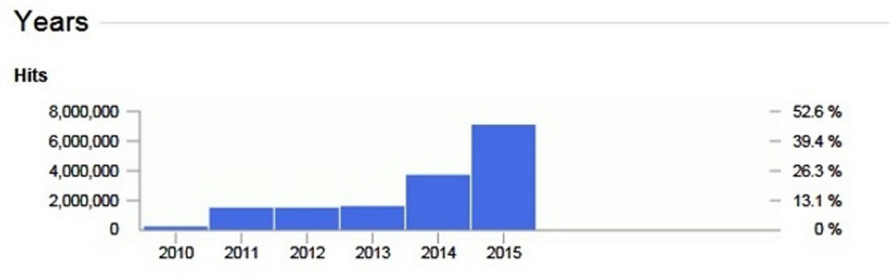

Fig. 1 — Accessi via *proxy*

L'aspettativa è stata a lungo che ci fosse un 'travaso' tra le due tipologie di accesso, al punto che era stata ipotizzata una pianificazione a lungo termine per rinunciare definitivamente all'autorizzazione via IP (e quindi anche al *proxy*).

Di fatto, nonostante effettivamente gli accessi via autenticazione federata siano in crescita, non sembra che questi vadano a detrarsi, bensì a sommarsi a quelli via IP.

La sensazione è che si sia creato un *gap* generazionale tra utenti 'da portale' e utenti 'web'; i primi sono abituati a passare dal canale delle biblioteche per l'accesso alle risorse, mentre i secondi tendono ad accedere direttamente sui portali di interesse.

Ma a quanto sembra i primi sono ancora di gran lunga prevalenti (o forse più attivi) rispetto ai secondi.

Criticità

- Gli editori sembrano interessati esclusivamente ad una soluzione di accesso remoto, non al supporto delle identità digitali. Per esempio sarebbe interessante personalizzare l'offerta dei servizi facendo leva sui ruoli (*affiliation*), oppure sull'afferenza a varie UO. Allo stesso modo sarebbe molto utile mappare queste informazioni nelle statistiche

d'uso COUNTER (per esempio "la risorsa X, pagata dal Dipartimento Y, quanto è usata da 'quel' Dipartimento?");
- i piccoli editori (italiani…) in particolare non sembrano avere le competenze (o l'interesse) necessarie per adottare la tecnologia SAML. È ipotizzabile che la diffusione della infrastruttura SPID (il sistema di autenticazione nazionale) 'costringa' gli editori ad allinearsi con le tecnologie basate su SAML;
- l'autenticazione federata è spesso vista in alternativa al *web proxy*, ma mentre la prima 'richiede' HTTPS, il secondo 'esclude' spesso HTTPS. Sta diventando sempre più difficile affiancare i servizi *legacy*. Considerate le sempre più pressanti esigenze di sicurezza, questo fattore potrebbe accelerare la transizione dal modello di autorizzazione per IP;
- in assenza di una reale politica di integrazione web, si rischia che l'utente 'bypassi' completamente le infrastrutture dei sistemi bibliotecari, oscurando i cataloghi e creando dipendenza nell'utente da risorse e criteri di ricerca proprietari. La cultura dominante nel mondo bibliotecario tende tuttora a sottostimare pesantemente l'impatto che lo sviluppo di Internet ha avuto sui sistemi informativi, lasciando una fetta sempre più grande di utenza senza riferimenti qualificati nelle proprie ricerche in rete;
- l'integrazione tra i vari servizi in SSO è di difficile comprensione per l'utente (e lo staff…) delle biblioteche e spesso non si va oltre il concetto di '*password* unica'. L'esperienza SSO a cui è ormai abituato l'utente è infatti del tipo 'Google', mentre in ambito web il SSO va comunque attivato manualmente (tipicamente cliccando qualche bottone). I fornitori dei servizi in questo non aiutano, presentando procedure complesse e diversificate per l'accesso federato.