Collaborare con facilità on line su molteplici piattaforme e con strumenti diversificati: strumenti ed opportunità per la didattica

Maria Laura MANTOVANI[1,2], Marco MALAVOLTI[1], Federica TANLONGO[1]

1 Consortium GARR, Roma (RM)

2 Università degli Studi di Modena e Reggio Emilia, Modena (MO)

Abstract

La didattica, sia nell'università che nelle scuole, è sempre più spesso arricchita dall'utilizzo di servizi "on premise" e "in cloud", sui quali l'utente, dopo aver effettuato la procedura di autenticazione, viene autorizzato ad accedere a determinati contenuti e servizi in base ai propri privilegi, ordinariamente gestiti a livello di gruppo o classe. Il proliferare di servizi diversificati e il loro utilizzo da parte di gruppi-classe pone il problema della replica delle medesime operazioni necessarie alla gestione dei gruppi di utenti che condividono l'accesso a servizi collaborativi. Questo si traduce da un lato in un maggior overhead per gli amministratori impegnati nella gestione, aggiornamento, protezione dei dati e dall'altro in un più elevato rischio di incidenti di sicurezza legato alla difficoltà nella manutenzione dei gruppi che si trovano replicati sui diversi servizi. L'adozione di un modello federato, oltre che nella gestione delle identità degli utilizzatori, anche nella gestione dei gruppi che essi formano, può semplificare questo stato di cose, minimizzando l'overhead di gestione e aumentando la sicurezza delle applicazioni: in questo modo si ottimizzano e si facilitano alcune incombenze di gestori e docenti. Anche per l'utente si riporta il contenuto al centro dell'esperienza di apprendimento, rendendo "trasparenti" gli strumenti utilizzati e migliorando così la user experience. In questo articolo, esploreremo alcuni casi d'uso e soluzioni tecniche per implementare nella pratica la gestione dei gruppi in ambito di federazioni di identità.

Keywords

autorizzazione federata, didattica on line, group management, federazioni di identità, user experience.

Introduzione

Il paradigma dell'identità digitale unica e federata come modalità di accesso per tutti i cittadini ai servizi della pubblica amministrazione sta facendosi strada anche in Italia grazie al "Sistema Pubblico di Identità Digitale" (*SPID*), iniziativa a cui il governo ha dato il via con il DPCM 24 ottobre 2014 (SPID, 2014). I protocolli, come ad esempio SAML (*Security Assertion Markup Language*) (Cantor et al., 2005) e le tecnologie, come ad esempio il framework Shibboleth (Shibboleth, 2000), prodotto dal progetto omonimo, che permettono di implementare i servizi di Identity Provider (IdP) e di Service Provider (SP) necessari per realizzare federazioni di identità (Morgan et al., 2004) ed offrire quindi la possibilità di ottenere l'identità digitale unica, vengono sperimentati già da oltre una decina di anni. Una sperimentazione di riconosciuto successo di queste tecnologie è stata fatta in Italia dalla Comunità delle Università e della Ricerca GARR (GARR, no date) con il Progetto IDEM, che nel 2009 ha dato alla luce la Federazione di identità IDEM (IDEM, 2009). Grazie alla Federazione IDEM oggi in Italia già 4 milioni (Mantovani, 2015) tra docenti universitari, ricercatori, studenti, laureati dispongono della propria identità IDEM, fornita a ciascuno dalla propria organizzazione di afferenza, e con questa identità unica possono accedere a oltre un migliaio di servizi messi in opera dalla rete delle organizzazioni che, a livello mondiale, aderiscono alla interfederazione eduGAIN (eduGAIN, no date).

Nel contesto dell'autenticazione pertanto sono molte le applicazioni e i servizi disponibili, in uso nelle università e nelle scuole, che soddisfano il paradigma federato, rendendo i concetti di Identity Provider e di Service Provider un dato acquisito sia nella consapevolezza degli integratori di sistemi, sia nella implementazione pratica, anche se maggiormente nelle università che nelle scuole.

Nell'offerta quotidiana di servizi federati i gestori, oltre che con l'autenticazione degli utenti, sono alle prese anche con la loro autorizzazione a poter compiere determinate azioni. Cresce quindi la necessità di avere, a fianco dell'autenticazione federata, anche l'autorizzazione federata e di conseguenza è necessario aggiungere un nuovo attore nell'ecosistema federato: l'Attribute Provider. Ad oggi le sperimentazioni di autorizzazione federata hanno superato il livello di Proof of Concept (Kremers, 2012), ma necessitano di una fase di preproduzione in contesti reali per poter essere adottate come soluzioni utili a permettere agli utenti di collaborare con semplicità. Tali sperimentazioni si adattano molto bene all'ambito dell'istruzione, sia nelle scuole che nelle università, perché le classi costituiscono gruppi di utenti omogenei che hanno la necessità di ottenere autorizzazioni comuni.

In questo lavoro mostreremo come il GARR ha implementato l'autorizzazione federata con la messa in opera di un Attribute Provider nella Federazione IDEM. Descriveremo anche la nostra implementazione di alcuni

componenti che sono necessari per integrare specifici servizi. Tali componenti software sono rilasciati in modalità Open Source per chiunque voglia sperimentarne la funzione di autorizzazione su un proprio servizio federato.

Stato dell'arte

Gli strumenti on line per la didattica
Moodle (Moodle, no date) è diventato lo strumento per eccellenza per erogare la didattica on line. Si tratta di un Learning Management System (*LMS*), ossia un sistema per la "gestione" dell'apprendimento: deve servire ad erogare contenuti didattici e facilitare l'apprendimento. Per offrire il miglior servizio possibile la piattaforma di erogazione LMS è di fondamentale importanza per chi eroga l'offerta formativa e deve essere perfetta nella sua funzionalità. Per questo motivo, iniziative come EduOpen (https://learn.eduopen.org), il primo MOOC delle Università italiane, hanno investito molto affinché la piattaforma LMS scelta, in questo caso appunto Moodle, offra la migliore user experience allo studente.

Un altro strumento che può essere molto utile in ambito didattico è il Wiki. Il wiki è un sistema online per la collaborazione nella redazione di contenuti. I wiki vengono utilizzati per collaborare nella creazione di documentazione, di banche dati del sapere, di enciclopedie (la più famosa è Wikipedia).

Il caso d'uso che in questo lavoro si vuole prendere in considerazione è l'utilizzo di diversi strumenti e piattaforme da parte di uno stesso gruppo di utenti per raggiungere uno scopo unico: fruire della formazione, studiare ed esercitarsi per apprendere e, alla fine del percorso, dimostrare le conoscenze acquisite. Due strumenti che spesso vengono a tal scopo utilizzati accoppiati sono quindi il LMS e il wiki. Mentre sul Learning Management System gli studenti di una classe seguono insieme un certo corso, gli stessi studenti insieme e in modalità collaborativa possono risistemare gli appunti presi a lezione utilizzando un wiki. È quello che già stanno facendo tanti studenti universitari in Italia utilizzando la piattaforma WikiToLearn (https://www.wikitolearn.org/), che come dice il nome è un wiki dedicato all'apprendimento. Usando WikiToLearn, il risultato del lavoro collaborativo della classe di studenti si materializza nella produzione di nuovo contenuto didattico sotto forma di dispense, che in fase finale può anche diventare una pubblicazione o un libro di testo.

Questo caso d'uso evidenzia che una classe di studenti può utilizzare quotidianamente, per studiare ed imparare, due sistemi on line (Figura 1): il Servizio 1, ad esempio EduOpen, e il Servizio 2, ad esempio WikiToLearn. Il caso d'uso si può complicare ulteriormente se la classe utilizza un numero di applicativi on line maggiore di due.

Gli utilizzatori
Se consideriamo un insieme di studenti che costituiscono una classe ed osser-

viamo dal loro punto di vista come accedono al LMS e al wiki, senza la possibilità dell'autenticazione federata, possiamo notare una serie di criticità. Lo studente deve ripetere la registrazione su ogni servizio. Questa ripetizione è critica per una serie di motivi: la digitazione dei propri dati nel modulo può portare ad inserire errori, imprecisioni o dati fasulli nel caso l'utente lo ritenga accettabile. La scelta delle credenziali comporta la tendenza per l'utente a ripetere in ogni sistema la stessa username e la stessa password, prestandosi all'introduzione di una vulnerabilità nella sicurezza del sistema.

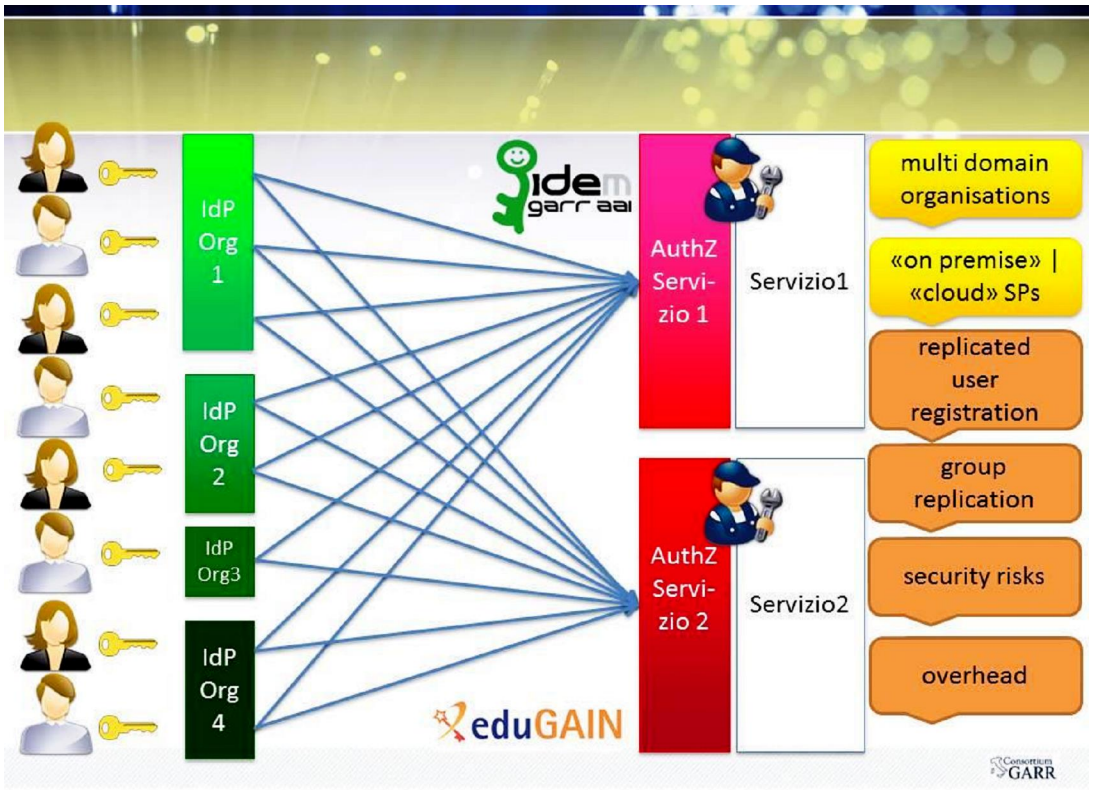

Figura 1 – Due servizi federati, con autenticazione federata, senza autorizzazione federata

Alle criticità riportate si aggiungono quelle per chi deve gestire la classe, che va gestita come gruppo su ogni diverso sistema: anche in questo caso abbiamo la ripetizione dello stesso task su sistemi diversi con conseguente introduzione di errori umani involontari e disallineamenti nei dati dei gruppi classe.

L'autenticazione federata

La gestione federata dell'identità permette di ottenere una serie di benefici rispetto a queste criticità.

La gestione federata dell'identità è basata sul disaccoppiamento della funzione di chi gestisce le identità digitali dagli erogatori dei servizi in rete (Figura 1). Il gestore dell'identità, l'Identity Provider (IdP) fornisce all'utente una identità digitale, che in base al livello di servizio (Level of Assurance, LoA) può essere anche molto sicura.

Il gestore di servizi in rete, il Service Provider (SP) non ha più l'onere di gestire le identità e le credenziali degli utenti (Figura 1). Avendo meno processi da controllare, il proprio sistema diventa più semplice e, dunque, più sicuro.

L'utente non deve ripetere lo stesso processo di registrazione su ogni sistema, non deve gestire diverse credenziali per ogni sistema a cui vuole accedere, invece possiede una propria identità digitale unica da custodire.

Il disaccoppiamento tra IdP e SP funziona anche oltre i confini della propria organizzazione (Figura 1, multi domain organisations), permettendo alle organizzazioni di gestire il proprio IdP e consentendo ai propri utenti, grazie alle identità digitali erogate, l'accesso a servizi anche esterni all'organizzazione, ossia ai servizi cloud erogati nella modalità Software as a Service (SaaS). Questo è reso possibile, ad esempio, dal protocollo SAML, un protocollo altamente sicuro nella trasmissione in rete di informazioni relative al diritto di accesso ai sistemi on line.

Implementazione di IdP e SP

Una organizzazione, in particolare una scuola, che voglia avvalersi dell'autenticazione federata deve installare il proprio IdP, utilizzando ad esempio un framework open source quale Shibboleth oppure SimpleSAMLphp (https://simplesamlphp.org/). Contestualmente deve aggiornare i propri sistemi in rete per dotarli della componente software che li abilita ad essere dei SP, oppure utilizzare servizi esterni in modalità SaaS che consentano l'accesso federato tramite l'IdP istituzionale.

Per quanto riguarda Moodle, il modo più semplice per renderlo un SP comporta l'aggiunta al sistema del software Shibboleth SP e la configurazione dell'autenticazione Shibboleth su Moodle già prevista nel pacchetto base (MoodleShib, 2016). Anche EduOpen ha implementato in questo modo l'autenticazione federata, è stato registrato nella federazione di identità IDEM e, grazie ad IDEM, nella interfederazione eduGAIN, risultando quindi immediatamente accessibile a milioni di studenti provenienti da tutto il mondo e provvisti di credenziali fornite dalla loro università o dalla loro scuola.

Per quanto riguarda il Wiki, sono varie le piattaforme integrate con Shibboleth SP (Confluence, DokuWiki, MoinMoin). Noi ci riferiamo a MediaWiki (https://www.mediawiki.org/wiki/MediaWiki) per il quale è possibile attivare l'estensione Shibboleth Authentication (ShibAuth, 2016). Un elenco abbastanza completo delle applicazioni e dei sistemi che è possibile utilizzare in modalità federata è reperibile nella documentazione di Shibboleth (ShibEnabled, 2013).

Metodologia

Come Servizio IDEM GARR AAI (Regolamento IDEM, 2014) ci siamo posti l'obiettivo di iniziare a promuovere la gestione e l'utilizzo dei gruppi di utenti, come ad esempio i gruppi classe, nell'ambiente federato. Il nostro lavoro prende in considerazione strumenti esistenti rispondenti alle specifiche SAML: l'IdP, quali esempi di SP i servizi Moodle e MediaWiki e il framework Grouper (Grouper, no date) quale gestore per i Gruppi. Il risultato è la loro integrazione in ambito di federazione di identità. Abbiamo raggiunto il risultato desiderato grazie allo sviluppo delle funzionalità applicative mancanti ai singoli servizi. Abbiamo quindi predisposto un ambiente di prova (*sandbox*) per dimostrare l'integrazione. Percorriamo ora i passi che descrivono il lavoro svolto.

L'autorizzazione basata sui gruppi
Supponiamo che ad un insieme di studenti, solitamente ad una classe, una scuola voglia dare la possibilità di collaborare utilizzando molteplici strumenti (LMS, Wiki, list-server, forum, …). Gli studenti devono essere riconosciuti da tutti i servizi in rete, ciascuno studente con le proprie credenziali e come appartenenti al proprio gruppo classe. Questa problematica è risolta da tempo con LDAP (*Lightweight Directory Access Protocol*) che fornisce il sistema unificato di autenticazione e la gestione dei gruppi a livello di organizzazione. Gestendo i gruppi classe sulla directory LDAP si centralizza la decisione sul controllo degli accessi di gruppo. Questa soluzione è perfetta se tutto viene gestito dentro i confini di sicurezza della propria organizzazione: la directory e le applicazioni devono tutte risiedere dentro i confini della scuola e la rete di accesso LAN deve essere opportunamente protetta da firewall se non si vuole incorrere in spiacevoli incidenti di sicurezza e di furto delle credenziali. Le classi, se gestite con LDAP, possono essere costituite solamente da studenti della stessa scuola a cui la scuola stessa ha fornito le credenziali. La soluzione descritta è molto limitativa in quanto le esigenze odierne richiedono l'accesso in sicurezza a sistemi esterni o cloud. Inoltre il servizio LDAP non ha in sé la possibilità di gestire gruppi di utenti afferenti a diverse organizzazioni. Per questo LDAP non è una soluzione per gestire i gruppi nelle federazioni di identità. Quando si vuole spaziare fuori dalla propria organizzazione e si vogliono utilizzare servizi in hosting o in cloud nella modalità "as a Service" è necessario dotarsi degli opportuni protocolli e servizi di sicurezza, come quelli basati ad esempio sul protocollo SAML. I requisiti connessi alla gestione di gruppi che si vogliono soddisfare in ambito federato sono i seguenti: il gruppo può essere composto da utenti appartenenti a differenti organizzazioni ed ognuno di essi si autentica con il proprio IdP; i servizi possono stare dentro l'organizzazione oppure in cloud; la definizione del gruppo e la sua gestione si deve effettuare in un unico posto al fine di evitare overhead nella duplicazione della gestione e rischi di sicurezza. Se semplicemente rendiamo i nostri servizi Moodle e Mediawiki dei SP della federazione, mediante gli strumenti di

integrazione ad oggi esistenti, ossia attivando i moduli di autenticazione Shibboleth rispettivamente su Moodle e su Mediawiki avremo soddisfatto i primi due requisiti, ma non il terzo.

L'autorizzazione federata

L'autorizzazione federata è un nuovo concetto che introduce nelle federazioni di identità, oltre all'IdP e all'SP, un'altra tipologia di entità: l'Attribute Authority (AA) o Attribute Provider (*AP*) (Figura 2).

Il SP ha necessità di verificare se l'utente è colui che dice di essere e per fare questa operazione si serve dell'IdP. Consequenzialmente il SP ha necessità di decidere se l'utente ha diritto di entrare e/o compiere una determinata azione. Per prendere questa decisione si può basare su qualità/attributi collegati all'utente. Ci sono 3 modelli per gestire gli attributi: 1. gli attributi vengono memorizzati nel SP e gestiti da esso, 2. gli attributi vengono memorizzati e gestiti dall'IdP e trasmessi all'SP, 3. gli attributi vengono richiesti ad una terza parte che li gestisce in autonomia: l'AA o AP. Il vantaggio di gestire questi attributi su un sistema terzo si manifesta palesemente quando l'attributo da gestire è l'appartenenza ad un gruppo. In questo modo la gestione del gruppo è totalmente disaccoppiata dall'IdP e dall'SP, pertanto possono appartenere al gruppo utenti provenienti da diversi IdP ed il gruppo può essere utilizzato da diversi SP. La gestione del gruppo stesso risulta più efficace poiché può essere delegata ad un manager di gruppo che ha a cuore la sua corretta gestione.

La gestione di gruppi o classi con Grouper

Grouper è un framework adatto a realizzare una AA da registrare in una federazione di identità. Il sistema Grouper federato viene gestito da un amministratore che a sua volta può delegare a diversi group manager la gestione dei gruppi. Ad esempio il docente di un certo corso può essere delegato a gestire il suo gruppo classe tramite Grouper. Il docente della classe conosce tutti gli studenti iscritti ad un certo corso o percorso formativo e decide di conseguenza di creare e manutenere il relativo gruppo classe su Grouper, in autonomia, senza doversi rivolgere ad uno specialista informatico, potendo utilizzare una interfaccia utente user friendly. È anche possibile realizzare una procedura che automatizzi o faciliti la gestione degli ingressi nel gruppo classe, ad esempio con email di invito, e la gestione del ciclo di vita dell'appartenenza al gruppo. Una volta creata la classe questa può essere utilizzata da qualsiasi SP, opportunamente configurato, per decidere di autorizzare all'accesso a determinati spazi riservati al corso soltanto i membri di quel gruppo classe. Ad esempio EduOpen può interfacciarsi a Grouper per consentire l'accesso per ciascun corso soltanto ai membri di quel determinato gruppo di persone iscritte al corso. Lo stesso gruppo può essere contemporaneamente utilizzato da WikiToLearn per garantire che solo gli studenti di quella classe possano collaborare a scrivere gli appunti del corrispondente corso in uno spazio del wiki dedicato esclusivamente al gruppo. Si possono immaginare anche altre applicazioni ad uso esclusivo da parte del gruppo. Ad esempio un list server che dal gruppo costruisce la mailing list della classe.

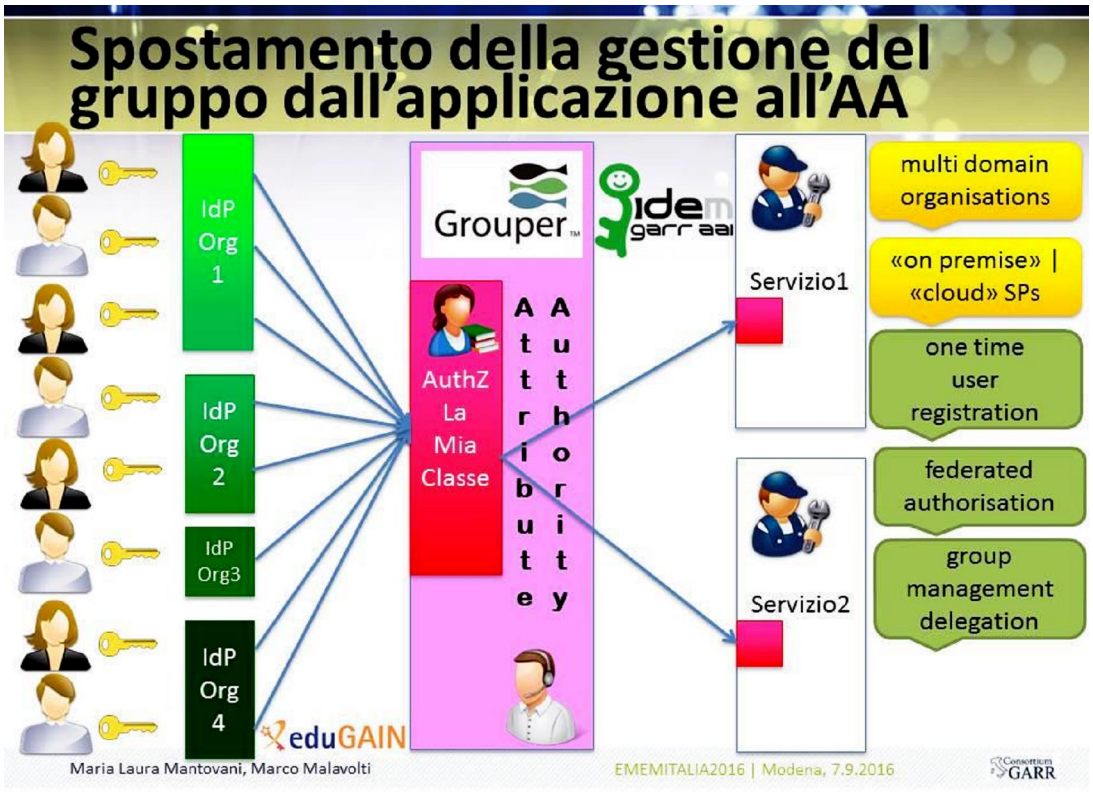

Figura 2 – Due servizi federati con autenticazione federata e con autorizzazione federata

Risultati e discussione

Scenari di integrazione

Per poter permettere le interazioni descritte è stata necessaria l'elaborazione di nuovi contributi per i software Grouper, Moodle e WikiMedia. Descriviamo quindi in cosa consistono i contributi che abbiamo sviluppato e l'ambiente in cui sono stati testati. Tali contributi, rilasciati in open source, verranno sottoposti alle rispettive community di sviluppo.

L'istanza di Grouper nella veste di AP deve poter essere consultata da tutti i SP che necessitano di recuperare da essa i gruppi e le relative identità digitali appartenenti ai gruppi. Per facilitare questa interazione l'istanza di Grouper è stata implementata dal Servizio IDEM GARR AAI e registrata nelle Federazioni IDEM ed eduGAIN. È quindi attiva la AA https://grouper.idem.garr.it. La stessa istanza di Grouper, oltre alla funzione di AA, ha anche la funzione di SP, infatti i manager dei gruppi definiti su Grouper possono collegarsi al servizio di Grouper, utilizzando un qualsiasi browser e scegliendo ciascuno il proprio IdP per autenticarsi. Una volta collegati, potranno di gestire il ciclo di

vita dei gruppi di cui sono intestatari. La versione di Grouper installata è la 2.3.0. Questa ha la nuova funzionalità di gestire gli "external user" tramite email di invito, e tale funzionalità è estremamente importante per il docente (o manager del gruppo) i cui studenti provengano da diverse organizzazioni. La funzionalità tuttavia, al momento dell'integrazione nell'ambiente dedicato al nostro caso d'uso, ha mostrato il seguente limite: quando un sistema esterno, tipicamente un SP, interrogava l'AA per avere la lista dei membri di un certo gruppo, usando ad esempio il protocollo VOOT (VOOT, 2014), veniva restituita una lista di identificativi degli utenti appartenenti al gruppo. Tali identificativi, nel caso su trattasse di external user, risultavano identificativi interni a Grouper e pertanto non correlabili con gli utenti che accedevano al SP. Occorreva che la lista di identificativi degli utenti appartenenti al gruppo venisse modificata usando identificativi univoci e persistenti anche per gli external user. Un tale genere di identificativo comunemente utilizzato nelle federazioni di identità è eduPersonPrincipalName (*ePPN*) (eduPerson, 2016). Il nostro contributo si è concretizzato nella produzione di una patch per Grouper (GARR patch 20160811) per esportare la lista degli utenti di un certo gruppo, identificandoli con ePPN.

Il SP Moodle, come già detto, implementa nel pacchetto base le funzionalità necessarie per poter utilizzare l'autenticazione federata. Invece per recuperare i gruppi, tramite procedura di enrollment, da una AA registrata nella federazione ed in particolare da https://grouper.idem.garr.it, il LMS deve essere configurato aggiungendo l'enrollment plugin realizzato da GARR (Biancini et al., 2015), disponibile open source (GARR, 2014), capace di connettersi a interfacce esterne e recuperare le informazioni sui gruppi tramite il protocollo VOOT al fine di ottenere le informazioni sui corsi. Attraverso le interfacce VOOT è quindi possibile recuperare: (i) la lista dei gruppi in Grouper, che viene tradotta da Moodle in una lista di corsi da creare sulla piattaforma e (ii) i membri di ogni gruppo e i loro ruoli; questa informazione permette di determinare chi sono i docenti e gli studenti di ogni corso. Infine, un processo schedulato con cron sul server di Moodle tiene aggiornato il suo database rispetto ai gruppi/corsi definiti in Grouper.

Questa integrazione consente ad ogni utente di Moodle, dopo aver effettuato l'autenticazione federata, di vedere immediatamente i materiali dei corsi a cui è iscritto come studente e di amministrare i corsi per i quali ha assunto il ruolo di docente. L'utilizzo dell'enrollment plugin consente di creare automaticamente nuovi corsi all'interno di Moodle, definendoli sotto forma di gruppi in Grouper. Le informazioni di accesso, per l'utente, vengono verificate ad ogni operazione di login, per evitare che ad uno studente o a un docente venga offerto un accesso cui non avrebbe diritto.

Abbiamo predisposto un ambiente Moodle di prova (sandbox: https://wiki.idem.garrservices.it/moodle) per permettere ai docenti e agli amministratori di sistemi LMS di sperimentare la nostra soluzione. Inoltre per permettere a qualsiasi amministratore Moodle di configurare il proprio LMS e,

avendolo registrato in IDEM, beneficiare dei vantaggi di Grouper, abbiamo predisposto una guida per l'integrazione di Moodle con Grouper (Malavolti, 2016a).

Il software MediaWiki implementa, nella stessa estensione già citata che serve per l'autenticazione, anche le funzionalità di recupero dei membri di un gruppo da una AA, tramite la lettura dell'attributo *isMemberOf*. In questo caso è quindi sufficiente abilitare il plugin, che è ufficialmente disponibile e contiene le migliorie introdotte da GARR (ShibAuth, 2016), per il recupero dei membri dei gruppi da una AA. A questo punto è possibile assegnare a spazi wiki distinti ai gruppi distinti, definiti su Grouper e da questo trasmessi al wiki, mediante le policy di accesso di MediaWiki.

Anche in questo caso abbiamo predisposto un ambiente MediaWiki di prova (sandbox: https://wiki.idem.garrservices.it/wiki) per permettere ad amministratori di sistemi wiki di sperimentare la nostra soluzione. Inoltre per permettere a qualsiasi amministratore MediaWiki di configurare il proprio sistema e, dopo averlo registrato nella federazione IDEM, configurarlo in modo da beneficiare dei vantaggi di Grouper, abbiamo predisposto una guida per l'integrazione di MediaWiki con Grouper (Malavolti, 2016b).

Conclusioni

L'applicazione in produzione dei risultati conseguiti permette di gestire, da una console di gestione centralizzata, gruppi formati da utenti afferenti a diverse organizzazioni, ma facenti parte del medesimo gruppo di lavoro. Permette inoltre l'utilizzo di meccanismi di delega granulare nella gestione delle autorizzazioni e una migliore la distribuzione delle responsabilità nella gestione delle informazioni sugli utenti federati.

I casi d'utilizzo discussi sopra evidenziano come, in uno scenario in cui si diffonde l'utilizzo di servizi e contenuti digitali come arricchimento (e al limite, nel caso delle università telematiche, sostituzione) delle lezioni frontali e dei gruppi di studio tradizionali, l'adozione di un modello federato nella gestione delle identità di studenti e docenti può offrire una serie di benefici soprattutto nel caso in cui si utilizzino contemporaneamente più tool differenti. Accanto alla semplificazione delle procedure di registrazione ai servizi e al conseguente miglioramento della user experience, questa soluzione garantisce anche di elevare i livelli di sicurezza e minimizzare l'overhead legato alla gestione delle identità e degli accessi, tanto per il gestore delle identità che per quello dei servizi. Queste caratteristiche di semplicità, sicurezza e trasparenza del mezzo informatico vengono mantenute anche quando si tratta di autenticare non solo un singolo utente ma anche un gruppo con caratteristiche uniformi, cui corrispondono determinati permessi, rendendo questo modello molto vantaggioso quando si tratti di gestire in modo semplice e flessibile

classi o gruppi di studio che debbano accedere agli stessi contenuti e servizi. La soluzione proposta integra all'interno di un contesto federato Grouper in veste di AA/AP, cioè come elemento in grado di assegnare una serie di attributi agli utenti in modo da poter creare questi gruppi uniformi e poterli autorizzare in base al ruolo o ad altre caratteristiche. Il grande vantaggio di questa soluzione consiste nel fatto di poter creare indifferentemente gruppi di utenti appartenenti a una o più organizzazioni, cosa non possibile un sistema di gestione dei gruppi basato su LDAP, pensato per funzionare all'interno di una singola organizzazione. Questi gruppi "misti" possono essere gestiti senza la necessità di modificare il sistema di directory esistente da parte delle organizzazioni coinvolte, utilizzando dei meccanismi di delega granulare nella gestione delle autorizzazioni. Nell'opinione di chi scrive, l'adozione generalizzata di questo approccio permetterebbe di aprire nuovi scenari di collaborazione nella erogazione di servizi e contenuti federati da parte di più università o scuole (cfr. Il caso di EduOpen e WikiToLearn), ma anche nuove opportunità di business per i gestori di servizi che interessano questo target.

Questa esigenza comincia quindi a farsi sentire in una comunità vasta e con forti spinte alla collaborazione e all'interazione come quella dell'Istruzione e della Ricerca, e la definizione di soluzioni adeguate è di conseguenza entrata nell'agenda di federazioni di identità come IDEM ed eduGAIN. Attività specifiche di pilot delle soluzioni già esistenti insieme ad attività di sviluppo di nuovi componenti e nuove funzionalità per la gestione dei gruppi, in determinati ambiti chiamati anche Virtual Organisation, sono attualmente attive nei progetti finanziati dalla Commissione Europea quali GÉANT GN4 (Poortinga-van Wijnene, 2016) e AARC (Authentication and Authorisation for Research and Collaboration) (Vaghetti et al. 2016) ai quali GARR partecipa attivamente.

Riferimenti bibliografici

BIANCINI A., MANTOVANI M.L., MALAVOLTI M. (2015), USARE GROUPER PER GESTIRE L'AUTORIZZAZIONE DI MOODLE, TEACH DIFFERENT! PROCEEDINGS DELLA MULTICONFERENZA EMEMITALIA2015 GENOVA, 9-11 SETTEMBRE 2015, 351-354. http://www.ememitalia.org/archivio/2015/atti-ememitalia2015

CANTOR, S., HIRSCH, F., KEMP, J., PHILPOTT, R., AND MALER, E. (2005). THE OASIS SECURITY ASSERTION MARKUP LANGUAGE (SAML) V2.0. TECHNICAL REPORT. http://saml.xml.org/saml-specifications

EDUGAIN, (NO DATE). https://en.wikipedia.org/wiki/EduGAIN

EDUPERSON, (2016). EDUPERSON OBJECT CLASS SPECIFICATION, http://software.internet2.edu/eduperson/internet2-mace-dir-eduperson-201602.html

GARR, (NO DATE). LA COMUNITÀ GARR, http://www.garr.it/a/utenti/comunita-garr

GARR (2014). MOODLE-ENROL_VOOT SOFTWARE, https://github.com/ConsortiumGARR/moodle-enrol_voot

GROUPER (NO DATE). INTERNET2, http://www.internet2.edu/products-services/trust-identity/grouper/

IDEM (2009), IDEM RENDE PIÙ FACILE ACCEDERE A SERVIZI CONDIVISI CON UNA UNICA CHIAVE DI ACCESSO, GARR, https://www.idem.garr.it/idem

KREMERS, M. (2012). SUPPORTING VIRTUAL ORGANISATIONS USING VOOT IN INTERNET2 MEMBER MEETING, FALL 2012, PHILADELPHIA, PA, USA. INTERNET2. http://meetings.internet2.edu/2012-fall-mm/detail/10002583/

MALAVOLTI M. (2016A), HOWTO INTEGRATE MOODLE WITH GROUPER ON UBUNTU LINUX 12.04, GARR, https://www.idem.garr.it/documenti/doc_download/454-eng-howto-integrate-moodle-with-grouper-on-ubuntu-linux-12-04

MALAVOLTI M. (2016B), HOWTO INTEGRATE MEDIAWIKI WITH GROUPER ON UBUNTU LINUX 14.04, GARR, https://www.idem.garr.it/documenti/doc_download/520-howto-integrate-mediawiki-with-grouper-on-ubuntu-linux-14-04

MANTOVANI, M.L. (2015), FEDERAZIONE IDEM: STATO DELL'ARTE. 10 ANNI DI INFRASTRUTTURE DI AUTENTICAZIONE E AUTORIZZAZIONE, GARR, QUINTO CONVEGNO IDEM - LECCE, 13-15 MAGGIO 2015, https://www.idem.garr.it/documenti/doc_download/412-m-l-mantovani-presentazione

MOODLE (NO DATE). https://docs.moodle.org/dev/Mission

MOODLESHIB, (2016) ▶ MANAGING A MOODLE SITE ▶ AUTHENTICATION ▶ SHIBBOLETH, http://docs.moodle.org/en/Shibboleth

MORGAN, R. L., CANTOR, S., CARMODY, S., HOEHN, W., AND KLINGENSTEIN, K. (2004). FEDERATED SECURITY: THE SHIBBOLETH APPROACH EDUCAUSE QUARTERLY, 27(4):12–17. http://er.educause.edu/articles/2004/1/federated-security-the-shibboleth-approach

POORTINGA-VAN WIJNEN R. (2016), REPORT ON THE ACHIEVEMENTS OF JRA3 TRUST AND IDENTITY RESEARCH TASK 1 ATTRIBUTES AND AUTHORISATIONS AND RECOMMENDATIONS ON FUTURE WORK, GÉANT, http://www.geant.org/Projects/GEANT_Project_GN4-1/Documents/D15-1_Report-on-the-Achievements-of-JRA3-T1-and-Recommendations-on-Future-Work.pdf

REGOLAMENTO DELLA FEDERAZIONE IDEM (2014), CAP.6, https://www.idem.garr.it/documenti/regolamento

SPID (2014), SISTEMA PUBBLICO PER LA GESTIONE DELL'IDENTITÀ DIGITALE – SPID, AGID, http://www.agid.gov.it/agenda-digitale/infrastrutture-architetture/spid

SHIBAUTH, (2016). MEDIAWIKI EXTENSION:SHIBBOLETH AUTHENTICATION, https://www.mediawiki.org/wiki/Extension:Shibboleth_Authentication

SHIBENABLED, (2013). SHIBBOLETH® ENABLED APPLICATIONS AND SERVICES, https://wiki.shibboleth.net/confluence/display/SHIB2/ShibEnabled

SHIBBOLETH (2000), WHAT'S SHIBBOLETH?, http://shibboleth.net/about

VAGHETTI D., MANTOVANI M.L., BIANCINI A. ET AL. (2016), DESIGN FOR THE INTEGRATION OF AN ATTRIBUTE MANAGEMENT TOOL, AARC, https://aarc-project.eu/wp-content/uploads/2016/06/MJRA1.3-Design-for-the-integration-of-an-Attribute-Management-Tool.pdf

VOOT (2014). https://github.com/andreassolberg/voot/wiki/Specifications.