Specifiche Tecniche per la Federazione IDEM

v 1.0

G. Birello, R. Conte, M. Ianigro, C. Marotta
con contributi di:
F. Malvezzi, B. Monticini

15 Settembre 2009

Revisioni

Versione	Data	Descrizione	Autori
1.0	15/9/2009	Versione iniziale	vedi frontespizio

Introduzione

Questo documento fornisce le raccomandazioni tecniche per i partecipanti alla Federazione IDEM (Identity Management per l'accesso federato, di seguito "Federazione") ed ha ha come obiettivo la regolamentazione di tutti quegli aspetti tecnici relativi all'interazione fra i partecipanti, ovvero fra Identity e Service Provider. Non è un manuale di supporto all'installazione del software.

In questo documento sono presentate le modalità generali di configurazione dei Servizi, che i partecipanti devono rispettare per ottenere l'interoperabilità fra gli aderenti alla Federazione. Le raccomandazioni sono fornite in maniera da essere applicabili a prescindere dal tipo di implementazione utilizzata, pur tenendo conto che la Federazione supporta ufficialmente Shibboleth. Le indicazioni che faranno esplicito riferimento a questo software verranno messe in evidenza con il simbolo a lato .

A causa della naturale rapida evoluzione del software il presente documento potrà subire numerose modifiche nel tempo. Si prega quindi di fare riferimento sempre all'ultima versione, reperibile sul sito della Federazione (idem.garr.it) nella sezione *Come partecipare*. Ogni modifica al documento verrà comunque notificata con le modalità indicate nella sezione *Comunicazioni ai partecipanti*.

Implementazioni e Software

Protocolli

SAML

IDEM, come altre federazioni, utilizza il protocollo SAML [1] attualmente nella versione 2.0. Per maggiori informazioni si prega di fare riferimento a [2] e [3].

NTP

Per ragioni di sicurezza il sincronismo fra i server è fondamentale per il pieno successo dell'interazione fra gli attori della federazione che devono scambiarsi informazioni. Risposte a messaggi inviate in ritardo (anche apparente) da una parte possono essere considerate come potenziali attacchi all'integrità della controparte e portano al fallimento della comunicazione. Per tale motivo si consiglia

l'uso di un protocollo di sincronizzazione dell'orario sui server della Federazione come il Network Time Protocol.

Al solo scopo di agevolare la configurazione, si consiglia di utilizzare i server messi a disposizione dall'iNRiM, Istituto Nazionale di Ricerca Metrologica [4], i cui server primari sono i raggiungibili agli indirizzi:

- ntp1.inrim.it;
- ntp2.inrim.it.

Applicativi

Shibboleth

Nonostante SAML 2.0 abbia diverse implementazioni [5], la Federazione, sin dalla sua nascita, ha stabilito l'adozione di Shibboleth [6].

Al momento della scrittura di questo documento, esistono diverse installazioni di Shibboleth 1.3. Considerate le maggiori difficoltà di configurazione, la peggiore formattazione e le minori informazioni fornite dai log, tale versione è considerata deprecata dalla Federazione. Inoltre già da ora Internet2 non aggiungerà più nessuna funzionalità a tale versione, il cui supporto cesserà il 30 Giugno 2010.

Per tutte le nuove installazioni si consiglia, pertanto, l'adozione della versione 2.x, l'unica versione supportata dalla Federazione.

È lasciata libertà ai singoli di adottare qualsiasi altro prodotto che implementi SAML 2.0, fermo restando che, in questo caso, non è previsto supporto tecnico da parte della Federazione.

Autenticazione

Apache vs Tomcat

Le attuali implementazioni di Shibboleth permettono all'amministratore di un IdP di scegliere fra due modalità per presentare all'utente la richiesta di credenziali per l'autenticazione:

- una soluzione (Apache-based) consiste nell'appoggiarsi direttamente sul server web: l'IdP presenta una finestra di pop-up (del browser) in cui l'utente inserisce le proprie credenziali;

- la soluzione alternativa (Java-based) utilizza l'autenticazione attraverso JAAS (Java Authentication and Authorization Service): questa seconda modalità presenta all'utente il form di autenticazione inserito in una pagina web, che può essere personalizzata applicando gli stessi stili dell'organizzazione che amministra l'IdP.

È evidente come la possibilità di modellare il form di autenticazione secondo lo stile del sito dell'organizzazione di appartenenza dell'utente aggiunga un tocco di *family-feeling* al processo di inserimento delle credenziali. L'utente sarebbe decisamente piu' disorientato nel veder comparire sul proprio browser un pop-up senza alcun tipo di spiegazione. La modalità *Java-based* aggiunge inoltre la possibilità di guidare l'utente nell'autenticazione, poichè permette di inserire nella pagina web istruzioni, riferimenti tecnici ecc..

In conclusione, **la Federazione consiglia fortemente l'utilizzo della modalità di autenticazione Java-based**.

Validità Temporale

Un altro punto cui è necessario dedicare attenzione è la **validità temporale** dell'autenticazione, ossia l'intervallo di tempo dopo il quale una sessione autenticata presso un Identity Provider decade.

Shibboleth 2 fissa di default questo intervallo a 30 minuti. Eventuali modifiche a questo valore possono essere apportate per esigenze locali solo dopo un'attenta valutazione dell'impatto sulla sicurezza all'interno delle singole organizzazioni.

Certificati

È necessario che l'Identity Provider disponga di un certificato per cifrare la pagina con la quale avviene l'autenticazione dell'utente. Questa prima fase dell'autenticazione, infatti, richiede che i dati transitino in maniera sicura dallo host utente allo host IdP. Inoltre, poiché la pagina di autenticazione deve avere il massimo grado di accessibilità, è importante che il certificato utilizzato per la cifratura della connessione sia rilasciato da una Certification Authority nota, il cui certificato di root, cioè, deve essere installato di default nel browser utilizzato. Non è assolutamente opportuno che l'utente venga distratto in fase di autenticazione, da un messaggio di sicurezza del browser per un certificato 'problematico'. Di conseguenza, nell'interazione fra IdP e utente (*front channel*) non sono accettati i certificati autofirmati o rilasciati da CA non accettate dalla Federazione.

CA supportate

Per i motivi di cui al paragrafo precedente, la Federazione considera validi i cer-

tificati rilasciati da CA i cui certificati root siano installati di default su **tutti** i browser più diffusi: Internet Explorer, Mozilla Firefox, Safari.

La Federazione potrà, a propria discrezione, modificare l'elenco precedente e prendere in considerazione eventuali eccezioni per le CA supportate.

Firewall

Per il funzionamento dell'intera architettura è necessaria la comunicazione tra SP ed IdP (Attribute Service o più comunemente back-channel) e tra utente e IdP su due canali distinti, oltre alla comunicazione tra utente e SP.

Nella pratica si utilizzano normalmente le seguenti porte:

- **8443 TCP** per la comunicazione Attribute Service
- **443 TCP** per l'autenticazione degli utenti
- **80/443 TCP** per l'accesso al servizio sull'SP.

Quindi per l'**IdP** è necessaria l'apertura delle porte 443 e 8443 TCP mentre per l'**SP**, in funzione di com'è esposto il servizio, della porta 80 o 443 TCP.

Discovery Service

La Federazione gestisce e mantiene il servizio centralizzato WAYF (Where Are You From) per la selezione dell'organizzazione di appartenenza dell'utente fra le organizzazioni partecipanti alla federazione.

Il servizio contiene l'elenco completo di tutti gli IdP e le coordinate dei relativi siti di autenticazione presso le corrispondenti Home Organization. La comunicazione col WAYF server avviene in modo protetto tramite https.

Il servizio può memorizzare permanentemente la scelta dell'organizzazione dell'utente. Per rimuovere tale memorizzazione è sufficiente accedere al server WAYF, all'indirizzo https://wayf.idem.garr.it, e seguire le istruzioni.

Nomenclatura

La Federazione garantisce l'uniformità della nomenclatura delle istituzioni appartenenti alla Federazione e di come esse compaiono nella lista del WAYF o nei metadati, eventualmente modificando le descrizioni proposte per uniformarle con gli altri partecipanti.

Per i fornitori di servizi che partecipano a più federazioni è necessario gestire un proprio servizio WAYF. È compito della Federazione comunicare a questi fornitori di servizi, i riferimenti da inserire e relative parti descrittive in modo da rendere uniforme all'utente la scelta della propria struttura di appartenenza all'atto dell'autenticazione presso il fornitore.

Le informazioni all'interno del WAYF saranno inserite dalla Federazione a seguito della procedura di adesione dell'organizzazione, come descritto nelle *Norme di Partecipazione*.

Attributi

La denominazione, la sintassi e la semantica degli attributi scambiati all'interno della Federazione sono definiti nel documento *Specifiche Tecniche - Compilazione e Uso degli Attributi*. Per ottenere un minimo livello di interoperabilità all'interno della Federazione è necessario che gli attributi *eduPersonScopedAffiliation* e *eduPersonTargetedID* siano rilasciati a tutti i partecipanti. Nonostante ciò non è garantito l'accesso a nessun servizio in quanto resta comunque a carico del fornitore decidere se e con quali attributi sarà possibile fruire del proprio servizio. Compito della Federazione è limitare la richiesta di attributi, in particolar modo di quelli personali, ai soli effettivamente necessari per l'accesso al servizio. Per maggiori dettagli sugli attributi si faccia riferimento al documento sopra citato.

Poiché come appena detto l'autorizzazione per l'accesso ad un particolare servizio resta a carico del fornitore, è buona norma che lo stesso fornitore metta a disposizione dei fruitori una pagina per il test di rilascio degli attributi necessari per l'accesso al servizio stesso.

Allo scopo di semplificare la configurazione di Shibboleth 2.x, la Federazione (tramite il sito www.idem.garr.it, sezione “Informazioni tecniche”) mette a disposizione il file `attribute-resolver.xml` preconfigurato per il recupero, da un server LDAP, degli attributi necessari, consigliati e opzionali definiti dalla Federazione. Sarà comunque necessario personalizzare la configurazione indicando esattamente lo *scope* dell'organizzazione, i ruoli o posizioni degli utenti all'interno della propria organizzazione, necessarie per il rilascio dell'attributo *eduPersonScopedAffiliation* ed i parametri del server LDAP.

Allo stesso modo viene fornito il file `attribute-filter.xml`, con la configurazione per il rilascio degli attributi necessari ai diversi Service Provider presenti all'interno della Federazione.

Nella configurazione per il recupero degli attributi dal backend (`attribute-resolver.xml`) è importante fare attenzione che gli attributi *scoped* (*eduPersonScopedAffiliation, eduPersonPrincipalName*) abbiano lo *scope* corrispondente a quello dichiarato nei metadati. Qualora questi non coincidessero gli attributi inviati

dall'IdP potrebbero essere scartati dal SP.

Metadati

Il file dei metadati è lo strumento con il quale si condivide la fiducia all'interno della Federazione. Tramite questo file la Federazione pubblica i dati descrittivi dei partecipanti e gli stessi partecipanti utilizzano i metadati per verificare l'identità del partner durante le comunicazioni, costruendo delle relazioni di fiducia. È necessario quindi prestare la massima attenzione a questo file in quanto include tutte le informazioni necessarie per il riconoscimento reciproco dei partecipanti. Ulteriori sistemi di verifica della controparte tramite configurazione del web server per la verifica delle CRL, l'autenticazione con certificati x509 ecc., sono ridondanti e fortemente sconsigliati.

N.B. Alcuni servizi potrebbero risultare non accessibili nel caso in cui si configuri il servizio per delegare ad applicazioni diverse dall'IdP la verifica dei certificati.

Come già anticipato nella sezione *Attributi,* è importante prestare attenzione al valore di scope definito per gli attributi *scoped* (*eduPersonPrincipalName* e *eduPersonScopedAffiliation*) contenuto anch'esso nei metadati. Nel caso in cui questo non corrisponda allo scope definito per gli attributi in `attribute-resolver.xml` e a quello definito nei metadati, il Service Provider potrebbe scartare gli attributi relativi ricevuti dall'Identity Provider.

Il file dei metadati **deve** essere prelevato all'indirizzo https://www.idem.garr.it/docs/conf/idem-metadata.xml con la frequenza stabilita. La Federazione opererà il relativo controllo.

Certificati nei metadati

È consentito che il certificato contenuto all'interno del file dei metadati possa essere di tipo *self-signed*. Ciò equivale ad inserire nei metadati la semplice chiave pubblica del Servizio.

Il certificato contenuto nei metadati è utilizzato nelle comunicazioni dirette fra IdP e SP (*back-channel*) e l'utilizzo di un certificato rilasciato da un'autorità nota non aggiunge nessun valore da un punto di vista della sicurezza. L'onere eventuale di richiedere la revoca del certificato alla CA è comunque a carico del titolare del certificato (interessato a che nessun altro si presenti con il suo nome). Di conseguenza nel caso di compromissione dei certificati *self-signed* è comunque il responsabile del servizio che deve prontamente notificare l'incidente alla Federazione comunicando i nuovi metadati (con un nuovo certificato). Questo metodo

mette in opera una più veloce esecuzione delle operazioni di verifica della controparte durante l'interazione ed un minore tempo di *downtime* del server in caso di compromissione del certificato. Le funzioni di garante affidate alla CA in una PKI tradizionale, in questo caso vengono svolte dalla Federazione, la quale verifica l'identità del partecipante all'atto della trasmissione dei propri metadati e certifica, tramite la firma della federazione, agli altri partecipanti l'autenticità dell'intero file dei metadati. La Federazione inoltre, in caso di problemi di sicurezza di un partecipante, a suo insindacabile giudizio, può escludere il partecipante dalla Federazione rimuovendo il corrispondente frammento dai Metadati (cfr. Norme di Partecipazione).

N.B. L'utilizzo di un certificato self-signed non implica l'utilizzo dello stesso certificato nelle pagine accessibili dall'utente (front-channel). Al contrario per queste comunicazioni è richiesto un certificato rilasciato da una CA approvata dalla federazione (si veda sezione *Autenticazione*).

L'utilizzo di un certificato che non sia self-signed ma rilasciato da una CA richiede, oltre all'utilizzo dei file contenenti il certificato stesso e la relativa chiave, anche l'aggiornamento del keystore java e la modifica manuale del file dei metadati. Al contrario, utilizzando certificati self-signed generati al momento dell'installazione di Shibboleth, per generare un nuovo certificato è sufficiente rieseguire lo script d'installazione in una directory differente copiando poi i file necessari nella directory opportuna dell'IdP in produzione.

Modalità di gestione dei metadati

In conseguenza di quanto detto nei paragrafi precedenti si richiede pertanto ai partecipanti una grande cura nella trattazione dei metadati, in particolare in questi passaggi:

- inserimento di un SP/IdP nei metadati: il frammento relativo al nuovo servizio dovrà contenere esplicitamente il certificato; si richiede la trasmissione del frammento alla federazione con modalità sicure (email firmata con certificato GARR o di una CA accettata dalla federazione, si veda la sezione “Autenticazione”) per verificare l'affidabilità del mittente e l'integrità dei dati;
- variazione dei metadati: ai partecipanti si richiede la trasmissione immediata delle variazioni dei dati, soprattutto in caso di variazione/revoca del certificato;
- scarico dei metadati aggiornati: i partecipanti sono tenuti a prelevare i metadati dalla federazione con cadenza almeno giornaliera. I metadati possono essere prelevati tramite il protocollo **https**, ma si raccomanda comunque la verifica della firma;

- memorizzazione del file dei metadati: il file scaricato deve essere mantenuto sul server con diritti tali da non consentirne la modifica.

Shibboleth prevede diverse modalità per la gestione dei metadati [7]. La Federazione IDEM consiglia la modalità *FileBackedHTTPMetadataProvider* in cui i metadati vengono recuperati periodicamente e scaricati in un file per la loro consultazione fino al successivo aggiornamento. I metadati messi a disposizione dalla Federazione hanno un periodo di validità di 24h. I partecipanti possono, per ragioni interne, decidere di diminuire l'intervallo di tempo in cui aggiornare gli stessi, intervenendo sull'attributo *cacheDuration*.

Riferimenti per gli utenti

Allo scopo di favorire l'utilizzo dei servizi in Federazione da parte degli utenti, l'Identity provider deve provvedere a realizzare una pagina web, il cui indirizzo deve essere comunicato alla Federazione, riferita dalla pagina di autenticazione. La pagina dovrà contenere le indicazioni relative a:

- denominazione dell'organizzazione (concordata con la Federazione);
- riferimenti per il supporto agli utenti del proprio IdP;
- nominativi, indirizzi e-mail e numeri telefonici dei contatti tecnici per IDEM.

È opzionale la presenza di un numero di fax e di un numero di telefono cellulare.

È consigliabile che la pagina non stia sullo stesso IdP in modo che sia raggiungibile anche quando questo dovesse non essere accessibile. Queste informazioni dovranno essere comunicate anche alla Federazione che le inserirà nel database centralizzato dei contatti presente sul sito idem.garr.it e aggiornate nel tempo, mediante invio per posta elettronica, all'indirizzo idem-help@idem.garr.it.

È inoltre obbligatoria la presenza di un indirizzo di posta elettronica finalizzato al supporto all'utenza. La Federazione potrà, nell'ambito delle attività di auditing, inviare e-mail che richiedano conferma di lettura (ad esempio mediante richiesta di conferma di presa visione del contenuto).

Comunicazioni ai partecipanti

Le comunicazioni ai partecipanti avvengono tramite una mailing list gestita dalla Federazione. Il referente organizzativo, il referente tecnico ed i contatti tecnici del partecipante sono inseriti d'ufficio nella sopra citata mailing-list. Ogni comunicazione verrà anche pubblicata sul sito ufficiale della Federazione all'indirizzo idem.garr.it.

Operatività del servizio

La Federazione, al fine di consentire una migliore qualità ed efficienza, adotta degli strumenti automatici di monitoraggio del servizio offerto dal partecipante. I punti che determinano la qualità del servizio sono i seguenti:

1. uptime del server di autenticazione (IdP) o di erogazione del servizio offerto (SP);
2. disponibilità di una pagina web per informazioni di supporto all'utenza;
3. disponibilità di un indirizzo email per l'helpdesk all'utenza.

Relativamente all'uptime del server di autenticazione, saranno implementati dei meccanismi automatici di autenticazione presso gli IdP, mediante l'utilizzo di client web automatici; sarà richiesto al partecipante di fornire un utente di prova da utilizzare per validare il processo di autenticazione. Per quanto concerne gli SP, sarà verificata la raggiungibilità degli url legati al servizio. Poichè è importante garantire la presenza di una interfaccia per il supporto agli utenti, i partecipanti dovranno fornire la url relativo a una pagina web che contenga i nominativi di riferimento per la gestione del servizio, e i loro contatti telefonici (vedi sezione *Riferimenti per gli utenti*). Tale pagina verrà acceduta automaticamente e ne verrà monitorata la sua disponibilità. I requisiti in questione devono essere posseduti al momento dell'ammissione alla federazione, e saranno soggetti a monitoraggio periodico. Il monitoraggio avverrà da macchine della rete e avrà cadenza casuale differenziata a seconda della funzionalità da monitorare. Al momento le tempistiche sono le seguenti:

- uptime del server (punto 1): cadenza settimanale;
- disponibilità pagina web (punto 2): cadenza settimanale;
- disponibilità indirizzo email (punto 3): cadenza mensile.

Il mancato superamento dei test sarà notificato al Comitato di Gestione e via email ai referenti tecnici indicati nel database centrale e potrà portare alla sospensione temporanea del servizio nei seguenti casi:

- mancata operatività del servizio per un periodo superiore ai 30 giorni;

- mancanza della pagina web per un periodo superiore ai 15 giorni;
- mancata verifica del supporto via email per un periodo superiore ai 60 giorni.

Logging

Come già richiamato nell'Accordo di Partecipazione, ogni Organizzazione partecipante si impegna a mantenere una registrazione delle attività legate ai propri servizi (Idp o SP) al fine di poter fornire un migliore supporto nella risoluzione di problemi tecnici o nella gestione di eventuali incidenti di sicurezza.

Tali log devono necessariamente contenere le informazioni che consentano di risalire agli host coinvolti nella operazione (indirizzo IP), agli utenti, al tipo di operazione effettuata e agli attributi rilasciati. Ai fini della partecipazione alla Federazione, Membri e Partner si impegnano a conservare tali informazioni per un periodo non inferiore a 6 mesi, in modo da poter consentire anche attività 'a posteriori'.

I log saranno custoditi dal Partecipante e non verranno trasferiti o condivisi con la Federazione o gli altri Partecipanti; la Federazione potrà però richiedere al Partecipante di fornire informazioni su specifici eventi, e il Partecipante, nel rispetto delle norme vigenti sulla privacy, è tenuto a fornire tali informazioni.

La Federazione potrà decidere, nell'ambito delle attività di auditing, di richiedere occasionalmente informazioni relative agli accessi effettuati dai propri sistemi di monitoraggio, al fine di riscontrare la correttezza dei dati registrati nei log. Tali richieste potranno avvenire con cadenza non inferiore ai 6 mesi. Il mancato rispetto delle specifiche relative al logging potrà comportare la sospensione del servizio.

Bibliografia

1: http://en.wikipedia.org/wiki/SAML
2: http://saml.xml.org/
3: http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security
4: http://www.inrim.it/
5: http://saml.xml.org/wiki/saml-open-source-implementations
6: http://shibboleth.internet2.edu/
7: https://spaces.internet2.edu/display/SHIB2/IdPMetadataProvider