Specifiche Tecniche per la Federazione IDEM

v 1.2

12 Giugno 2012

Revisioni

Versione	Data	Descrizione	Autori
1.0	15/09/2009	Versione iniziale	G. Birello R. Conte M. Ianigro C. Marotta con contributi di: F. Malvezzi B. Monticini
1.1	23/02/2010	Introduzione di "Abbreviazioni" e "Contatti"; Modificato terzo capoverso dell'Introduzione; Modificato primo e quarto capoverso del paragrafo Shibboleth e ridenominato in SAML e Shibboleth; Ridenominato paragrafo Apache vs Tomcat in Login dell'utente e aggiunte note su CAS; Modificata Introduzione nel paragrafo Firewall; Modificato ordine testo nel capitolo "Validità temporale"; Modificato testo nel paragrafo Certificati; Modificato capoverso 3 del capitolo Metadati e capoverso 2 nel paragrafo Certificati dello stesso capitolo; Sostituzione sezione Riferimenti per gli utenti con Pagina web di supporto agli utenti; Introduzione sezione Comunicazioni con Servizio IDEM GARR AAI richiamata da Modalità di gestione dei metadati e introdotta la possibilità di comunicazione degli stessi tramite sito esterno; Spostamento nella sezione Operatività del servizio di 2 frasi da Riferimenti agli utenti e aggiunta informazione sulla data di attivazione del servizio di monitoring.	V. Calabritto R. Cecchini R. Conte R. Gaffuri T. Podestà
1.2	07/02/2011 12/06/2012	Modifiche alla sezione 3.1 – Login dell'utente Traduzione Inglese – correzioni minori	A.De Nicola M.L. Mantovani

Premessa

Per la segnalazione di suggerimenti, errori o inesattezze relative a questo documento, vi preghiamo di scrivere a idem@garr.it

Abbreviazioni

STA = Specifiche Tecniche per la compilazione e l'uso degli attributi
NdP = Norme di Partecipazione
IPRR= Identity Provider Registration Request
RRR = Resource Registration Request
IdP = Identity Provider
SP = Service Provider
CA = Certification Authority
WAYF = Where Are You From

Contatti

Sito IDEM = https://www.idem.garr.it

Federazione IDEM : idem@garr.it

Servizio IDEM GARR AAI : idem-help@garr.it

1 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 IdP e SP. 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 del protocollo SAML utilizzata, pur tenendo conto che il supporto a framework diversi da Shibboleth è attualmente limitato. Le indicazioni che faranno esplicito riferimento a questo software verranno messe in evidenza con il simbolo:

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 IDEM, nella sezione "Come partecipare". Ogni modifica al documento verrà comunque notificata con le modalità indicate nella sezione "Comunicazioni ai partecipanti".

2 Protocolli e Software

2.1 Protocolli

2.1.1 SAML

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

2.1.2 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[4], Istituto Nazionale di Ricerca Metrologica, i cui server primari sono i raggiungibili agli indirizzi:

[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/

ntp1.inrim.it (193.204.114.232)

ntp2.inrim.it (193.204.114.233)

2.2 Software

2.2.1 Shibboleth

Fra le diverse implementazioni[5] dello standard SAML, la Federazione IDEM ha scelto di adottare inizialmente il framework Shibboleth[6], che offre adeguate garanzie di funzionamento e di aderenza agli standard e del quale hanno ampia diffusione implementazioni open source.

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 è cessato il 30 Giugno 2010.

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

2.2.2 Altri software

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

3 Autenticazione

3.1 Login dell'utente

La pagina web da presentare all'utente con la richiesta di credenziali per l'autenticazione (pagina di Login) deve aderire a precise linee guida ovvero deve soddisfare i requisiti obbligatori sotto indicati. Tali requisiti saranno verificati al momento della richiesta di registrazione del servizio e periodicamente nell'ambito dell'attività di auditing (v. sezione Operatività del servizio).

In particolare tale pagina di Login deve obbligatoriamente:

a) utilizzare l'autenticazione in modalità web based tramite form: questo metodo presenta all'utente il form di autenticazione inserito in una pagina web, che può essere personalizzata applicandovi le scelte stilistiche proprie dell'organizzazione che amministra l'IdP. È quindi espressamente vietato l'utilizzo della modalità di autenticazione basata su pop-up;

b) contenere ALMENO UN riferimento ipertestuale o logo di IDEM con link alla pagina di contatto tecnico; in caso di pagine di autenticazione centralizzata legacy (tipo CAS), che diventa anche pagina di autenticazione per IDEM, il riferimento/logo può essere inserito in modo "discreto" così da non disturbare la familiarità sviluppata dagli utenti.

È inoltre, fortemente consigliato, ma non obbligatorio, inserire nella pagina di Login ulteriori informazioni che l'organizzazione ritenga utili a far conoscere e comprendere ai propri utenti quale sia l'utilizzo di IDEM per l'accesso ai servizi. In particolare si consiglia di inserire nella pagina di Login:

[5] http://saml.xml.org/wiki/saml-open-source-implementations

[6] http://shibboleth.internet2.edu/

- un contesto alla navigazione utente che indichi chiaramente che l'accesso al servizio avviene/può avvenire tramite sistema di autenticazione federata IDEM;
- informazioni relative alle credenziali di accesso ed a come ottenerle in base al proprio profilo utente;
- informazioni su IDEM e sulle modalità di adesione a IDEM;

3.2 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 IdP decade.

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.

Shibboleth 2 fissa di default questo intervallo a 30 minuti.

3.3 Certificati

È necessario che l'IdP 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 dall'host utente all'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 (evitando potenziali rischi). Inoltre 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.

3.3.1 CA accettate

Per i motivi di cui al paragrafo precedente, la Federazione considera validi i certificati rilasciati da CA i cui certificati root siano installati di default sui 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 accettate.

4 Firewall

In Shibboleth 2.x la comunicazione fra IdP e SP avviene sempre attraverso il browser dell'utente (è importante notare che le asserzioni scambiate sono firmate). In particolare il passaggio degli attributi avviene con modalità push (e cifratura degli stessi). Nel caso invece di Shibboleth 1.3, successivamente all'autenticazione, il SP richiede gli attributi all'IdP su un canale distinto (Attribute Service o più comunemente back-channel). Poiché IDEM supporta ancora IdP o SP Shibboleth 1.3 è

importante che anche questa comunicazione venga consentita pena il fallimento nell'accesso al servizio.

Nella pratica quindi si utilizzano normalmente le seguenti porte:

- 8443 TCP per la comunicazione Attribute Service (Shibboleth 1.3);
- 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.

5 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 l'organizzazione scelta dall'utente. Per rimuovere tale memorizzazione è sufficiente accedere al server WAYF, all'indirizzo https://wayf.idem.garr.it, e seguire le istruzioni.

6 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 per l'utente la scelta della propria struttura di appartenenza all'atto dell'autenticazione presso il fornitore.

7 Attributi

La denominazione, la sintassi e la semantica degli attributi scambiati all'interno della Federazione sono definiti nel documento Specifiche tecniche per la compilazione e l'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 IDEM) 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 SP 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.

8 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 nel capitolo 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 non ci sia corrispondenza tra il valore di scope definito per gli attributi, in attribute-resolver.xml e quello definito nei metadati, un SP potrebbe scartare i valori relativi ricevuti dall'IdP.

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

8.1 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 (anche se attraverso il browser dell'utente) e l'utilizzo di un certificato rilasciato da un'autorità nota non aggiunge nessun valore da un punto di vista della sicurezza. Infatti, 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. NdP).

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 cap. *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.

8.2 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 (si veda sezione Comunicazioni col Servizio IDEM GARR AAI);
- 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 solo 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 (si faccia riferimento qui[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.

9 Pagina web di supporto agli utenti

La predisposizione di una pagina web di supporto agli Utenti è un requisito base per ogni Partecipante, previsto in NdP. L'indirizzo della pagina deve essere comunicato a IDEM tramite i moduli di registrazione Servizi IPRR e RRR.

I requisiti obbligatori, sotto indicati, saranno verificati al momento della richiesta di registrazione del servizio e periodicamente nell'ambito dell'attività di auditing (v. sezione Operatività del servizio).

9.1 Pagina associata all'IdP

La pagina deve obbligatoriamente contenere le indicazioni relative a:

- indirizzo di posta elettronica per il supporto agli utenti in merito a IDEM e alle credenziali di autenticazione;
- informativa all'utente sul rilascio degli attributi utente ai fornitori di risorse .

Facoltativamente, potranno essere inserite nella pagina ulteriori informazioni che l'organizzazione ritenga utili per far conoscere IDEM ai propri utenti e per favorire l'utilizzo dei servizi, quali:

- denominazione dell'organizzazione (riportata nel WAYF);
- ulteriori recapiti (indirizzi e-mail, numeri di telefono, fax e cellulari) che gli utenti possono contattare per ottenere supporto in merito al sistema di gestione identità e ai servizi fruibili tramite l'autenticazione federata IDEM;
- riferimenti alla privacy policy adottata dall'organizzazione (ad es. link all'informativa che descrive il trattamento dei dati personali o al regolamento sul trattamento dei dati personali, resi noti tramite i siti web istituzionali);
- nominativi, indirizzi e-mail e numeri telefonici dei referenti e dei contatti tecnici per IDEM;
- logo di IDEM e link al sito IDEM;
- elenco di Risorse a disposizione degli utenti dell'organizzazione e/o link alla pagina Risorse del sito IDEM;
- FAQ predisposte localmente e/o link alla pagina FAQ del sito IDEM;
- link alla pagina di autenticazione.

È consigliabile che la pagina non risieda sullo stesso IdP, in modo che sia raggiungibile anche quando questo non lo fosse. A seguito dell'approvazione del servizio da parte della Federazione la pagina

[7] https://spaces.internet2.edu/display/SHIB2/IdPMetadataProvider

dovrà essere riferita dall'interfaccia di autenticazione.

9.2 Pagina associata alla Risorsa

La pagina deve obbligatoriamente contenere le indicazioni relative a:

- denominazione dell'organizzazione;
- indirizzo di posta elettronica per il supporto agli utenti della risorsa ed ai gestori dei servizi di identity management;
- riferimenti alla privacy policy adottata nella gestione della risorsa (es. informativa agli utenti su attributi richiesti e relativo trattamento).

A seguito dell'approvazione della risorsa da parte della Federazione la pagina dovrà essere riferita dalla pagina di accesso alla risorsa.

10 Comunicazioni

10.1 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.

10.2 Comunicazioni col Servizio IDEM GARR AAI

Le comunicazioni dal Servizio IDEM GARR AAI ai Referenti e ai Contatti Tecnici avvengono tramite messaggi di posta elettronica firmati con certificato della CA GARR o di una CA accettata da IDEM (si veda sezione Autenticazione). Al fine di effettuare la verifica dell'affidabilità del mittente e dell'integrità dei dati, si richiede che anche la trasmissione del frammento dei metadati e di altri dati critici alla Federazione avvenga con modalità sicure (invio email firmata all'indirizzo idem-help@garr.it con certificato della CA GARR o di una CA accettata da IDEM o, in alternativa, pubblicazione su una pagina https protetta da un certificato con le caratteristiche di cui sopra).

11 Operatività del servizio

La Federazione, al fine di consentire una migliore qualità ed efficienza, adotterà degli strumenti automatici di monitoraggio del servizio offerto dal partecipante (*attualmente il servizio di monitoring è in fase sperimentale, la sua entrata in produzione è prevista per il 2011*).

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.

La pagina web che ogni partecipante deve mettere a disposizione per fornire informazioni agli utenti del servizio (vedi sezione Pagina web di supporto agli utenti) verrà acceduta automaticamente e ne verrà monitorata la disponibilità. La Federazione potrà inoltre inviare e-mail che richiedano conferma di lettura (ad esempio mediante richiesta di conferma di presa visione del contenuto) agli indirizzi di posta elettronica a disposizione degli utenti.

I requisiti in questione devono essere posseduti al momento dell'ammissione alla federazione, e saranno soggetti a monitoraggio periodico. Il monitoraggio avverrà da macchine con indirizzi preventivamente comunicati ai Contatti Tecnici della risorsa ed avrà cadenza casuale differenziata a seconda della funzionalità da monitorare. Si prevede che le tempistiche potrebbero essere 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 Tecnico Scientifico 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 (punto a) per un periodo superiore ai 30 giorni;
- mancanza della pagina web (punto b) per un periodo superiore ai 15 giorni;
- mancata verifica del supporto via email (punto c) per un periodo superiore ai 60 giorni.

12 Logging

Come già richiamato in NdP, 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.

Technical Specifications for IDEM Federation

v 1.3

June 12th, 2012

Revisions

Versione	Data	Descrizione	Autori
1.0	15/09/2009	Initial version	G. Birello R. Conte M. Ianigro C. Marotta With contribution from: F. Malvezzi B. Monticini
1.1	23/02/2010	Introduction of "Abbreviations" and "Contacts"; Modified third paragraph of the introduction; Modified first and forth paragraph of section Shibboleth and renamed in SAML e Shibboleth; Renamed paragraph Apache vs Tomcat in user Login and added notes on CAS; Modified Introduction in Firewall paragraph; Modified text order in the chapter "Validity time"; Modified text in the Certificates chapter; Modified paragraph 3 of the Metadata chapter and paragraph 2 in the Certificates section of the same chapter; Substitution of Reference for users with web Page for user support; Introduction of Communications with IDEM Service GARR AAI section invoked by Metadata managing Methods and has been introduced the possibility of communication of the same through external site; Shift in the section Operation of Service of 2 sentences from Users Reference and added information on the date of activation of the monitoring service.	V. Calabritto R. Cecchini R. Conte R. Gaffuri T. Podestà
1.2	07/02/2011 12/06/2012	Amendments to section 3.1 – User's Login English translation – minor revisions	A.De Nicola M.L. Mantovani

Preamble

To report suggestions, errors or inaccuracies in this document, please write to: idem@garr.it

Abbreviations

STA = Technical Specifications for Compilation and Use of Attributes

NdP = Rules of participation

IPRR= Identity Provider Registration Request

RRR = Resource Registration Request

IdP = Identity Provider

SP = Service Provider

CA = Certification Authority

WAYF = Where Are You From

Contacts

IDEM Site = https://www.idem.garr.it

IDEM Federation idem@garr.it

IDEM GARR AAI Help desk: idem-help@garr.it

1 Introduction

This document provides technical recommendations for participants to the IDEM (IDEntity Management for federated access) Federation (hereinafter referred to as “the Federation”), and aims at the regulation of all those technical aspects in relation to interaction between participants, or between IdP and SP. It is not a support booklet for software installation.

In this document you can find the general configuration modalities of Services that the participants need to meet to achieve interoperability between the members of the Federation. The recommendations are provided so as to be applicable despite of the type of implementation used of the SAML protocol, keeping in mind though that the support to frameworks different from Shibboleth is actually limited. The information that will make explicit reference to this software will be highlighted with the following icon:

Due to the natural rapid software evolution the present document may incur in different changes in time. Therefore it is recommended to always rely upon the latest version, available on the IDEM site, in the section “Join”. Each new change to this document will be notified as described under "Communications to participants."

2 Protocols and Software

2.1 Protocols

2.1.1 SAML

IDEM, like other federations, uses the SAML[1] protocol at the present in the 2.0. For further information you are requested to refer to saml.xml.org[2] and OASIS[3].

2.1.2 NTP

For security reasons the synchronism between the servers is crucial for the successful interactions between the actors of the Federation that need to exchange information. Answers to messages sent too late (even apparent) on the one hand can be regarded as potential threats to the integrity of the party and lead to communication failure. This is the reason why we recommend the use of a time synchronization protocol on the servers of the Federation as the Network Time Protocol.

Aiming towards simplifying the configuration, it is advisable to use the server provided by iNRiM[4], National Institute of Metrological Research, whose primary servers are reachable at the following addresses:

ntp1.inrim.it (193.204.114.232)

[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/

ntp2.inrim.it (193.204.114.233)

2.2 Frameworks

2.2.1 Shibboleth

Between the different implementations[5] of SAML standard, the IDEM Federation had initially chosen to adopt the Shibboleth[6] framework, that provides adequate guarantees of function and adherence to standards and which are widespread open source implementations.

At the time this document is being written, several Shibboleth 1.3 installation exist. Given the configuration difficulties, the poor readability and the little information provided by logs, such version is deprecated by the Federation. Furthermore as of now Internet2 will not add any more features to this version whose support has ceased on June 30, 2010.

For all new installations it is thus advised the adoption of version 2.x, the only version supported by the Federation.

2.2.2 Different frameworks

Participants may adopt any other product that implements the SAML 2.0, provided that, in this case, technical support cannot be guaranteed by the Federation.

3 Authentication

3.1 User login

The web page to be presented to the user with the request of insert credentials for authentication (login page) must adhere to strict guidelines that must meet the mandatory requirements below mentioned. These requirements will be verified at the time of application for registration of the services and periodically during auditing activity (see operation service section).

In particular such Login page must mandatorily:

a. use authentication in a web based mode form which can be customized by applying their stylistic choices of the organization that administers the IdP. It is therefore expressly forbidden to use the authentication mode based on pop-up

b. contain AT LEAST ONE IDEM hypertext reference or logo of IDEM with link to the technical contact page; in case of centralized legacy authentication pages (i.e. CAS) that also becomes the authentication page for IDEM, the reference/logo can be placed in a “discreet” way so as not to disturb the familiarity developed by users.

It is therefore, highly recommended, but not mandatory, to insert in the Login page further information that the organization judges as useful to make understand and let know the usage of IDEM for the access to the services. In particular it is advised to insert in the Login page:

- a user navigation context which clearly indicates that the access to the service takes place/can take place through the IDEM federated authentication system;
- information on access credentials and how to obtain them according to own user profile;

[5] http://saml.xml.org/wiki/saml-open-source-implementations
[6] http://shibboleth.internet2.edu/

- information on IDEM and how to join it;

3.2 Validity Time

Another point where attention is needed is the validity time of the authentication, i.e. the time interval after which an authenticated session from an IdP expires.

Possible changes to this value can be made for local needs only after careful evaluation of security impact within the individual organizations.

Shibboleth 2 sets to 30 minutes the default interval.

3.3 Certificates

It is necessary that the IdP has a certificate to encrypt the page with which the user is authenticated. This first authentication phase actually requires that the data travels in a secure way by the user client to the IdP host. Moreover, since the authentication page must have the highest degree of accessibility, it is important that the certificate used to encrypt the connection is issued by a well known Certification Authority, whose root certificate must be installed by default in the user browser (avoiding potential risks). Besides it is not absolutely necessary that the user gets distracted during the authentication phase, by a security message of the browser for 'problematic' certificate. Consequently the interaction between user and IdP (front channel) self-signed certificates are not accepted or released by CA not accepted by the Federation.

3.3.1 Accepted CAs

For the reasons referred to in the preceding paragraph, the Federation considers valid the certificates issued by CAs whose root certificates are installed by default on most popular browsers: Internet Explorer, Mozilla Firefox, Safari.

The Federation may, at its sole discretion, modify the list above and take into account possible exceptions for CAs accepted.

4 Firewall

In Shibboleth 2.x the communication between IdP and SP takes place through the user's browser (it is important to note that the exchanged assertions are signed). In particular, the transition of the attributes takes place with the push mode (encryption of the same). In the Shibboleth 1.3 case, following the authentication, the SP requires the IdP attributes on a separate channel (Attribute Service or more commonly back-channel). Since IDEM still supports Shibboleth 1.3 it is important that this communication is allowed otherwise access to the service will fail.

Practically the following ports are the ones used normally:

1. **8443** TCP for the Attribute Service communication (Shibboleth 1.3);
2. **443** TCP to authenticate users;

3. 80/443 TCP for access to the SP Service.

Therefore for the IdP it is necessary to open the ports 443 and 8443 TCP while for the SP, in accordance to how the service is exposed, of the 80 or 443 port TCP.

5 Discovery Service

The Federation manages and maintains the centralized WAYF (Where Are You From) for the selection of the user organization among the participant organizations to the Federation.

The service contains the complete list of all the IdP and the coordinates of its authentication sites at the corresponding Home Organization. Communication with the WAYF server is secured via https.

The service can permanently store the user's chosen organization. To remove this stored choice it is sufficient to access the WAYF server, at https://wayf.idem.garr.it, and follow the instructions.

6 Nomenclature

The Federation will ensure consistency of nomenclature of institutions belonging to the Federation and how they appear in the list of the WAYF or in metadata, possibly modifying proposed descriptions where appropriate, for consistency with the other participants.

For service providers who participate in multiple federations it is necessary for them to manage their own WAYF service. It is the responsibility of the Federation to disclose to these service providers, references to be included and their descriptive parts in order to make uniform to the user the choice of his home organization.

7 Attributes

The name, the syntax and semantics of the attributes exchanged within the Federation are defined in the document Technical Specifications for Compilation and Use of Attributes. To obtain a minimum level of interoperability with the Federation it is necessary that the attributes eduPersonScopedAffiliation and eduPersonTargetedID are released to all participants. Nevertheless the access to each service is not guaranteed because is the service provider who decides whether and through which attributes authorize the access of its service. The duty of the Federation is to limit the request of attributes, especially the personal ones, to only the ones really necessary to access the service. For more details about attributes, please refer to the above mentioned document.

Since, as just mentioned authorization to access a particular service is in charge of the supplier, it is of good habit that the service provider provides the users with a page for the release test of the necessary attributes to access the service itself.

In order to simplify the shibboleth 2.x configuration, the Federation (through the IDEM site) provides the file attribute-resolver .xml preconfigured to recover from an LDAP server, the required, recommended and optional attributes defined by the Federation. However It will be necessary to customize the configuration by indicating exactly the scope of the organization, roles or positions of the users within their organizations, needed to assign a value to the attribute eduPersonScopedAffiliation and the parameters of the LDAP server. Similarly, the Federation provides attribute-filter.xml file, with the

configuration for the release of the necessary attributes to the different SP within the Federation.

In the configuration for retrieving attributes from the backend (attribute-resolver.xml) it is important to note that scoped attributes (eduPersonScopedAffiliation, eduPersonPrincipalName) have the correspondent scope stated in the metadata. If these do not coincide the attributes sent by the IdP may be discarded by the SP.

8 Metadata

The metadata file is the tool with which trust is shared within the Federation. Through this file the Federation publishes the participant's descriptive data who use metadata to verify the partner's identity during communications, establishing trust relations. It is therefore extremely important to pay very much attention to this file since it holds all necessary information for mutual recognition of participants. Further verification systems of counterparts through web server configuration for the CRL verifications, authentication with x509 certificates etc., are redundant and strongly discouraged.

Note. Some services can appear non accessible in case a service is set-up to delegate to applications different from the IdP data verification.

As already anticipated in the "Attributes" chapter it is important to pay attention to the scope value defined for scoped attributes (eduPersonPrincipalName e eduPersonScopedAffiliation) defined as well in the metadata. In case the scope defined for the attributes, in attribute-resolver.xml does not correspond to the one defined in the metadata, a SP could discard the relative attributes received from the IdP.

The metadata file must be downloaded at the URL https://www.idem.garr.it/docs/conf/idem-metadata.xml, or at the URL https://www.idem.garr.it/docs/conf/signed-metadata.xml for signed version, with the agreed frequency. The Federation will apply the relative control.

8.1 Certificates within metadata

the certificate included within the metadata file can be self signed. This means that the public key of the service is included in metadata.

The certificate included in the metadata is used in the direct communications between IdP and SP (even if through the user's browser) and the use of a certificate released by a well known authority doesn't add value from a security point of view. In fact the eventual burden to have to request the cancellation of the certificate to the CA is anyway in charge on the owner of the certificate (in his interest that no one shows up with his name). Therefore in the case of compromising self signed certificates it is however responsible of the service that has to promptly notify the incident to the Federation communicating the new Metadata (with a new certificate). This method activates a faster execution of the verification tests of the counterparts during interaction and a lesser time of downtime of server in case of compromised certificate. The guarantor functions entrusted to the CA in a traditional PKI, in that case they are handled by the Federation, which verifies the participant's identity at the act of transmitting its metadata and certifies to the other participants, the authenticity of the whole metadata file through the Federation signature. The Federation also, in case of a

participant's security problem, can at its own unquestionable judgment, exclude the participant from the Federation removing the corresponding fragment from the Metadata (Cfr. NdP).

Note. The usage of a self signed certificate doesn't imply the usage of the same in the pages accessible to the user *(front-channel)* on the contrary for these communications it is requested a certificate released by a CA approved by the Federation (see Authentication chapter).

The usage of a non self signed certificate but released from a CA requests, besides the usage of the files containing the certificate itself and the relative key, also the updating of the java keystore and the manual modification of the metadata file. On the contrary using self signed certificates generated instantly at the time of installing Shibboleth, to generate a new certificate it is sufficient to rerun the installation script in a different directory copying later the necessary files in the appropriate directory of the IdP in production.

8.2 Procedures for managing Metadata

As a result of what has been said in the preceding paragraphs it is therefore requested from the participants a great care in handling metadata, especially in the following steps:

1. Entry of a SP/IdP in the metadata: the relative fragment to the new service will have to explicitly enclose the certificate; it is requested the fragment transmission to the Federation via secure procedures (see communication section with the IDEM GARR AAI service);
2. Variation of metadata: it is requested from the participants to immediately transmit the data variation especially in case of certificate variation/cancellation;
3. Downloading of the updated metadata: participants must collect the metadata from the Federation at least once a day. The metadata can be collected only through HTTPS protocol but the signature verification is recommended;
4. Storing the metadata file: the downloaded file must be stored on the server without modification rights.

Shibboleth foresees different ways for managing metadata (please refer here[7]). The IDEM Federation suggests the modality FileBackedHTTPMetadataProvider where metadata are periodically picked up and downloaded in a file for their consultation until the next update. The metadata provided by the Federation have a life span of 24hrs. Participants can, for internal reasons decide to decrease the time interval for updating the metadata intervening on the cache Duration attribute.

9 Web page for users support

The preparation of a web page for users support is a basic requirement for every Participant, foreseen in NdP. The address of the page must be communicated to IDEM through the Service

[7] https://spaces.internet2.edu/display/SHIB2/IdPMetadataProvider

registration forms IPRR e RRR.

The mandatory requirements, mentioned below, will be verified at the moment of registration request of the service and periodically within the auditing activity (see section Operation of the service).

9.1 Page associated with IdP

The page must include the information relating to:

1. E-mail address for user support concerning IDEM and authentication credentials;
2. Information to the user on release of user attributes to resource providers.

Optionally, further information can be inserted in the page that the organization considers useful to make IDEM known to is users and to encourage the use of services, such as:

1. Name of the organization (shown in the WAYF);
2. Further details (e-mail addresses, phone numbers, fax and mobile) that users can contact to get support on the identity management system and on the services available through the IDEM Federation;
3. References to the privacy policy adopted by the organization (i.e. link to the information to the users that describes the processing of personal data or regulation on the processing of personal data made available via institutional websites);
4. Names, e-mail addresses and telephone numbers of the Referente Organizzativo (RO), of the Referente Tecnico (RT), and of Service Contact Persons for IDEM;
5. IDEM logo and link to the IDEM website;
6. List of available Resources for the organization’s users and/or link to Resource page to IDEM website;
7. FAQ prepared locally and/or links to the FAQ page of the IDEM;
8. link to the authentication page.

It is recommended that the page doesn’t reside on the same IdP, so that it can be reached independently from the other. Following the service approval by the Federation the page will have to be referred by the interface authentication.

9.2 Page associated with the resource

The page must include the following information relating to:

- Name of the organization;

1. e-mail address for supporting resource users and IDPs managers;
2. References to the privacy policy adopted in resource management (e.g. information to users on the attributes required and its treatment).

After approval of the resource by the Federation the page must be linked by the access page to the resource.

10 Communications

10.1 Communications to participants

Notices to the participants occur through a mailing list managed by the Federation. The organizational contact, technical contact person and technical contacts of the participant are by rule inserted in the above mentioned mailing-list.

10.2 Communications with the IDEM GARR AAI Service

Communications from IDEM GARR AAI Service to referents and Technical contacts take place through e-mail messages signed with GARR CA certificate or by a CA accepted by IDEM (see the Authentication section). In order to carry out verification of reliability of the sender and data integrity, it is required that the transmission of metadata fragment and other critical data to the Federation is secured (send email to the address idem-help@garr.it with signed certificate of the CA or a CA GARR accepted by IDEM or, alternatively, publication on a https page protected by a certificate with the features mentioned above).

11 Operation of the service

The Federation, in order to provide better quality and efficiency, intend to adopt automatic tools for monitoring the service provided by the participant (*currently the monitoring service is in experimental stage, going into production is scheduled for 2011*).

The points that determine the quality of the service are the following:

1. uptime of the identity provider (IdP) or the service provider (SP)
2. availability of a web page for support information to users;
3. availability of an e-mail address as helpdesk for users.

Regarding IDP uptime, , automatic mechanisms will be implemented for authentication at the IdP, through the use of automated web client; the participant will be asked to provide a test user to be used to validate the authentication process.

With regard to the SP, reachability of urls of the service will be checked.

The web page that each participant has to make available to provide information to users of the service (see Web support page to users section) will be automatically accessed and its availability will be monitored. The Federation will be also able to send e-mails that request the reading confirmation (for example through confirmation request of having read the content) to the e-mails addresses available to users.

The requirements in question must be owned at the time of admission at the Federation, and will be subject to periodic monitoring. The monitoring will be done by machines with addresses notified in advance to the technical contacts of the resource and will be held randomly depending on the features to be monitored. It is expected that the timing could be as follows:

- uptime of the server (point 1) weekly;;
- web page availability (point 2): weekly;
- e-mail address availability (point 3): monthly.

Failure to pass the tests will be notified to the Technical Scientific Committee and via e-mail to the Technical Contact persons indicated in the central database and may result in a temporary suspension of service in the following cases:

- inoperability of the service (point a) for a period exceeding 30 days;
- absence of the web page (point b) for a period exceeding 15 days;
- Failure to check the support via email (point c) for a period exceeding 60 days.

12 Logging

As already mentioned in NdP, each participating Organization undertakes to maintain a record of the activities linked to their own services (IdP or SP) in order to provide better support in the resolution of technical problems or in the management of any security incidents.

These logs must necessarily contain the information that makes it possible to trace the hosts involved in the operation (IP address), the users, the type of operation and attributes issued. For the purposes of participating in the Federation, Members and partners undertake to keep such information for a period of not less than 6 months, in order to allow also activity ‘in retrospect’.

The log will be kept by the Participant and will not be transferred or shared with the Federation or other Participants; however, the Federation will also require the Participant to provide information on specific events, and the Participant, in compliance with the rules on privacy, is required to provide such information.

The Federation will also decide, within the framework of auditing activities, to require occasionally information relating the access made by their own monitoring systems, in order to verify the correctness of the data recorded in the log. Such requests may be made with intervals not less than 6 months. Failure to comply with the specifications to the logging may lead to the suspension of the service.