Specifiche Tecniche per la Federazione IDEM

G.Birello

R. Conte

M. Ianigro

C. Marotta

con contributi di:
F. Malvezzi

B. Monticini

v 1.2
Febbraio 2011

Revisioni

Versione	Data	Descrizione	Autori
1	15/09/'09	Versione iniziale	*vedi frontespizio*
1.1	23/2/'10	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/'11	Modifiche alla sezione 3.1 - *Login dell'utente*	

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 - Compilazione e 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 Implementazioni e Software

2.1 Protocolli

2.1.1 SAML

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

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, Istituto Nazionale di Ricerca Metrologica, i cui server primari sono i raggiungibili agli indirizzi:

ntp1.inrim.it (193.204.114.232)

ntp2.inrim.it (193.204.114.233)

2.2 Applicativi

2.2.1 SAML 2 e Shibboleth

Fra le diverse implementazioni dello standard SAML, la Federazione IDEM ha scelto di adottare inizialmente il framework Shibboleth, 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 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 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:

- 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 ad 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 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.

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 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 NdP.

7 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 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 questo non corrisponda allo scope definito per gli attributi, in attribute-resolver.xml ed a quello definito nei metadati, un SP potrebbe scartare gli attributi relativi ricevuti dall'IdP.

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.

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 manule 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). 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 della 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 sul rilascio degli attributi utente ai fornitori di risorse .

Facoltativamente, potranno essere inserite nella pagina ulteriori informazioni che l'organizzazione ritenga utili a far conoscere IDEM ai propri utenti e a 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'infomativa che descrive il trattamento dei dati personali effettuato tramite i siti web istituzionali o al regolamento sul trattamento dei dati personali);
- 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 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 su attributi richiesti e relativo trattamento).

A seguito dell'approvazione del servizio 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. Ogni comunicazione verrà anche pubblicata sul sito IDEM.

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, adotta 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. 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 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.