Norme di partecipazione alla Federazione IDEM

v 0.9

20 Maggio 2009

Revisioni

Versione	Data	Descrizione	Autore
00.09.00	20 Maggio 2009	Versione iniziale	

Premessa

Il presente documento definisce:

- le regole e le procedure di adesione alla Federazione IDEM (Identity Management per l'accesso federato, di seguito "**Federazione**"), nonché le modalità di sospensione e cessazione della partecipazione;
- le condizioni e le modalità di registrazione di Servizi da parte dei Partecipanti;
- l'insieme di norme che regolano lo scambio di informazioni su utenti finali e servizi.

I Partecipanti, sottoscrivendo la **Richiesta di Adesione** (RA) o l'**Accordo di Collaborazione** (AC), accettano il **Regolamento**, le **Norme di Partecipazione** (NdP), le **Specifiche tecniche** (ST) e le **Specifiche tecniche per la compilazione e l'uso degli attributi** (ST-A). La somma di questi documenti costituisce l'infrastruttura tecnico-legale della Federazione

Partecipazione alla Federazione

Partecipanti

Ai fini dell'adesione alla Federazione è indispensabile la partecipazione con un Servizio, che può essere:

- un servizio di gestione e verifica delle identità, tramite la messa in opera di un componente software denominato **Identity Provider** (IdP);
- una Risorsa accessibile in rete a seguito di una procedura di autenticazione e autorizzazione, tramite la messa in opera di un componente software denominato **Service Provider** (SP).

I Partecipanti alla Federazione, ai sensi del Regolamento, si distinguono in:

1. **Membri**: organizzazioni afferenti alla comunità GARR;
2. **Partner**: organizzazioni esterne a GARR.

I Membri registrano principalmente un servizio di gestione e verifica delle identità, ma possono registrare anche una o più Risorse. I Partner generalmente registrano una o più Risorse.

L'Organizzazione che intende aderire come Membro deve compilare la **Richiesta di adesione** ed inviarla, completa degli allegati, alla Federazione.

L'Organizzazione che intende aderire come Partner deve compilare l'**Accordo di Collaborazione** ed inviarlo, completo degli allegati, alla Federazione.

La Richiesta, o l'Accordo, deve essere firmata dal legale rappresentante dell'Organizzazione che richiede l'adesione. Se i requisiti sono soddisfatti, il GARR controfirma il Documento e lo fa pervenire all'Organizzazione.

Il Membro preferibilmente registra nella Federazione un solo IdP relativo al sistema di Identity Management della propria Organizzazione. In funzione di uno specifico contesto, a fronte di domanda fatta pervenire dal Membro alla Federazione e supportata da una relazione tecnica della configurazione proposta, il Comitato di Indirizzo può consentire la registrazione di più di un IdP.

In via eccezionale, e a fronte di richiesta accuratamente motivata, il Comitato di Indirizzo può consentire anche al Partner la registrazione dell'IdP dell'Organizzazione.

Tutti i nominativi e i dati personali delle persone indicate nei contratti e nei moduli necessari all'adesione dell'Organizzazione verranno utilizzati per gli scopi della Federazione e trattati con strumenti cartacei e informatizzati. Essi potranno essere comunicati e resi accessibili anche su pagine web agli altri Partecipanti alla Federazione e i relativi indirizzi email inseriti in liste di distribuzione. L'Organizzazione partecipante si impegna a dare questa informativa ai propri membri.

Requisiti per l'adesione

Requisiti base per ogni Partecipante

- La Federazione deve ricevere dal Partecipante comunicazioni tempestive in merito a ogni variazione dei nominativi e dei recapiti del Referente Organizzativo, ove applicabile, del Referente Tecnico, ove applicabile, e dei Contatti Tecnici;
- il Partecipante deve realizzare una pagina web secondo il modello descritto in ST e provvedere all'aggiornamento delle informazioni in essa contenute;

Requisiti per la registrazione di un servizio

- I Servizi, IdP e SP, devono essere conformi alle specifiche dei documenti ST e ST-A;
- i Servizi, IdP e SP, devono essere sotto la completa responsabilità del Partecipante che li registra anche quando gestiti tramite contratti di *outsourcing*;
- per ogni Servizio registrato, il Partecipante deve fornire i propri metadati, che deve mantenere aggiornati secondo le indicazioni della Federazione, rispettando la procedura e i tempi indicati in ST;
- per ogni Servizio registrato, il Partecipante deve indicare almeno un Contatto Tecnico[1], il principale responsabile tecnico per la configurazione del Servizio; questi mantiene i contatti con il Servizio IDEM-AAI per la corretta configurazione del Servizio, secondo le indicazioni della Federazione; la variazione del Contatto Tecnico deve essere tempestivamente comunicata alla Federazione;
- i certificati sui Servizi devono essere configurati seguendo le indicazioni fornite in ST.

1 Il partner può, a sua discrezione, includere tra i contatti tecnici l'eventuale figura commerciale che deve ricevere le comunicazioni dalla Federazione

Ulteriori requisiti per la registrazione di un IdP

- Gli attributi relativi agli utenti devono essere resi disponibili e utilizzati nel rispetto della privacy dell'utente e in modo conforme a denominazione, sintassi e semantica indicate in ST-A;
- deve essere reso disponibile agli altri Partecipanti un documento contenente i dati salienti riguardo il sistema di identity management ed i relativi attributi supportati, secondo lo schema **DOPAU** (DOcumento Processo di Accreditamento degli Utenti), predisposto dalla Federazione; i fornitori di Risorse potranno utilizzare le informazioni relative alle procedure operative di gestione degli utenti per determinare il livello di fiducia delle asserzioni per ogni Partecipante.

Ulteriori requisiti per la registrazione di una Risorsa

- Deve essere reso disponibile agli altri Partecipanti un documento contenente i dati salienti riguardo il sistema di accesso alle Risorse secondo lo schema **DOPAR** (DOcumento Processo Accesso alla Risorsa) predisposto dalla Federazione; i Membri della Federazione potranno valutare le regole e le procedure operative adottate dai fornitori di Risorse in merito a uso e raccolta degli attributi utente, nonché i termini e le condizioni di eventuali contratti da stipulare per l'accesso alle Risorse.

Adesione e registrazione servizi

Richiesta di adesione/Accordo di Collaborazione

Per l'adesione alla Federazione, l'Organizzazione:

- prende visione di tutta la documentazione legale e tecnica messa a disposizione dalla Federazione e valuta la fattibilità della propria partecipazione con uno o più servizi, IdP e/o SP;
- compila in duplice copia la Richiesta di Adesione, se Membro, ovvero l' Accordo di Collaborazione, se Partner, e lo invia alla Federazione, completo degli allegati e firmato dal Legale Rappresentante: tramite questo documento l'Organizzazione accetta le regole derivanti dalla partecipazione alla Federazione e nomina i Referenti;
- contestualmente all'adesione, invia la richiesta di registrazione di un IdP e/o di una o più Risorse; ulteriori richieste di registrazione servizi potranno essere presentate in seguito.

Registrazione di un IdP

L'Organizzazione invia alla Federazione:

- il modulo di Registrazione IdP, compilato in duplice copia e sottoscritto dal Referente Organizzativo, ove applicabile, o dal Rappresentante Legale o dal suo delegato;
- il documento descrittivo del processo di accreditamento dei propri utenti compilato secondo lo schema DOPAU predisposto dalla Federazione: a seguito della registrazione dell'IdP la Federazione renderà disponibile tale documento ai soli Partecipanti che ne facciano richiesta;
- il frammento di metadati corrispondente al servizio da registrare, compilato con i dati richiesti in ST.

Comment [raf1]: Metterei nota con "Fare riferimento al documento ST per le modalità di invio dei MetaDati", inoltre occorre concordare la denominazione del membro. Questa verrà inserita poi dal servizio AAI all'atto dell'inserimento del frammento nei metadati, insieme al riferimento del contatto tecnico

Registrazione di una Risorsa

L'Organizzazione invia alla Federazione:

- il modulo di Registrazione Risorsa, compilato in duplice copia e sottoscritto dal Referente Organizzativo, ove applicabile, o dal Rappresentante Legale o dal suo delegato;
- il documento descrittivo del sistema per l'accesso alla Risorsa compilato secondo lo schema DOPAR predisposto dalla Federazione: a seguito della registrazione della Risorsa la Federazione renderà disponibile tale documento ai soli Partecipanti che ne facciano richiesta;
- il frammento di metadati corrispondente al servizio da registrare compilato con i dati richiesti in ST;

Impegni dei Partecipanti

Ogni Partecipante si impegna ad accettare le seguenti regole per il periodo di durata del presente accordo, oltre ad ogni altro obbligo ivi indicato:

- effettuare le modifiche che saranno decise dalla Federazione, incluse quelle relative alle specifiche tecniche o alle regole di partecipazione, entro i tempi previsti;
- riconoscere alla Federazione il diritto di pubblicare e utilizzare i metadati necessari al suo funzionamento
- riconoscere alla Federazione il diritto di pubblicare il nome dell'Organizzazione per scopi di promozione della Federazione stessa;
- evitare ogni atto che abbia come conseguenza un danno, anche potenziale, una violazione delle misure di sicurezza o un effetto negativo sulla reputazione per gli altri Partecipanti e la Federazione;
- collaborare con la Federazione all'effettuazione di controlli periodici (*auditing*);
- adottare regole tecniche e organizzative al fine di favorire il rispetto del diritto d'autore e, più in generale, della legislazione correlata ai contenuti e ai servizi messi a disposizione dagli altri Partecipanti e dalla Federazione.

Il Partecipante che registra un IdP si impegna a :

- mantenere sui propri sistemi dei registri d'uso (*log*) che consentano di risalire agli utenti

delle sessioni di autenticazione, con le modalità e per il tempo definiti in ST e fornire ogni ragionevole collaborazione alla Federazione o agli altri Partecipanti qualora fossero necessari chiarimenti e approfondimenti su attività rilevate come insolite e su eventuali incidenti di sicurezza;
- verificare periodicamente la conformità a quanto dichiarato tramite il DOPAU;
- fornire indicazioni ai propri utenti sulle Risorse della Federazione alle quali possono accedere.

Il Partecipante che registra una o più Risorse si impegna a:

- limitare la richiesta di dati sugli utenti alle informazioni utili ai fini dell'erogazione del servizio;
- mantenere traccia delle operazioni, fornire i dati utili al monitoraggio e alla valutazione dell'utilizzo della Risorsa e attenersi alle leggi vigenti per quanto riguarda il trattamento dei dati personali e la sicurezza informatica;
- non comunicare a terzi alcun dato relativo all'utente di cui sia venuto in possesso tramite la Federazione, in mancanza di accordi espliciti con l'Organizzazione di appartenenza;
- non effettuare aggregazioni di dati relativi all'attività degli utenti a fini commerciali senza permesso esplicito o previsto dai contratti in essere con le loro Organizzazioni di appartenenza;
- verificare periodicamente la conformità a quanto dichiarato tramite il DOPAR.

Comment [Roberto C2]: togliere? è chiaro che bisogna rispettare le leggi, e poi: quali leggi?

Comment [Roberto C3]: togliere? non è ambiguo?

Procedura di approvazione

Per ogni richiesta di adesione alla Federazione e ogni successiva richiesta di registrazione di Servizi verrà avviata dalla Federazione la procedura di approvazione, nel corso della quale potranno essere chieste ai Contatti indicati dall'Organizzazione informazioni aggiuntive rispetto a quelle ricevute. La procedura, in ogni caso, si concluderà entro e non oltre novanta giorni dalla data di ricevimento della richiesta.

La procedura di approvazione ha lo scopo di verificare che il candidato e i servizi proposti soddisfino i requisiti richiesti nel presente NdP e nella restante documentazione tecnico-legale della Federazione.

In primo luogo verranno verificati:

- per le richieste di adesione in qualità di Membro, l'appartenenza alla comunità GARR;
- per le richieste di adesione in qualità di Partner e la registrazione di nuove Risorse, l'effettivo interesse dei Partecipanti per le Risorse proposte e gli eventuali rischi a renderle disponibili tramite la Federazione.

Successivamente si procederà alla valutazione della completezza e congruità della documentazione inviata e alla conformità dei servizi proposti ai requisiti tecnici stabiliti dalla Federazione, verificando, fra l'altro:

- i certificati digitali installati;
- la correttezza della registrazione del Servizio nei metadati della Federazione;

- il funzionamento del Servizio;
- la completezza delle informazioni della pagina web predisposta dall'Organizzazione secondo lo schema fornito dalla Federazione in ST;
- la congruità dei dati rispetto alla documentazione inviata.

Le verifiche vengono effettuate dal Comitato Tecnico Scientifico, che trasmette la documentazione e l'esito dei controlli al Comitato di Indirizzo.

A seguito dell'esito positivo della procedura di adesione, l'Organizzazione è ammessa nella Federazione e viene inviato al richiedente l'accordo, o la richiesta, controfirmato. In caso contrario all'Organizzazione viene notificato il motivo del rifiuto.

Il Comitato Tecnico Scientifico provvede a dare comunicazione via web e posta elettronica all'Assemblea dei Membri dei nuovi Partecipanti e dei relativi Servizi.

Durata della partecipazione

Sospensione

Sospensione di un Partecipante

La Federazione può sospendere la partecipazione di un'Organizzazione qualora questa non sia in grado di soddisfare i requisiti richiesti, non rispetti le regole previste dal presente documento o arrechi danno, anche involontariamente, per incuria o negligenza, alla Federazione e/o a terzi.

Comment [Roberto C4]: Not a per il revisore legale:

i termini sono sinonimi o vanno specificati entrambi?

Il provvedimento di sospensione è comunicato al Partecipante con un preavviso commisurato alla rilevanza dell'irregolarità. Nei casi di grave violazione e danno arrecato alla Federazione, il provvedimento viene attuato con effetto immediato.

La sospensione comporta l'esclusione temporanea del Partecipante dalla Federazione e la rimozione del frammento di metadati corrispondente ai suoi servizi.

Sospensione di un Servizio

Qualora il Partecipante abbia registrato più di un servizio, il provvedimento di sospensione può essere limitato a singoli servizi (IdP o SP).

Il Partecipante può richiedere in qualsiasi momento la sospensione di qualsiasi servizio offerto direttamente dalla Federazione nel caso di compromissione dei sistemi interni al Partecipante o delle proprie chiavi di cifratura. La richiesta potrà essere comunicata alla Federazione via email o, in caso di emergenza, tramite telefono.

La sospensione di un Servizio comporta la rimozione del frammento di metadati corrispondente per il tempo necessario alla risoluzione del problema riscontrato.

La sospensione dell'unico Servizio equivale alla sospensione del Partecipante .

Scadenza e Rinnovo

La partecipazione, indipendentemente dalla data di iscrizione, si conclude il 31 dicembre di ogni anno, fatta salva la possibilità del Partecipante di terminare anticipatamente la propria partecipazione e l'esclusione del Partecipante da parte dalla Federazione. La partecipazione è automaticamente rinnovata per l'anno successivo se il Partecipante soddisfa i requisiti in vigore alla data del rinnovo.

Comment [Roberto C5]: Not a per il revisore legale:

Il paragrafo potrebbe essere tolto, a meno che non serva a fini legali (qualcuno ha avanzato questa ipotesi)

Risoluzione

La partecipazione può essere terminata se il Partecipante, in seguito a procedura di sospensione, non ha provveduto a soddisfare i requisiti descritti nelle presenti norme e nei documenti collegati per ulteriori trenta giorni dalla comunicazione ufficiale scritta da parte della Federazione.

L'esclusione del Partecipante deve essere decisa dal Comitato di Indirizzo, su proposta del Comitato Tecnico Scientifico.

Il Partecipante può recedere dalla Federazione comunicando tale decisione per iscritto con un preavviso di trenta giorni. I metadati relativi al Partecipante verranno rimossi.

Qualora non dovessero sussistere più le condizioni perché possa continuare ad offrire i propri servizi, la Federazione potrà in qualsiasi momento cessare la propria attività, comunicando tale decisione ai Partecipanti per iscritto e con un preavviso di novanta giorni.

In tutti i casi di risoluzione della partecipazione il Partecipante non avrà diritto ad alcun rimborso in nessuna forma.

Servizi della Federazione

La Federazione, tramite il Servizio IDEM AAI :

- rende disponibili il catalogo e i metadati dei Servizi disponibili: validità, veridicità e tempestivo aggiornamento di tali informazioni sono di esclusiva responsabilità dei Partecipanti;
- fornisce alle Organizzazioni della Comunità GARR il *know-how* per la realizzazione dei Servizi attraverso attività di *help-desk*, formazione e aggiornamento;
- fornisce ai potenziali Partner la documentazione e il supporto necessario all'interoperabilità delle Risorse;

- mette a disposizione il Discovery Service (WAYF);
- gestisce e mantiene il sito web ufficiale della Federazione;
- effettua attività di monitoraggio e auditing.

Comment [Roberto C6]: e per shib2?

Inoltre, la Federazione promuove la propria attività e i servizi offerti mediante l'organizzazione di workshop, conferenze, incontri di studio e, più in generale, la partecipazione ad eventi che vedano coinvolte Organizzazioni potenzialmente interessate ad aderire alla Federazione o a stabilire rapporti di collaborazione con essa.

L'appartenenza alla Federazione non garantisce agli utenti finali del Partecipante l'accesso alle Risorse della Federazione che vengono fornite da altri Partecipanti dietro stipula di appositi contratti.

I termini e le condizioni contrattuali eventualmente necessari per l'accesso a determinate Risorse utilizzate dai Partecipanti e rese disponibili da altri Partecipanti devono essere concordati tra le parti stesse, inclusi i termini e le condizioni tecniche, economiche, sulla proprietà intellettuale e ogni altro requisito per l'accesso.

Auditing

Il Partecipante accetta e consente che vengano effettuate dalla Federazione verifiche periodiche della conformità dei servizi registrati ai requisiti tecnici, come specificati in ST e ST-A e a quanto dichiarato in DOPAU e/o DOPAR, secondo le modalità descritte in ST.

Il Partecipante coopererà e fornirà l'assistenza necessaria per l'esecuzione delle verifiche, consentendo, ove richiesto, l'accesso ai propri Servizi mediante utenze di test. Le credenziali relative a tali accessi saranno custodite dalla Federazione e da essa utilizzate esclusivamente ai fini di monitoraggio e auditing.

La mancata aderenza ai requisiti tecnici verrà notificata al Partecipante contestualmente alla richiesta di provvedere all'adeguamento del Servizio, pena la sospensione della partecipazione.

I controlli di conformità vengono sottoposti a revisione con cadenza annuale dal Comitato Tecnico Scientifico.

Le procedure di verifica saranno condotte sia in modo automatizzato sia non automatizzato nei confronti di tutti i Partecipanti e avverranno in maniera continuativa, anche senza notifica preventiva.

Rispetto della privacy

I Partecipanti accettano di rispettare la riservatezza delle informazioni riguardanti i dati personali ed ogni altra informazione contenuta nei dati memorizzati o ricevuti durante i processi di gestione e controllo delle identità.

In particolare, il Partecipante conviene che non può memorizzare permanentemente, né condividere, né

rendere pubblico, né usare per qualsiasi motivo diverso dallo scopo proprio, qualsiasi dato personale che riceva da altri Partecipanti alla Federazione, salvi gli accordi di delega della responsabilità, previsti ai sensi del D.Lgs. 196/2003.

Il Partecipante conviene che la memorizzazione e la condivisione di risorse si effettua tra i Partecipanti alla Federazione e non sotto la responsabilità del gestore dell'infrastruttura (Federazione e GARR).

La Federazione richiede che ogni attributo condiviso nella Federazione non venga utilizzato per scopi differenti da quelli definiti in ST-A, e che tali attributi vengano distrutti alla fine della sessione o dell'evento per il quale sono necessari.

Fermo restando che i Partecipanti italiani si attengono alla legislazione nazionale vigente in materia di trattamento dei dati personali (D. Lgs. 196/2003), gli eventuali Partecipanti non italiani devono attenersi a una legislazione nazionale che faccia riferimento alla "*Direttiva 95/46/CE del Parlamento europeo e del Consiglio del 24 ottobre 1995 relativa alla tutela delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati*".

Comment [Roberto C7]: Not a per il revisore legale:

verificare se è l'ultima e se la dicitura è corretta e scoprire come fare ad includere anche le nazioni extracomunitarie

Esonero e limitazione di responsabilità

Qualsiasi servizio fornito dalla Federazione o dai Partecipanti, viene fornito come è, sulla base della disponibilità, senza garanzie di alcun tipo, sia esplicite che implicite, incluse, ma non limitate a, garanzie sulla commercializzazione, sulla idoneità ad un particolare scopo e sulla non violazione di alcuna legge. La Federazione nega espressamente qualsiasi garanzia sul fatto che i Servizi siano privi di errori, siano sicuri o non possano venire interrotti. Nessuna dichiarazione orale o scritta data dalla Federazione o dalle persone ad essa afferenti o da qualsiasi altra persona potrà costituire una garanzia. I Partecipanti e ogni altra persona non devono fare affidamento su tali dichiarazioni per alcun motivo.

La Federazione, i Partecipanti e gli eventuali fornitori di servizio esterni alla Federazione, ma ad essa connessi, si riservano il diritto di interrompere, sospendere o ridurre la fornitura di qualsiasi servizio destinato ai Partecipanti o ad ogni altra persona, inclusi gli utenti finali dei Partecipanti, quando tale azione si rende necessaria all'esclusivo giudizio della Federazione. La Federazione farà ogni sforzo, ove ragionevolmente possibile, ma senza alcuna garanzia, per avvisare anticipatamente i Partecipanti riguardo eventuali interruzioni, sospensioni o riduzioni del servizio. Conseguentemente ad interruzioni, sospensioni o riduzioni del servizio la Federazione contatterà i partecipanti nel tentativo di risolvere eventuali problemi e riattivare il servizio. In ogni caso la Federazione, i partecipanti alla Federazione e i fornitori di servizio esterni alla Federazione ma ad essa connessi non sono responsabili nei confronti dei partecipanti o di qualsiasi persona per qualsiasi errore di trasmissione, o perdita, o terminazione o interruzione sia parziale che totale, sia intenzionale che accidentale (incluso ogni errore, interruzione o terminazione dovuto alla deliberata cattiva condotta e negligenza di qualsiasi persona), sia che ne fosse stata data comunicazione anticipata oppure no.

La Federazione non è responsabile verso i Partecipanti o verso gli utenti finali per reclami o danni causati interamente o in parte da:

- colpa o negligenza dei Partecipanti o incapacità degli stessi ad ottemperare le proprie responsabilità;

- reclami di terzi contro i Partecipanti;
- qualsiasi azione od omissione di qualsiasi altro soggetto che fornisce prodotti o servizi alla Federazione o ai Partecipanti alla Federazione.

Inoltre la Federazione non è responsabile dell'accesso non autorizzato agli apparati di trasmissione dei Partecipanti, alla loro strumentazione, oppure all'accesso non autorizzato o all'alterazione, ritardo nella trasmissione, furto, o distruzione di file, programmi, procedure o altre informazioni dei Partecipanti o dei loro utenti finali. Un eventuale danno causato da un'azione intenzionale e volontaria è imputabile alla sola responsabilità personale di chi l'ha compiuto.

Il Partecipante è l'unico responsabile per l'uso di qualsiasi servizio o risorsa ottenuta come risultato della partecipazione alla federazione, inclusi, ma non esclusivamente, audio, video, testo, dati, oggetto di comunicazione originata o trasmessa da ogni sito posseduto o gestito dal Partecipante, inclusi tutti contenuti e tutti i materiali di terze parti instradati, attraversati, memorizzati, o trasmessi a qualsiasi altro Partecipante o utente (detti "contenuti del Partecipante"). La Federazione non intende operare revisioni sui contenuti del Partecipante, ed il Partecipante si assume tutte le responsabilità connesse all'uso dei propri contenuti.

NOTA PER IL REVISORE LEGALE:

Bisognerebbe aggiungere un paragrafo che dica qualcosa del genere:

"La Federazione fa un sacco di controlli sui partecipanti, come indicato nel paragrafo **Auditing**, però non può essere ritenuta responsabile se gli sfugge qualcosa, se, ad esempio, un partecipante riceve un danno a causa di un altro partecipante che non aveva rispettato le regole della Federazione e che era sfuggito ai controlli di questa, oppure aveva rispettato le regole, ma, ciò non ostante, i cattivi sono riusciti a non farsi scoprire"