



Norme di partecipazione alla Federazione IDEM

v 0.9.7

30 Luglio 2009

Revisioni

Versione	Data	Descrizione	Autore
0.9	20/5/09	Versione iniziale	
0.9.4	11/6/09	Modifiche minori e cancellazione note a margine che si trovano nella 0.9.3 Normalizzazione nome IDEM GARR AAI	lm
0.9.5	12/6/09	Modifiche nel paragrafo "Servizi" (rif doc 0.94) Tolto l'impegno a rispettare la legge (pag. 7) Tolto la frase "a fini commerciali" nel divieto di aggregazione dati (pag. 8)	cb rc rc
0.9.6	20/7/09	Reinseriti con modifiche i paragrafi: "Scadenza e Rinnovo" e "Esonero e limitazione di responsabilità"	lm
0.9.7	24-30/7/09	Revisione legale Aggiunta privacy per paesi extra EU Riscritta "Limitazione di Responsabilità"	

1 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 tecnica e normativa della Federazione.

2 Partecipazione alla Federazione

2.1 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.

2.1.1 Informativa ai Partecipanti

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.

2.2 Requisiti per l'adesione

2.2.1 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.

2.2.2 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 Tecnico¹, il principale responsabile tecnico per la configurazione del Servizio; questi mantiene i contatti con il Servizio *IDEM GARR 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.

2.2.3 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.

2.2.4 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.

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

3 Adesione e registrazione servizi

3.1 Richiesta di adesione/Accordo di Collaborazione

Per l'adesione alla Federazione, l'Organizzazione:

- prende visione di tutta la documentazione normativa 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.

3.2 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.

3.3 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 docu-

mento ai soli Partecipanti che ne facciano richiesta;

- il frammento di metadati corrispondente al servizio da registrare compilato con i dati richiesti in ST.

3.4 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 DO-PAU;
- 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;
- 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'Or-

- ganizzazione di appartenenza;
- non effettuare aggregazioni di dati relativi all'attività degli utenti senza permesso esplicito o previsto dai contratti in essere con le loro Organizzazioni di appartenenza;
- verificare periodicamente la conformità a quanto dichiarato tramite il DO-PAR.

3.5 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 documento NdP e nella restante documentazione tecnica e normativa 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.

4 Durata della partecipazione

La durata della partecipazione è illimitata fatta salva la possibilità del Partecipante di terminare anticipatamente la propria partecipazione e l'esclusione del Partecipante da parte della Federazione; le modalità di terminazione sono descritte nel paragrafo "Risoluzione".

4.1 Sospensione

4.1.1 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, o per negligenza, alla Federazione e/o a terzi.

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.

4.1.2 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 da questi offerto attraverso la 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 ai recapiti indicati nel Regolamento.

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.

4.2 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.

In tutti i casi la risoluzione della partecipazione avverrà senza oneri per le parti.

5 Servizi della Federazione

Il GARR, tramite il Servizio *IDEM GARR AAI* mette a disposizione della Federazione i seguenti servizi:

- 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.

Inoltre, il GARR promuove le attività della Federazione 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 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.

6 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.

7 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 ef-

fettua 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.

In materia di trattamento dei dati personali i Partecipanti italiani si attengono alla legislazione nazionale vigente (D. Lgs. 196/2003) e i Partecipanti degli stati dell'Unione Europea (EU) e dell'Area Economica Europea (EEA) si attengono ad una legislazione nazionale che fa riferimento alla vigente Direttiva del Parlamento Europeo. I Partecipanti che hanno la propria sede legale in paesi fuori dall'Unione Europea (EU) o dall'Area Economica Europea (EEA) devono dichiarare nell'Accordo di Collaborazione di aderire alla vigente Direttiva Europea in materia di trattamento dei dati personali.

8 Esonero e limitazioni di responsabilità

Il GARR e la Federazione faranno ogni sforzo possibile per garantire il corretto funzionamento del Servizio GARR IDEM AAI e della Federazione stessa.

Il GARR e la Federazione non sono tuttavia responsabili per l'uso improprio delle risorse messe a disposizione della comunità degli utenti GARR mediante la Federazione e per l'uso improprio del meccanismo di Federazione nel suo complesso.

L'utilizzo della rete GARR da parte della propria comunità di utenti è consentito solo per attività istituzionali di ricerca scientifica e/o di sviluppo tecnologico, con espressa esclusione di qualunque attività, anche indirettamente a carattere commerciale.

Come meglio illustrato nel documento sulle Regole di Utilizzo della rete GARR o "Acceptable Use Policy GARR - AUP", è responsabilità delle istituzioni GARR (e quindi Membri potenziali della Federazione IDEM) adottare tutte le azioni ragionevoli per garantire la conformità delle proprie norme con quelle esposte nel documento AUP, al fine di assicurare che non avvengano utilizzi non ammessi della Rete GARR e dal presente documento.

Ogni istituzione con accesso alla Rete GARR deve inoltre portare a conoscenza dei propri utenti (con i mezzi che riterrà opportuni) le norme contenute nelle AUP e nel presente documento.

Le istituzioni GARR si obbligano infine ad attuare tutte le misure che impediscano l'accesso alla Rete GARR a soggetti non autorizzati.

Il GARR non assume alcuna responsabilità connessa all'impiego, da parte di terzi, della connessione alla Rete GARR.