Norme di partecipazione alla Federazione IDEM

v 1.6

04 Giugno 2019

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
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"	
1.0	9/9/09	Tolto il richiamo all'AUP GARR poiché non adatto ai Partner; (viene contestualmente introdotto nella “Richiesta di adesione”).	
1.0.1	9/11/09	Aggiunto un paragrafo in “Ulteriori requisiti per la registrazione di una Risorsa” con l'indicazione della necessità del rispetto della privacy dell'utente	
1.2	03/03/10	Modifiche per reintroduzione della figura (opzionale) del Referente Organizzativo per il Partner in: "Requisiti base per ogni Partecipante", "Registrazione di un IdP", "Registrazione di una Risorsa" Modifica a "Registrazione di un IdP" e "Registrazione di una Risorsa" al fine di migliorare l'allineamento a "Ulteriori requisiti per la registrazione di un IdP" e "Ulteriori requisiti per la registrazione di una Risorsa"	
1.3	04/17/12	Eliminato requisito del DOPAR	
1.4	21/01/13	Modificate Premesse e art. 3.4	
1.5	15/05/15	Modifiche ai par. 3.1, 3.2, 3.3, 3.5 riguardanti le modalità di invio delle comunicazioni	lp
1.6	04/06/19	Consentito avere più IdP per sole funzioni di test. Inserito chiarimento su quali certificati usare per IdP e SP. Semplificate istruzioni per invio comunicazioni. Inserito richiamo a collaborazione e informazione verso Servizio IDEM GARR AAI e GARR CERT per incidenti di sicurezza. Eliminato il requisIto del DOPAU, inserendo al suo posto un insieme di requisiti di base per la registrazione di un IdP.	

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.

Il Consortium GARR (di seguito “GARR”) ha il ruolo di operatore di federazione al quale ogni Organizzazione richiede l'adesione alla Federazione. GARR mette a disposizione un servizio tecnico-amministrativo di supporto denominato “Servizio IDEM GARR AAI”.

I Partecipanti, sottoscrivendo la **Richiesta di adesione** (RA) o l’**Accordo di collaborazione** (AC), accettano il **Regolamento della Federazione IDEM** (RFI) e le **Norme di partecipazione** (NdP). Questi documenti, insieme alle **Specifiche tecniche** (ST) e alle **Specifiche tecniche per la compilazione e l'uso degli attributi** (ST-A), costituiscono il riferimento tecnico e normativo 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, fatta salva la registrazione di IdP ai fini di test o relativi a procedure di aggiornamento. 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, l'Assemblea dei membri può consentire la registrazione di più di un IdP.

In via eccezionale, e a fronte di richiesta accuratamente motivata, l'Assemblea dei membri 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 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 alle persone di cui sopra.

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, 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 Tecnico[1], il principale responsabile tecnico per la configurazione

[1] Il Partner può, a sua discrezione, includere tra i contatti tecnici un'eventuale figura commerciale che deve ricevere le comunicazioni dalla Federazione.

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 utilizzati dagli Identity Provider e dai Service Provider devono essere configurati seguendo le indicazioni fornite in ST.

3. Adesione e registrazione servizi

3.1. Richiesta di adesione/Accordo di Collaborazione

Per l'adesione alla Federazione, il Partecipante:

- 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 la Richiesta di Adesione se idoneo come Membro, ovvero l'Accordo di Collaborazione se idoneo come Partner, accludendo ove possibile la firma digitale (FD) o, in alternativa la firma in originale ed il timbro del Legale Rappresentante. Il Partecipante tramite la Richiesta di Adesione o l'Accordo di Collaborazione accetta le regole derivanti dalla partecipazione alla Federazione e nomina i Referenti (vedi par. 4 RFI);
- contestualmente all'adesione, compila e firma la richiesta di registrazione di almeno un IdP e/o di una o più Risorse; ulteriori richieste di registrazione servizi potranno essere presentate in seguito.

Tutti i documenti devono essere inviati solo ed esclusivamente per posta elettronica all'indirizzo idem@garr.it.

3.2. Registrazione di un IdP

Per registrare un IdP il Partecipante invia alla Federazione:

- il modulo di Registrazione IdP, compilato e sottoscritto ove possibile con firma digitale (FD) o, in alternativa, con firma in originale e timbro del Referente Organizzativo o del Rappresentante Legale;
- il frammento di metadati corrispondente al servizio da registrare, compilato con i dati richiesti in ST.

Tutti i documenti devono essere inviati solo ed esclusivamente per posta elettronica all'indirizzo idem@garr.it.

3.3. Registrazione di una Risorsa

Per registrare un SP il Partecipante invia alla Federazione:

- il modulo di Registrazione Risorsa, compilato e sottoscritto ove possibile con firma digitale (FD) o, in alternativa, con firma in originale e timbro del Referente Organizzativo o del Rappresentante Legale;
- il frammento di metadati corrispondente al servizio da registrare compilato con i dati richiesti in ST.

Tutti i documenti devono essere inviati solo ed esclusivamente per posta elettronica all'indirizzo idem@garr.it.

3.4. Impegni dei Partecipanti

Ogni Partecipante, in aggiunta agli obblighi indicati nei documenti della Federazione, si impegna ad accettare le seguenti regole finché parteciperà alla Federazione.

Il Partecipante deve:

- 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 nello svolgimento di controlli periodici sullo stato dei servizi registrati (*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;
- informare tempestivamente il Servizio IDEM GARR AAI ed il Servizio GARR-CERT in caso di incidenti di sicurezza relativi ai propri servizi registrati in Federazione.

Il Partecipante che registra un IdP si impegna a:

- impiegare per tutti gli utenti procedure di accreditamento ben definite e documentate;
- accreditare gli utenti previo riconoscimento;
- gestire ogni identità digitale in modo che la persona a cui essa si riferisce sia identificabile;
- impiegare metodi di autenticazione basati su almeno un fattore (password, certificato, ecc.);
- adottare misure di sicurezza per la consegna o la creazione dei fattore di autenticazione tali da evitare eventuali furti o compromissioni;
- fornire agli utenti informazioni relativamente alle loro responsabilità nella custodia e nel mantenimento della sicurezza dei propri account;
- definire delle politiche di disabilitazione degli account e/o delle autorizzazioni ad essi associati e darne comunicazione agli utenti;

- mantenere sui propri sistemi dei registri d'uso (*log*) che consentano di risalire agli utenti delle sessioni di autenticazione;
- fornire ogni ragionevole collaborazione alla Federazione o ad altri Partecipanti qualora fossero necessari chiarimenti e approfondimenti su attività rilevate come insolite e su eventuali incidenti di sicurezza;
- 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'Organizzazione 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;
- comunicare alla Federazione ed ai suoi partecipanti quali attributi sono necessari per accedere alla risorsa secondo le modalitá specificate in ST e ST-A.

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 indicati nel presente documento 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 in ST;
- la congruità dei dati rispetto alla documentazione inviata.

Le verifiche tecniche sono a carico del Servizio IDEM GARR AAI.

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

Il Servizio IDEM GARR AAI 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 dall'Assemblea.

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:

- catalogo e 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;
- Discovery Service;
- gestisce e mantiene il sito web ufficiale della Federazione;
- 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.

Il Partecipante coopera e fornisce l'assistenza necessaria per l'esecuzione delle verifiche.

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

Le procedure di verifica saranno condotte sia in modo automatizzato sia manuale 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 Regolamento UE 2016/679.

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 dichiarati, e che tali attributi vengano distrutti alla fine della sessione o dell'evento per il quale sono necessari.

8. Esonero e limitazioni di responsabilità

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

GARR e la Federazione non possono tuttavia essere ritenuti responsabili per:

- ogni conseguenza derivante dall'adesione e/o dall'uso del Servizio IDEM GARR AAI e delle Risorse registrate;
- l'uso improprio delle Risorse messe a disposizione mediante la Federazione da parte degli utenti dei Partecipanti.