



Norme di partecipazione alla Federazione IDEM

Italian version, English version available at page 11.

v 1.7

11 Novembre 2022

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.	dv, cts
1.7	04/11/2022	Il Referente Tecnico sostituisce i Contatti Tecnici nei rapporti con Servizio e Federazione. I Contatti Tecnici sono indicati direttamente nei metadata.	dv, cts

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 e dei contatti definiti per i servizi registrati.

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;
- ogni Referente Tecnico è responsabile dei servizi che ha registrato nella Federazione IDEM GARR AAI;
- il Referente Tecnico mantiene i contatti con il Servizio IDEM GARR AAI per la corretta configurazione dei servizi, secondo le indicazioni della Federazione;
- nel caso in cui il Referente Tecnico responsabile del servizio sia indisponibile, il Referente Organizzativo assume la responsabilità del servizio.

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 autografa del Referente Tecnico;
- 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 autografa del Referente Tecnico;
- 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 modalità 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.



Rules of Participation to the IDEM Federation

Versione inglese, versione italiana disponibile a pagina 1.

v 1.7

November 4th 2022

1. Introduction

This document defines:

- The terms and procedures of participation to the IDEM (IDentity Management for federated access) Federation (hereinafter referred to as “the Federation”), as well as terms of interruption and termination of participation.
- The terms and conditions of Service registration for Participants.
- The rules about the exchange of information about end-users and services within the Federation.

Consortium GARR (from now on just “GARR”) has the role of the federation operator to whom any Organization requests to join the Federation. GARR makes available a technical and administrative support service named “IDEM GARR AAI Service”.

When subscribing the Member Accession Form (RA, Richiesta di adesione) or the Partnership Memorandum of Understanding (AC, Accordo di collaborazione), Organizations accept the IDEM Federation Regulation (RFI, Regolamento della Federazione IDEM) and the Rules of Participation (NdP, Norme di partecipazione). These documents, Technical Specifications (ST, Specifiche tecniche) and Technical Specifications for Compilation and Use of Attributes (ST-A, Specifiche tecniche per la compilazione e l'uso degli attributi) form the Federation’s technical and normative reference.

2. Participation

2.1. Participants

In order to join the Federation, Organizations must register at least one Service, which can be either:

- An identity management and verification Service, through a software component known as Identity Provider (IdP).
- An online Resource, accessible after an authentication and authorization procedure, through a software component known as Service Provider (SP).

Federation Participants are:

1. Members: Organizations belonging to the GARR User Community;
2. Partners: other Organizations.

Usually, Members register one Identity management service. However they can register one or more Resources. Usually, Partners register online Resources.

An Organization willing to join as a Member must fill the RA and send it to the Federation, together with the required enclosures.

An Organization willing to join as a Partner must fill the AC and send it to the Federation, together with the required enclosures.

The document must be signed by the Organization’s Legal Representative. If all the requirements are met, GARR undersigns the document and sends it back to the Organization.

Usually, each Member registers only one IdP, belonging to the Organization’s Identity Management system, except for test IdP or for update procedures. Upon request, the Assembly

of Members can allow the registration of more IdPs. The registration of multiple IdP's is allowed only in special cases and it must be clearly justified by the requiring Member. A technical report illustrating the proposed configuration must support the request.

Exceptionally, and upon a clearly motivated request, the Assembly of Members can allow a Partner to register its Organization's IdP.

2.1.1. Privacy notice

The names and personal information of the people mentioned in all agreements and forms will be collected and processed, electronically or on paper, to fulfill the Federation purposes. The collected information may be communicated to other Participants and published on web pages accessible by Federation Participants. E-mail addresses of appointed representatives and delegates shall be added in the Federation's mailing lists. Participant Organizations must communicate this information to the persons above mentioned.

2.2. Participation requirements

2.2.1. General requirements

Participants shall promptly communicate to the Federation any change related to the names and contact details of the Organizational Representative ("Referente Organizzativo" in Italian, abbreviated as RO), Technical Representative ("Referente Tecnico" in Italian, abbreviated as RT) and of the contacts defined in the metadata of the registered services.

Participants shall create a web page according to the model described in ST and keep the information up to date.

2.2.2. Service registration requirements

- Services (IdP and SP) must comply to technical specification given in ST and ST-A.
- Services (IdP and SP) must be under the complete responsibility of the Organization, even if outsourced to third parties.
- For each registered service, Participants must provide their metadata and keep them up to date according the Federation procedures, as described in ST.
- Each Technical Representative is responsible for the services the he registered in the IDEM GARR AAI Federation.
- The Technical Representative mantain contacts with the IDEM GARR AAI Service for the right configuration fo the services, according to the instructions of the Federation.
- In the case a Technical Representative responsible for a service is not available anyomer, the Organizational Representative acquires the responsibility for the service.

3. Joining and Service registration

3.1. Joining request

In order to join the Federation, a Participant:

- Reads the technical and policy documentation provided by the Federation and evaluates

the feasibility of participating with one or more services (IdP and/or SP).

- Fills in the joining request as a Member, or as a Partner. The request must be digitally signed by the Participant's Legal Representative or alternatively with original signature and stamp. Subscribing the joining request, the Participant accepts all the policies and rules of participation and appoints its representatives in the Federation.
- Along with the joining request, the Participant fills in and signs the registration request for one IdP and/or one or more resources; further Service registrations requests may be submitted afterwards.

All the documents must be sent exclusively via email to idem@garr.it.

3.2. IdP Registration

In order to register an IdP, the Participant must send the following:

- The IdP Registration Form, filled in and digitally signed by, or alternatively with handwritten signature of, the Technical Representative.
- The metadata fragment corresponding to the Service to be registered, compiled according to ST.

All the documents must be sent exclusively via email to idem@garr.it.

3.3. Resource Registration

In order to register an SP, the Participant must send the following:

- The SP Registration Form, filled in and digitally signed by, or alternatively with handwritten signature of, the Technical Representative.
- The metadata fragment corresponding to the Service to be registered, compiled according to ST.

All the documents must be sent exclusively via email to idem@garr.it.

3.4. Participants' Commitments

In addition to other obligations specified in the Federation documents, each Participant commits to submit to the following rules, as long as they take part in the Federation.

Participants must:

- Adopt the amendments to the technical specifications or to terms of participation approved by the Federation within the established deadline.
- Acknowledge the Federation the right to publish and use needed metadata required for its operations.
- Acknowledge the Federation the right to publish the name of the Organization for disseminating and promoting the Federation and its objectives.
- Avoid any action that may result in a damage or violation of security procedures, or cause any bias against the reputation of other Participants and the Federation as a whole.
- Collaborate with the Federation for the periodic check on the status of the registered services (*audits*).
- Adopt technical and administrative rules in order to safeguard copyright and to enforce the laws on content and services made available by other participants and the Federation

itself.

Participants registering an IdP are committed to:

- Make use of well defined and documented enrollment procedures for all the users.
- Enroll the users only upon identification.
- Identify each and every person to which a digital identity has been issued.
- Employ authentication procedures that relies at least on one factor (password, certificate, etc).
- Employ secure procedures for the creation and delivering of the authentication factors in order to avoid theft and compromise
- Maintain logs which allow to track users of authentication sessions.
- Provide information to their users about their responsibilities on the custody and secure maintenance of their accounts.
- Define account and authorizations deprovisioning policies and inform the users about them.
- Provide all reasonable cooperation to the Federation or to others Participants should clarifications and further details be required on activities found to be unusual and about any security incidents;
- Provide information about the available Federation resources to their users.

Participants registering one or more Resources are committed to:

- Limit the request of user data information to those needed to provide the service.
- Keep track of operations, supply useful data for monitoring and evaluating the resource usage.
- Do not transfer to third parties user information obtained through the Federation, unless specific agreements are in place with their home Organization.
- Do not aggregate any information about end-user activities without an explicit permission or previous agreement with their home Organization.
- Inform the Federation and its Participants about the attributes needed in order to access the resource as specified in ST and ST-A.

3.5. Approval Procedures

For each application to join the Federation and any subsequent request for Services registration, the Federation will start an approval procedure, during which the Federation may ask further information in addition to those received to the contact persons appointed by the Organization. However, the procedure will end no later than ninety days from the date of receipt of the request.

The aim of the approval procedure is to verify that the Candidate and/or the proposed Services fulfill all requirements in this document and in the other Federation's technical and regulatory documents.

First, the following will be verified:

- The GARR membership (for Members only).
- The Participants' interest for the offered Resource(s), and the risks, if any, in making them available through the Federation (for Partnership Requests, and for the registration of new Resources).

Then, the IDEM GARR AAI Service will verify the completeness, consistency of the documentation and compliance to technical requirements of Services provided by the

Organization, including:

- The service certificates.
- The correctness of the Service registration in the Federation metadata.
- The operational availability of the Service.
- The completeness of the information provided on the web page published by the Organization according to ST.
- The consistency with the information provided through the request forms.

Upon acceptance, the Organization shall receive the joining request countersigned by GARR. In the event of rejection, the Organization shall be notified about the refusal.

In the event of a positive outcome, the Organization shall receive the joining request countersigned by GARR. In the event of rejection, the Organization is notified with the reason for the refusal.

IDEM GARR AAI Service notifies the Members about the new services.

4. Duration

The duration of participation is unlimited, unless the Participant is excluded or recedes from the Federation. Termination conditions are described in the “Cancellation” paragraph.

4.1. Suspension

4.1.1. Suspension of a Participant

The Federation may suspend an Organization from Participation if it fails to fulfill the requirements or to comply with the provisions given in this document or causes any damage, even unintentional, to Participants of the the Federation and/or Third Parties.

The Participant is given notice of the suspension measure with enough anticipation, however in case of security breaches and damage caused to the Federation, the suspension is inflicted immediately.

Being suspended implies the temporary exclusion of the Participant from the Federation and the removal of the metadata fragments corresponding to the Participant’s Services.

4.1.2. Suspension of Services

In case of multiple Services registered by a Participant, the suspension can be limited to specific Services (IdP or SP).

In case the Organization’s systems or encryption keys are damaged or compromised, a Participant may ask for the immediate suspension of its own Service. The request shall be communicated to the Federation via email or, in an emergency, via phone, using the contact details indicated in the Federation Regulation.

Interrupting a Service implies the removal of the corresponding metadata fragment for the time needed to solve the issue. In case of Participants with only one registered Service, the suspension is equivalent to the Participant suspension.

4.2. Cancellation

Upon suspension, should the Participant fail to fulfill the requirements described hereby or in the other Federation documents or more than 30 days has passed from the official notification, its participation may be revoked.

The cancellation of a Participant must be approved by the Technical Committee.

Participants may withdraw from the Federation by communicating their decision with a 30 days notice. The Participant's metadata will be removed.

In any case, the cancellation will be free of charge for the Parties.

5. Services provided by the Federation

GARR, through the IDEM GARR AAI Service, makes available the following services:

- The catalog and metadata of available Services. Validity, truthfulness and update of the information rest solely under the Participant responsibility.
- Help-desk, training and other knowledge transfer activities, in order to provide the know-how for setting up Services to Organizations of the GARR Community.
- Documentation and support for resource interoperability to potential Partners.
- A Discovery Service (WAYF);
- The Federation's official website.
- Monitoring and auditing activities.

Furthermore, GARR promotes the Federation's activities and services through the organization of workshops, conferences, meetings and the participation to external events that involve new potential Partner or Member organizations.

Being a Member of the Federation does not grant access to Resources provided by other Participants upon subscription.

The technical, financial and Intellectual Property Rights terms and conditions for accessing specific Resources used by a Participant and made available by another shall be agreed between the interested parties.

6. Auditing

Participants acknowledge and agree that the Federation carries out periodic audits, aiming at verifying the compliance of registered Services to the technical requirements described in ST and ST-A.

Participants will cooperate and provide assistance to the audit.

Any failures in fulfilling the technical requirements will be notified to Participants, together with the request to conform. Failure to comply may lead to suspension.

Audit procedures will be carried out automatically or manually, and will concern all Participants even without previous notice.

7. Privacy Notice

Participants are committed to respect privacy and confidentiality of personal information and of any other information acquired in the authentication and authorization procedures.

More specifically, Participants acknowledge that they cannot permanently record, share, make publicly available or exploit any personal information received from the Federation's Participants but for the purposes connected with the Federation activities. An exception to this provision are the liability proxy agreements as per the EU Regulation 2016/679.

Participants acknowledge that the recording and sharing of Resources is carried out amongst the Federation Participants, and it is not under responsibility of the manager of the Infrastructure (Federation and GARR).

The Federation requires that each shared attribute in the Federation is not used for other purposes than those defined in ST-A, and that those attributes are canceled at the end of the session or event for which they are needed.

8. Disclaimer and Limitation of Liability

GARR and the Federation will strive to ensure the GARR IDEM AAI Service and the Federation itself work properly.

However, GARR and the Federation are not liable for:

Any consequence that may arise from the participation in IDEM, from the use of the GARR IDEM AAI Service, and from the operation of registered Resources.

The improper usage of Resources, provided through the Federation, by Participants' users.