Norme di partecipazione alla Federazione IDEM

v 1.0.2

23 02 2010

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"	
1.0	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	
1.0.2		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 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 Tecnico[1], 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.

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

2.2.3 Ulteriori requisiti per la registrazione di un IdP

- Gli attributi relativi agli utenti devono essere resi disponibili 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

- Gli attributi relativi agli utenti devono essere 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 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.

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 documento ai~~ soli~~ Partecipanti che ne facciano richiesta;
- il frammento di metadati corrispondente al servizio da registrare compilato con i dati richiesti in ST.

3.4 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 chiari-

menti 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;
- 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;
- verificare periodicamente la conformità a quanto dichiarato tramite il DOPAR.

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 dalla 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 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.

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

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 IDEM Federation

v 1.0.2

23rd February 2010

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 regulations about the exchange of information about end-users and services within the Federation..

When subscribing the **Member Accession Form** (**RA, Richiesta di Adesione**)or the **Partnership Memorandum of Understanding** (**AC, Accordo di Collaborazione**), Participants accept the **Federation Regulation**, the **Rules of Participation (NdP, Norme di Partecipazione)**, the **Technical Specifications (ST, Specifiche Tecniche)** and **Technical Specifications for Compilation and Use of Attributes (ST-A, Specifiche Tecniche: Attributi)**. As a whole, these documents form the Federation's Technical and Regulative Infrastructure.

2 Participation

2.1 Participants

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

- an identity management and verification Service, acting through a software component known as **Identity Provider** (IdP);
- an online Resource, accessible after an Authentication and Authorization procedure, acting 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.

Mainly, Members register one Identity management service, however they can register one or more Resources. Partners usually register Resources.

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

An Organization willing to join as a Partner must fill in the Partnership **Memorandum of Understanding** and send it to the Federation, together with the required enclosures.

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

Normally, each Member registers only one IdP, belonging to the Organization's Identity Management system. Upon request, the Policy Committee may allow the registration of more than one IdP per Organization to meet specific requirements. 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.

Upon a clearly motivated request, the Policy Committee may exceptionally allow a Partner to register its Organization's IdP.

2.1.1 Privacy notice to Participants' end-users

The names and personal information of persons mentioned in all agreements and forms will be collected and processed, electronically or on paper, to fullfil 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 are committed to communicate this information to their end-users.

2.2 Participation Requisites

2.2.1 General requisites (for all Participants)

- Participants shall communicate to the Federation the replacement of the Referente Organizzativo (RO), ~~when applicable,~~ of the Referente Tecnico (RT), when applicable, and of Service Contact Persons, as well as any changes in their contact details, in good time;
- Participants shall create a web page along the model described in ST and keep the information in it up to date.

2.2.2 Service registration requisites

- Services (IdP and SP) must comply to technical specification given in the ST and ST-A;

- Services (IdP and SP) must be under the complete responsibility of the Organization, even when they are 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;
- for each registered Service, Participants must indicate at least one Service Contact Person[2], who acts as the main technical point of contact for that service; he or she interacts with the IDEM GARR AAI Service staff to ensure that the service is correctly configured, as required by the Federation. The replacement of the Service Contact Person shall be communicated to the Federation in good time;
- Service certificates must be configured according to the provisions given in ST.

2.2.3 Further requisites to register an IdP

- User-related attributes must be made available respectfully of the user's privacy, and in compliance with naming, syntax and semantic specifications, as indicated in ST-A;
- a document containing key facts on the Organization's Identity Management System and the attributes it supports shall be made available; the document shall comply with the **DOPAU** (DOcument on the Procedure of Accrediting of Users) model provided by the Federation. Resource Providers shall use the information describing user management (operational) procedures to determine the level of trust for each Participant.

2.2.4 Further requisites to register a Resource

- User-related attributes must be exploited respectfully of the user's privacy, and in compliance with naming, syntax and semantic specifications, as indicated in ST-A;
- a document containing key facts on the access system to Resources shall be made available, along the **DOPAR** (DOcument on the Procedure of Accessing the Resource) model provided by the Federation. Members of the Federation shall use the information to evaluate rules and (operational) procedures adopted by the Resource Provider in terms of collection and exploitation of user-related attributes, as well as the terms and conditions of the contract(s) for accessing the resource(s), if any.

2 Partners may, at their own discretion, include in the Technical Contacts an Account contact ~~who will receive the Federation's messages.~~

3 Accession to the Federation and Service registration

3.1 Member Accession Form/Partnership Memorandum of Understanding

In order to join the Federation, the candidate Organization:

- looks over the technical and regulative documentation provided by the Federation and evaluates the feasibility of participating (with?) one or more services (IdP and/or SP);
- fills in two copies of the Member Accession Form (if wishing to join as a Member) or the Partnership Memorandum of Understanding (if wishing to join as a Partner). These shall be signed by the Organization's Legal Representative and sent to the Federation, together with the appropriate enclosures. With signing this document, the Organization accepts the Rules of Participation and appoints its representatives in the Federation;
- sends, together with the Member Accession Form, the registration request for one IdP and/or one or more Resources; further Service registrations requests can be put forward afterwards.

3.2 IdP Registration

The Organization sends to the Federation:

- two copies of the IdP Registration Form, filled and signed by the RO (when applicable) or by the Organization's Legal Representative ~~or his/her delegate~~;
- the document describing the Organization's Identity Management System, drafted according the **DOPAU** model. Once the IdP is registered, the document will be made available to other Participants upon request only;
- the metadata relating to the Service to be registered, which will include the data required in ST.

3.3 Resource Registration

The Organization sends to the Federation:

- two copies of the Resource Registration Form, filled and signed by the RO (when applicable) or by the Organization's Legal Representative ~~or his/her delegate~~;
- the document describing the system to access the Resource, drafted according the **DOPAR** model. Once the Resource is registered, the document will be made available to other Participants upon request only;

- the metadata relating to the Service to be registered, which will include the data required in ST.

3.4 Obligations of Participants

In addition to other obligations specified elsewhere in the Federation documents, Participants are bound to submit to the following rules as long as they take part in the Federation. Participants must:

- adopt any changes approved by the Federation, including those to technical specifications or to terms of participation, within the (foreseen) deadline;
- acknowledge the right, for the Federation, to publish and exploit needed metadata;
- acknowledge the right, for the Federation, to publish the name of the Organization for disseminating and promoting the Federation and its objectives;
- avoid any action that may imply any damages or violations of security procedures, or cause any bias against the reputation of other Participants and the Federation as a whole;
- collaborate with the Federation in occasion of periodic audits;
- adopt technical and administrative rules such as to safeguard copyright and to enforce the observance of the law on content and services in general.

Participants registering an IdP are committed to:

- maintain logs on the Organization's servers, which allow to track users of authentication sessions, according to the provisions set out in ST, and collaborate with other Participants or the Federation in the event of security incidents or of the observation of unusual activities such as to require inquiries or clarifications;
- periodically verify the IdP compliance with what stated in the DOPAU;
- provide end-users with information about which resources provided by the Federation they can access.

Participants registering one or more Resources are committed to:

- limit the request for user information to those needed to provide the service;
- keep track of operations, and provide the Federation with statistics for monitoring and evaluating the Resource(s) usage;
- keep private the user information obtained through the Federation, and not communicate it to third parties, unless specific agreements with their home Organization exist;
- not aggregate any information about end-user activities without an explicit permission, or previous agreements with their home Organization;

- periodically verify the Resource(s) compliance with what stated in the DOPAR.

3.5 Approval Procedures

For each request to join the Federation and for any subsequent Service registration, an approval procedure will start. During the procedure, the Federation may ask further information to the contact persons appointed by the Organization. In any case, the procedure will end in 90 days from the date of receipt.

Objective of the approval procedure is to verify that the Candidate and/or the proposed Services fulfil all requisites described in this document and in the other Federation's technical documents.

In the first place, the following will be verified:

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

The completeness, consistency of the documentation and compliance to technical requirements of Services provided by the Organization will be then verified; the latter will include:

- installed certificates;
- the accuracy of the Service registration in the Federation metadata;
- the proper working of the Service;
- the completeness of the information provided on the web page published by the Organization along the model provided in ST;
- the consistency with the information provided through the request forms.

Audits are carried out by the Technical and Scientific Committee, that delivers the documentation and the outcome of the checks to the Policy Committee.

In the event of positive outcome, the Organization or the new Service is accepted, and the Organization receives the countersigned Member Accession Form or Memorandum of Understanding. In the event of rejection, the Organization is notified with the reason of the refusal.

The Technical and Scientific Committee notifies the new Participants and the availability of new services to the Member board via the web and/or e-mail.

4 Duration

The duration of participation is unlimited, unless the Participant is excluded or recedes from the Federa-

tion; termination conditions are described in the “Cancellation” paragraph.

4.1 Suspension

4.1.1 Suspension from Participation

The Federation may suspend an Organization from Participation in the event of:

- failure to fullfil the requirements or to comply with the provisions given in this document;
- damage, even unintentional, caused by the Participant to the the Federation and/or Third Parties through negligence or fraud.

The Participant is given notice of the measure, however in case of serious breach 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 fragment corresponding to the Participant’s Services.

4.1.2 Suspension of Services

The Federation may suspend an Organization from Participation in the event of:

- failure to fulfil the requirements or to comply with the provisions given in this document;
- damage, even unintentional, caused by the Participant to the the Federation and/or Third Parties through negligence or fraud.

The Participant is given notice of the measure, however in case of serious breach 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 fragment corresponding to the Participant’s Services.

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

Participant may ask the interruption of its own specific Service that he offer to others through the Federation at any time, in case the Organization’s systems or coding keys be damaged or compromised. 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 problem or irregularity.

In case of Participants with one registered Service, interrupting the Service is equivalent to suspending the Participant.

4.2 Cancellation

Should the Participant fail to fulfil the requisites described hereby or in the other Federation documents for 30 more days from the official notification, the participation shall be revoked.

The cancellation of a Participant can be proposed by the Technical and Scientific Committee and must be ratified by the Policy Committee.

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

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

5 Services provided by the Federation

Through the IDEM GARR AAI Service, GARR:

- provides the catalogue and metadata of available Services; validity, truthfulness and update of the information rest solely (on charge) on responsible Participants;
- carries out help-desk, training and other knowledge transfer activities, in order to provide Organizations in the GARR Community with the know-how for setting up Services;
- provides potential Partners with the documentation and support for Resource interoperability;
- caters for the Discovery Service (WAYF);
- updates and maintains the Federation's official website;
- carries out monitoring activities and audits.

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 Member of the Federation does not grant access to those Resources provided by other Participants upon the signature of specific contracts.

The technical, financial and IPR(?) terms and conditions for accessing specific Resources used by and Participant and made available by another shall be agreed between the interested parties.

6 Auditing

Participants acknowledge and assent 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, and to the information provided in the DOPAU and/or DOPAR.

Participants will cooperate and provide assistance to the audit; this may include granting access to Services with test accounts. The Federation will keep private the related credentials, and use the accounts solely for monitoring and auditing purposes.

Any failures in fulfilling the technical requirements will be notified to Participants, together with the request to conform, on pain of suspension.

Conformity checks are reviewed yearly by the Technical and Scientific Committee.

Audit procedures will be carried out permanently, either automatically or manually, and will concern all Participants, also without 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. Participants acknowledge that they cannot record, share, make publicly available or exploit the personal information received from the Federation but for the purposes connected with the Federation activities; an exception to this provision are the liability proxy agreements, foreseen under D.Lgs. 196/2003.

Participants acknowledge that the recording and sharing of Resources is carried out amongst the Federation Participants, and 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 cancelled at the end of the session or event for which they are needed.

Italian Participants shall follow the Italian privacy regulation in force (D. Lgs. 196/2003); Participants based in other states in the European Union (EU)or the European Economic Area (EEA) shall follow the National regulation referring to the European Parliament Directive in force on the same matter. Participants based outside the EU or the EEA must declare to follow the European Parliament Directive on privacy in the Partnership Agreement.

8 Discharge 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 consequences 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 Members' users.