Norme di partecipazione alla Federazione IDEM

v 1.5

15 Maggio 2015

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 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 agente centrale 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. 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 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 del Servizio; questi mantiene i contatti con

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

il Servizio IDEM GARR AAI per la corretta configurazione del Servizio, secondo le indicazioni della Federazione; la variazione del Contatto Tecnico deve essere tempestivamente comunicata alla Federazione;

- i certificati sui Servizi devono essere configurati seguendo le indicazioni fornite in ST.

2.2.3 Ulteriori requisiti per la registrazione di un IdP

- Gli attributi relativi agli utenti devono essere resi disponibili 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;

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 eleggibile come Membro, ovvero l'Accordo di Collaborazione se eleggibile 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 un IdP e/o di una o più Risorse; ulteriori richieste di registrazione servizi potranno essere presentate in seguito.
- invia alla Federazione i documenti suddetti, solo per Posta Elettronica Ordinaria (PEO) all'indirizzo: idem@garr.it, NON è richiesto l'invio cartaceo.

3.2 Registrazione di un IdP

Il Partecipante invia alla Federazione all'indirizzo di Posta Elettronica Ordinaria: idem@garr.it

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

La procedura d'invio dovrà essere espletata solo per Posta Elettronica Ordinaria (PEO) all'indirizzo: idem@garr.it, NON è richiesto l'invio cartaceo.

3.3 Registrazione di una Risorsa

L'Organizzazione invia alla Federazione all'indirizzo di Posta Elettronica Ordinaria idem@garr.it:

- 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.

La procedura d'invio dovrà essere espletata solo per Posta Elettronica Ordinaria (PEO) all'indirizzo: idem@garr.it, NON è richiesto l'invio cartaceo.

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 nell'effettuazione di controlli periodici (*auditing*);
- adottare regole tecniche e organizzative al fine di favorire il rispetto del diritto d'autore e, più in generale, della legislazione correlata ai contenuti e ai servizi messi a disposizione dagli altri Partecipanti e dalla Federazione.

Il Partecipante che registra un IdP si impegna a :

- mantenere sui propri sistemi dei registri d'uso (*log*) che consentano di risalire agli utenti delle sessioni di autenticazione, con le modalità e per il tempo definiti in ST e fornire ogni ragionevole collaborazione alla Federazione o agli altri Partecipanti qualora fossero necessari chiarimenti e approfondimenti su attività rilevate come insolite e su eventuali incidenti di sicurezza;
- verificare periodicamente la conformità del processo di accreditamento dei propri utenti con quanto descritto nel DOPAU presentato e, in caso di difformità, a rivedere tale documento e ad inviarlo alla Federazione per sottoporlo a valutazione ed approvazione;
- 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.

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 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 Ordinaria (PEO) 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 dal Comitato di Indirizzo.

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 e a quanto dichiarato nel DOPAU, secondo le modalità descritte in ST.

Il Partecipante coopera e fornisce 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.

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 the IDEM Federation

v 1.5

May 15th, 2015

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 ;
- 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**), 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 g 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 requisites 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. Upon request, the CdI can allow the registration of more than one IdP per Organization. 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 can allow a Partner to register its Organization's IdP.

2.1.1 Privacy notice to Participants' contact persons

The names and personal information of persons 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 Requisites

2.2.1 General requisites (for all Participants)

Participants shall promptly communicate to the Federation the replacement of the Referente Organizzativo (RO), of the Referente Tecnico (RT), when applicable, and of Service Contact Persons, as well as any changes in their contact details.

Participants shall create a web page according to 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 **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**;
- 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 configured as required by the Federation; the substitution 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 Partners can, at their own discretion, include in the Technical Contacts an Account contact

2.2.3 Further requisites to register an IdP

User-related attributes must be made available respecting 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 can 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 respecting the user's privacy, and in compliance with naming, syntax and semantic specifications, as indicated in **ST-A**.

3 Accession to the Federation and Service registration

3.1 RA / AC

In order to join the Federation, the Participant:

- 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 the **RA** (if wishing to join as a Member) or the **AC** (if wishing to join as a Partner), which will be digitally signed by the Participant's Legal Representative or alternatively with original signature and stamp. The Participant through the RA or the AC accepts the Rules of Participation and appoints its representatives in the Federation;
- along with the RA, fills and signs the registration request for one IdP and/or one or more Resources; further Service registrations requests may be submitted afterwards;
- sends to the Federation all the above mentioned documents only by email to idem@garr.it; it is not required to submit any hard copy.

3.2 IdP Registration

The Organization sends to the Federation at the following email address idem@garr.it:

- the IdP Registration Form, filled in and digitally signed by the RO or by the Organization's Legal Representative or alternatively with original signature and stamp;
- the document describing the Organization's Identity Management System, drafted according to the **DOPAU** model; once the IdP is registered, the document will be made available to the other Participants upon request;

- the metadata fragment corresponding to the Service to be registered, filled with the requested data which will include the data specified in **ST.**

The IdP registration procedure must be dispatched only by electronic mail to the address idem@garr.it. Hard copy submission is not required.

3.3 Resource Registration

The Organization sends to the Federation at the following email address idem@garr.it:

- the **Resource Registration Form**, filled and digitally signed by the RO or by the Organization's Legal Representative or alternatively with original signature and stamp;
- the metadata fragment corresponding to the Service to be registered, which will include the data specified in **ST**.

The IdP registration procedure must be dispatched only by electronic mail to the address idem@garr.it. Hard copy submission is not required.

3.4 Participants' Commitments

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

Participants must:

- adopt changes approved by the Federation, including those related to the technical specifications or to terms of participation, within the deadline;
- acknowledge the Federation the right to publish and use needed metadata required for its operation;
- 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 imply any damages 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 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 made available by other participants and the Federation itself.

Participants registering an IdP are committed to:

- maintain logs on the Oganization'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 case of security incidents or of the observation of unusual activities such as to require inquiries or clarifications;
- periodically check if the end users registering procedures and the e-identity lifecycle reflect what is written in the DOPAU document and, in case of discrepancy, reviewing the document and resubmit it to the Federation for evaluation and approval;

- provide end-users with information about which resources provided by the Federation they can access.

Participants registering one or more Resources are committed to:

- minimize 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(s) usage;
- keep private the user information obtained through the Federation, without communicating it to third parties, unless specific agreements with their home Organization exist;
- do not aggregate any information about end-user activities without an explicit permission or previous agreements with their home Organization.

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.

To start with, the following will be verified:

- the GARR membership (for **RA** 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).

The completeness, consistency of the documentation and compliance to technical requirements of Services provided by the Organization will be then verified by the IDEM GARR AAI Service. The latter will include:

- installed certificates;
- the accuracy of the Service registration in the Federation ;
- 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.

Upon acceptance of the RA or AC, the Organization receives exclusively to the provided email addresses the countersigned **RA** or **AC**. If rejected, the Organization is notified with the reason of the refusal.

In the event of a positive outcome, the Organization or the new Service is accepted, and the Organization receives exclusively to the provided email addresses the countersigned **RA** or **AC**. In the event of rejection, the Organization is notified with the reason of the refusal.

IDEM GARR AAI Service notifies the Member Board of the new services availability.

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 in the event of:

- failure to fulfill 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

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

Participant may asks the interruption of its own specific Service that it offers 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 fragment for the time needed to solve the problem or irregularity.

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

4.2 Cancellation

Should the Participant fail to fulfill the requisites described hereby or in the other Federation documents

for more than 30 days from the official notification, its participation might be revoked.

The cancellation of a Participant can be proposed by the **CTS** and must be ratified by the **CdI**.

Participants may withdraw from the Federation by communicating their 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 catalog and metadata of available Services; validity, truthfulness and update of the information rest solely on charge on the responsible Participants;
- carries out help-desk, training and other knowledge transfer activities, in order to provide Organizations 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 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 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 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 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, according to the modalities described in **ST**.

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 for monitoring and auditing purposes only.

Any failures in fulfilling the technical requirements will be notified to Participant, together with the re-

quest to conform, on pain of suspension.

Audit procedures will be carried out continuously, automatically or manually, and will concern all Participants even 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 permanently, 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 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.

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 in the AC to follow the European Parliament Directive on privacy.

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 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 Participants' users.