

XIV Assemblea dei Membri della Federazione IDEM in VC 04/11/2022 dalle 14.30.00 alle 16.30

Presenti:

BATTISTA Claudia

VAGHETTI Davide

RANALDI Andrea

FASANELLI Enrico M.V.

PIRELLI Laura

Presidente Assemblea IDEM

Responsabile del Servizio IDEM

Coordinatore CTS IDEM biennio 2022-2023

Membro del CTS IDEM

verbalizzante Segreteria IDEM GARR

Programma ed Ordine del Giorno:

Ora	Intervento	Relatore
14:30 14:40	Apertura dell'Assemblea	Claudia Battista (GARR e Presidente Assemblea)
14:40 15:10	Relazione del Coordinatore del Comitato Tecnico Scientifico	Andrea Ranaldi (ISPRA e Coordinatore del CTS)
15:10 15:40	Relazione del Coordinatore del Servizio IDEM GARR AAI	Davide Vaghetti (Servizio IDEM GARR AAI)
15:40 16:10	Presentazione proposta di modifica Norme e Regolamento --- vedi ModificaRegNorme2022 Votazione	Enrico Fasanelli (CTS IDEM)
16:10 16:30	Varie ed eventuali e conclusione dei lavori.	Claudia Battista (GARR e Presidente Assemblea)

In data 4 novembre 2022, a causa del prolungarsi del periodo pandemico, l'Assemblea dei Membri IDEM è convocata nuovamente in un'aula virtuale riservata ai membri della federazione.

1. Apertura dell'Assemblea

L'Assemblea ha inizio come da programma con il Presidente dell'Assemblea IDEM, **Claudia BATTISTA**, che dà il benvenuto a Davide VAGHETTI, Responsabile del Servizio IDEM ad Andrea RANALDI, Coordinatore del CTS IDEM, Enrico M.V. FASANELLI membro del CTS IDEM e tutti i membri collegati da remoto.

Il Presidente dell'Assemblea fa una breve introduzione sugli argomenti previsti in agenda e cede la parola al Coordinatore del CTS IDEM.

2. Relazione del Coordinatore del Comitato Tecnico Scientifico

https://wiki.idem.garr.it/wiki/File:Andrea_Ranaldi_Relazione_CTS_Assemblea_4-11-2022.pdf

Prende la parola **Andrea RANALDI** che, in qualità di Coordinatore del CTS IDEM, che illustra in dettaglio gli scopi dei gruppi di lavoro: OI DC Proxy e Identity Assurance.

L'**OI DC Proxy** ha come obiettivo primario di permettere ad applicazioni OI DC di autenticare su IDEM/EduGAIN. RANALDI denota positivamente che si inizia a parlare di protocollo OI DC e si augura un domani di parlare di OI DC Federation. Spiega quale soluzione transitoria è stata pensata per sviluppare un proxy OI DC SAML2 e creare sia un sistema semplice, che desse ad ogni service provider la possibilità di istanziarlo per far accedere la propria applicazione ad IDEM. La soluzione si basa sul proxy Satosa SAML2Spipd sviluppato da Developers Italia. RANALDI considera questo sistema, come anticipato al workshop GARR di ottobre, una utility fondamentale per la Comunità GARR e per tutti i membri ed i partner che vorranno pubblicare un servizio su IDEM, in quanto ad oggi tutti i programmi escono OI DC.

Introduce l'**Identity Assurance** come altra attività dei gruppi di lavoro del CTS. Informa che la collaborazione dei vari gruppi di lavoro a confronto, ha prodotto un unico documento ancora non ufficiale, che diventerà il nuovo standard di Identity Assurance per la Federazione IDEM e che verrà presentato in uno dei **Seminari IDEM** dedicati agli argomenti più discussi nella federazione IDEM-GARR-AAI, strutturati volutamente per accogliere tutte le esigenze di confronto e di collaborazione.

Presenta infine una proposta di nuova attività per i gruppi di lavoro del CTS: l'**Attribute Authority OIDC** come un progetto da condurre in collaborazione con AGID, che prevede la partecipazione attiva di AGID per testare un caso d'uso reale.

Domande:

Interviene sull'argomento **Alessandro BRUNENGO**, della Sezione INFN di Genova, chiedendo se i seminari IDEM prevedono un'attività lavorativa preparatoria con scambi di informazioni o sono pensati solo per creare un posto dove fare la discussione. RANALDI informa che ogni seminario prevede un relatore e ha la durata di un'ora e mezza, circa quarantacinque minuti sono dedicati alla presentazione in cui viene approfondito l'argomento già studiato e portato avanti, altri quarantacinque minuti sono pensati alla discussione diretta con il relatore e con tutti gli altri partecipanti. Aggiunge che saranno aggiunte nuove date nel caso serva approfondire l'argomento o altri temi, perché l'idea è proprio quella di offrire momenti periodici di confronto. Le date sono volutamente programmate una ogni due settimane e attualmente sono in elenco argomenti per arrivare fino a Pasqua. I **seminari IDEM** saranno pubblicati alla pagina <https://learning.garr.it/> senza l'obbligo di registrarsi e con la possibilità di richiedere l'attestato di partecipazione.

VAGHETTI interviene chiarendo che la doppia formula open di partecipazione, è sperimentale e volutamente pensata per rispondere a due esigenze: aumentare la partecipazione il più possibile alle Istituzioni lontane dalla nostra comunità come Developers Italia e mantenere l'attestato di partecipazione per i partecipanti del mondo della ricerca.

Chiede la parola **Salvatore TODARO**, dell'Università degli Studi di Messina, proponendo la possibilità di offrire agli studenti STEM l'opportunità di partecipare a questi seminari. Comunica che è in contatto con i Responsabili di Dipartimento di Ingegneria Informatica per divulgare l'invito di partecipazione, con il vantaggio di mettere a confronto più competenze.

3. Relazione del Coordinatore del Servizio IDEM GARR AA

https://wiki.idem.garr.it/wiki/File:Davide_Vagheti_Relazione_Servizio_Assemblea_4-11-2022.pdf

Riprende la parola RANALDI ed introduce **Davide VAGHETTI** ed in qualità di Coordinatore del Servizio IDEM GARR AAI, allinea i presenti sullo stato della Federazione: n.140 IdP e n.121 SP. Elenca gli Istituti che hanno alimentato gli Identity Provider ed i Service Provider del 2022, sottolineando che la crescita degli IdP è principalmente dovuta all'ingresso di Atenei Statali e non, IRCCS, non ancora in IDEM, permettendo per ben l'88% rispetto l'anno precedente, maggiore copertura studentesca e personale docente. Motiva il perché le risorse pubblicate sono state apparentemente in numero inferiore rispetto al 2021: si è assistiti a due fenomeni, il primo è che molti SP non sono più visibili perché sono protetti da un unico gateway (un caso è il GARR che ha pubblicato nuove risorse federate in Federazione, tutte protette da un unico service provider, gateway, che di fatto è un proxy), realmente esistono nuovi servizi in termini di risorse ma il numero rimane fermo; una tendenza che si sta affermando sempre più, per cui ci sono nuovi editori che non pubblicano nuove risorse, non mettono in piedi nuovi servizi ma utilizzano un unico gateway per l'autenticazione di accesso alle proprie risorse. Il secondo motivo la cui tendenza avviene già da anni, è che buona parte delle risorse sono prese direttamente da eduGAIN senza fare registrazioni ad hoc in IDEM. Ricordando che eduGAIN è nato proprio con il fine di evitare che la stessa risorsa potesse essere registrata in più federazioni e permettendo l'utilizzo all'interno della comunità della ricerca mondiale. Ribadisce che la risorsa che entra a far parte di una federazione che ha aderito a eduGAIN e che ne condivide almeno le regole di base, può essere utilizzata anche dalle altre federazioni che ne

importano i metadata, in virtù del fatto che eduGAIN garantisce un certo livello di fiducia ma non garantisce sempre il livello qualitativo, soprattutto per quanto riguarda il rilascio degli attributi. VAGHETTI legge i dati di eduGAIN relativi ad una partecipazione sostenuta di paesi e fattiva in numero di IdPs e SPs e ricorda che il GARR gestisce la funzione di coordinamento a lui delegata. Tra i nuovi partecipanti ad eduGAIN rende noto la presenza di due aree mondiali fino ad ora poche interessate: l’Africa ed il Sud America.

Ricorda che le attività del Servizio IDEM GARR AAI continuano nell’opera di informazione tecnica per quanto riguarda la configurazione tecnica delle **Risorse Editoriali**, le cui istruzioni su chi contattare, quali dati fornire e quali attributi vanno rilasciati, sono consultabili sul wiki alla pagina: https://wiki.idem.garr.it/wiki/Configurazioni_Risorse_Editoriali

VAGHETTI comunica l’avanzamento sull’altra attività portata avanti, quella di **European Student Identifier**, sia a livello di documentazione, che di partecipazione ai tavoli, dove si decide su come il servizio debba essere utilizzato. Su questo aspetto informa che la Commissione Europea dovrebbe entro fine o inizio anno, prendere una decisione definitiva sulle altre modalità di accesso a Erasmus Plus che attualmente avviene anche tramite Google ed EIDAS e che non dovrebbe essere più possibile, in quanto l’obiettivo per accedere a tutti i servizi relativi all’Erasmus Plus dovrà avvenire tramite l’*European Student Identifier*.

La pagina dedicata a questo argomento è disponibile sul wiki: https://wiki.idem.garr.it/wiki/Erasmus_Plus_e_ESI.

Aggiorna i presenti sul lavoro di **IDEM MDX** che ha coinvolto il Servizio IDEM, anticipato al WS GARR del 2021 ed il cui lancio ufficiale è avvenuto in occasione dell’Assemblea dei Membri a fine febbraio 2022. Ricorda che IDEM MDX è un servizio dinamico dei metadata che permette di risolvere il problema generato dalle grandi dimensioni dell’aggregato di metadata. VAGHETTI utilizzando le informazioni rappresentate in una slide del collega Mario DI LORENZO, spiega che il peso dell’aggregato di metadata di eduGAIN e di tutte le risorse IDEM è di 77 MB e che al proprio interno contiene più di ottomila entità, evidenziando quanto il lavoro di scaricare per ogni entità i files per una serie di dati xml e certificati relativi, comporta un dispendio di tempo e risorse molto elevato, tempo che varia con l’aggregato di metadata da un minimo di un minuto, a quindici minuti, a secondo dell’implementazione software che si utilizza per IdP o SP. Porta in esempio l’implementazione di Shibboleth, come quella più performante. Sottolinea la validità di quanto il servizio di distribuzione dinamico dei metadata risolve una serie di problemi, tra cui il tempo per riavviare un servizio in produzione critico come un IdP e l’utilizzo delle risorse in termini di ram, in considerazione del trend di crescita costante ed elevato di eduGAIN, seppur ci si aspetta un cambio di tendenza con tanti servizi dietro un proxy, ad oggi ancora non manifestato. Evidenzia quanto questo servizio stia prendendo piede, illustrando i picchi nel grafico e quanto sia maggiormente interessante rispetto l’aggregato di metadata, perchè capace di misurare e rilevare l’utilizzo in base alle richieste delle risorse federate; dati ricavati dall’analisi di una cache di raccolta impostata per quarantotto ore.

La documentazione del servizio che fa parte del processo di sviluppo è pubblicata sul sito del servizio alla pagina: <https://mdx.idem.garr.it/>

Un altro tema rappresentato da VAGHETTI nella slide è la modalità e la qualità delle importazioni dei Service Provider da eduGAIN in IDEM, sottolineando che eduGAIN può garantire un livello di fiducia sui dati dell’entità che GARR importa dalle altre federazioni, ma non sempre può garantire un livello qualitativo dei metadata. Spiega come avviene il processo d’importazione da eduGAIN e quali sono i passaggi attuati dal Servizio IDEM, che hanno inizio dal grande aggregato di metadata tra federazioni, in cui avviene la verifica della validità della firma, la pulizia del xml, il filtraggio dell’entità e termina con l’integrazione dei metadata di IDEM, per essere pronti alla pubblicazione nello stream di eduGAIN IDEM.

Riguardo la qualità dei metadata della Federazione IDEM, VAGHETTI esplicita che va fatto un discorso a parte sul rilascio degli attributi. Sottolinea quanto l’interpretazione del Servizio alle restrittive Norme di Partecipazione ad IDEM, che obbliga tutti i service provider a dichiarare in modo esplicito e puntuale quali sono gli attributi di cui hanno bisogno nei metadata distinguendoli tra obbligatori e opzionali, permetta un livello alto di fiducia, di puntualità e qualità che non è garantita in eduGAIN.

Conclude dicendo che se ci si fida dei metadata rilasciati dalla Federazione IDEM utilizzando filtri resi automatizzabili sugli attributi degli SP e non custom, è possibile semplicemente dire se il Register è la Federazione IDEM, seppur il servizio ha dovuto creare ugualmente dei filtri custom per esigenza di alcune risorse con metadata imprecisi.

La pagina dedicata ai filtri resi disponibili dal Servizio è consultabile su: <https://wiki.idem.garr.it/wiki/RilascioAttributi>

VAGHETTI cambia argomento e ritorna su un discorso già affrontato: **InAcademia** di GEANT, nato per verificare lo status dello studente e a cui il Servizio IDEM contribuisce nella gestione del servizio. Dalle indagini risulta che gli Student verification services in IDEM tramite eduGAIN, sono molto utilizzati. Ricorda l'incidente causato da SheerID ed in seguito filtrato, perché offriva accesso ad una serie di risorse sia commerciali che di scontistica, senza la necessità di supporto lato IDEM. Solleva dubbi sulla trasparenza, sulla privacy e sulla circolazione dei dati di vario tipo richiesti, non necessari per lo scopo finale di tali servizi. Informa che il servizio InAcademia è no profit, viene richiesto un piccolo contributo, utilizzato per essere rimesso in circolazione nel circuito che alimenta i servizi di trust identity come ad esempio quello di una biblioteca che ha bisogno di effettuare verifiche di autenticazione, ed è a pagamento per la parte commerciale. Dal punto di vista del flusso InAcademia è anch'esso un proxy, da una parte si interfaccia a eduGAIN tramite un service provider, mentre nei confronti dei servizi espone un'interfaccia openID Connect, standard maggiormente utilizzato dai nuovi provider. VAGHETTI informa che GARR fa parte della Governance di InAcademia e una delle proposte che avanzerebbe come servizio nel CTS, da portare in una prossima assemblea e su cui sarebbe interessato a conoscere l'opinione dei presenti, è quella di non limitarsi a filtrare solo SheerID, ma anche gli altri Student verification services importati da eduGAIN, allo scopo di far utilizzare questi servizi solo tramite InAcademia ed evitare lo sfruttamento a scopi di lucro dell'infrastruttura, costituita grazie all'effort tecnico volontario di chi ha contribuito. VAGHETTI conclude il suo intervento e dà spazio alle domande.

Domande:

Prende la parola **Salvatore TODARO**, dell'Università degli Studi di Messina, che condivide il senso etico e non commerciale della questione, ma pone il dubbio che la privazione ai provider commerciali possa limitare il servizio e propone, una visione alternativa. TODARO considera l'opportunità di estendere questa realtà a società spin-off/start-up, al fine di creare valore aggiunto sul territorio e dare la possibilità alle stesse, di partire con un vantaggio competitivo rispetto società analoghe. VAGHETTI risponde che tale proposta necessita del benestare da parte di GARR e del Board di InAcademia, oltre che di un approfondimento dell'argomento in un altro contesto.

BATTISTA interviene e sottolinea la delicatezza dell'argomento, considerando che il concetto di società spin off/start up in Italia è abusato ed è usato in maniera impropria, visto il perdurare per molti anni, di alcune realtà oltre i due/tre anni previsti in fase di nascita dell'impresa. E' comunque d'accordo a valutare l'ipotesi di stabilire fasce di fatturato per distinguere l'entità di tipo commerciale o no profit, prevedendo un contributo di valore simbolico in base al fatturato quando l'azienda svolge attività egregie. VAGHETTI coglie l'occasione per condividere la pagina del tariffario di InAcademia e garantendo la convenienza dei costi (<https://inacademia.org/pricing/>).

4. Relazione del membro del CTS GARR

https://wiki.idem.garr.it/wiki/File:Enrico_Fasanelli_Modifica_Norme_Regolament_Assemblea_4-11-2022.pdf

Non essendoci altri interventi, VAGHETTI passa la parola ad **Enrico FASANELLI** che introduce la sua presentazione sulle proposte di modifiche relative al Regolamento della Federazione IDEM e alle Norme di Partecipazione, di fatto già circolate in Federazione e pronte per la votazione diretta con sistema di voto elettronico durante l'Assemblea dei Membri.

FASANELLI informa che insieme al Servizio IDEM ha provveduto a razionalizzare alcuni aspetti riguardanti la fonte autoritativa dei dati di contatto delle entità, il ruolo ed il numero dei referenti tecnici, il cui iter di approvazione è stato gestito in due consultazioni aperte tra settembre e ottobre, fino all'approvazione finale il giorno dell'Assemblea. Gli aggiornamenti sono stati recepiti come modifiche nelle Norme di Partecipazione ai punti 2.2.1 Requisiti base

per ogni Partecipante; 2.2.2 Requisiti per la registrazione di un servizio; 3.2 Registrazione di un IdP e 3.3 Registrazione di una Risorsa.

Si passa alla votazione e nel frattempo si concede la possibilità di fare domande.

Domande:

Segue l'intervento di **Sergio STORARI**, dell'Università di Bologna che chiede quali sono esattamente le responsabilità che vengono passate dal Referente Organizzativo, al Referente Tecnico. Risponde VAGHETTI chiarendo che non ci sono responsabilità che passano dal Referente Organizzativo, al Referente Tecnico ma dal Contatto Tecnico, al Referente Tecnico. Aggiunge che il Referente Tecnico ha sempre la delega automatica e per la responsabilità trasferitagli dal Referente Organizzativo, può con questa modifica registrare la risorsa divenendo responsabile dei metadata di quella risorsa. RANALDI completa spiegando che nel momento in cui un Referente Tecnico registra una risorsa, la stessa è associata a chi l'ha registrata. L'idea di fondo secondo FASANELLI è quella di avere un referente diretto senza dover arrivare al Referente Organizzativo, che tipicamente ha un incarico più alto nell'organizzazione dell'Ente. VAGHETTI aggiunge che un'altra ratio fondamentale è la distinzione tra il ruolo operativo del Referente Tecnico, in cui rientra la registrazione delle risorse, ed il ruolo politico del Referente Organizzativo che invece è chiamato a decidere su norme e regolamenti.

Domande:

Segue l'intervento di **Marco NAIMOLI** dell'Università di Padova, che chiede se l'email nei metadata deve essere quindi personale e non quindi un alias di posta. Risponde VAGHETTI informando che questa specifica non è indicata nel Regolamento e nelle Norme di Partecipazione, vi subentra arbitrariamente il Servizio, in veste di operatore di Federazione che è GARR, dando preferenza per la gestione dei servizi ad indirizzi di posta non personale e possibilmente alle liste, immaginando che la maggior parte dei servizi siano gestiti da più di una persona, da un team.

La votazione si chiude alle 16.10 e VAGHETTI informa in tempo reale quali i risultati raggiunti: su n.31 partecipanti, n.31 votazioni favorevoli convalidano la proposta di modifica.

Il Presidente dell'Assemblea IDEM Claudia Battista conclude l'incontro, anticipando che la collega Sabrina TOMASSINI subentrerà a lei in qualità di nuovo Referente Organizzativo GARR e ringrazia tutti per la partecipazione.

La riunione si chiude nei tempi stabiliti.