

## XVI Assemblée dei Membri della Federazione IDEM 09/11/2023 dalle 16.30 alle 18.00

Presenti:

**BATTISTA Claudia**  
**VAGHETTI Davide**  
**RANALDI Andrea**  
**PIRELLI Laura**

Presidente Assemblée IDEM  
Responsabile del Servizio IDEM  
Coordinatore CTS IDEM biennio 2022-2023  
verbalizzante Segreteria IDEM GARR

### Programma ed Ordine del Giorno:

Ora	Intervento	Relatore
16:30 16:40	Apertura dell'Assemblea	Claudia Battista (Direttrice GARR e Presidente Assemblée)
16:40 17:00	Relazione del Coordinatore del Comitato Tecnico Scientifico della Federazione IDEM	Andrea Ranaldi (ISPRA e Coordinatore del CTS)
17:00 17:10	Discussione	
17:10 17:30	Relazione del Coordinatore del Servizio IDEM GARR AAI	Davide Vaghetti (Servizio IDEM GARR AAI)
17:30 17:40	Discussione	
17:40 18:00	Varie ed eventuali e conclusione dei lavori.	Claudia Battista (Direttrice GARR e Presidente Assemblée)

In data 09 novembre 2023, l'Assemblea dei Membri IDEM riservata ai membri della Federazione, è convocata in presenza nei locali della Biblioteca Nazionale Centrale (Viale Castro Pretorio, 105 - 00185 Roma).

### 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 e tutti i membri presenti in sala.

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:Assemblea\\_Ranaldi\\_20231109.pdf](https://wiki.idem.garr.it/wiki/File:Assemblea_Ranaldi_20231109.pdf)

**Andrea RANALDI**, Coordinatore del CTS IDEM, saluta i membri in aula fa il punto della situazione sui tre argomenti che sostanzialmente sono stati trattati nell'ultimo periodo di lavoro dal CTS: **i Profili di garanzia IDEM** oggetto di votazione nella precedente assemblea, che ha dato vita al **nuovo Regolamento** e alla **Formazione**, necessaria ai membri della federazione per aderire ai Profili di garanzia.

Il CTS scadrà a febbraio e RANALDI in qualità di Coordinatore del CTS, anticipa che i prossimi tre mesi saranno destinati ancora alla formazione, approfondendo il concetto dei profili, come adeguarli, come eventualmente migliorarli.

Nello specifico la formazione sarà dedicata: all'aggiornamento di Shibboleth (alla versione\_5); ai profili di garanzia; alla realizzazione di guide basate sugli argomenti dei corsi tenuti dal CTS e dal Servizio.

Propone per il prossimo CTS la possibilità di ampliare i gruppi di lavoro ai responsabili amministrativi, per creare esempi di procedure per l'adesione ai profili di garanzia e definire un sistema che certifichi la partecipazione, utile per un feedback verso l'Ente di rappresentanza e per concorsi interni.

Le attività svolte in IDEM ed in Federazione rappresentano un lavoro molto importante, su cui c'è scarsa competenza. RANALDI sottolinea anche che è difficile trovare tecnici e ditte competenti in OIDC e SAML. A tal proposito invita il prossimo CTS a offrire più occasioni di confronto, propone di continuare a raccogliere le esigenze e gli argomenti di tutti i membri federati per continuare a creare collaborazioni e trovare standard comuni, visto che si lavora tutti sulle stesse cose. Cita a titolo di esempio **DOCKER** nel settore sviluppo, che è stato implementato in ISPRA, soltanto dopo che un collega del CNR lo ha introdotto tramite un progetto pubblico. Allo stesso modo oggi ISPRA collabora attivamente allo sviluppo di **Satosa-Saml2Spid** insieme al CNR, all'Università della Calabria, all'Università di Milano e altri ancora, un lavoro di cinque anni fa, generato dalla presentazione del collega Giuseppe DE MARCO, oggi in sala, per aver presentato l'Identity wallet. E altrettanto fa GARR con **Shibboleth**, perché open source non è soltanto prendere gratuitamente, ma è soprattutto avere l'occasione di influenzare lo sviluppo e avere voce in capitolo sulle scelte strategiche.

RANALDI, prima di introdurre VAGHETTI, conclude il suo intervento ricordando che unire le proprie forze nei gruppi di lavoro è una vera occasione di crescita e può confermarlo in prima persona.

Riprende la parola BATTISTA, che sulla questione dei gruppi di lavoro e la possibilità di confrontarsi sulle esperienze e sulle buone pratiche sollecitate da RANALDI, ricorda che uno dei ruoli che il GARR riveste, è proprio quello di facilitatore tra le varie organizzazioni e i vari interessi. Ribadisce che il modo di operare del CTS IDEM è l'esempio che tende a promuovere anche in altri contesti, per convergere e attrarre altre persone. Suggestisce che tale metodo è il più efficace per lavorare insieme ad un'idea, soprattutto se come nel CTS IDEM, i gruppi di lavoro hanno tempi di vita molto brevi che permettono di arrivare velocemente ad un risultato, compreso, com'è giusto, il fallimento precoce.

RANALDI d'accordo con il suggerimento del Presidente, passa la parola a VAGHETTI.

### 3. Relazione del Coordinatore del Servizio IDEM GARR AAI

**Davide** VAGHETTI in qualità di Coordinatore del Servizio IDEM GARR AAI, scorre gli argomenti oggetto della sua relazione, relativa: allo stato della Federazione; l'aggiornamento dei servizi; i profili di garanzia IDEM secondo il processo di adesione e REFEDS Identity Federation Baseline Expectations.

Per dettagli vedi la presentazione pubblicata sul wiki della Federazione IDEM:  
[https://wiki.idem.garr.it/wiki/File:Relazione\\_del\\_Servizio\\_IDEM\\_GARR\\_AAI\\_AdM\\_2023-2.pdf](https://wiki.idem.garr.it/wiki/File:Relazione_del_Servizio_IDEM_GARR_AAI_AdM_2023-2.pdf)

Riprende la parola BATTISTA, dando spazio alle domande.

## Domande:

**Salvatore TODARO dell'Università degli Studi di Messina** chiede al PRESIDENTE di formalizzare il modello vincente dei gruppi di lavoro IDEM, banalmente per allocare ore e continuare a stringere collaborazioni, al fine di raggiungere i risultati a fine anno.

BATTISTA ricollegandosi al precedente suggerimento di RANALDI, finalizzato a dimostrare il tempo impiegato, in un'attività svolta, con il raggiungimento degli obiettivi e condividendone l'idea con VAGHETTI, risponde che pensava alla redazione di un documento finale che andasse oltre le nuove specifiche, un "deliverable di progetto" che ne descrivesse le attività e ne elencasse le persone coinvolte, stabilendo l'obiettivo e le tempistiche.

TODARO specifica che l'allocazione delle ore e delle risorse deve essere definito "ab initio". In effetti, risponde BATTISTA, questo avviene solo per la nomina del CTS IDEM, ed è possibile trovare un metodo che possa andare in questa direzione. Secondo RANALDI il chiedere troppe formalizzazioni potrebbe diventare vincolante, suggerisce che la partecipazione al gruppo dovrebbe rimanere una comunicazione monodirezionale, in quanto richiedere formalizzazioni da parte dell'Istituto, per ogni gruppo di lavoro, potrebbe diventare un impegno che limiterebbe la partecipazione delle persone.

TODARO ritorna sulla questione e propone che l'allocazione "ab initio" avvenga in occasione della convenzione, supposizione non attuabile secondo BATTISTA perché gli Enti che partecipano sono già tutti convenzionati, e neanche per i nuovi Enti, trattandosi di convenzioni pluriennali e per questi incontri che riguardano eventi annuali, occorre trovare semmai una forma più funzionale e dinamica.

TODARO rivolgendosi a VAGHETTI chiede maggiori livelli di assurance riguardo ai controlli remoti e formali degli enti che aderiranno ai Profili di Garanzia, in particolare per l'ambito sanitario. Nel rispondere VAGHETTI distingue due ambiti, spiegando che le verifiche da remoto avvengono a seguito della pubblicazione di accreditamento e la verifica è su quanto è effettivamente dichiarato, rispetto ai processi di accreditamento; mentre le verifiche tecniche e non formali avvengono quando si trasmette l'assurance nell'ambito dell'autenticazione e dell'implementazione dell'MFA, così come avviene da dichiarazione ed il resto è sulla fiducia.

Prende la parola **Arnaud CEOL dell'IRCCS IEO di Milano**, rivolgendosi a VAGHETTI ed anticipando le perplessità che saranno oggetto dei prossimi mesi, relative alle aspettative sull'IdP in caso di in the cloud e nello specifico sulle responsabilità di IDEM, rispetto a quelle dell'Istituto.

Interviene BATTISTA chiarendo che verrà fatto un approfondimento su come verrà definito il doppio livello di responsabilità e VAGHETTI aggiunge che GARR, in qualità di gestore e non IDEM che è la Federazione, ha la responsabilità tecnica di implementare il servizio e che nell'ambito del trattamento dei dati è l'Istituto ad essere titolare dei dati.

**Giuseppe DE MARCO** chiede come sia possibile bloccare una Federazione in eduGAIN, quando non sono aggiornati i metadati e quando non sono rispettati i requisiti fondamentali.

VAGHETTI motiva che ciò è possibile e accade ipotizzando tre casistiche:

1. quando scadono i termini di pubblicazione dei metadati che vanno dai 5 ai 28 giorni;
2. quando oltre ai metadati scaduti, della Federazione non c'è più traccia, come il caso in Mozambico, in cui sono stati spenti i server, licenziato il personale e non hanno avuto più attiva la rete della ricerca;
3. quando a seguito di decisioni della Comunità Europea ed in ottemperanza all'utilizzo dei fondi ricerca, sono stati sospesi i fondi europei a Russia e Bielorussia e si è stati costretti ad estromettere due Federazioni russe ed una bielorussa.

Fa una domanda **Marco MALAVOLTI del GARR**, chiedendo se idem-test, che sarà messo in produzione ad aprile 2024, potrebbe essere lo strumento per adeguare la ricerca dei metadati secondo quelle che saranno le nuove direttive indicate da eduGAIN.

VAGHETTI conferma che, in prospettiva, idem-test potrebbe essere lo strumento idoneo per questo scopo e che potrebbe essere lui lo sviluppatore di edugain connectivity check service, al fine di verificare che un IdP sia attivo, stia consumando i metadata e che risponda in modo adeguato ad ogni authentication request da service provider sia di eduGAIN che non.

Chiede parola **Sergio STORARI dell'Università di Bologna**, spiega che il loro Ateneo è coinvolto in diversi progetti pilota legati all'Identity wallet, che come anticipato dal collega DE MARCO, pur non essendo attualmente una realtà, lo diventerà a breve. Tra le esigenze manifestate dall'Università di Bologna come Ateneo pilota, è emersa quella di avere una credenziale che rappresenti il profilo dello studente o dello staff all'interno delle loro istituzioni da portare in una credenziale digitale in considerazione del nuovo paradigma di autenticazione che, di per sé, toglie il concetto di più IdP che sono nati con una Federazione come IDEM. Aggiunge che bisognerebbe capire a livello nazionale il ruolo della Federazione IDEM in questo nuovo paradigma, in cui c'è Gèant che però non è attivo come lo si aspetta.

STORARI conclude il suo intervento, auspicando un maggiore coinvolgimento delle federazioni di eduGAIN e delle federazioni nazionali nel gestire questo aspetto in tempi brevi.

Sulla questione VAGHETTI risponde che in parte lo stesso STORARI ha già anticipato la risposta e conferma che il paradigma cambia ma sussistono tante cose in comune, come il credential issuer. Il ruolo dell'IdP potrebbe essere lo stesso del credential issuer almeno nell'ambito che compete ad IDEM, che non deve essere quello dell'anagrafica, quindi paradossalmente più che riguardare la Federazione IDEM, alla fine si potrebbe certificare il ruolo all'interno dell'accademia degli Enti ricerca e di quelli con pari caratteristiche. Quello che probabilmente IDEM non dovrà più trattare sono le informazioni sull'anagrafica delle persone, che la Federazione riceve e non possiede. Conferma inoltre che al di là delle similitudini, saranno necessari profili di implementazione e di deployment per occuparsi in concreto di Identity wallet e, come suggeriva Silvio RANISE dell'Università di Trento all'ultima Conferenza GARR, e che a livello di eduGAIN e di Gèant si sta portando ai vari tavoli, bisogna evitare di mandare a monte l'attuale infrastruttura mondiale di trust per il nuovo paradigma wallet. L'idea è di ancorare all'infrastruttura esistente, tutti gli attori che avranno bisogno di parlare in modo fidato all'interno del nuovo paradigma.

STORARI concorda e ribadisce che, parlando di credenziali autoritative, come esistono le regole ben scritte e i requisiti formalizzati per la creazione degli attributi e dei claims interni, ci dovrà essere qualcuno come IDEM che sovrintenda, guidi e controlli se questi dati siano scritti in maniera corretta. STORARI conclude e segnala che gli altri Enti a livello nazionale hanno già espresso la catena di trust e l'Italia, non quanto per la parte tecnica, ma quanto per la parte organizzativa, è un po' "latitante".

Il Presidente dell'Assemblea IDEM Claudia BATTISTA conclude l'incontro e ringrazia i presenti per i preziosi spunti e l'intera comunità per la preziosa collaborazione.

La riunione termina alle 18.30.