XVII Assemblea dei Membri della Federazione IDEM
08/03/2024 dalle 10.30 alle 12.30

Presenti:

BATTISTA Claudia	Presidente Assemblea IDEM
VAGHETTI Davide	Responsabile del Servizio IDEM
RANALDI Andrea	Coordinatore CTS IDEM biennio 2022-2023
PIRELLI Laura	verbalizzante Segreteria IDEM GARR

Programma e

Ordine del Giorno:

Ora	Intervento	Relatore
10:30 10:40	Apertura dell'Assemblea	Claudia Battista (Direttrice GARR e Presidente Assemblea)
10:40 10:55	Relazione del Coordinatore del Comitato Tecnico Scientifico: File:Relazione del Coordinatore CTS IDEM - AdM 2024.pdf	Andrea Ranaldi (ISPRA e Coordinatore del CTS)
10:55 11:20	Relazione del Coordinatore del Servizio IDEM GARR AAI: File:Relazione del Servizio IDEM GARR AAI - AdM 2024.pdf	Davide Vaghetti (GARR), Coordinatore del Servizio IDEM
11:20 12:00	Presentazione delle candidature a Coordinatore del Comitato Tecnico Scientifico 2024-2026 e discussione delle proposte tematiche per il nuovo CTS. Candidati a ruolo di Coordinatore: **Andrea Ranaldi** (ISPRA), CV: File:Andrea Ranaldi CV 2024-CTS-IDEM.pdf; Link per la votazione (accesso via IDEM): https://evento.renater.fr/survey/nomina-del-coordinatore-cts-idem-2024-2026-w3zs1pi4	
12:00 12:20	Termine della votazione e nomina del Coordinatore del Comitato Tecnico Scientifico 2024-2026 **Risultato del voto:** Andrea Ranaldi (ISPRA) è stato nominato Coordinatore del CTS IDEM 2024-2026	
12:20 12:30	Conclusione dei lavori	Claudia Battista (Direttrice GARR e Presidente Assemblea)

In data 08 marzo 2024, l'Assemblea dei Membri IDEM è convocata in un'aula virtuale riservata ai membri della Federazione.

1. Apertura dell'Assemblea

L'Assemblea ha inizio come da programma con la Presidente dell'Assemblea IDEM, **Claudia BATTISTA**, che dà il benvenuto a Davide VAGHETTI, Responsabile del Servizio IDEM, ad Andrea RANALDI, Coordinatore a termine del suo mandato del CTS IDEM 2022-23 e ai membri collegati, al consueto appuntamento giunto alla XVII edizione.

Fa una breve introduzione sugli argomenti previsti in agenda e ricorda che la missione del Consortium GARR è quella di completare una infrastruttura di rete sempre più performante, al fine di garantire il miglior modo di accedere ai servizi e alle applicazioni di tutte le utilities di interesse per la comunità GARR. Questo lo spirito portato avanti insieme a tutte e tutti i componenti della federazione, perché il GARR da solo rappresenta un importante strumento di supporto tecnico, organizzativo gestionale, che opera alla base della federazione, le cui regole e prassi sull'attività

sono svolte ognuno nel proprio Istituto di appartenenza secondo le proprie esigenze e, trovare regole e pratiche comuni che facilitano vicendevolmente queste attività, è l'obiettivo della federazione, sia a livello nazionale, ma anche e soprattutto a livello internazionale in cui GARR tende a svolgere al meglio questo ruolo, portando le istanze della comunità federata.

La Presidente dell'Assemblea IDEM, terminato il discorso di apertura dell'Assemblea, ringrazia tutti i candidati e le candidate uscenti dal mandato CTS IDEM 2022-23 e coloro che per il rinnovo del CTS 2024-2026 hanno inviato nei termini previsti la loro candidatura e cede la parola al Coordinatore in carica del CTS IDEM.

2. Relazione del Coordinatore del Comitato Tecnico Scientifico

Andrea RANALDI, Coordinatore del CTS IDEM a termine del suo mandato, saluta i membri presenti e inizia il suo intervento con un recap dei progetti portati avanti nell'ultimo anno, relativi a:

- Profili di garanzia
- modifiche apportate al regolamento IDEM per l'adesione ai profili di garanzia
- Formazione per i membri IDEM
- Sviluppo di applicazioni ed utility per membri IDEM

Fa presente che sui nuovi "Profili di Garanzia" si è lavorato con un'unica qualità di identità e di autenticazione, e l'avere un profilo generico è limitante in quanto non garantisce la qualità con cui l'utente è stato riconosciuto.
Risalta l'utilità del REFEDS Assurance Framework (RAF) v2.0 e di SPID che permettono un accesso ragionato a dati sensibili, in quanto rendono stabili la compatibilità con i nuovi profili di garanzia che, basati su NIST 800-63B, distinguono i concetti di "identificazione" ed "autenticazione" e ricorda la procedura necessaria che i profili devono possedere:

- Identificazione dell'utente
- Consegna e rinnovo dei fattori di autenticazione
- Tempi di rinnovo degli attributi rilasciati

RANALDI menziona cosa è stato possibile fare a seguito delle modifiche votate e apportate lo scorso anno nel regolamento di federazione:

- rendere l'adesione ai profili di garanzia facoltativa
- definire i controlli necessari per l'adesione ai profili di garanzia
- definire i processi che gli enti devono aver previsto per l'adesione ai profili di garanzia
- definire una durata per l'adesione ai profili di garanzia che dovrà essere rinnovata annualmente;

e riguardo la Formazione, elenca i webinar ed i corsi in presenza tenuti dal CTS per un totale di oltre 1500 iscritti, ne ricorda la pagina web in cui sono disponibili:
https://learning.garr.it/course/index.php?categoryid=33

In qualità di Coordinatore del CTS informa che la sua partecipazione al board di sviluppo di Shibboleth ha permesso di avvantaggiare la federazione nello sviluppo dell'IDP, di fatto più utilizzato nella federazione, mentre il contributo del CTS nel partecipare attivamente allo sviluppo di Satosa-Saml2Spid ha permesso ai membri di avere accesso per un proxy OIDC/SAML e federare facilmente anche software che supportavano esclusivamente il protocollo OpenID Connect.

A nome di tutto il CTS, RANALDI introduce le proposte per il nuovo CTS 2024-26, e ne provvede a specificare gli ambiti progettuali distinguendo le aree di intervento.

Per l'area di **Formazione** si propone di affrontare i seguenti argomenti:

- Aggiornamento di Shibboleth, migrazione alla versione 5
- Profili di garanzia
    - Adesione ai profili di garanzia
    - Requisiti dei livelli di garanzia
    - Fattori di autenticazione, definizione dei requisiti di ogni fattore
    - Autenticazione multi fattore, requisiti e gestione degli ulteriori fattori
    - Configurazione dei profili con Shibboleth
    - Configurazione dei profili con SimplaSAMLPHP
- Approfondimenti verso le nuove tecnologie
    - OIDC Federation
    - Digital Wallet
    - Passwordless authentication

Per l'area dei **Gruppi di Lavoro** si propone di creare gruppi misti che includano oltre a tecnici anche DPO ed RDT per creare procedure di esempio per l'adesione ai profili con particolare attenzione ai seguenti argomenti:

- Processi di identificazione
- Processi di consegna e rinnovo fattori
- Analisi dei rischi e conservazione di log e credenziali

Si manifesta inoltre l'intenzione di proporre gruppi di approfondimento relativi all'integrazione con le nuove tecnologie emergenti ed in generale l'integrazione con il concetto di identità digitale unica.

Per l'area "**Comunità"** si suggerisce di coinvolgere RTD e RDP/DPO nelle problematiche di identità digitale, autenticazione ed autorizzazione. e definire un sistema per far certificare da IDEM la presenza nei gruppi di lavoro e dare la possibilità ai dirigenti di verificare l'effettiva partecipazione del personale alle attività IDEM.

Come Coordinatore uscente del CTS esorta ad organizzare un nuovo IDEM Day in presenza, per fortificare la comunità e a creare eventi IDEM per i fruitori del servizio (studenti, docenti, dipendenti degli enti federati e fornitori di servizio) allo scopo di sensibilizzare le persone sull'importanza e sul corretto utilizzo dell'identità digitale, spiegando l'utilità della federazione.

RANALDI termina il suo intervento e, prima di passare la parola a VAGHETTI, cede la parola a BATTISTA, che cogliendo il suggerimento di RANALDI sul certificare l'attività svolta, informa i membri che al fine di dare seguito a tale richiesta, sono ben accette eventuali proposte anche sulla base di esperienze analoghe in altri contesti.

3. Relazione del Coordinatore del Servizio IDEM GARR AAI

Davide VAGHETTI, in qualità di Coordinatore del Servizio IDEM GARR AAI, si allaccia a quando anticipato da RANALDI sulla questione che la federazione è una comunità, ma soprattutto ricorda che è un servizio tecnico, e GARR in veste di operatore di federazione esprime il servizio nella NREN ed introduce la sua relazione dettagliando per punti ogni argomento:

- **Stato della Federazione**
  tra i nuovi membri i risalta l'alto numero di IRCCS; tra gli SP evidenzia che l'INFN continua a registrarne di nuovi, e rileva tra i nuovi richiedenti gli editori italiani, mentre gli editori vengono importati direttamente da eduGAIN; annuncia tra i nuovi servizi quello di GARR per le conferenze, che sarà in utilizzo a partire dalla prossima Conferenza GARR (c/o l'Università di Brescia, 29-31 maggio). Fa un breve riepilogo sui numeri ed informa che sono stati raggiunti 152 IdP e 131 Servizi, mentre a livello di eduGAIN continua la crescita di entità registrate, ricordando il significativo arresto dovuto all'esclusione delle due federazioni russe in ottemperanza alle decisioni dell'UE;

- **Statistiche di utilizzo**
  il periodo preso in esame analizza i dati statistici anonimi del mondo della ricerca e l'accesso ai servizi forniti da eduGAIN, messi a disposizione da tutti i membri della Federazione e maggiormente espressi nel periodo da sett-2023 a genn-2024.

  Tra i login aggregati per mese, dei 75 IdP, 40 sono relazionati agli IRCCS e nello specifico:
  - **i login aggregati per organizzazione** identificano l'IdP utilizzato per Ente, l'Università degli Studi Torino è il membro della Federazione IDEM con il maggior numero di login mensili (4/5 milioni);
  - **i login aggregati per provenienza delle risorse** evidenziano il dato statistico classificato in tre diverse macro aree:
    IDEM - relativo alle risorse registrate in IDEM, i servizi maggiormente utilizzati sono l'*e-learning* dell'Università di Padova e l'*e-learning* dell'Università di Milano Bicocca ed il servizio *wifi* dell'Università di Torino; importanti gli ingressi da parte di nuovi editori italiani, come Criterium e Medialibrary;
    eduGAIN - oltre ai grandi gruppi editoriali, spiccano alcune risorse di verifica status studente di tipo commerciale come Inacademia di GEANT e altre commerciali;
    point-to-point - il 92.2% degli accessi avviene su risorse locali dell'Ente, *e-learning* è il servizio più presente;

- **Obiettivi e progetti del Servizio IDEM per il 2024**
  in buona parte sono allineati ai progetti del CTS IDEM a cui lo staff del servizio IDEM partecipa ed in parte sono relativi alla gestione tecnica del servizio che gestisce, firma e distribuisce i metadata.
- ***Formazione, ricerca e sviluppo***

  - **Shibboleth IdP 5** - prevista una formazione in presenza il prossimo 28/5 in occasione della Conferenza GARR (c/o l'Università di Brescia, 29-31 maggio), che affronterà sia l'installazione della versione 5 di Shibboleth, sia la configurazione del plugin OpenID Connect;

  - **Multi Factor Authentication** – in previsione formazione online o in presenza, a seconda della soluzione più adatta, garantendo la massima partecipazione;

  - **Passwordless Authentication** - oltre all'autenticazione a più fattori, si stanno diffondendo strumenti che permettono di attuare la Passwordless Authentication come

WebAuthn/Passkey/Fido2, protocolli standard che tipicamente si basano su autenticazione di chiavi simmetriche per ogni servizio a cui si vuole accedere. La Passwordless Authentication fa riferimento a come si accede alla chiave privata. L'Authentication diventa forte perché esegue il multifattore sul device (es. l'accesso multifattore tramite impronta digitale e codice di accesso);

- **OpenID Federation** - progetto pilota a livello di eduGAIN, la cui tecnologia come il wallet affianca e non soppianta SAML.

- ***Supporto casi d'uso per la ricerca e l'istruzione***

Nella relazione sono specificati i **casi d'uso** riferiti a: **Student Mobility** e **HPC,** e su quest'ultimo si sofferma per apprezzare il fondamentale lavoro svolto sui profili di garanzia, visto l'altissimo livello di requisiti sulla sicurezza e sull'identità richiesti.

- ***Policy e standard***

Riguardo la **policy** e lo **standard** VAGHETTI menziona:

- **Entity Attributes e Category;**
- **REFEDS MFA v1.2;**
- **Profili di garanzia dell'identità digitale della Federazione IDEM;**
- **REFEDS Identity Federation Baseline Expectations.**

Riprende la parola BATTISTA, dando spazio alle domande.

Domande:

RANALDI invita i presenti a suggerire nuovi temi da affrontare nel prossimo CTS, a questo proposito VAGHETTI coglie l'occasione per ricordare la volontà di creare un gruppo di lavoro di implementazione dei profili di garanzia della Federazione IDEM, anche in virtù di richieste di chiarimenti sui profili di garanzia, pervenute da parte di qualche ateneo che lo sta implementando.

BATTISTA, ricollegandosi al quanto anticipato da VAGHETTI, ribadisce l'importanza di un feedback sul piano delle attività 2024, e chiede se tra i presenti ci siano suggerimenti su altri temi di interesse o di maggiore approfondimento o privi di interesse, al fine di mantenere alto il focus delle esigenze della comunità e nell'Assemblea di comprenderne il soddisfacimento.

RANALDI sottolinea ancora una volta, quanto sia importante essere partecipi in questo periodo di grande fermento, in cui i sistemi di identificazione e autenticazione evolvono rapidamente e andranno integrati con la nuova identità digitale europea.

VAGHETTI legge in chat la domanda sui sistemi di Identity Management in Cloud e conferma che molti Enti hanno introdotto sistemi come questo. Molti enti di ricerca e di educazione li hanno adottati, in particolare negli Stati Uniti e in Olanda, mentre in Italia lo stesso fenomeno sta avvenendo con un certo ritardo. Spiega il perché questo tema non sia stato proposto in scaletta: è una strategia su cui GARR ha forti dubbi per la forte cessione di controllo verso soggetti commerciali che comporta ed inoltre l'expertise del servizio è limitato.

RANALDI legge la domanda di **Maria VERINA dell'ICTP** sulla fruibilità dei corsi erogati in passato e ne ricorda la pagina dedicata: https://learning.garr.it/course/index.php?categoryid=33.
Risponde che i corsi disponibili non sono stati registrati per tale scopo, ma riproporli può essere una buona idea, e trasformare quelli esistenti in autoapprendimento era già tra le intenzioni del CTS.

Salvatore TODARO dell'Università degli Studi di Messina chiede al PRESIDENTE di organizzare un incontro con la CRUI, per essere portavoce di situazioni critiche e analoghe a vari Atenei e cita a titolo di esempio il caso del proprio Ateneo di afferenza, i cui servizi sono migrati a Microsoft, scelta forzata dettata dalla pandemia, apportando conseguentemente l'implementazione di policy sulla sicurezza e di contro quanto anticipato da VAGHETTI, in quanto le infrastrutture di sicurezza open source non permettono livelli di retention come quelli garantiti dai prodotti commerciali di Microsoft.

BATTISTA coglie l'occasione per anticipare che con la Prof.ssa Giovanna Iannantuoni, neo Presidente della CRUI, è stato concordato per il prossimo 18 aprile un incontro in CRUI, in coda all'Assemblea della CRUI, insieme al Presidente GARR per un intervento di tipo politico e dedicato al piano strategico delle attività GARR. Nello stesso pomeriggio è previsto un altro incontro con i Delegati dei Rettori e dei Referenti Tecnici che vorranno partecipare. L'idea è di stabilire in maniera più sistematica questo tipo di incontri, con l'obiettivo di fare recepire meglio le esigenze degli Atenei sugli aspetti di rete, sulle nuove infrastrutture di ricerca e sui servizi di connettività che meglio rispondono, a tutti i progetti in corso, come il PNRR, anche dal punto di vista dei servizi che GARR fornisce alla comunità e agli Atenei e, a tal proposito sarà coinvolto il Prof. Cupertino, Referente CRUI del gruppo CTI, per approfondire lo stato d'arte e gli sviluppi che ne conseguiranno.

RANALDI aggiunge che il passaggio di gestore per una gestione centralizzata data a terzi, messo in risalto da TODARO, non è solo un problema di costi, ma anche di complicazione sulle competenze, limitando di fatto l'intervento degli esperti, afferma nuovamente quanto sia necessario aumentare la competenza in IDEM delle applicazioni in open source, per avere una strategia d'uscita.

VAGHETTI aggiunge e conclude affermando che la libertà, i diritti e la preservazione dello spazio pubblico della ricerca e l'educazione non possono passare in secondo piano e, prosegue con la votazione del Coordinatore del CTS, ricordando che le votazioni erano state aperte il giorno prima. Ripete le regole della votazione, citando il nominativo di Andrea RANALDI come unico candidato al ruolo di Coordinatore del CTS IDEM 2024-26, ribadendo che le candidature pervenute per il ruolo a membri del CTS saranno vagliate successivamente dal nuovo Coordinatore del CTS.

Nell'attesa della votazione interviene nuovamente **Salvatore TODARO dell'Università degli Studi di Messina** che suggerisce l'integrazione a largo spettro di HPC con IDEM, eduGAIN, proxi come SATOSA per l'impatto alla migrazione.

Interviene **Marco Pirovano, dell'Università Commerciale Luigi Bocconi di Milano**, consigliando che la passwordless authenticartion consente sempre di passare da shibboleth, e su questo ultimo intervento VAGHETTI concorda per la soluzione fornita e aggiorna i presenti dell'esito della votazione:

4. Risultato votazione e nomina del Coordinatore del Comitato Tecnico Scientifico 2024-2026

su 42 partecipanti, con 41 voti favorevoli ed 1 voto astenuto
Andrea RANALDI viene nominato Coordinatore del CTS IDEM per il biennio 2024-26.

Il Presidente dell'Assemblea IDEM Claudia BATTISTA conclude l'incontro e ringrazia nuovamente RANALDI per la sua disponibilità ed i presenti per i nuovi spunti e l'intera comunità per la preziosa collaborazione.

La riunione termina alle 12.30.