XV Assemblea dei Membri della Federazione IDEM in VC
24/05/2023 dalle 14.30.00 alle 16.30

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 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	Presentazione del documento "Profili di garanzia delle identità digitali della Federazione IDEM" vedi ConsultazioneProfiliDiGaranziaIDEM	Davide Vaghetti (Servizio IDEM GARR AAI)
15:40 16:10	Votazione per approvare il documento "Profili di garanzia delle identità digitali della Federazione IDEM": https://evento.renater.fr/survey/assemblea-dei-membri-della-federazione-idem-votazione-online-k1rfh3bf	
16:10 16:30	Varie ed eventuali e conclusione dei lavori	Claudia Battista (GARR e Presidente Assemblea)

In data 24 maggio 2023, 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 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 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:RelazioneCTS_2023-1.pdf

Prende la parola **Andrea RANALDI** che, in qualità di Coordinatore del CTS IDEM, illustra in dettaglio il risultato dei lavori portati avanti nell'anno dai gruppi di lavoro: Identity Assurance (Profili di garanzia IDEM), IAM proxy OIDC Proxy e Cruscotto IDEM.

Introduce l'**Identity Assurance** come primo gruppo di lavoro (GdL) a cui lui stesso ha partecipato, che ha prodotto di fatto i **Profili di garanzia IDEM**, oggetto di votazione nell'assemblea del giorno, documento essenziale per chiudere i profili. Elogia il grande lavoro svolto e di confronto portato avanti da VAGHETTI a cui è riconoscente in quanto se ne parlava da anni e anticipa che i profili saranno compatibili con buona parte degli standard utilizzati anche da altri enti e gruppi.

Passa al gruppo **OIDC Proxy**, terminato da poco e ne spiega gli obiettivi. Ricorda che la maggior parte delle nuove applicazioni supporta OIDC e meno frequentemente SAML, pertanto l'idea del gruppo è stata quella di fornire uno strumento a tutti i membri IDEM per agganciare in maniera semplice le applicazioni OIDC alle Federazioni SAML, EDUGAIN inclusa. Spiega che si è lavorato per includere IDEM in Satosa-SAML2Spid, il progetto di Giuseppe De Marco incluso in Developers Italia per la creazione di proxy compatiili con SPID, potendo così offrire un doppio risultato, ossia un prodotto mantenuto anche da altri e che potesse offrire varie connessioni. E' stato un buon risultato e comincia ad essere utilizzato - commenta RANALDI e aggiungendo quanto sarebbe auspicabile offrire un sistema pubblico che spinga i produttori di servizio ad agganciarsi alla nostra rete e a far crescere la rete di servizi IDEM.

Riguardo il GdL del **Cruscotto IDEM -** spiega RANALDI, le cui attività non sono ancora concluse, prevede la creazione di un sito in cui dare informazioni strutturate su tutti i servizi raggiungibili tramite IDEM.

Espone un'altra attività portata avanti, quella relativa ai **seminari IDEM** organizzati come occasione di formazione, in cui sono stati affrontati argomenti non semplici e in cui non è sempre stato facile avere persone con cui confrontarsi, visto il rapporto inferiore di specialisti, rispetto alle esigenze di molti. Per tale motivo ci si è orientati sugli argomenti più richiesti, affrontati con una doppia finalità, sia di tipo seminario frontale per presentare la tecnologia, che di confronto su come implementarla. L'iniziativa del webinar ha riscosso molto successo, più di 1400 iscritti in totale e per numero di iscritti per corso:

- **OIDC federation analisi protocollo** (239 iscritti)
- **OIDC federation procedura di Onboarding** (193 iscritti)
- **Identity Assurance** (189 iscritti)
- **OIDC federation Prova su strada** (136 iscritti)
- **MFA** (302 iscritti)
- **Configurazione avanzata Identity Provider** (205 iscritti)
- **IDP resiliente: strategie per rendere più affidabile il sistema** (206 iscritti)

Conferma il proseguiremo di questa attività viste le numerose richieste degli iscritti.

RANALDI ricorda che il CTS scadrà nell'anno in corso e non sono stati fatti progetti a lungo termine per lasciare spazio a nuovi colleghi.
Focalizza l'attenzione su quelli che saranno i due canali principali:

- la Formazione sui temi:
  Identity Provider; Service Provider;
  Nuovi seminari con temi da definire in base alle richieste;
- i Gruppi di Lavoro con gli argomenti:
  analisi e supporto ai processi necessari di garanzia (obiettivo: convertire le prassi, formalizzazione dei processi per affermali pubblicamente verso IDEM);
  Cruscotto (obiettivo: rendere partecipi gli studenti).

RANALDI conclude il suo intervento ricordando che fare parte di un gruppo di lavoro e lavorarci gratuitamente non è tempo sprecato. Il tempo investito per i nuovi traguardi è di ritorno verso sè stessi, verso il proprio Ente e verso la comunità.

Rispondendo ad una domanda in chat si ricorda la pagina dedicata ai **seminari IDEM** (https://learning.garr.it/course/index.php?categoryid=33) che permette l'accesso autenticato sui **seminari IDEM** e la possibilità di richiedere l'attestato di partecipazione. Le date sono volutamente programmate una ogni due settimane, con argomenti già in elenco fino a Pasqua.

3. Relazione del Coordinatore del Servizio IDEM GARR AA

https://wiki.idem.garr.it/wiki/File:Profili_di_garanzia_delle_identita_digitali_della_Federazione_IDEM.pdf

Riprende la parola BATTISTA ed introduce **Davide VAGHETTI** in qualità di Coordinatore del Servizio IDEM GARR AAI, che ringrazia della riconoscenza e di quanto anticipato dal collega RALANDI e conferma che è stato fatto un lavoro collegiale e, per quanto uno possa diventare indispensabile, in realtà non lo è, considerando che per i lavori come questi sono le persone che definiscono le policy, quelle che poi le attuano negli Enti.

VAGHETTI procede con la condivisione della pagina dedicata alla consultazione dei "Profili di garanzia delle identità digitali della Federazione IDEM" e spiega i motivi di adozione di un quadro regolatorio condiviso, sia in termini di accreditamento che di verifica identità, sia di gestione degli account che in termini di robustezza dell'autenticazione.

Per esprimere la garanzia di affidabilità delle identità digitali, VAGHETTI analizza i vantaggi che derivano dall'adozione di un quadro regolatorio condiviso:

- permette ai membri della Federazione IDEM di accedere ai servizi della ricerca che richiedono il supporto dei profili di garanzia dell'identità digitale definiti dal REFEDS Assurance Framework;
- allinea le pratiche di gestione dell'identità digitale dei membri della Federazione IDEM alle norme che regolano l'identità digitale governativa europea e italiana (eIDAS, SPID e CIE) e agli standard internazionali di riferimento (ITU X.1254 e NIST 800-63);
- aumenta il grado di sicurezza e affidabilità dei sistemi di gestione dell'identità digitale dei membri della Federazione IDEM;
- alimenta la diffusione di metodi di autenticazione a più fattori.

Introduce il documento "Profili di garanzia delle identità digitali della Federazione IDEM" (https://wiki.idem.garr.it/w/images/4/42/Profili_di_garanzia_delle_identita_digitali_della_Federazione_IDEM.pdf) composto, nello specifico:

- dalla parte introduttiva, che definisce il documento come un sistema di regole per la verifica e l'asserzione della qualità delle identità digitali all'interno della Federazione IDEM. Le regole compongono i profili di garanzia che rispondono sia ai Service Provider (che devono essere in grado di valutare il grado di affidabilità delle identità ricevute), che agli Identity Provider (che in qualità di gestori di sistemi di autenticazione devono poter fare riferimento alle regole per implementare i processi e i metodi di gestione delle attività), specificando su cosa si basano le componenti che caratterizzano la *garanzia delle identità digitali* in termini di processi di accreditamento, verifica dell'identità, gestione delle credenziali e qualità degli attributi e la *robustezza del processo di autenticazione*;
- dai termini e le definizioni le cui parole chiave devono essere interpretate secondo quanto indicato nella [RFC 2119]:
- dalla sezione "Ambito, Conformità e Verifica", dove sono indicate le regole di adesione e controllo.
- dai requisiti operativi per le organizzazioni della Federazione IDEM che assegnano e gestiscono credenziali, rispettando i requisiti validi per i profili IDEM-P0, IDEM-P1, IDEM-P2 e IDEM-P3;
- dai riferimenti "Allegato A - Rappresentazione dei valori di garanzia dell'identità digitale per la Federazione IDEM"
- "Allegato B - Sintesi dei profili di garanzia dell'identità digitale della Federazione IDEM"

VAGHETTI conclude il suo intervento e dà spazio alle domande.

Domande:

Prende la parola **Marco CONGIA**, dell'Università degli Studi di Roma La Sapienza, spiega quanto a proposito di profili di garanzia, nella sua organizzazione in cui sono presenti sia risorse locali che esterne, sia faticosa l'implementazione associata ad una persona e al processo di

gestione del ciclo di una identità. Ad esempio gli viene chiesto di accedere ad una risorsa di calcolo dall'esterno e a farlo è il dipendente che nel frattempo è andato in quiescenza, o uno studente che prima accede alle risorse da neo iscritto, poi quando laureato non accede più, perchè ha concluso la sua carriera universitaria. CONGIA spiega qual è la policy adottata per gestire tali richieste, ossia l'attivazione dell'account per 6 mesi, la modalità lettura per 12 mesi, la cancellazione dall'account o il passaggio ad altro account e chiede come trattare questi casi tramite profili di garanzia e con quali attributi.

VAGHETTI suggerisce che la soluzione è nella risposta del service provider in base ai valori di assurance che richiede l'Ente, come ad esempio quello di garantire che gli utenti che vi accedono, siano ancora dipendenti a tutti gli effetti. Quello che indichiamo con REFEDS Assurance Framework approfondisce VAGHETTI, è il tempo in cui si aggiorna il valore dell'affiliazione, come potrebbe essere quello del passaggio da docente, a docente emerito o a member staff. Lo stesso vale per gli account degli studenti che continuano ad avere un rapporto di affiliazione con l'Ateneo in quanto ex studenti, o "alum".

Prende la parola **Arnaud CEOL** dell'IRCCS IEO di Milano, che trova coerente l'intervento di Marco CONGIA, sulla scelta di chiudere un account in assenza di affiliazione.

Interviene BATTISTA che è d'accordo con il suggerimento di VAGHETTI di cambiare il grado di affiliazione, marcando l'importanza del legame stesso di affiliazione e del suo cambio di stato, da docente operativo, a docente emerito/associato.

Secondo RANALDI il fatto che il Service Provider richieda il tipo di affiliazione, è più un problema amministrativo che tecnico.

CEOL ritorna sulla questione chiarendo che per loro è un problema tecnico, perchè non essendoci tempistiche veloci, tutto si ripercuote in ambito tecnico. Il lasso di tempo tra l'accessibilità all'account di un utente operativo, a utente emerito, è un disagio temporale per la persona che nel frattempo non vi accede. Di fatto secondo CEOL mancherebbe un attributo che valorizzi questo slot temporale, soprattutto per un fatto di numerosità di identità digitali da gestire.

RANALDI recepisce la questione, anticipa che partiranno dei GdL per adattare quanto prima i processi di lavoro e pubblicarne i profili.

Interviene **Enrico FASANELLI** dell'INFN della Sezione di Lecce, precisando che l'identificativo deve essere associato al profilo e ai dati dell'utente, è una dichiarazione relativa a quanto rapidamente i dati dell'utente sono aggiornati rispetto allo stato giuridico. L'associazione del profilo dipende dai tempi del processo di gestione per l'aggiornamento dell'identità digitale degli utenti dell'Università/Ente.

Sullo stesso argomento prende la parola Raimondo SEPE dell'Università Telematica Internazionale UNINETTUNO, spiegando che la loro segreteria studenti utilizza la procedura automatizzata del CINECA, cioè che lo studente a completamento della carriera universitaria, che solitamente corrisponde con la laurea, riceve una comunicazione per la chiusura del suo l'account con scadenza massima di 30 gg, mediante un meccanismo di *grace period.*

VAGHETTI comprende la questione del de-provisioning, processo obbligatorio alla conclusione del rapporto lavorativo dei docenti/studenti con l'organizzazione, ma specifica che l'argomento di cui si sta parlando è la velocità con cui si aggiornano i valori dei processi di affiliazione, che non riguarda tutto il profilo e che non indica la scadenza entro cui eliminare il profilo.

SEPE considera nello specifico, il caso delle riviste scientifiche e VAGHETTI su questo esempio spiega che i valori di affiliazione si basano sui contratti in essere tra la persona e l'Ente ed in altri casi è l'Ente stesso che ne indica i valori di affiliazione, come per il docente in pensione.

Anche per **Antonio ACCARDO** di IRCCS Burlo Garofolo che, agganciandosi all'argomento, sostiene che non ci sia un meccanismo di mitigazione dell'effetto dei dati aggiornati, tra docente e affiliazione.

BATTISTA conferma che il passaggio da accesso ad accesso privilegiato deve essere disciplinato e che è l'Ateneo a riconoscerne la valenza dell'utente, che ritiene prezioso il contributo del docente, non più docente.

Salvatore TODARO dell'Università degli Studi di Messina prende la parola e cita un esempio pratico di profilazione con l'affiliazione, risolta nel proprio Ateneo tramite l'applicativo CSA (Carriere e Stipendi di Ateneo), con decreto del Consiglio di Dipartimento che ha determinato il ruolo di collaboratore di ricerca a titolo gratuito. Suggerisce questa soluzione come prassi standard del tutto amministrativa, da predisporre semmai con un mese in anticipo, rispetto il pensionamento della persona. Conclude ricordando che in qualità di certificatori di dati altrui, non è possibile decidere, se a monte non vengono formalizzate una serie di figure.

Anche **Massimo DEL SARTO** della Fondazione Stella Maris che si aggiunge all'intervento, è d'accordo che l'affiliazione dell'utente debba essere giustificata da un contratto esterno.

BATTISTA sottolinea quanto sia evidente che in alcune prassi non si è tenuto conto di questioni come quelle citate e che per l'inerzia nell'abituarsi a queste tematiche, ogni Istituzione deve trovare un impatto operativo, che sia il più possibile contenuto, conforme ed in equilibrio con la propria organizzazione interna.

VAGHETTI riporta l'attenzione sulla votazione e informa in tempo reale quali i risultati raggiunti: su n.46 partecipanti, n. 2 astenuti e n.44 votazioni favorevoli convalidano la proposta di modifica.
BATTISTA chiede ai presenti se ci sono altri interventi sul punto, altri ed eventuali.

Chiede di parlare **Giovanni Battista BARONE** dell'Università degli Studi di Napoli Federico II ed informa che nel suo Ateneo sono gli Alumni (ex studenti ed ex docenti) a rappresentare la questione come problema interno.
Su questo aspetto VAGHETTI ricorda che nella Federazione IDEM esistono già le specifiche sugli attributi che ne definiscono le soluzioni.

RANALDI coglie l'occasione per informare i presenti che tale tematica sarà oggetto di webinar, visto l'interesse generale di tutti.
Prende la parola **Maria VERINA** dell'ICTP per chiedere quali sono i casi d'uso dove l'Assurance viene richiesta. VAGHETTI cita:

1. Il sito di sSupercalcolo EuroHPC LUMI, tramite il servizio GEANT MyAccessID (https://wiki.geant.org/display/MyAccessID)
2. La European LifeScience Research Infrastructure (https://lifescience-ri.eu).
3. I servizi del National Institute of Health americano (NIH).

Il Presidente dell'Assemblea IDEM Claudia BATTISTA conclude l'incontro, anticipando gli appuntamenti della CONFERENZA GARR di giugno 2023 e invita i partecipanti alla formazione promossa in occasione della conferenza.

La riunione si chiude nei tempi stabiliti.