XIII Assemblea dei Membri della Federazione IDEM in VC
02/02/2022 dalle 14.30 alle 16.30

Presenti:

Claudia BATTISTA	Presidente Assemblea IDEM
Davide VAGHETTI	Responsabile del Servizio IDEM
Enrico M.V. FASANELLI	Coordinatore CTS biennio 2019-2021 (esteso al 2/2/22)
Laura PIRELLI	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 14:55	Relazione del Coordinatore del Comitato Tecnico Scientifico	Enrico Fasanelli (INFN e Coordinatore del CTS)
14:55 15:10	Relazione del Coordinatore del Servizio IDEM GARR AAI	Davide Vaghetti (Servizio IDEM GARR AAI)
15:10 15:20	Servizi di verifica status studente: InAcademia	
15:20 15:40	Discussione sulle proposte di lavoro per il nuovo CTS	
15:40 16:00	Presentazione delle candidature a Coordinatore del Comitato Tecnico Scientifico 2022-2023	
16:00 16:20	Votazione e nomina del Coordinatore del Comitato Tecnico Scientifico 2022-2023	
16:20 16:30	Conclusione dei lavori.	Claudia Battista (GARR e Presidente Assemblea)

In data 2 febbraio 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 ed Enrico M.V. FASANELLI, Coordinatore del CTS IDEM e a tutti i membri collegati da remoto.

Il Presidente dell'Assemblea fa una breve introduzione sugli argomenti previsti in agenda e sofferma l'attenzione sulla crescita della Federazione a distanza di un anno, citando alcuni dei nuovi membri come le Università Statali e non, tra cui: il Consorzio Interuniversitario Sistemi Integrati per l'Accesso (CISIA), alcuni IRCCS, l'Archivio Centrale dello Stato (ACS) e altri enti della comunità scientifica, accademica e culturale italiana e dei nuovi partner come service provider tra cui: Il Sole 24 ORE, Zanichelli Editore, l'Associazione Italiana dei Comunicatori di Università (AICUN) ed anche la registrazione di molti service provider di membri già federati, a conferma di quanto l'interesse della comunità necessita di identità digitale "trusted" in sicurezza.

Esprime apprezzamento per le significative candidature pervenute da tutta la compagine istituzionale per il rinnovo del CTS, che evidenziano l'importanza della volontà di mettersi in gioco per la comunità, per affrontare insieme temi complessi e di interesse comune dal punto di vista tecnico e di policy.

Cede la parola all'uscente Coordinatore del CTS IDEM Enrico M.V. FASANELLI, ringraziandolo per il ruolo assunto ed il lavoro svolto per la comunità IDEM.

2. Relazione del Coordinatore del Comitato Tecnico Scientifico

https://wiki.idem.garr.it/wiki/File:Relazione_Coordinatore_IDEM-CTS-Assemblea-20220202.pdf

Prende la parola **Enrico M.V. FASANELLI** che accoglie i ringraziamenti e richiama l'attenzione sul compito dell'Assemblea chiamata a rinnovare il Comitato Tecnico Scientifico per il 2022-2023 e relativo Coordinatore, in sostituzione del CTS 2019-2021. Coglie l'occasione per ringraziare tutti i membri del CTS 2019-2021 e a tutte le persone che hanno partecipato nei vari gruppi di lavoro.

Illustra il Piano di Sviluppo distinto per codici di colori, a seconda del lavoro affrontato, concluso e rimasto in sospeso (modelli policy GDPR), manifestando con rammarico quanto le circostanze dovute al periodo pandemico abbiano reso più lungo e difficile il raggiungimento degli obiettivi prefissati, nella serena consapevolezza che il lavoro che lo ha coinvolto insieme a tutti gli operatori dell'ambito information technology per la fornitura di supporto e sevizio ai colleghi è stato particolarmente pesante e impegnativo.
Spiega che la maggior parte dell'attività approvata nella precedente assemblea è stata raggruppata in un unico grande gruppo di lavoro, coordinato da Andrea RANALDI di ISPRA, che ha coperto tutti gli argomenti. FASANELLI passa la parola a RANALDI elogiandolo per come ha gestito il Gruppo di Lavoro.

Andrea RANALDI dà inizio alla sua presentazione, dedicata al macro gruppo di lavoro, dal titolo: Gruppo SPID, CIE, EISAS e Proxy. Chiarisce a chi ha seguito il workshop GARR che rivedrà trattare gli stessi punti, ma per l'assemblea sarebbero stati affrontati con una prospettiva differente.
Spiega il perché ci sia stata la necessità di inglobare in un unico gruppo i precedenti tre gruppi di lavoro, che si concentravano su aree distinte: autenticazione SPID/CIE/EIDAS; Proxy SAML OIDC, Cloud IDM/IAM; Specifiche Tecniche e Documentazione.
I primi due gruppi di lavoro specifica RANALDI, si sono rapidamente accorpati, perché avevano un'ampia area di sovrapposizione di argomenti e di interessi, come ad esempio per implementare un service provider SPID/CIE/EIDAS al 90% è utilizzato un IAM Proxy.
Spiega le ragioni per cui questo gruppo ha funzionato. Il gruppo ha risposto a bisogni specifici in comune per tutti e richiesti dai tanti membri della federazione, come l'esigenza di autenticazione, di account linking, SPID, EIDAS. Questa comune necessità ha generato interesse e quindi partecipazione e confronto tra gli stessi partecipanti, il cui risultato è stato un forte engagement che ha mantenuto il gruppo attivo, anche oltre il tempo di vita naturale del gruppo stesso.

Riassume gli obiettivi del gruppo, così definiti:

- *Produrre un documento di confronto attributi dei vari sistemi di autenticazione: SPID/CIE/EIDAS/IDEM*.

  Tale documento è da considerare come base di ogni sviluppo o implementazione di un sistema di autenticazione con più identity provider, ed è disponibile alla pagina wiki:
  https://wiki.idem.garr.it/w/images/b/b7/Confronto_attributi_SPID_CIE_EIDAS.ods

- *Produrre un documento di riferimento come linee guida sui sistemi SSO per la PA; implementazione di proxy, IDP, SP nei vari sistemi di autenticazione.*

  Le schede relative ai sistemi di autenticazione raccolgono e riassumono i dati emersi dal confronto di vari sistemi di implementazione tra membri. Ciò ha permesso di affrontare gli stessi problemi risolti in differenti modi e di conoscere le soluzi
  oni applicate dai vari membri, fornendo spunti di riflessione per migliorare i propri sistemi. Tali schede identificano i punti forti e le debolezze di ogni sistema implementato facilitando la scelta di chi deve implementare un nuovo sistema, lasciandogli traccia di chi lo ha già fatto. Le schede sono disponibili nella pagina wiki del gruppo di lavoro:
  https://wiki.idem.garr.it/wiki/Gruppo_di_Lavoro_SPID-CIE-eIDAS-Proxy#Sistemi_di_autenticazione_presentati

RANALDI continua l'intervento soffermandosi sul *confronto SPID/SAML*, ricordando che SPID si basa su SAML ma non segue tutte le sue regole. Informa che è stata fatta un'analisi dettagliata sul confronto tra i due standard, basata sulle regole tecniche che hanno generato la differenziazione, di fatto determinate dallo scostamento tra le regole e la prassi.
Prosegue con la *Mini guida all'account linking,* commenta quanto sia ostico il collegamento degli account e motiva lo scopo della guida, pensata per semplificare chi vuole utilizzare SPID e gli altri sistemi di autenticazione interna dei propri sistemi come l'IDEM.
La pagina dedicata a questo argomento è disponibile sul wiki:
https://wiki.idem.garr.it/w/images/e/ef/MiniguidaAccountLinking.pdf

Riguardo ai temi aperti e le discussioni affrontate chiarisce che, non tutti gli argomenti esaminati hanno portato la stesura di un documento. Numerosi argomenti sono stati discussi ma non hanno avuto un ritorno sul pubblico, rimanendo come appunti per i futuri lavori.
La pagina dedicata a questo argomento è disponibile in un documento condiviso:
https://docs.google.com/document/d/1JlwgueklluiwFQ25bh0S47_M3F6AYdGcXgXt-19_XH8g

RANALDI ribalta il punto di vista esposto al Workshop GARR che era dedicato al risultato che hanno ricevuto i partecipanti dal gruppo e riporta in Assemblea quanto di riflesso il gruppo ha riportato nei propri enti di origine, migliorando i sistemi di autenticazione del proprio ente.
Sottolinea quanto l'importanza di partecipare ad un gruppo, non sia limitata al solo lavoro che si fa per IDEM o per GARR, è un investimento che dà risultati perché offre dei momenti di crescita e di confronto che è difficile avere nelle realtà di importanti dimensioni come nei nostri Istituti e i nostri Atenei. Nel suo caso lo ha aiutato a ridurre di un terzo i tempi di implementazione SPID.
In conclusione ed in riferimento alle proposte per il futuro, RANALDI ritorna sugli argomenti rimasti in sospeso e che ha rappresentato, distinguendole in due categorie:

- Funzionali: i cui argomenti sono necessari al corretto funzionamento di IDEM (immagine satosa, Identity assurance, specifiche tecniche e documentazione);

- Formative/implementative: i cui argomenti sono necessari ai membri IDEM, ricordando che SPID non è un argomento specifico di IDEM che non autentica su SPID, ma che i suoi membri che ne fanno parte ne usano parlare (OIDC applicato alle identità digitali: IDEM, SPID, CIE e EIDAS; Identità wallet: identità europea; Sistema di gestione deleghe nazionale), (Gestione segreti: token, credenziali, cloud; GDPR).

Presentazione pubblicata sul wiki della Federazione alla pagina:
https://wiki.idem.garr.it/wiki/File:Report_GdL_SPID_et_all_Assemblea-20220202.pdf

Termina RANALDI il suo intervento ringraziando tutti i componenti del gruppo di lavoro e passa la parola a Davide VAGHETTI.

3. Relazione del Coordinatore del Servizio IDEM GARR AAI

https://wiki.idem.garr.it/wiki/File:Relazione_Servizio_IDEM-Assemblea-20220202.pdf

Prende la parola **Davide VAGHETTI** e ringrazia RANALDI per il suo intervento e si presenta ai membri dell'Assemblea in qualità di Coordinatore del Servizio IDEM GARR AAI.
Nella sua presentazione illustra lo stato attuale della Federazione dal punto di vista numerico, rappresentato in 129 Identity Provider e 120 Service Provider ed un saldo netto sempre in crescita nonostante la continua attività tra le nuove registrazioni di IdP e SP e le dismissioni di vecchi provider. Elenca i nuovi ingressi in Federazione dei nuovi Membri e Partner IDEM 2021-22, così come già anticipati dal Presidente dell'Assemblea IDEM, esprimendo apprezzamento per i nuovi membri appartenenti a categorie importanti tra cui anche alcune università che erano rimaste ancora fuori lista.
Commenta quanto sia positivo il confronto della copertura IDEM tra la fine del 2021 e gli anni precedenti, ben l'89% della popolazione studentesca degli Atenei italiani statali. Positivo anche il confronto tra gli atenei statali e non, la cui copertura IDEM della popolazione studentesca in generale è maggiore e anche riguardo l'adesione degli Atenei più piccoli, il cui investimento è più grande per disposizioni di risorse più limitate.

Relativamente allo stato della Federazione in *eduGAIN,* da cui provengono la maggior parte delle risorse in termini di SP come le risorse editoriali, VAGHETTI spiega che per cambio di politica di default, dove possibile, si è evitata la registrazione delle risorse in Federazione IDEM, importando direttamente i metadata da eduGAIN perché pubblicati in altre Federazioni, in particolare nelle due Federazioni di riferimento per le risorse editoriali Stati Uniti e Inghilterra, in cui si trovano la maggior parte degli editori del settore accademico.
I numeri di eduGAIN sono ragguardevoli e se confrontati ad oggi, con l'Assemblea dello scorso febbraio 2021, osserviamo una notevole crescita di entità (+11.6% ossia un migliaio di entità in più) , IdP (+ 12.6%) e sugli SP (+10.4%).
In merito alle attività del Servizio IDEM GARR AAI, VAGHETTI comunica che negli ultimi tempi il lavoro ha riguardato la configurazione delle risorse editoriali, in quanto ci si è accorti che in presenza di sottoscrizioni attive per l'accesso alle riviste scientifiche, molti membri trovano difficoltà nell'attivare l'accesso federato. Ancora di più per una serie di soggetti dell'area biomedica che fino a poco tempo fa utilizzavano il sistema Bibliosan, servizio adesso dismesso.
La pagina wiki dedicata alla *attivazione accesso risorse editoriali* è disponibile sul wiki della Federazione: https://wiki.idem.garr.it/wiki/Configurazioni_Risorse_editoriali

Un'altra attività di cui si è occupato il Servizio IDEM spiega VAGHETTI, è l'implementazione dell'European Student Identifier (ESI), necessario per accedere ai servizi relativi all'Erasmus Plus all'interno della European Student Card Initiative, specificando che in questo contesto GEANT ha messo a disposizione un servizio di accesso chiamato MyAcademicID, che altro non è un proxy che permette a tutti i membri di eduGAIN di accedere a queste risorse e, uno degli attributi più importanti che devono essere rilasciati per l'accesso a queste risorse è appunto lo European Student Initiative.
La guida del Servizio è disponibile sul wiki della Federazione: https://wiki.idem.garr.it/wiki/Erasmus_Plus_e_ESI

Altra attività che ha coinvolto il Servizio IDEM a partire dall'estate 2021, è stata l'implementazione di un servizio di distribuzione di metadata dinamico, che implementa il protocollo MDQ, allo scopo di migliorare il consumo di risorse e i tempi di avvio. Il lavoro è stato presentato in occasione del Workshop GARR 2021, attualmente è in fase di affinamento ed il lancio ufficiale è previsto alla fine del mese in corso, per cui è in programma anche dell'attività di training.

Un altro progetto che il Servizio IDEM intende portare avanti è lo *standard F-Ticks* relativo alle statistiche, tramite il quale è possibile trasmettere dati statistici di IdP mantenendo il completo anonimato, ad un servizio centralizzato che raccoglie le statistiche e le elabora all'interno di una architettura ELK, mettendoli a disposizione tramite una interfaccia pubblica per la consultazione di tutti gli operatori, allo scopo di analizzare quali siano i servizi più utilizzati all'interno dell'ente, oltre che all'esterno ed utili a prendere decisioni strategiche sull'utilizzo del servizio stesso. Tutto ciò contribuendo al al progetto eduGAIN F-Ticks che raccoglie le statistiche di autenticazione di tutte le Federazioni di identità per una visione globale dell'autenticazione federata nell'ambito della ricerca e dell'educazione.
VAGHETTI conclude l'argomento dicendo che GARR tramite il proprio servizio IdP in the cloud partecipa già alla raccolta degli F-Ticks per eduGAIN, i cui dati permettono di capire come sono utilizzati i sistemi.

Prima di introdurre la presentazione sul servizio InAcademia di GEANT, VAGHETTI rievoca l'incidente che ha riguardato SheerID. Spiega che il Servizio IDEM insieme a eduGAIN Security Team ed il GARR CERT ha seguito tutti passi di questo incidente, in quanto il GARR è service owner di eduGAIN. Nel dettaglio riassume che cos'è SheerID. Spiega che è un SP pubblicato dalla federazione inglese, esportato in eduGAIN ed importato da tutti i partecipanti di eduGAIN. Il 14 aprile 2021 un partecipante di IDEM ha scoperto che SheerID aveva messo in piedi un sistema che non reindirizzava l'autenticazione all'identity provider del nostro partecipante, ma utilizzava una pagina di login artefatta, da cui prendere il nome utente e la password per l'invio al servizio di autenticazione. VAGHETTI motiva il perché era stata adottata questa soluzione catch-all con la possibilità di un doppio utilizzo, sia per le Università in particolare federate, che quelle non federate che però esponessero un qualsiasi servizio di autenticazione. Spiega che questa unica soluzione implementava il servizio di controllo dell'afferenza degli studenti che volevano consumare il servizio SheerID, che essendo un servizio di verifica dello status dello studente, permetteva loro l'accesso a scontistiche su una serie di prodotti e servizi commerciali.
EduGAIN si è mossa chiedendo a SheerID, e prima ancora lo aveva fatto il Servizio IDEM, di far cessare questo servizio, chiedendo la garanzia che nessuna credenziale fosse stata condivisa con terze parti. SheerID all'inizio è stata reticente perché non voleva riconoscere la natura dell'incidente di sicurezza, ma poi ha fornito tutti i dati che ci hanno permesso di verificare che si trattava di un incidente tutto sommato triviale, ma di dimensioni gigantesche, perché 37 erano le nazioni coinvolte e 427 le organizzazioni.

Perché quindi in InAcademia chiarisce VAGHETTI nell'ultima parte del suo intervento. Spiega che è un servizio di GEANT che si frappone agli *Student verification services* offerti da varie entità, tra cui appunto appunto SheerID, che offrono accesso agli sconti per gli studenti generando una serie di dubbi sulla privacy e la trasparenza, visto che oggettivamente il fine di ogni accesso, è monetizzare il servizio. Da un'analisi statistica questi servizi sono ampiamente utilizzati in IDEM.

VAGHETTI spiega brevemente perchè i metadata vengono importati da eduGAIN esattamente così come sono. L'importazione dell'entità di eduGAIN avviene tramite una serie di passaggi attuati dal Servizio IDEM, tra cui l'attività di filtraggio blacklist per le entità già registrate in IDEM e quelle con problemi noti o segnalate, allo scopo di unire i metadata con quelli di IDEM per pubblicarli nello stream di eduGAIN IDEM. Il problema con questo approccio è dovuto alla modalità con cui vengono rilasciati gli attributi. Il Servizio IDEM fornisce anche una serie di filtri standard per rilasciare questi attributi che si avvalgono di regole che sono ritagliate o su uno specifico servizio nella minoranza dei casi o su determinati entity categories tramite tag che identificano il tipo di risorsa, permettendo filtri dinamici, le cui due particolari categories utilizzate sono: Research and Scholarship e il GEANT Data Protection Code of Conduct.
Chiarisce VAGHETTI che alcuni di questi servizi di verifica sullo status dello studente, a seconda del percorso di registrazione avvenuto all'interno della Federazione, in cui per la prima volta sono stati registrati prima ancora di essere pubblicati su eduGAIN, si possono qualificare per uno di questi tag, tra cui SheerID. Questo pone una serie di problemi, motivo per il quale dopo l'incidente che ha riguardato SheerID, con il CTS IDEM si è deciso di filtrarlo. SheerID non fa più parte della federazione IDEM in alcun modo, in quanto non viene più importata da eduGAIN, Si è pensato di avere lo stesso approccio anche con gli altri Student verification services.
InAcademia di GEANT, in cui c'è anche il contributo del Servizio IDEM nella parte di gestione, è un servizio di verifica sullo status dello studente che, in parte monetizza per ogni verifica studentesca tutta l'architettura di identificazione federata, perché fa pagare a chi lo vuole utilizzare come in questo caso i vari SheerID di turno, un prezzo minimo rispetto a quello che in realtà fanno pagare questi servizi ai loro clienti, allo scopo di sostenere la stessa InAcademia. Il servizio in sé è realizzato con un semplice proxy che espone una interfaccia OpenID Connect ai servizi di verifica dello status di studente come SheerID e Student Beans. Invece nei confronti delle Federazioni espone un'interfaccia SAML, garantendo che gli attributi richiesti siano solo ed unicamente quelli necessari, ma esponendo molte meno informazioni di quelle che noi manderemmo con gli attributi stessi. Nel senso che nel momento in cui ad esempio un Identity Provider autentica uno studente, rilascia a InAcademia l'affiliazione ad es. student@unimi per citare un nostro Identity Provider.
Il servizio InAcademia invece dà una sola risposta al service provider che ha fatto la richiesta, magari per concedere lo sconto a Spotify o acquistare un computer con la scontistica studenti, completamente privacy preserving, dato che indica solo se la persona è uno studente o meno, senza informazioni che identifichino l'affiliazione o l'IdP con cui ci si è autenticati. Da questo punto di vista per IDEM e GARR il servizio InAcademia è strategico in quanto offre affidabilità e trasparenza ai suoi membri. Il GARR è entrato a far parte della governance di InAcademia e partecipa a tutte le decisioni relative allo sviluppo del servizio stesso.

Con questo ultimo argomento VAGHETTI conclude il suo intervento.

Riprende la parola RANALDI Andrea di ISPRA che avendo coordinato il Gruppo di Lavoro IDEM GARR 2019-2021, introduce le proposte di lavoro per il nuovo CTS 2022-23 con un'altra presentazione. Il nuovo intervento ripropone le proposte pensate per il futuro, distinte in Funzionali e Formative/implementative e continua dettagliando nella slide le problematiche di ogni argomento e le relative soluzione adattabili, riguardo a:
- *IAM Proxy OIDC/SAML,*
- *Identity assurance,*
- *Specifiche tecniche e documentazione,*
- *OIDC applicato alle identità digitali, Identity wallet, Sistema di gestione deleghe nazionale*
- *Gestione segreti*.

Presentazione disponibile alla pagina:
https://wiki.idem.garr.it/wiki/File:Relazione_Servizio_IDEM-Assemblea-20220202.pdf

RANALDI conclude il suo intervento e dedica spazio alle domande.

Domande:

Interviene **Salvatore TODARO** dell'Università degli Studi di Messina e membro del CTS di IDEM apprezzando il Gruppo di Lavoro gestito da RANALDI e gli argomenti proposti per il futuro, in quanto stimolanti. Propone di aggiungere due argomenti in più:

- la disseminazione verso la popolazione studentesca informando che l'account IDEM darebbe accesso anche agli sconti, come InAcademia, valorizzando di riflesso anche il lavoro che c'è dietro. Suggerisce come divulgazione un canale di comunicazione e pillole informative di cinque/dieci minuti per il management delle proprie Istituzioni, magari da rendere visibili anche sul sito IDEM, in cui lo studente è informato che il proprio accesso non né limitato al proprio Ateneo di afferenza, ma a N entità sparse nel mondo e qualcuna utile per la propria formazione, come ad es. un abbonamento; cita le Linee Guida per la PA che definiscono l'utente al centro;
- l'integrazione dei nostri IdP con soluzioni commerciali di Identity Management, ed in particolare alle implementazioni di Multi Factor Authentication (MFA).

VAGHETTI concorda sull'importanza della disseminazione suggerita da TODARO e per poterlo fare a livello strategico e per coinvolgere tanti professionisti della comunicazione presenti all'interno dei nostri enti, suggerisce un intervento fuori dal proprio ambito.

Riprende la parola TODARO citando la CRUI a titolo di esempio che ha una convezione attiva con Microsoft. Spiega che Microsoft mette a disposizione una console di security che permette di vedere in tempo reale l'attvità in corso e di fare delle azioni proattive sulle identità presenti (ad es. in caso di furto di identità).
VAGHETTI ricorda che va sempre tenuto presente lo spirito che coinvolge la federazione in questo ambito e ricorda quali siano i valori finora condivisi: gli standard aperti, il software aperto, per evitare in tutti i modi il vendor lock-in e la creazione di ecosistemi chiusi.

E' semmai importante fornire delle linee guida che permettano di prevenire gli aspetti più nefasti dell'integrazione, specifica VAGHETTI.
TODARO è d'accordo ma ribadisce che non è possibile negarne l'esistenza.
Anche RANALDI si unisce all'argomento confermando la presenza di tanti servizi di identità commerciali.

VAGHETTI legge la domanda in chat di **Nunzio NAPOLITANO** dell'Università degli Studi di Napoli Parthenope che, ricordando d'essere una federazione di Università ed Enti di Ricerca, propone di collaborare con OIDC Federation per contribuire al miglioramento di tale protocollo, piuttosto che implementare tutta una serie di proxy per bypassare quella che è la mancanza attuale di OIDC.
Per VAGHETTI quanto proposto da NAPOLITANO non risolve il problema, per mancanza di uno standard di federazione per OIDC, che permetterebbe la terza parte fidata, federazioni multilaterali, peer to peer. Chiarisce che, seppur uno standard esiste ed è un draft, il problema principale è la mancanza di implementazioni di tutti i tool che servono a gestire una federazione di OIDC, anche se su questo esiste del lavoro molto valido e si sta facendo, ma l'altro vero grosso problema è lo stesso che si ha quando si vuole federare una cosa come ad esempio Jira o vari prodotti di Enterprise in ambito SAML, cioè non supportano nessuno di questi, non esiste ad oggi un relying party o un IdP OIDC che supporti OIDC Federation. Da questo punto di vista il problema reale e principale è questo. Ci potranno essere evoluzioni ma non sicuramente a breve termine. Quindi i proxy ora sono l'unico modo per utilizzare in ambito federato un relying party OIDC.

Interviene FASANELLI condividendo quanto espresso da VAGHETTI ed aggiunge che sarebbe difficile aspettarsi che grossi provider o grosse case produttrici di software, inizino a spendere tempo/uomo per lo sviluppo dei propri connettori OIDC Federation prima che lo standard diventi draft utilizzabile. Anche se così fosse - aggiunge VAGHETTI, se l'estensione di shibboleth come IdP supportasse lo standard OIDC Federation, cosa difficile visti i grossi dubbi sull'attuale standard, il problema rimarrebbe. Cita come esempio il servizio edumeet federato come GARR grazie ai colleghi di INFRA, in SAML su un proxy satosa, che essendo un service provider OIDC, non interagisce con OpenID Connect Federation. Ribadisce che se ci fossero gli standard avremmo comunque bisogno di un proxy che da un lato è in grado di parlare con OpenID Connect Federation e dall'altro con OpenID Connect Vanilla. I proxy nelle fasi iniziali ma anche nelle fasi mature sono inevitabili in questo tipo di tecnologie, per anni infatti uno scenario simile si è avuto anche con il protocollo SMTP. RANALDI aggiunge come informazione che OIDC in Python punta sulla gestione delle federazioni, però è una libreria su un linguaggio. Ci vuole il tempo operativo di sviluppo, di verifica per capire se il processo di federazione sarà questo o arriverà nel tempo. SPID potrebbe essere uno dei capostipiti perchè nell'implementazione SPID di ogni OIDC, dovrà connettersi a dei servizi esterni e su questo si ci sta lavorando.

Chiede la parola **Giuseppe DE MARCO** dell'Università della Calabria condividendo pienamente il ruolo dei proxy che assolvono alle funzioni di interoperabilità, specie quando si ha a che fare con una federazione multilaterale, con molte tecnologie e tante organizzazioni per cui risulta difficile poi decidere quale debba essere la data "x" oltre la quale tutti dovranno avanzare tecnologicamente su un protocollo, su una specifica o altro. DE MARCO sostiene che i proxy sono necessari e che a livello di federazione si collocano su due livelli differenti: OIDC Federation e OICD Core. Specifica che OIDC Core definisce come le autorizzazioni vengano rilasciate ed integrate al di sopra di OIDC Core con ulteriori standard di specifiche draft. Chiarisce che sono tanti gli aspetti di OIDC che sono ancora draft, cita a titolo di esempio il profilo IGov che è draft da tanti anni, ma che è abbastanza robusto da poter essere considerato di normale pratica. Precisa che OIDC Federation è un draft ed è un cantiere aperto che delinea gli aspetti alla base e quelli stabili che non muteranno, puntualizzando che altri aspetti riceveranno sicuramente altre migliorie. Si domanda dove si collocano OIDC Federation e OIDC Core e su come la fiducia viene stabilita da entrambe le parti, ricordando che di fatto è quello che è stato fatto in SAML2 con lo scambio dei metadata. Rammenta che i metadata possono essere scambiati in diversi

modi, come per assurdo e a titolo di esempio, con l'invio di una email o con la pubblicazione di un indirizzo e che questo è il mezzo sul quale si ripone una delle condizioni di sicurezza che consente di stabilire la fiducia tra le parti tramite metadata e quindi riconoscere le entità come partecipanti membri afferenti ad un'unica federazione. Tutto questo tecnicamente per ribadire - secondo DE MARCO che, non è necessario che i vendor debbano supportare di default OIDC Federation, in quanto sono due layer che funzionano diversamente. Specifica che di certo per attivare le operazioni alla base del funzionamento di OIDC, se si utilizzasse OIDC Federation, sarebbe necessario che questo layer venisse attivato prima o intercettasse le chiamate, tale poi da conservare il metadata finale del richiedente o del destinatario. DE MARCO specifica che OIDC Federation è uno strumento per l'interscambio di questi metadata e suggerisce di non agire nel core delle applicazioni. Anche per shibboleth esorta a lasciarlo così com'è, considerando che shibboleth per riconoscere un relying partner ha bisogno dei suoi metadata e che ad ogni middleware attiverà automatic client registration di OIDC Federation configurerà quei metadata che shibboleth si aspetta.
VAGHETTI ringrazia DE MARCO per l'intervento e conferma che saranno argomenti trattati dal GdL a cui spera possa partecipare. RANALDI anticipa a DE MARCO che sarà lui a seguire nel gruppo questi argomenti.

FASANELLI chiede al Presidente dell'Assemblea e alla Segreteria IDEM GARR se, in mancanza di altri argomenti, sia possibile passare alle fasi successive dell'Assemblea.

BATTISTA aggiunge che le proposte di lavoro avanzate risultano essere un buon punto di partenza per il Gruppo di Lavoro che sarà costituito e che nulla vieta l'integrazione di altri temi di interesse della comunità. FASANELLI coglie l'occasione per ricordare ai presenti lo scopo dell'Assemblea invitando a seguire l'iter, secondo cui scelto il nuovo Coordinatore del CTS (selezionato tra le candidature pervenute alla Segreteria IDEM e votato dalla presente Assemblea), con il Responsabile del Servizio IDEM avrebbero in seguito valutato le candidature a membro per costituire il nuovo CTS 2022-23 e per l'appunto definire il lavoro per il prossimo anno. Ricorda che non sarebbe stato deciso tutto durante l'Assemblea, perché ci sarebbe stata una prossima assemblea di veloce riscontro per ratificare il lavoro con l'ausilio dei vari gruppi di lavoro, utile per l'approfondimento, la rivalutazione degli argomenti e la sequenza temporale di sviluppo dei vari argomenti.

Si procede alla votazione del nuovo Coordinatore del CTS IDEM sulla piattaforma ad accesso federato Evento|RENATER. Nella lista a Coordinatore per il nuovo CTS 2022-23 è presente un unico candidato: Andrea RANALDI di ISPRA, già presentatosi all'Assemblea per avere coordinato il GdL su SPID, CIE, EISAS e Proxy e proposto argomenti di lavoro per il futuro.

FASANELLI menziona le regole per la votazione riservata ai ROM o in assenza ai RTM/altro delegato. A tal proposito Laura PIRELLI della segreteria IDEM rassicura Alessandro BRUNENGO circa il suo diritto al voto per delega ricevuta.

A votazione conclusa Andrea RANALDI è nominato a Coordinatore per il nuovo CTS 2022-23 con 41 voti favorevoli su 41 votazioni, 0 astenuti e 0 contrari.

Seguono i complimenti al neo Coordinatore del CTS da parte del Presidente dell'Assemblea, del Coordinatore uscente del Comitato Tecnico Scientifico, del Coordinatore del Servizio IDEM GARR AAI ed i presenti.

Il Presidente dell'Assemblea IDEM Claudia Battista conclude l'incontro con l'impegno di continuare a considerare l'utente al centro e di favorire gli aspetti della comunicazione di livello piuttosto tecnico rendendola più comprensibile, in quanto non sempre condivisibile, se non da chi è principalmente coinvolto nella gestione e nello sviluppo delle implementazioni.
Reputa importante divulgare queste tematiche in senso più ampio che nella quotidianità coinvolgono studenti, docenti, ricercatori e altri utenti interessati e sempre più vicini ad un futuro di digitalizzazione massiva.
Ringrazia i colleghi del Servizio IDEM e della Segreteria IDEM per il lavoro in ombra che mantiene attivo l'operatività della Federazione nazionale e di riflesso internazionale, i membri ed i Coordinatori dei gruppi di lavoro per tutti i contributi dati e l'interesse mostrato per la federazione.

La riunione si chiude nei tempi stabiliti.