XI Assemblea dei Membri della Federazione IDEM - 11 Marzo 2020

Presenti:

BATTISTA Claudia	Presidente Assemblea IDEM
VAGHETTI Davide	Responsabile del Servizio IDEM
FASANELLI Enrico M.V.	Coordinatore CTS
PIRELLI Laura	verbalizzante Segreteria IDEM GARR

Ordine del Giorno:

- Stato Avanzamento Lavori dei Gruppi di Lavoro
- MFA (Autenticazione Multi Fattore)
- OIDC (Protocollo OpenID Connect)
- Identity Assurance

In data 11 marzo 2020 si tiene la prima Assemblea della Federazione IDEM in video conferenza. Il Presidente dell'Assemblea IDEM dà il benvenuto ad Enrico M.V. FASANELLI, Coordinatore del CTS IDEM, Davide VAGHETTI, Responsabile del Servizio IDEM e a tutti i membri collegati da remoto e dà inizio alle presentazioni.

1. Relazione del Coordinatore del Comitato Tecnico Scientifico

https://wiki.idem.garr.it/w/images/b/bf/20200311-XI-assemblea-idem-cts.pdf

Enrico FASANELLI presenta gli organi della Federazione in vigore dal nuovo regolamento approvato a giugno 2019 che sono l'Assemblea dei Membri e il Comitato Tecnico-Scientifico (CTS). Ricorda chi sono i componenti del CTS 2019-2021:

FASANELLI Enrico M. V. (Coordinatore)	INFN – Lecce
ALBRIZIO Daniele	Università di Trieste
CANFORA Marco	IRCCS IFO – Roma
CICLOSI Francesco	Università di Macerata
COMMIS Enrico	Università di Catania
DE MARCO Giuseppe	Università della Calabria
FESTI Maurizio	Università di Trento
MANFREDDA Stefano	Università di Cagliari
MARTUSCIELLO Loredana	IIT CNR Pisa
MONDUCCI Antonella	INFN - Bologna
ROSSINI Angelo	CINECA
TODARO Salvatore	Università di Messina
VAGHETTI Davide	Servizio IDEM GARR AAI

Nella presentazione ricorda gli appuntamenti annuali: almeno 3 riunioni l'anno; le modalità di confronto: in video conferenze e votazioni on-line; il Piano di sviluppo 2020 ed il fondamentale supporto dei Gruppi di Lavoro designati per il compimento delle attività in essere.
Tra gli obiettivi del Piano di sviluppo 2020, evidenzia i seguenti:

- Identity Assurance
- Multi Factor Authentication
- Open ID Connect
- eIDAS
- SPiD
- Modelli GDPR

e illustra i Gruppi di Lavoro attivati:

- **Identity Assurance**
  coordinato da Davide Vaghetti (Servizio IDEM GARR AAI) ed Enrico Fasanelli (INFN e Coordinatore del CTS);
- **Multi Factor Authentication**
  coordinato da Salvatore Todaro (Università di Messina) ed Daniele Albrizio (Università di Trieste);
- **Open ID Connect**
  coordinato da Giuseppe De Marco (Università della Calabria) e Maurizio Festi (Università di Trento).

Infine, in considerazione del sempre maggior ricorso al lavoro agile determinato dalla grave emergenza dovuta al virus COVID-19, FASANELLI annuncia che il CTS si rende disponibile per dare supporto nella configurazione del Single Sign On per gli strumenti di collaborazione dei provider Microsoft (Teams) e Google (Meet).

2. Gruppo di Lavoro Identity Assurance

https://wiki.idem.garr.it/w/images/e/ec/20200311-XI-assemblea-idem-assurance-wg.pdf

Davide VAGHETTI presenta i componenti del gruppo di lavoro Identity Assurance:

MONDUCCI Antonella	INFN - Bologna
MARTUSCIELLO Loredana	CNR – IIT
CANFORA Marco	IRCCS IFO - Roma
CICLOSI Francesco	Università di Macerata
COMMIS Enrico	Università di Catania
FASANELLI M. V. Enrico	INFN – Lecce
MANFREDDA Stefano	Università di Cagliari
VAGHETTI Davide	GARR

Lo scopo del gruppo di lavoro è creare profili di Identity Assurance per stabilire il grado di affidabilità delle identità digitali per la rete della ricerca italiana.

VAGHETTI informa che il gruppo sta lavorando a tre profili: base, intermedio e forte, quest'ultimo dovrà corrispondere al primo livello SPID.
Chiarisce quale sarebbe il vantaggio per la Federazione IDEM si riuscisse a creare, a diffondere e ad applicare un profilo di identity assurance che si mappi con il Livello1 di SPID, cioè quello che porterebbe a diventare, quale step successivo, Registration Authority. Ciò permetterebbe che tutti quegli enti che sono in grado di garantire un livello alto di assurance, potrebbero utilizzare le identità elettroniche erogate dal proprio ente per registrare direttamente presso un IdP SPID.

Domande relative al Gruppo di Lavoro Identity Assurance:
DE MARCO Giuseppe *chiede se si prevede all'interno della Federazione IDEM di valorizzare l'attributo eduPersonAssurance.*
VAGHETTI conferma che è prevista la valorizzazione dell'attributo eduPersonAssurance, come previsto nel REFEDS Assurance Framework che sta alla base del lavoro del gruppo e come citato nelle slides di backup che fondamentalmente presentano i valori che l'attributo di personal Assurance Framework dovrebbe avere in relazione ai i vari aspetti dell'identità: IDENTIFIERS (identificatori), ID PROOFING (verifica identità), ATTRIBUTES (attributi), mentre l'AUTHENTICATION rimane separato.
In generale, per essere compatibili, eduPersonAssurance va valorizzato come indicato nel REFEDS Assurance Framework, sebbene, di per sé, valorizzare non vuol dire niente se dietro non c'è un profilo di assurance riconosciuto all'interno della Federazione.

3. Gruppi di lavoro Multi Factor Authentication

https://wiki.idem.garr.it/w/images/b/b0/20200311-XI-assemblea-idem-mfa-wg.pdf

Daniele ALBRIZIO sostituisce nella presentazione Salvatore TODARO e al suo posto presenta i componenti del Gruppo di lavoro Multi Factor Authentication (MFA):

TODARO Salvatore (Coordinatore)	Università di Messina
ALBRIZIO Daniele (Coordinatore)	Università di Trieste
FESTI Maurizio	Università di Trento
PIROVANO Marco	Università Bocconi
MALAVOLTI Marco (revisore)	GARR
DE MARCO Giuseppe (osservatore)	Università della Calabria

Il gruppo è impegnato a studiare il sistema di autenticazione multifattoriale che aumenterebbe la sicurezza degli accounts, delle risorse IT e di conseguenza di tutta la Federazione IDEM e la cui tipologia di autenticazione è parametro richiesto nel tool AGID di Cyber Risk Management.

Il gruppo di lavoro è volutamente suddiviso in due sottogruppi perché impegnati nelle Attività da "cacciavite" (come la realizzazione dei PoC con soluzioni MFA per Identity Provider e tramite Shibboleth, SimpleSAMLphp, ADFS, ...) e nelle Attività di Analisi e Progetto (come l'analisi comparativa soluzioni MFA per IDP e la produzione di strumenti di valutazione degli stessi parametrizzabile e riutilizzabile dai membri).

ALBRIZIO specifica qual è attualmente l'Architettura IDP – MFA chiarendone le questioni Progettuali e di Analisi (tecnologiche) se utilizzabile solo per le Web Application / Mobile e considerando se non sia meglio vagliare anche soluzioni infrastrutturali per dare accesso MFA a tutti i servizi/applicazioni/piattaforme.

Nella presentazione definisce che può esistere un secondo fattore univoco per tutte le risorse IT di un Ente, siano esse on premise o su cloud. Allo scopo di valutarne benefici e controindicazioni, comunica i primi dati emersi del sottogruppo dedicato allo studio delle Soluzioni MFA – Infrastruttura sul primo confronto per: la Tipologia di secondo fattore tra OTP Software: Smartphone e OTP Hardware: Token (USB); analisi di costi ed impatto economico/organizzativo.

Domande relative a Gruppi di Lavoro Multi Factor Authentication:

CEOL Arnaud Gerard Michel *chiede informazioni su google authenticator TOTP*
ALBRIZIO la definisce come una one time password basata su una secret e sul tempo; in vari ambiti informatici è stata considerata meno sicura, comunque più prona ad attacchi man-in-the-middle .
Esiste un one time password generator simile a google authenticator integrato con FreeIPA e distribuibile sui cellulari.

GRANDI Claudio *chiede se è possibile usare contemporaneamente il sistema hardware e software. Si aspetta sia che il software abbia costi più bassi e che esistano casi individuali in cui non tutti hanno uno smartphone.*
ALBRIZIO risponde che uno dei risultati che è venuto fuori da questo GdL è che non si parla di secondo fattore di autenticazione ma di autenticazione a fattore multiplo, proprio perché è stato valutato che all'interno di una organizzazione complessa, l'utilizzo di più fattori va verificata per livelli di sicurezza e di utenza; quindi per certi servizi occorrerà un livello di secondo fattore più alto e di conseguenza più costoso.
Il sistema di gestione secondo fattore dovrebbe prevedere l'utilizzo di più di un secondo fattore di autenticazione, soprattutto quando ci sono casi in cui l'utente si trova in difficoltà ad avere l'autorizzazione o la consegna ad un secondo fattore, perché non ha a disposizione mezzi con

cui ha creato a casa quel fattore o quando qualche sistema di sicurezza proattivo gli chiede il secondo fattore in quanto si sta collegando da un altro paese o da indirizzi non verificati.
Quindi sarebbe preferibile che ci fosse un secondo fattore gestibile sullo stesso canale dell'applicazione da cui sta accedendo permettendo la fruizione del servizio anche in caso di indisponibilita' di altri canali (ad esempio non e' sempre scontato avere una connessione al web e la possibilita' di ricevere sms contemporaneamente). Questo da un certo punto di vista diminuisce relativamente la sicurezza del secondo fattore, tuttavia si possono mettere in campo degli altri meccanismi per ovviare a questa minore sicurezza
Un'altra considerazione per motivare la possibilità di accedere ad un servizio con più di un fattore secondario a scelta dell'utente è che l'utente potrà scegliere l'uso dello strumento in base al mezzo che avrà a disposizione come ad esempio tra la Carta Nazionale dei Servizi, SPID o la Carta d'Identità Elettronica, ma questo ha un costo di infrastruttura lato IT non trascurabile, perché bisogna implementare, gestire e mantenere in buono stato tutti questi connettori di autenticazione.

***MONDUCCI Antonella** chiede maggiori chiarimenti sulla tabella dei costi e dei tempi rappresentate nelle slides.*
ALBRIZIO snellisce il concetto sui costi e sui tempi spiegando che più tempo ci si mette a rilasciare il token, più aumentano i costi, perché determinati dalle ore-uomo. Ad esempio nelle Università non possono permettersi di perdere tempo ore-uomo nella distribuzione del secondo fattore.

***ROSSINI Angelo** chiede se esistono soluzioni che consentono l'installazione del client per il secondo fattore anche sulla postazione di lavoro, non solo sullo smartphone.*
ALBRIZIO risponde che esistono soluzioni, ma che bisogna stare attenti alla vera esigenza dell'Istituzione, se occorre che la soluzione sia in mobilità è una questione, contrariamente se serve una cosa più sicura da gestire sulla postazione di lavoro, come succede nella Sanità, allora si può risolvere con smartcard e questo vuol dire comprare software o almeno comprare lettori smartcard.

4. Gruppo di lavoro OpenID Connect

https://wiki.idem.garr.it/w/images/1/10/20200311-XI-assemblea-idem-oidc-wg.pdf

Giuseppe DE MARCO presenta i componenti del Gruppo di Lavoro OpenID Connect:

DE MARCO Giuseppe (coordinatore)	Università della Calabria
FESTI Maurizio	Università di Trento
D'AMICO Michele	Agid
PIROVANO Marco	Università Bocconi
ZANELLI Stefano	Università di Trento
NAPOLITANO Nunzio	Università degli Studi di Napoli Parthenope
ROSSINI Angelo	Cineca
PILORI Dario	INRIM
FLORIO Antonio	AgID

Il gruppo in questione propone di analizzare, esemplificare e prototipare l'adozione di OIDC nel contesto delle federazioni unilaterali, mediante OIDC core 1.0, nel contesto delle federazioni multilaterali mediante OIDC Federation 1.0. Tra i suoi componenti figurano operatori di servizio, tecnologi e sviluppatori software nel contesto delle IAM (Identity and Access Management).

Il gruppo si adopera nel collaudo, documentazione e descrizione dei profili individuati, contribuisce inoltre allo sviluppo di alcune librerie di base. Il gruppo pone inoltre una particolare attenzione alla comparazione con le esperienze trascorse in ambito SAML2.

5. Relazione Servizio IDEM GARR AAI

https://wiki.idem.garr.it/w/images/1/1b/20200311-XI-assemblea-idem-servizio-wg.pdf

Davide VAGHETTI riepiloga per i nuovi membri qual è il modo in cui il Servizio IDEM GARR AAI è l'operatore della Federazione, ovvero la terza parte fidata, a cui dovrebbero essere affidate le identità degli utenti per accede ai servizi e viceversa dei servizi nei provider per il fatto che effettivamente rappresentino le organizzazioni che hanno sottoscritto quei servizi.

Presenta il gruppo di cui lui è il Coordinatore del Servizio IDEM:

MONTICI Barbara (Supporto e Servizi TCS)	GARR
MALAVOLTI Marco (Supporto e dev-ops)	GARR
PIRELLI Laura (Adesioni e Segreteria)	GARR

ed elenca i principali compiti del servizio tra cui: la distribuzione dei metadati tramite la validazione e la firma; il supporto nelle organizzazioni; la collaborazione con la comunità internazionale della ricerca e dell'educazione.

Evidenzia un aumento dal 2017 degli IdP e un rallentamento dei servizi se non proprio una dismissione degli stessi per passaggio a eduGAIN dopo relativo controllo.

Come supporto proattivo ricorda che il servizio verifica gli IdP tramite il eduGAIN Connectivity Chach Service sviluppato da GARR e allerta gli IdP Admin; provvede alla formazione tramite webinar e corsi in presenza; supporta attività internazionali come REFEDS (Federazione della Ricerca e dell'Educazione partecipando a GdL sull'evoluzione standard relativi alle federazioni delle identità) e come eduGAIN (Servizio mondiale di inter-federazione tramite il quale le federazioni si scambiano i metadati e attraverso cui gli Idp accedono ai servizi pubblici anche nelle altre federazioni e viceversa).

Il Servizio IDEM partecipa alla task force del gruppo di lavoro EOSC Architecture il cui compito è definire i requisiti delle infrastrutture di autenticazione e autorizzazione nell'ambito di EOSC.

Infine, il Servizio IDEM partecipa attivamente al progetto GEANT GN4-3 in cui VAGHETTI è il Service Owner del task eduGAIN, MONTICINI lavora nel team che fornisce il supporto di eduGAIN e MALAVOLTI è responsabile del servizio eduGAIN ECCS.

6. Varie

Nessuna.

FASANELLI ringrazia tutti per le presentazioni e gli interventi e anticipa, come emerso nella recente riunione del CTS, che a breve saranno definiti strumenti collaborativi.

La riunione è terminata nei tempi stabiliti.