Identity Assurance Framework
il caso d'uso INFN

IDEM DAYS 2021

Casa, 24 febbraio 2021

Enrico M. V. Fasanelli

Gruppo di Lavoro CTS-IDEM 2020

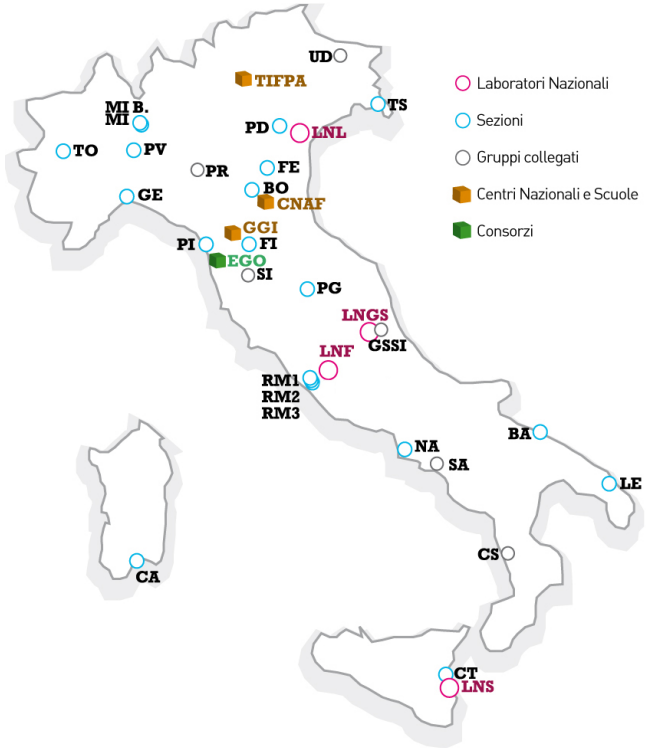
L’importanza di Identity Assurance

- La veridicità dei dati forniti da un IdP è una informazione fondamentale, senza la quale i SP non possono prendere decisioni sul concedere o meno l’accesso ai servizi erogati.
- Tutti gli operatori di federazione stanno definendo o hanno già definito i propri contesti di classificazione delle Identità Digitali in funzione delle caratteristiche di qualità delle informazioni ad esse associate.
- Siamo partiti dal caso d’uso dell’INFN (che data la sua natura federata ha iniziato ad affrontare il problema alcuni anni fa) per generalizzarla nell’Identity Assurance Framework di IDEM

INFN

- Istituto Nazionale di Fisica Nucleare
  - 26 Sezioni
  - 4 Laboratori Nazionali
  - 6 Gruppi Collegati
  - 3 Centri Nazionali
  - Amministrazione Centrale
  - Ufficio di Presidenza
  - Consorzio EGO

- Sezioni, Gruppi Collegati e Centri presso dipartimenti universitari



Caso d'uso INFN

- Diffusione dell'uso di IdP per l'accesso alle risorse IT delle varie strutture
  - Gestione omogenea delle identità digitali
    - Staff/member/Affiliate → identità "verificate"
    - Walk-in/visitors/external-users →identità anche non "verificate"
- Distinzione del tipo di identità sia rispetto ai ruoli che rispetto alla "tracciabilità" (o veridicità delle informazioni)

INFN LoA Framework

- Permettere l'accesso ad alcuni servizi ICT "pubblici" a chiunque, ma con accesso autenticato (non dimentichiamoci le AUP del GARR)
- Importare identità digitali
  - IAM di dipartimenti (servizi INFN non federati)
  - IdP SPiD
- Delegare la registrazione di Identità Digitali (uffici preposti, utenti finali)
- Distribuire il compito di "verificatore" di identità
- Framework multi-purpose:
  - Accessi logici a risorse IT
  - Accesso fisico, ad esempio al territorio nei Laboratori Nazionali

Framework di riferimento: LoA

- Level of Assurance
  - ITU-T X.1254 o ISO/IEC 29115 o NIST SP 800-63-2 (pubblicati nel 2012)
  - Quattro livelli (1-4) con focus sui sistemi di autenticazione
  - Riferimento dei livelli SPiD (che, però non considera il LoA1)

ITU-T X.1254 o ISO/IEC 25115	SPiD
LoA1	N/D
LoA2	Livello 1
LoA3	Livello 2
LoA4	Livello 3

Framework di riferimento: IAL & AAL

- NIST SP 800-63-3 (giugno 2017) IAL & AAL
  - Identity Assurance Level (processo di identificazione)
    - **IAL1**: attributi auto-dichiarati
    - **IAL2**: persona, “semplice” riconoscimento de visu (sia in rempto che in presenza)
    - **IAL3**: riconoscimento in presenza, verifica effettuata da un ufficiale predisposto ed appositamente formato
  - Authenticator Assurance Level (robustezza dei sistemi di autenticazione)
    - **AAL1**: comprende sia fattore singolo (username/password) che fattori multipli via (non meglio specificati) “protocolli di autenticazione sicuri”
    - **AAL2**: solo fattori multipli e tecniche di cifratura “approvate”
    - **AAL3**: possesso di una chiave (token hardware/caratterischiche biometriche) e fattori multipli

LoA vs IAL & AAL

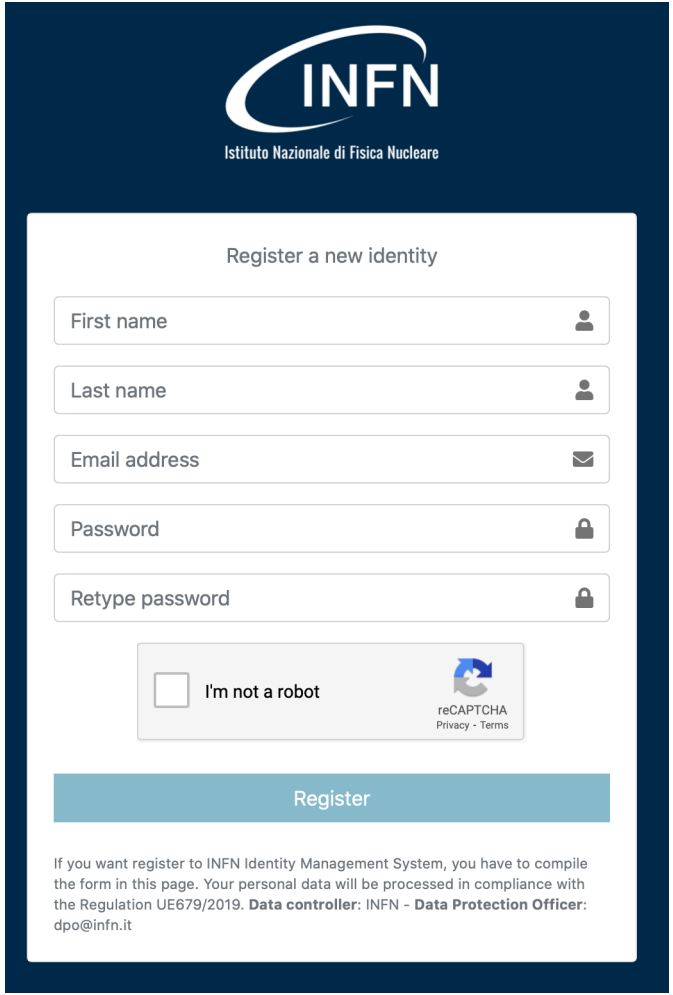
LoA	IAL	AAL
LoA1	IAL1	AAL1
LoA2	IAL2	AAL1
LoA3	IAL2	AAL1 o AAL2
LoA4	IAL3	AAL2 o AAL3

Identità (anche) agli sconosciuti

- Il framework INFN prevede due livelli di confidenza per le identità digitali
- Il primo livello è caratterizzato da “little or no confidence in the asserted identity”
  - Level of Assurance 1 → `eduPersonAssurance=urn:mace:infn.it:loa1`
- Il secondo livello prevede che il riconoscimento sia fatto “de visu” (in remoto o in presenza)
  - Level of Assurance 2 → `eduPersonAssurance=urn:mace:infn.it:loa2`

Framework & Tools: LoA1(IAL1)

- L’accreditamento di un utente alla cui identità digitale è assegnato il valore LoA1 avviene in autonomia attraverso un sistema di auto-registrazione che:
  - Acquisisce Nome, Cognome, e-mail (e password, ovviamente)
  - Verifica la correttezza dell’indirizzo e-mail via short-live feedback-tocken inviato all’indirizzo e-mail indicato in fase di registrazione
  - Registra l’dentità nallo IAM INFN (GODiVA) e quindi nell’LDAP di INFN-AAI
  - Ovviamente, nessun ruolo assegnato

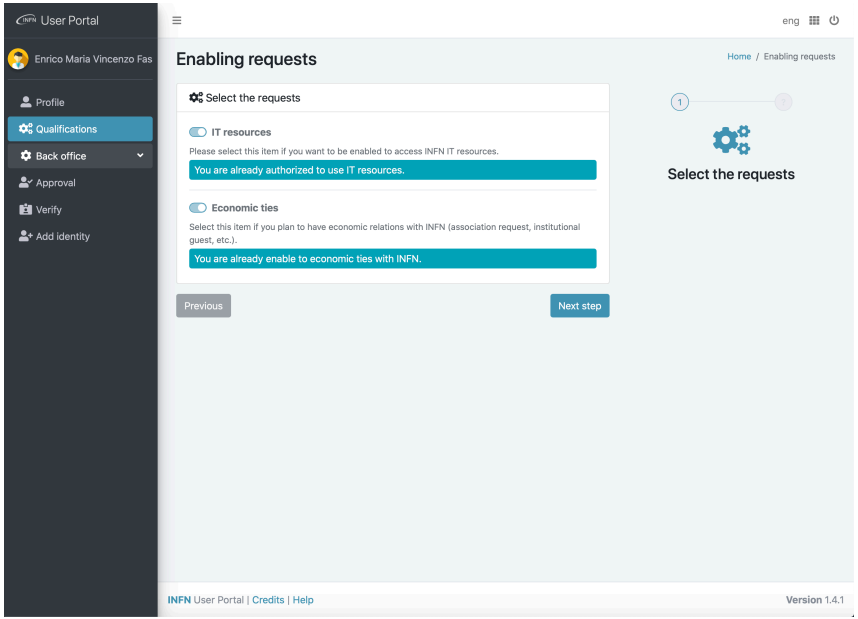


Framework & Tools: LoA2 (IAL2)

- Gli utenti “affiliate” INFN sono anche utenti “esterni” (non italiani) di risorse IT (risorse di calcolo di esperimenti del Laboratori Nazionali) che non hanno rapporti ecnomico/finanziari con l’ente
  - La chiave primaria non può essere il Codice Fiscale
  - Secondo il principio di minimizzazione dei dati del GDPR non chiediamo il Codice Fiscale se non necessario
- Due flussi (per ora) abilitanti che prevedono un riconoscimento “de visu” (in remoto o in presenza) nel processo di verifica della identità e dei dati inseriti e che portano quindi a LoA2
  - Accesso risorse IT
  - Rapporti economico fnanziari

User Portal

- Nelle richieste abilitanti tutti i dati sono obbligatori e acquisiranno lo stato di LoA2 ad identità verificata
  - Luogo e data di nascita, sesso
  - +Codice Fiscale (solo rapporti eco/fin)
- Back-office
  - Approvazione richieste (accesso IT)
  - Verifica Identità e dati inseriti
  - Registrazione Identità (uffici competenti)



LoA1 → LoA2

- L'assegnazione dello stato LoA2 avviene solo per identità digitali per le quali sia andata a buon fine:
  - L'operazione di riconoscimento de visu (in presenza o in remoto)
  - L'import di dati da un DB di strutture in convenzione, che effettuano riconoscimento de visu
    - Dipartimenti universitari
    - SPiD/CIE/CNS
  - La presa di servizio che richiede la firma (in presenza) di un contratto di lavoro o di associazione

Identity import/linking

- L'import di identità da strutture in convenzione porta alla ribalta il problema delle identità multiple
- Le fonti "esterne" sono tutte sorgenti di identità LoA2
  - In caso di corrispondenza *certa* con una identità già registrata le identità vengono "fuse" in una
  - In via di sviluppo il tool di fusione "on demand" che sarà disponibile nello User Portal, previa doppia autenticazione (devo dimosrare di essere il possessore delle due identità che voglio fondere) e solo di identità con lo stesso LoA (vogliamo evitare che un indirizzo e-mail self-asserted → LoA2)

Da INFN a IDEM

- Il famework descritto fin qui è su misura per le esigenze dell'INFN
- E' (ahimè ancora) in corso la generalizzazione per la comunità IDEM
  - E' compatibile con i framework già definiti da altri operatori di federazione e con il RAF (REFEDS Assurance Framework)
- Disponibile per un "commento pubblico" al più presto.

IDENTITY ASSURANCE FRAMEWORK
IL CASO D'USO INFN

FINE

IDEM DAYS 2021
Casa, 24 febbraio 2021

Enrico M. V. Fasanelli
Gruppo di Lavoro CTS-IDEM 2020