Contribution ID: **6** Type: **Comunicazione orale**

Implementazione di un sistema di autenticazione federato nell'ambito della rilevazione dei settori ERC del personale Ricercatore e Tecnologo del DSB

Thursday, 14 October 2021 14:30 (30 minutes)

Background

Al fine di delineare la distribuzione degli ambiti di ricerca definiti dall'ERC all'interno del personale afferente al Dipartimento di Scienze Biomediche del Consiglio Nazionale delle Ricerche (da ora denominato CNR-DSB) è stato appositamente progettato e sviluppato un servizio web per permettere ai ricercatori e tecnologi l'indicazione dei propri ambiti di ricerca.
L'infrastruttura realizzata è composta da tre moduli inter-comunicanti tra loro:
- Server
- Client
- Autenticazione

Il modulo server, sviluppato in GO, è responsabile delle interazioni col database per il salvataggio e controllo delle informazioni inserite. Il modulo client, realizzato in Angular, permette la visualizzazione e l'inserimento dei valori per la determinazione degli ambiti di competenza degli utenti.

Gestione dell'Autenticazione

Il modulo Autenticazione, realizzato mediante l'applicazione di Identity and Access Management enterprise Keycloack, si occupa del recupero dei dati associati agli utenti, della loro gestione e alla associazione di ulteriori metadati specifici per la piattaforma utilizzata.
Tramite questa applicazione il modulo server e il modulo client sono in grado di gestire le sessioni utente a seguito della autenticazione sulla piattaforma con le credenziali CNR "SIPER" mediante il protocollo OpenID Connect.
I dati associati agli utenti sono acquisiti dal server centrale del personale CNR tramite accesso LDAP mediante credenziali di sola lettura e filtro di accesso tramite IP forniti a seguito di una richiesta formale.
Le informazioni associate ad ogni utente (tranne la password) sono poi importate (e controllate periodicamente) nel sistema per permettere l'autenticazione ai soli utenti del CNR-DSB attraverso un filtro appositamente creato. Questo processo permette di importare solo i dati degli utenti abilitati all'accesso al servizio non solo in base all'istituto di appartenenza ma anche in base al tipo di profilo lavorativo; in questo modo, il modulo di autenticazione non importa o utilizza dati non inerenti allo specifico scopo della piattaforma.
Al fine di agevolare la gestione delle informazioni associate agli utenti nel modulo di autenticazione sono stati definiti anche dai campi dedicati che vengono associati alle informazioni reperite dal server CNR. Questo permette di estendere il set di metadati forniti alle applicazioni facenti parte della piattaforma cosi da renderli tutti accessibili con la medesima modalità.
Il processo di autenticazione e gestione delle sessioni utente tra il modulo autenticazione e i moduli client e server avviene mediante il protocollo di sicurezza OpenID Connect attraverso l'esposizione di specifiche API di tipo REST richiamate ed utilizzate dalle applicazioni sviluppate. In questo modo le attività degli utenti tra il modulo client e il modulo server, sono costantemente sincronizzate e controllate cosi da garantire una maggiore sicurezza.

GDPR e Privacy

Inoltre, come precedentemente descritto, la piattaforma sviluppata richiede l'utilizzo di alcuni dati sensibili associati ai dipendenti afferenti al CNR-DSB. Questo ha richiesto anche una stretta collaborazione con il Data

Protection Officer al fine di rendere il servizio conforme alla normavia Europea legata alla gestione dei dati personali (denominata GDPR). a tal proposito sono stati redatti due specifici documenti:
- Analisi del rischio relativo ad eventuali problematiche di sicurezza
- Privacy policy, direttamente scaricabile dalla applicazione, relativa alla modalità di utilizzo dei dati trattati

Futuri Sviluppi

Attualmente l'interconnessione tra la piattaforma sviluppata e il sistema di gestione utenti CNR "SIPER" si basa su accesso tramite protocollo LDAP. Il passaggio ad un sistema basato su Service e Identity provider non richiederebbe modifiche ai moduli client e server in quanto utilizzano un sistema di comunicazione standard e indipendente dalla modalità di reperimento delle informazioni riguardanti l'utente che sta operando sulla piattaforma. Questo rende l'intera infrastruttura modulare e facilmente estendibile in termini di funzionalità e sicurezza.

Primary author: GNOCCHI, MATTEO (CNR-ITB)

Co-author: MOSCATELLI, MARCO (CNR - ARMi4)

Presenter: GNOCCHI, MATTEO (CNR-ITB)

Session Classification: Sicurezza informatica, gestione delle identità e dei dati

Track Classification: Sicurezza informatica, gestione delle identità e dei dati