Contribution ID: **354** Type: **Presentazione orale**

Evoluzione di INDIGO IAM: sicurezza, interoperabilità e nuove funzionalità

Friday, 30 May 2025 09:20 (20 minutes)

INDIGO IAM è un servizio per la gestione dell'autenticazione e dell'autorizzazione nelle infrastrutture di ricerca distribuite. Supporta la federazione dell'identità, il controllo degli accessi e l'autorizzazione basata su token. Gli sviluppi attuali e futuri si concentrano sul miglioramento di prestazioni, interoperabilità e sicurezza. In questo contributo dedichiamo particolare attenzione al supporto per l'autenticazione a più fattori (MFA), alla gestione dei client obsoleti e all'adozione delle linee guida della AARC Blueprint Architecture (BPA) per garantire conformità agli standard di federazione e interoperabilità, inclusa la European Open Science Cloud (EOSC).

Il supporto di un secondo fattore di autenticazione è un obiettivo chiave, anche nel contesto di EOSC Beyond. Introdotto in IAM v1.11.0 come funzionalità opzionale per le credenziali locali, è stato poi esteso ai flussi di autenticazione con provider remoti (OIDC, SAML) e certificati X.509, seguendo le specifiche per la segnalazione dell'uso del MFA definite nel progetto europeo EOSC Beyond. Questo miglioramento rafforza la sicurezza e la gestione degli accessi nelle infrastrutture federate.

La gestione dei client obsoleti è un altro tema rilevante, in particolare per DataCloud, dove l'accumulo di client non più attivi può compromettere sicurezza ed efficienza. Sfruttando il tracciamento dell'ultimo utilizzo del client già presente, è possibile realizzare tool esterni, come script che utilizzano le API per rimuovere i client obsoleti.

La possibile adozione di INDIGO IAM nel nodo italiano della EOSC richiede anche lo sviluppo della *proxied token introspection*, un'estensione di OAuth2 che delega a un infrastructure proxy locale le richieste di introspezione agli authorization server remoti. A tal fine, in questo contributo, discuteremo l'evoluzione e l' integrazione di ESACO in IAM, un servizio che verifica la validità e la firma dei token OAuth per i server di autorizzazione registrati.

Infine, verrà presentato il Proof-of-Concept sviluppato nei progetti ICSC/TeRABIT, un passo chiave per trasformare IAM in un Infrastructure Proxy/Community AAI per il nodo EOSC italiano, facilitando una maggiore sinergia con la comunità di ricerca e i servizi distribuiti.

Primary authors: VIANELLO, Enrico (Istituto Nazionale di Fisica Nucleare); AGOSTINI, Federica (CNAF-INFN); GIACOMINI, Francesco (Istituto Nazionale di Fisica Nucleare); GASPARETTO, Jacopo (Istituto Nazionale di Fisica Nucleare); MICCOLI, Roberta (Istituto Nazionale di Fisica Nucleare); ZOTTI, Stefano Enrico (Istituto Nazionale di Fisica Nucleare)

Presenter: MICCOLI, Roberta (Istituto Nazionale di Fisica Nucleare)

Session Classification: Servizi ICT

Track Classification: Servizi ICT