WORKSHOP GARR 2026

NET MAKERS

Nodo EOSC European Digital Twin Ocean

Federare identità e accessi in un'infrastruttura in produzione

Alfredo Oliviero

CNR-ISTI · EOSC Node European DTO

Cos'è EOSC, in parole semplici

EOSC in un paragrafo

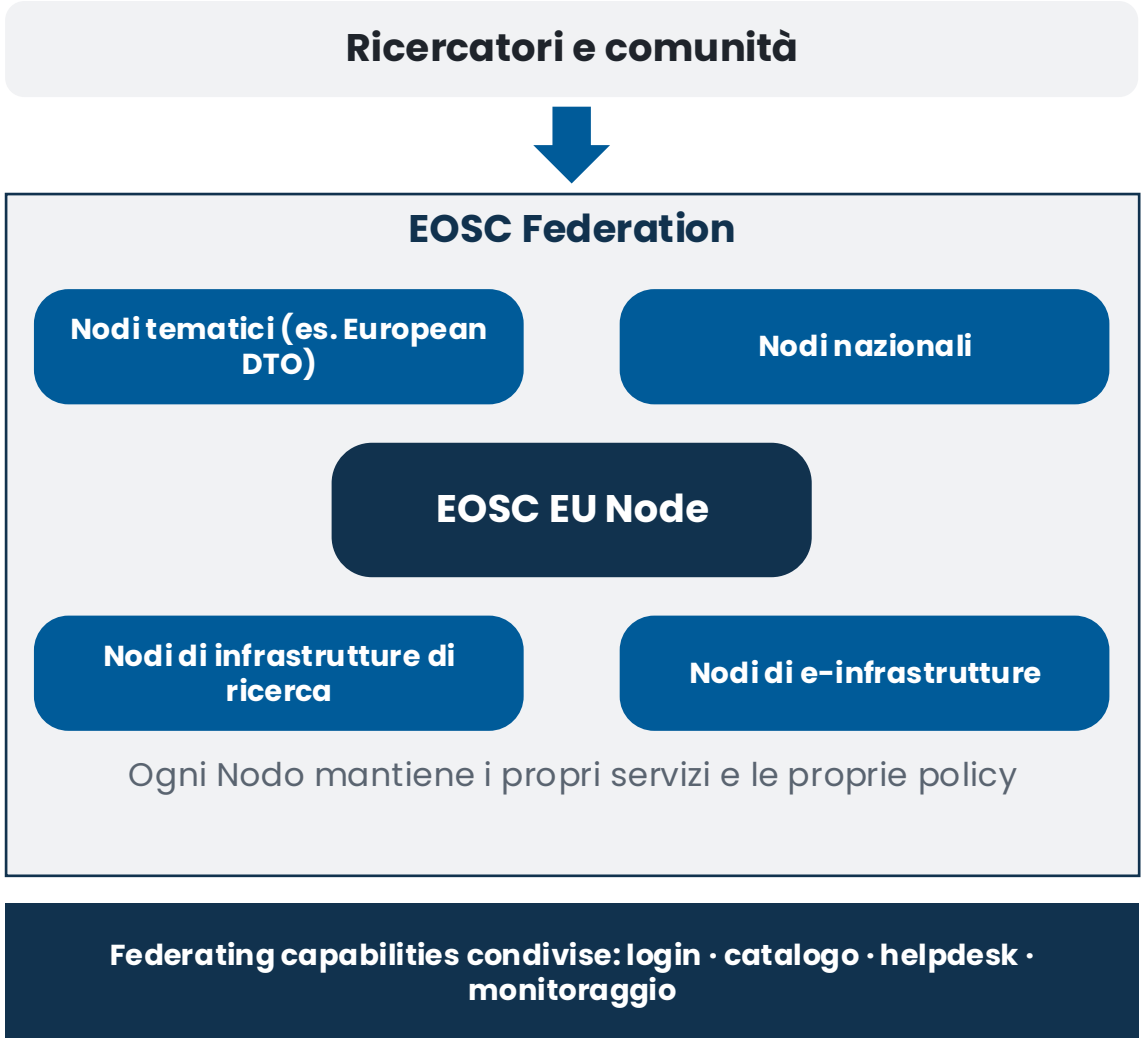
La **European Open Science Cloud** è lo spazio dati dell'UE per la ricerca e l'innovazione. Permette ai ricercatori di conservare, condividere, elaborare, trovare e riusare dati, software e servizi **FAIR**, tra discipline e paesi diversi.

Non è una grande piattaforma unica. È una **federazione di Nodi autonomi**: ogni Nodo gestisce i propri servizi con le proprie policy, e un piccolo insieme di regole e servizi condivisi (le *federating capabilities*) li fa funzionare insieme.

L'**EOSC EU Node**, gestito per la Commissione Europea, è in produzione da ottobre 2024 ed è il riferimento comune.

Perché un'organizzazione diventa Nodo

- **Portata**: utenti oltre il proprio dominio o paese, e potenzialmente industria e settore pubblico
- **Economie di scala**: login, cataloghi, monitoraggio e helpdesk condivisi, invece di costruirli da soli
- **Standard comuni**: regole europee per i prodotti della ricerca e l'erogazione dei servizi



Fonti: Building the EOSC Federation – Requirements for EOSC Nodes (EOSC Tripartite Governance, 24 maggio 2024); Guidelines on onboarding policies (28 novembre 2025).

La governance in pratica: NCC e NOC

Una struttura transitoria della EOSC Tripartite Governance accompagna la Federation verso la produzione.

Commissione Europea

DG RTD / DG CONNECT

EOSC Steering Board

Stati Membri e Paesi Associati

EOSC Association

Comunità e infrastrutture di ricerca

Insieme: la EOSC Tripartite Governance, che guida strategicamente la costruzione della Federation.

Node Coordinators Committee (NCC)

Allineamento strategico

- riunisce i Node Coordinator dei Nodi
- allinea le priorità
- verifica la prontezza alla produzione
- approva i mandati dei Working Group

Per il nostro Nodo: Pasquale Pagano

Node Operations Committee (NOC)

Coordinamento operativo

- riunisce gli Operations Manager dei Nodi
- coordina priorità, requisiti e validazione
- coordina i Working Group

Per il nostro Nodo: Massimiliano Assante, co-chair

Il NOC e i Working Group



Il NOC coordina le priorità operative; i Working Group svolgono il lavoro mirato, con i Nodi che forniscono, validano e gestiscono le capacità.

Federating capabilities: servizi condivisi tra i Nodi

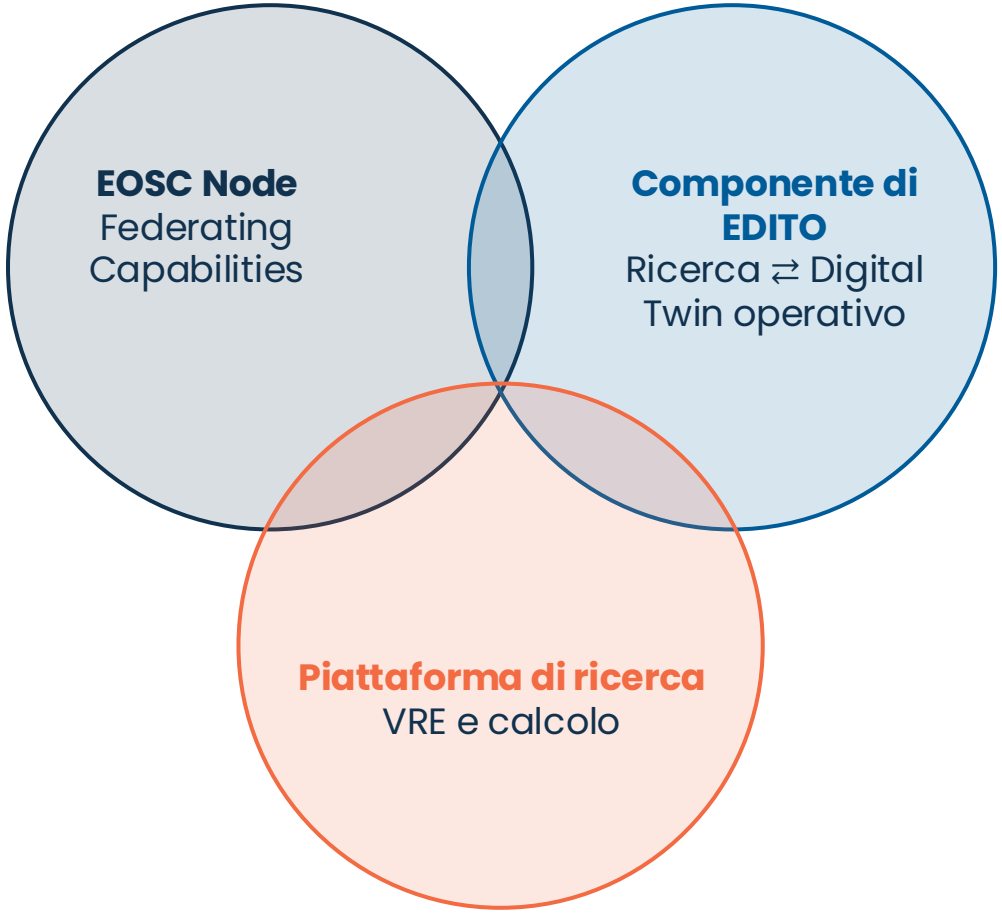
FC-1 Login (AAI)	FC-2 Cataloghi	FC-3 Helpdesk	FC-4 Monitoraggio
Un solo login per tutti i Nodi, tramite MyAccessID e l'EOSC AAI. L'utente vede: entra una volta, usa i servizi di più Nodi. *In produzione: obbligatorio (P.2)*	I Nodi pubblicano le descrizioni dei servizi; l'EU Node le aggrega nell'EOSC Resource Hub. L'utente vede: cerca una volta, trova risorse di tutti i Nodi. *In produzione: obbligatorio (P.3)*	Gli helpdesk dei Nodi sono collegati, così un ticket può seguire l'utente tra i Nodi. L'utente vede: assistenza dal Nodo che usa, inoltrata se serve. *Helpdesk del Nodo obbligatorio (P.5); test di federazione a fine 2026*	Ogni Nodo controlla i servizi del proprio catalogo e li riporta in un formato concordato. L'utente vede: se un servizio è attivo e affidabile. *Raccomandato (P.8): prossimo passo*

Principio: **implementate una volta, riusate da ogni Nodo**. I Nodi restano autonomi sui propri servizi.

Fanno parte del quadro anche FC-5 gestione dei servizi (FitSM) e FC-6 accounting dei servizi (uso), ancora in definizione.

Fonti: EOSC AAI Architecture 2025; EEN Registration of EOSC Service Catalogues v7.1; FC-3 Helpdesk Executive Summary; FC-4 Service Monitoring proposal v3; EOSC Federation & Nodes' SMSs proposal.

EOSC DTO - Un Nodo tematico in produzione



EOSC Node

Implementa le Federating Capabilities ed è raggiungibile da ogni altro Nodo, compreso l'EOSC EU Node.

Componente di EDITO

La componente Open Science dell'European Digital Twin Ocean: i prodotti FAIR della ricerca alimentano i servizi operativi del DTO, e i dati operativi tornano alla ricerca.

Piattaforma di ricerca

VRE, calcolo e storage per i ricercatori marini, in linea con la Missione UE “Restore our Ocean and Waters”.

D4Science · la piattaforma operativa sottostante

Oggi EOSC-Marine sostiene l'operatività del Nodo

Dalla candidatura alla produzione

Le tappe della Federation e il lavoro del nostro Nodo

EOSC AAI Working Group e Federation

Avvio del WG e Cracovia
11 ott: primo incontro
20 dic: candidati della prima ondata
17-18 giu: incontro del Build-up Group

Acceptance, lancio, MoU
Lug: ambiente di acceptance
Set: notebook di test G052
3-5 nov: lancio al Symposium
18 nov: firma del MoU

Requisiti
Dic 2025: v2025 con priorità
30 gen 2026: mandato del WG
Mar 2026: notebook di test G069

Autorizzazione e pilota
31 lug: modello di autorizzazione
11 set: pilota OpenID Federation

Symposium
14-16 ott: Firenze

4° trim. 2024 - giu 2025 | **Lug-nov 2025** | **Dic 2025-mar 2026** | **Mag-set 2026** | **Ott 2026**

EOSC Node European DTO

Prima ondata e avvio
20 dic: candidato come Blue-Cloud
Giu: membri del WG; incontri ogni due settimane su protocolli e casi d'uso

Ambiente di sviluppo
11 lug: autenticazione con MyAccessID
Set: introspection con TIP integrata
1 ott: test G052 superati
Ott: provider nativo

G069 superato
25 mar 2026: test superati in sviluppo

Login in produzione
22 giu: login federato funzionante in produzione
Set: partecipazione al pilota OpenID Federation

Nodi in produzione
8 ott: inserito ufficialmente tra i Nodi in produzione

In corso: pilota OpenID Federation per la fiducia automatica tra Nodi

Cosa significa AAI federata

Infrastruttura di autenticazione e autorizzazione federata tra i Nodi

L'autenticazione è delegata all'istituzione di appartenenza; la decisione sull'accesso resta al Nodo

Per l'utente

Si autentica presso la **propria istituzione** ed è **riconosciuto** in tutta la Federation

Per l'infrastruttura

Delega l'autenticazione, mantiene la **decisione sull'accesso**

Le credenziali restano a casa

Le password restano all'**istituzione di appartenenza**: nessun nuovo account, nessuna nuova password

Viaggia un **token** con identità, attributi, gruppi e ruoli

L'accesso resta locale

Un **Infrastructure Proxy** collega il Nodo alla Federation (il nostro: **Io IAM Keycloak**)

L'autenticazione è delegata all'istituzione di appartenenza e condivisa tra i Nodi

La decisione sull'accesso resta al Nodo

La sfida: federare un'infrastruttura già in produzione

Un'AAI matura e in produzione, prima della federazione

I requisiti della EOSC Federation sono stati integrati nell'AAI esistente, non costruiti accanto

1 · Preservare ciò che funziona

Mantenere l'AAI che le **comunità già usano**

2 · Isolare la federazione

Definire un **livello di astrazione** nello IAM che integra le AAI federate

3 · Disaccoppiare i servizi

Delegare interamente **validazione e interpretazione dei token** al livello di astrazione

Infrastruttura consolidata

D4Science è operativa dal **2014**: **oltre 30.000 utenti registrati**, decine di progetti e centinaia di VLab nel tempo.

Il suo IAM è basato su **Keycloak** ed era già in **produzione** quando è iniziata la federazione.

Cosa ha aggiunto la federazione

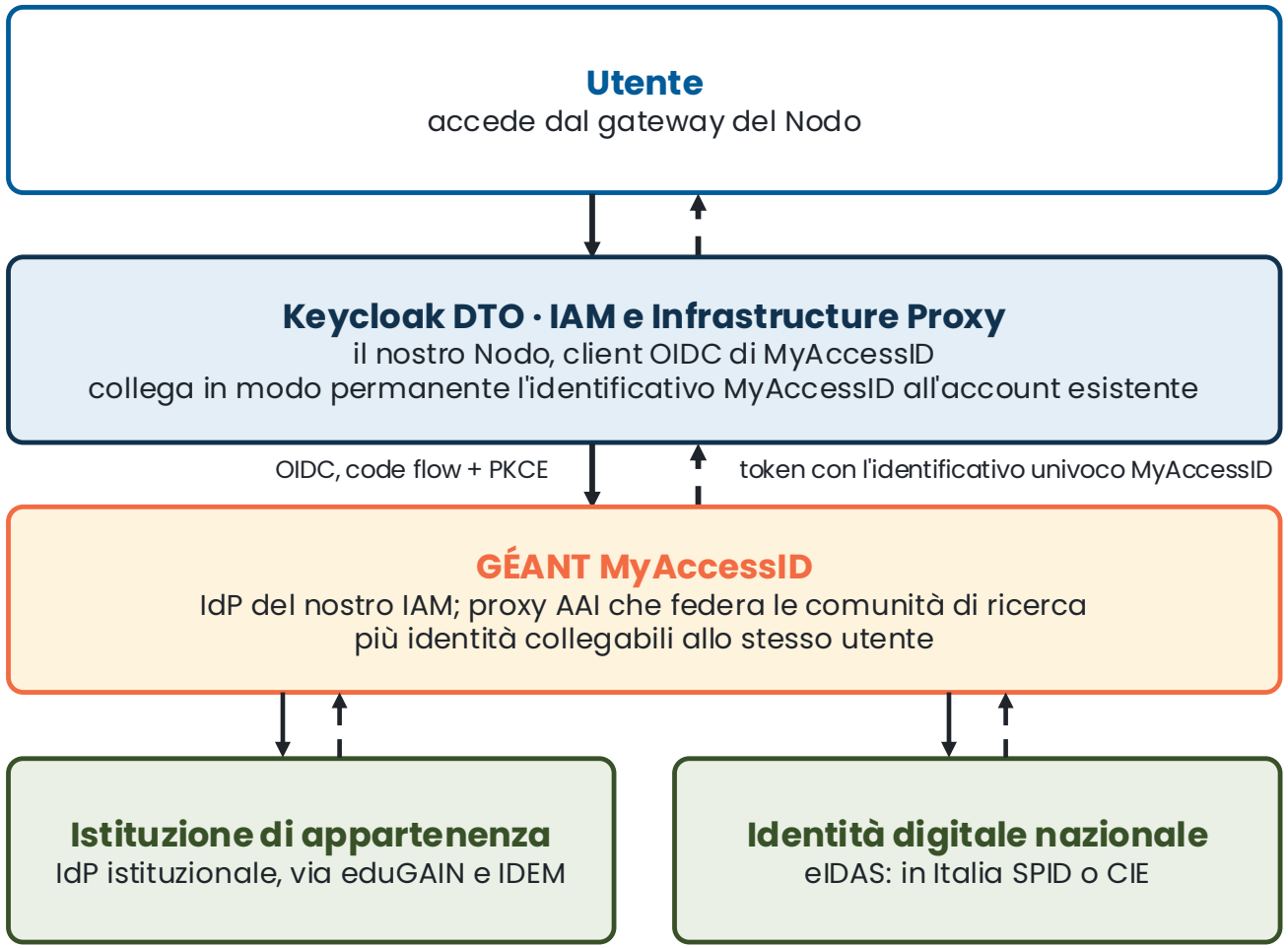
Login tramite GÉANT MyAccessID

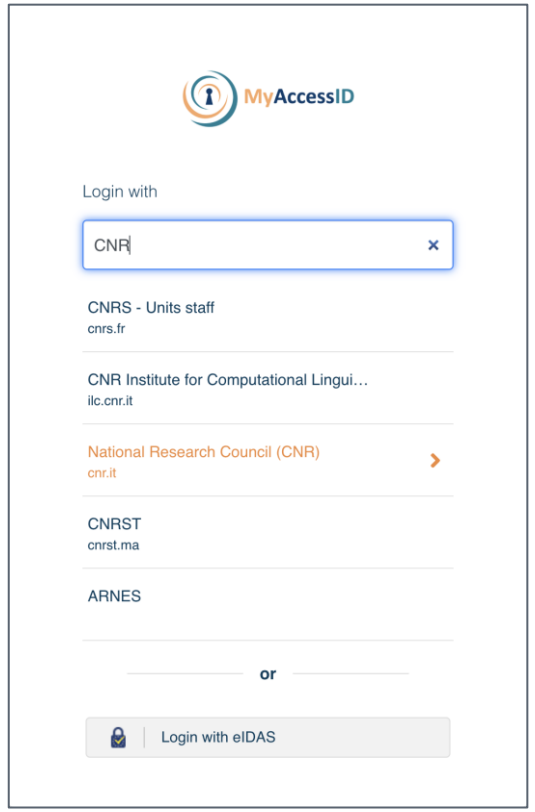
Token introspection tra Nodi (AARC-G052)

Sintassi comune per gruppi e ruoli (AARC-G069)

Login federato con GÉANT MyAccessID

MyAccessID federa i login delle comunità di ricerca europee; il nostro Keycloak ne è client OIDC





MyAccessID: scelta dell'istituzione di appartenenza

AARC-G052: verificare i token emessi da altri Nodi

Requisito: un Nodo deve poter fare l'introspection di un token emesso da un altro Nodo fidato

Il problema

Un token emesso da **un Nodo** arriva a **un altro Nodo**:
formato: sa leggerlo?
fiducia: si fida di chi l'ha emesso?
identità: a quale dei suoi utenti corrisponde?

Come funziona

Lo **IAM** inoltra la domanda all'**emittente** del token, tramite il **Central Hub**, **in modo trasparente per il servizio**. La risposta è nel **formato standard di introspection (RFC 7662)**, con gruppi e ruoli secondo **AARC-G069**.

Flusso a runtime nel Nodo European DTO



Stesso formato standard per token locali ed esterni: i servizi restano agnostici rispetto alla federazione

AARC-G069: gruppi e ruoli in una sintassi comune

Una sola sintassi URN, perché gruppi e ruoli siano espressi allo stesso modo in ogni Nodo



NAMESPACE
registrato presso GÉANT, in minuscolo

LETTERALE
valore di tipo gruppo

GRUPPO + SOTTOGRUPPI
la gerarchia fino al VLab

RUOLO
vale sul gruppo più a destra

Regole della specifica

Gerarchia: chi ha un ruolo in un VLab è membro anche dei gruppi superiori, ma il ruolo vale solo nel VLab.

Normalizzazione: namespace in minuscolo; caratteri speciali percent-encoded.

Claim: rilasciato come entitlements; la parte #authority è deprecata.

Ambito: il namespace dice di chi è un gruppo.

Il nostro mapping

Il ruolo VRE-Manager, valido solo nel VLab EOSCNodeEUDTO-Lab, diventa:

urn:geant:d4science.org:dto:group:

d4science.research-infrastructures.eu:
D4OS:EOSCNodeEUDTO-Lab:role=VRE-Manager

Namespace: un Keycloak serve più di un Nodo, un namespace URN per client.

Testato in sviluppo: formato verificato con il notebook GÉANT, superato il 25 marzo 2026.

Autorizzazione tra Nodi: cosa c'è e cosa manca

Modello comune di autorizzazione in definizione nel Working Group

L'EOSC AAI trasporta i claim; ogni Nodo decide chi può accedere alle proprie Risorse

1 · Progetto ↔ Gruppo

Un **Progetto** approvato da un Nodo è collegato a un **Gruppo** gestito in una **Community AAI**

2 · Il nostro mapping

Un progetto (VRE) ha più **VLab**, mappati come sottogruppi; i ruoli sono **per VLab**

3 · Decidono Nodo e Servizio

Il **Nodo** collega Progetto e Gruppo; il **Servizio** applica la propria policy ai claim

Implementato

Accesso just-in-time: claim al login e, tra Nodi, tramite proxied introspection (AARC-G052). Ogni Servizio applica la propria policy.

Ancora aperto

Un utente deve completare l'**onboarding** (accettare i termini del Nodo) prima di accedere alle sue risorse. Preparare account **in anticipo**, per un gruppo o per un singolo utente, richiede il **consenso** dell'utente.

In sintesi

A che punto è l'EOSC Node European DTO su login e accessi

1 · Login

Federato tramite MyAccessID, **in produzione**

2 · Verifica dei token

Tra Nodi (AARC-G052), **implementata**, tutti i test previsti superati

3 · Gruppi e ruoli

Una sola sintassi (AARC-G069), **implementata**, tutti i test previsti superati

4 · Accesso

I claim viaggiano; **ogni Nodo decide** (modello in definizione)

Cosa ottengono le applicazioni

Un'identità riconosciuta tra i Nodi

Lo **stesso formato standard** per token locali ed esterni

Gruppi e ruoli in **una sola sintassi**

Cosa resta a ogni Nodo

Chi può accedere alle sue Risorse

La **policy** dei propri servizi

I propri **progetti, gruppi e VLab**

Il login federato è operativo; ogni Nodo mantiene il controllo dell'accesso alle proprie Risorse

Grazie

alfredo.oliviero@isti.cnr.it
eosc-dto.d4science.org · eosc-dto.eu

Per le domande
www.partici.fi
codice **83995288**

WORKSHOP GARR 2026
NET MAKERS