Infrastruttura di Autenticazione e Autorizzazione (AAI) dell'INFN in ambito Grid e Cloud

Roberta Miccoli
21 marzo 2024

Infrastruttura di calcolo distribuita dell’INFN

- Da diversi anni, l'INFN gestisce e supporta la più grande infrastruttura distribuita per la ricerca e l'università in Italia, con un data center nazionale molto grande (CNAF) e altri 9 data center di grandi dimensioni, tutti interconnessi ad altissima capacità attraverso la rete della ricerca gestita da GARR
- Questa infrastruttura utilizza protocolli **Grid** e **Cloud** per servire le esigenze di diverse decine di collaborazioni scientifiche nazionali e internazionali in fisica e in molti altri ambiti

Grid

- E’ un **sistema di calcolo** distribuito geograficamente che permette l’utilizzo coordinato di migliaia di computer sparsi nel mondo
- E’ stato inizialmente sviluppato per immagazzinare, rendere accessibili e processare i dati prodotti dagli esperimenti all'acceleratore LHC del CERN di Ginevra: circa **15 milioni di GB** ogni anno
- Il funzionamento è garantito dalla presenza di un complesso insieme di componenti software (*middleware*) open-source disponibili per Linux

Grid

- Coinvolge circa 140 centri di calcolo distribuiti in 33 paesi e ha una potenza di calcolo pari a quella di 100.000 computer
- L'INFN è uno dei promotori principali del progetto Grid e ospita al **CNAF di Bologna** uno degli undici nodi di primo livello (Tier-1) della Grid
    - questi nodi ricevono direttamente dal CERN i dati prodotti da LHC, per smistarli successivamente ad altri siti minori

Grid Security - AuthN & AuthZ

- La Grid permette di dare una risposta al problema della *condivisione coordinata delle risorse presenti nei vari siti tra organizzazioni virtuali dinamiche e multi-istituzionali*
  - Un tipico esperimento di fisica delle alte energie conta migliaia di ricercatori provenienti da centinaia di istituti in decine di paesi

Prospettiva dell'utente

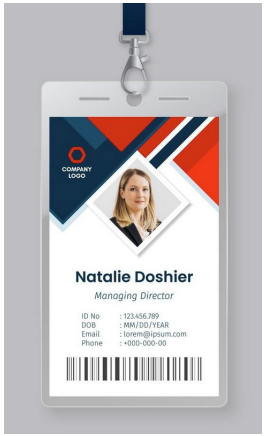
- Voglio essere in grado di utilizzare le risorse secondo le mie necessità
- Non mi interessa dove si trovano queste risorse e chi le possiede

Prospettiva del sito

- Ho il pieno controllo delle risorse che fornisco
- Ho io l'ultima parola su chi è autorizzato a utilizzare le mie risorse

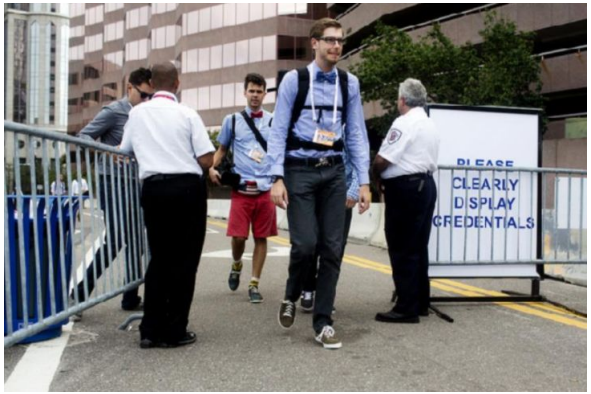
Grid Security - AuthN & AuthZ

Autenticazione, Identità



CHI è l'utente?

Autorizzazione



COSA può fare l'utente?

GSI (Grid Security Infrastructure)

Di cosa ha bisogno un utente per usare la Grid?

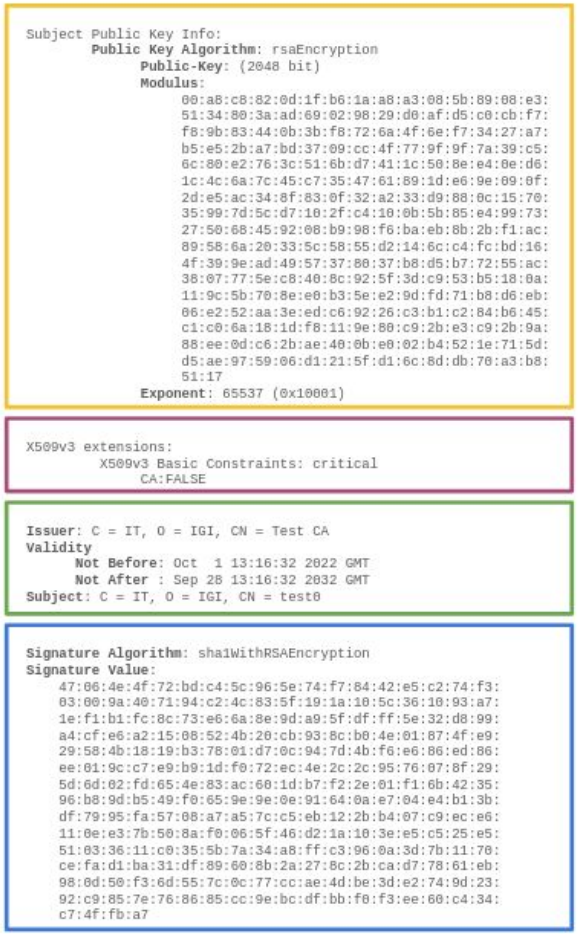
- Un **certificato personale X.509**
- Essere affiliato con una o più **collaborazioni scientifiche**
- Disporre degli **strumenti software** necessari per l'accesso alle risorse

Certificato X.509

- Documento digitale che rappresenta un'entità, associando una chiave pubblica a un’identità
  - un servizio/sito web, una macchina o una persona
- Firmato digitalmente da un'**autorità di certificazione** (CA), terza parte fidata che verifica l'identità e i dati personali del richiedente
- Di lunga durata: in genere un certificato scade dopo un anno e va rinnovato

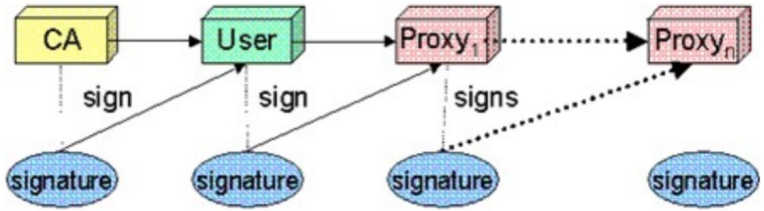
Certificati per la ricerca

- I certificati sono stati utilizzati per la ricerca dalla fine degli anni ‘90
- Le Autorità di Certificazione (CA) usate nella ricerca sono regolamentate dalla Interoperable Global Trust Federation (IGTF)
  - IGTF rilascia periodicamente una lista di certificati X.509 appartenenti alle CA in modo che si possano verificare le loro firme
- L’**autenticazione** avviene tramite l’identità espressa in un certificato
- L’**autorizzazione** avviene in base a informazioni contenute in *estensioni* incluse in certificati derivanti da un certificato personale



Proxy e delega

- Gli utenti non presentano il loro certificato di lunga durata ai servizi Grid con cui interagiscono
  - le chiavi private non devono MAI lasciare il computer dell'utente
- Si utilizzano invece i certificati **proxy**
  - per evitare di inserire la password ogni volta che ci si deve autenticare con un servizio Grid (**single sign-on**, **SSO**)
  - per consentire la **delega**: un processo remoto si autentica per conto dell'utente, ad esempio un lavoro in esecuzione su un sito remoto che deve contattare un server di archiviazione per trasferire file



Proxy

Il certificato dell’utente viene utilizzato per generare e firmare un

- Certificato Proxy
  - identità dell’utente
  - durata breve (24-48 ore)
  - scadenza
- Chiave privata
  - nessuna password
  - leggibile solo dall'utente

Da un certificato proxy e dalla sua chiave privata si possono generare ulteriori proxy

Proxy

Perché generare un certificato proxy e non inviare l'originale?

- I proxy hanno una durata più breve
  - se vengono compromessi, il danno è limitato
  - esistono altre forme di limitazione, mai realmente utilizzate
- La chiave privata di un certificato è protetta da una password nota solo all'utente
  - è fondamentale che tali informazioni rimangano private e quindi la chiave privata dell'utente non può essere utilizzata per la firma da un sistema
- L’affidamento di un proxy a un servizio è una forma di delega
  - più precisamente è una forma di “impersonation”, visto che l’identità del proxy è sempre a nome dell’utente

VOMS

- Una collaborazione scientifica va sotto il nome di **Virtual Organization** (VO)
- Il **Virtual Organization Membership Service** (VOMS) è un servizio utilizzato per gestire le adesioni a una VO
  - Gli utenti chiedono di far parte di una VO
  - Devono accettare l'Acceptable Use Policy (AUP) definita per quella VO
  - Il gestore della VO accetta/rifiuta la richiesta

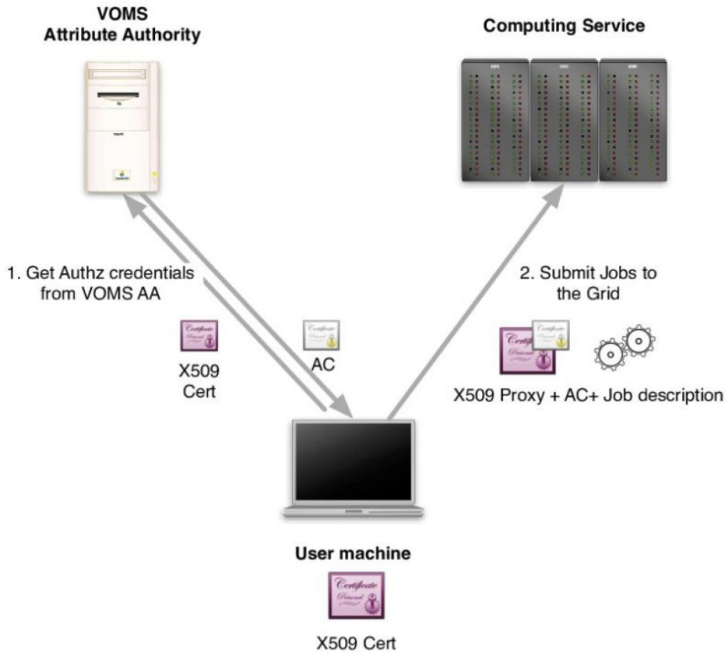
VOMS

Rappresenta una repository centrale per le informazioni di autorizzazione degli utenti della VO, fornendo supporto per l'ordinamento degli utenti in gerarchie di gruppi, tenendo traccia dei loro ruoli e di altri attributi

VOMS server @CNAF

Proxy VOMS

- Per l'accesso a una risorsa, oltre a dimostrare la propria identità, è necessario dimostrare anche l'appartenenza a una VO
- **Proxy VOMS**: un proxy Grid con estensioni relative alla VO
- Per creare un proxy VOMS, si contatta il server VOMS della propria VO che restituisce un **Attribute Certificate** (AC) contenente informazioni sulla VO, sui gruppi di appartenenza e suoi ruoli rivestiti in tali gruppi
- I servizi Grid possono leggere tali estensioni VOMS e prendere decisioni di autorizzazione basandosi sul loro contenuto (ad es., posso leggere questo file? posso sottomettere un *job* di computazione?)



Uso dei certificati - pro e contro

Pro

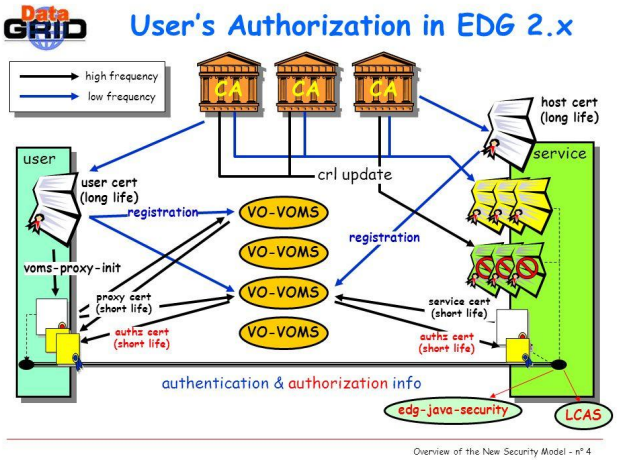
- Tecnologia ben consolidata, i servizi sono predisposti per accettare certificati
- Stessa credenziale valida per web e non web

Contro

- Impatto sulla sicurezza se compromesso
- Problemi di usabilità
- Problemi di mobilità tra computer diversi

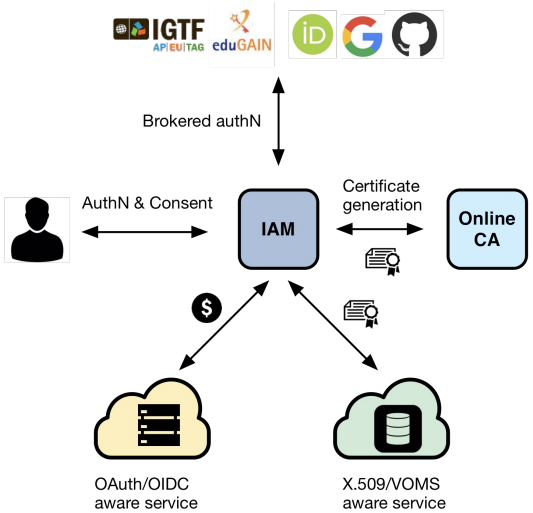
AAI attuale e futura

AAI attuale, basata su X.509

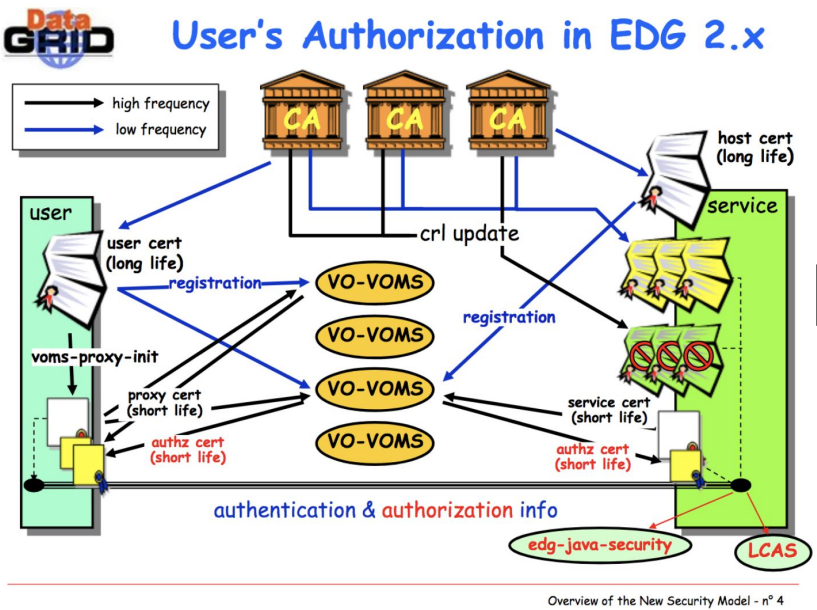


Oltre X.509

AAI futura, basata sui token



Evoluzione dell'AAI oltre X.509



Per accedere alle risorse di calcolo e di archiviazione della comunità, gli utenti utilizzano un **proxy VOMS**

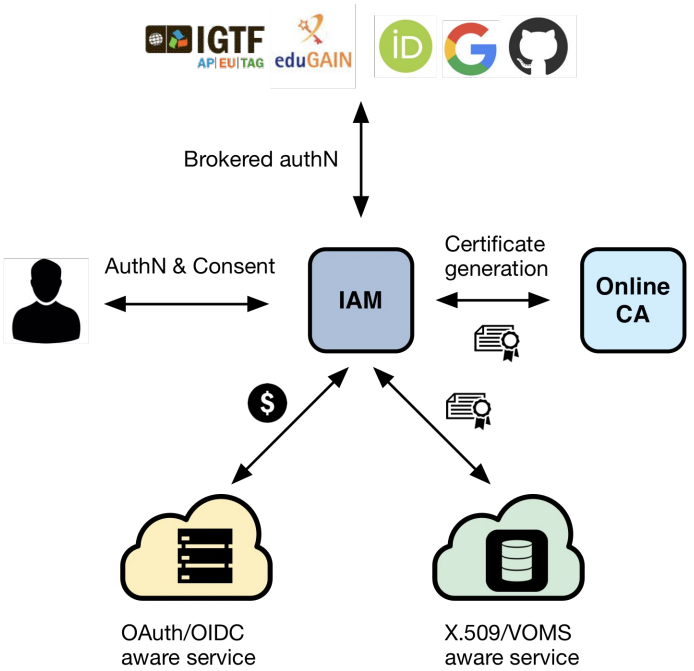
Un proxy VOMS fornisce informazioni su chi siete, per quale Organizzazione Virtuale (VO) state agendo e cosa potete fare sull'infrastruttura (es. gruppi e ruoli VOMS)

Evoluzione dell'AAI oltre X.509

Nel prossimo futuro utilizzeremo i **token**, che forniranno più o meno le stesse informazioni

I token sono ottenuti da un VO token issuer (es. INDIGO IAM) utilizzando gli scambi di messaggi (alias flussi) del protocollo **OAuth/OpenID Connect**

I token vengono inviati a servizi/risorse seguendo le raccomandazioni di **OAuth**

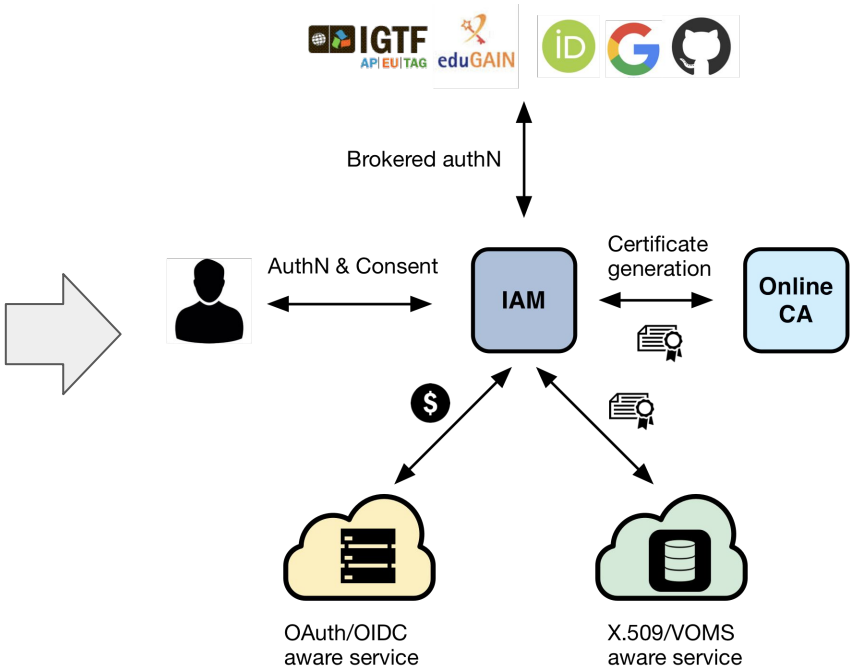


Evoluzione dell'AAI oltre X.509

L'**autorizzazione** viene **eseguita presso i servizi** sfruttando le informazioni estratte dal token:

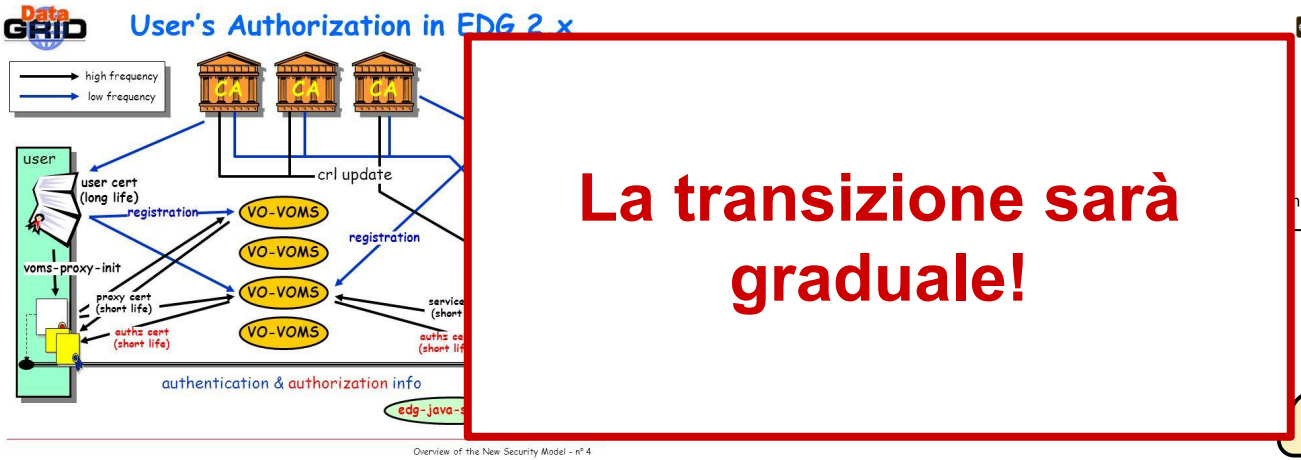
- **Attributi di identità**: ad es. gruppi
- **Scope OAuth**: capacità collegate agli access token al momento della loro creazione

I servizi possono quindi concedere o negare l'accesso alle funzionalità in base a queste informazioni



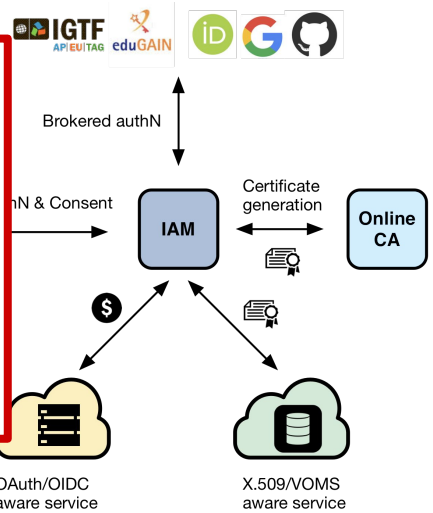
Evoluzione dell'AAI oltre X.509

AAI attuale, basata su X.509



La transizione sarà graduale!

AAI futura, basata sui token



INDIGO IAM

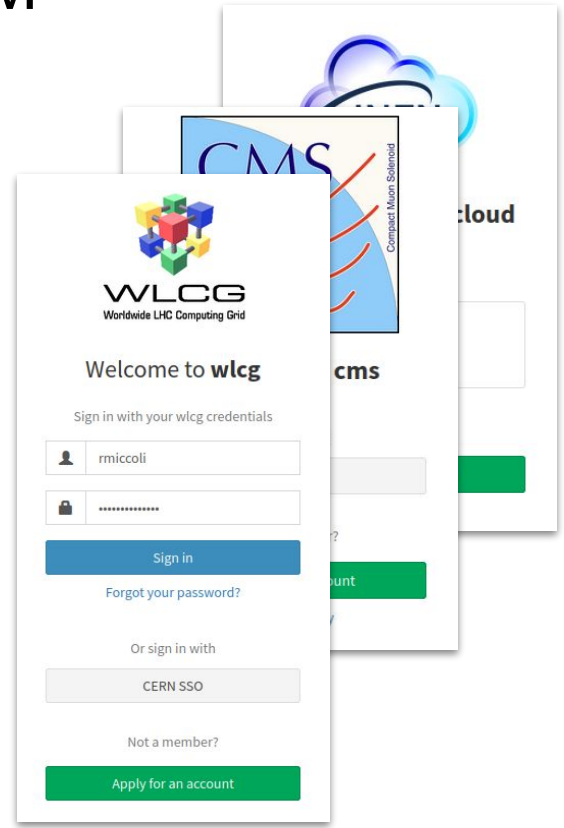
- Servizio di autenticazione e autorizzazione centrale a scala comunitaria
  - IAM sta per *Identity and Access Management*
- Supporta **più meccanismi di autenticazione**
  - Username/password, X.509, Google, Github, federazioni di identità (eduGAIN), ecc.
- Fornisce agli utenti un **identificatore persistente**
- Espone le informazioni sull'identità, gli attributi e le capacità ai servizi tramite **token JWT** e i protocolli standard **OAuth** e **OpenID Connect**
- Supporta l'**accesso Web** e **non Web**, la **delega** e il **rinnovo dei token**
- Supporta l'**account linking**

Modello di implementazione di IAM

Un'istanza IAM viene distribuita per una **comunità di utenti** (VO) che condividono risorse

Le applicazioni e i servizi client sono integrati con questa istanza tramite standard **OAuth/OpenID Connect**

La pagina di login di IAM può essere personalizzata per includere il **logo** della comunità, l'**AUP** e l'**informativa sulla privacy**



WLCG IAM instance

Tecnologie

- **OAuth 2.0**
  - un framework standard per l'autorizzazione delegata
  - ampiamente adottato nel mondo dell’industria
- **OpenID Connect**
  - un livello di identità standard costruito sulla base di OAuth2
  - informazioni su chi è l'utente e come è stato autenticato
  - offre la possibilità di stabilire sessioni di login (SSO)
- **JSON Web Tokens (JWTs)**
  - uno standard aperto che definisce un mezzo compatto e sicuro dal punto di vista degli URL per rappresentare i “claim” da trasferire tra due (o più) parti
  - i token sono stringhe di dati codificati, emessi da un emittente con cui il client (ricevitore) ha un rapporto di fiducia

Access token (decoded):


```
{
  "sub": "8b7b42fd-0e42-43c5-8254-729aa8f6a12d",
  "iss": "https://iam-dev.cloud.cnaf.infn.it/",
  "name": "Admin User",
  "exp": 1710503088,
  "iat": 1710499488,
  "jti": "04d6af17-a1b5-40c8-81e8-5474fb42bb9c",
  "client_id": "42999a63-7449-43fb-952e-42f2d75b865b",
  "groups": [
        "dev",
        "test.vo"
  ],
  "scopes": "openid profile"
}
```

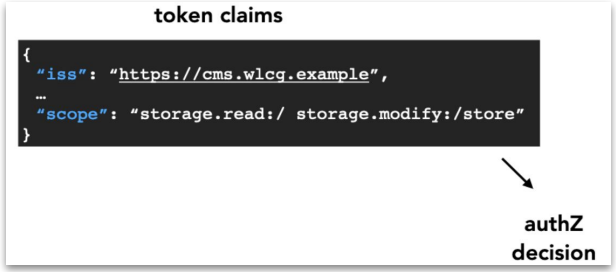
Autorizzazione

Autorizzazione basata sull'identità

- il token contiene informazioni sugli **attributi relativi all'utente** (ad es., gruppi/ruoli)
- il servizio mappa questi attributi in una **politica di autorizzazione locale**

Autorizzazione basata sugli scope

- il token contiene informazioni su quali **azioni devono essere autorizzate** presso un servizio
- il servizio deve **comprendere questi privilegi** e **rispettarli**
- la politica di autorizzazione è **gestita a livello di VO**

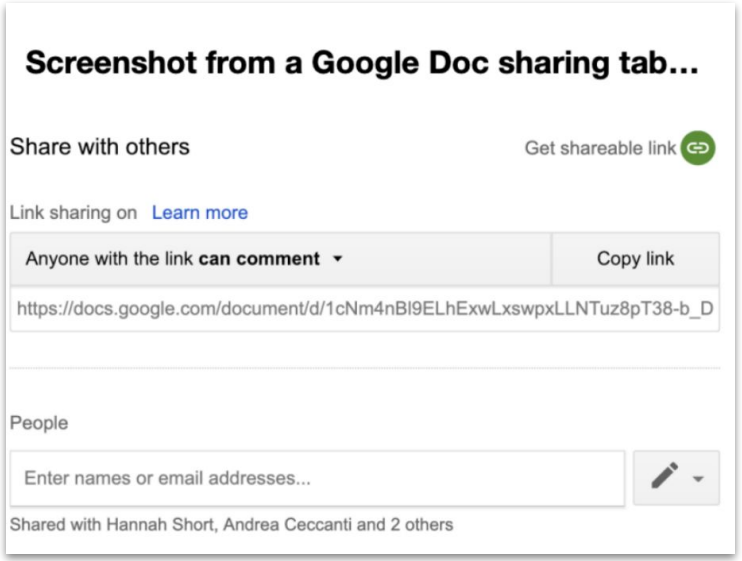


Autorizzazione

I due modelli possono coesistere, anche nel contesto della stessa applicazione!

AuthZ basata sugli scope →

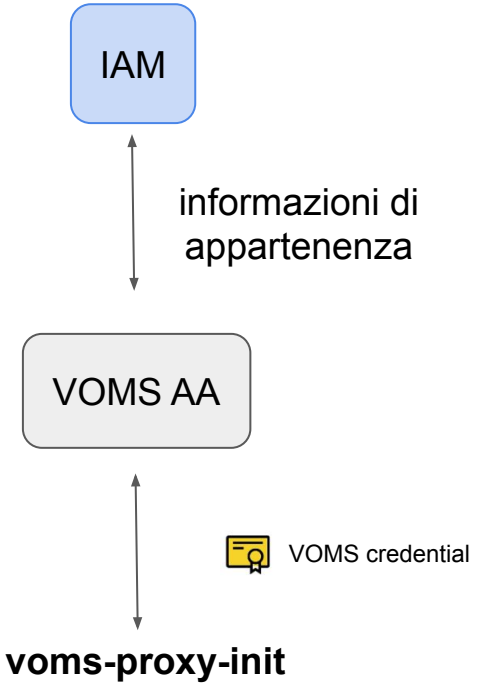
AuthZ basata sull'identità →



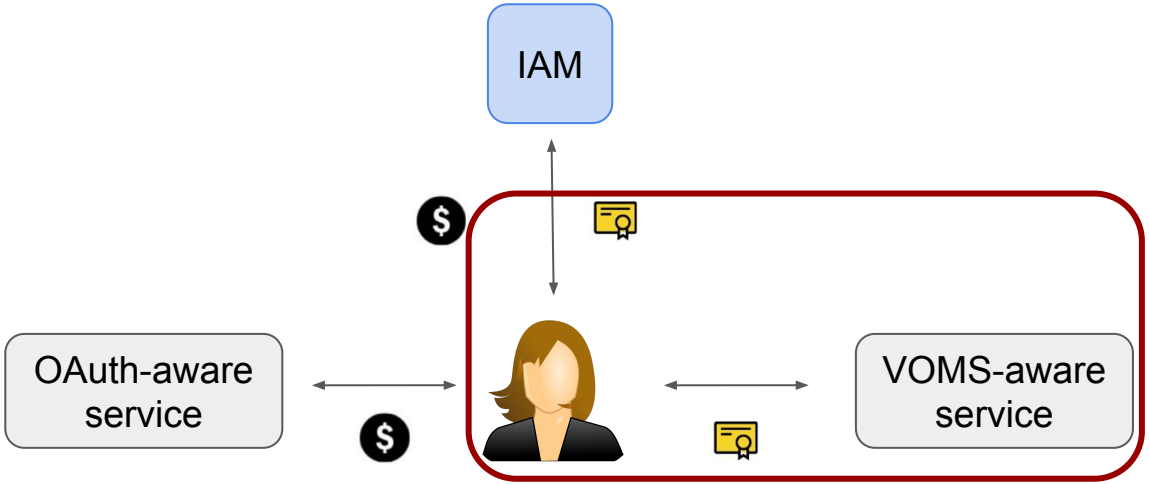
Transizione graduale oltre X.509

IAM include un micro servizio di autorità di attributi VOMS (VOMS AA) che può codificare le informazioni di appartenenza a IAM in un **certificato di attributi VOMS standard**

VOMS AA può rilasciare credenziali VOMS (`voms-proxy-init`) comprese dai client esistenti



Transizione graduale oltre X.509



Approvvigionamento VOMS compatibile con i client esistenti

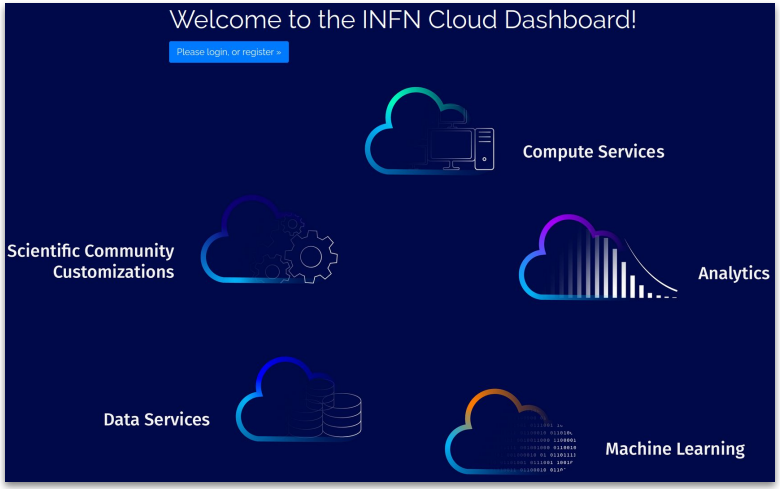
JWT access token

INFN Cloud

- L'INFN offre ai suoi utenti una serie completa e integrata di servizi Cloud attraverso la sua **infrastruttura dedicata INFN Cloud**
- Il **portfolio di INFN Cloud**, disponibile tramite un'interfaccia web di facile utilizzo, è definito sulla base di chiare esigenze degli utenti
  - si basa su **soluzioni composte** e **open source** e può essere facilmente esteso dal team di supporto INFN Cloud o direttamente dagli utenti finali

https://my.cloud.infn.it/home/login

INFN Cloud



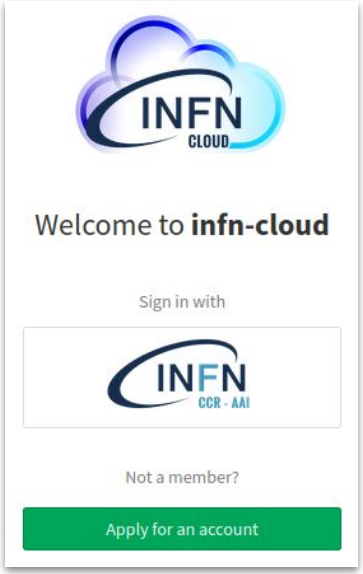
- I **servizi di INFN Cloud** sono basati su componenti modulari e abbracciano i modelli **IaaS**, **PaaS** e **SaaS** sia per l'elaborazione che per i dati
- Tutti i servizi sono descritti da **modelli TOSCA**
- I servizi possono essere distribuiti tramite la **dashboard di INFN Cloud** o tramite linea di comando

INFN Cloud

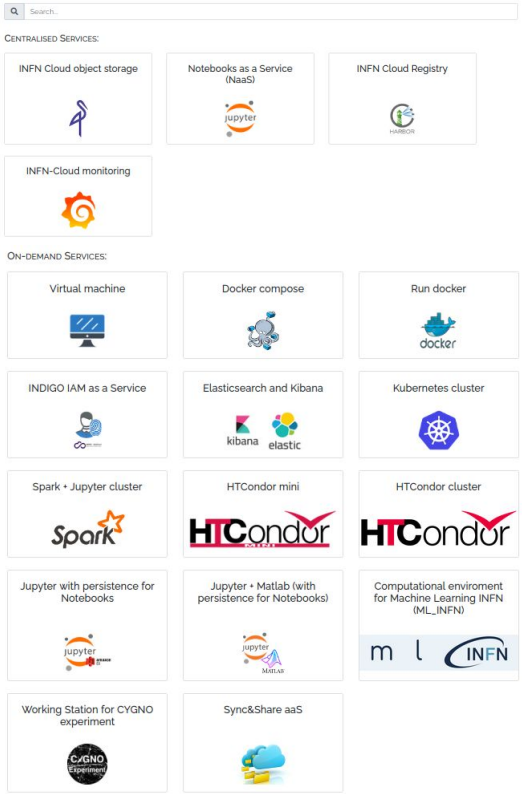
- Si basa su una dorsale centrale che collega i grandi data center del CNAF e di Bari, e su diversi siti federati che si collegano alla dorsale
- In caso di accordi speciali, può essere estesa in modo trasparente ad altri fornitori Cloud pubblici o privati per aumentare la sua capacità o le sue soluzioni
- L'**accesso ai servizi Cloud** dell'INFN è attualmente **riservato al personale dell'INFN** o al personale con cui l'INFN ha stabilito collaborazioni formali, come ad esempio gli associati di ricerca

INFN Cloud

L'**autenticazione** e l'**autorizzazione** per l'accesso a tutti i servizi del Cloud dell'INFN sono garantite dalla soluzione federata **INDIGO IAM**, pienamente conforme agli standard European Open Science Cloud (EOSC) e agli standard del settore



INFN Cloud dashboard



Grazie per l’attenzione!

Link utili

Codice IAM su GitHub: https://github.com/indigo-iam/iam

Documentazione IAM: https://indigo-iam.github.io/docs

Informazioni generali:

- OAuth 2.0: https://oauth.net/2/ e OAuth 2.1: https://oauth.net/2.1/
- OpenID Connect: https://openid.net/connect/
- JSON Web Token: https://www.rfc-editor.org/rfc/rfc7519
- OpenID Connect Federation: https://openid.net/specs/openid-connect-federation-1_0.html

Contatti:

- iam-support@lists.infn.it