

# INFN-AAI

---

Il progetto di infrastruttura AAI dell' INFN

# Agenda

---

- Perché INFN-AAI
- Le fasi del progetto INFN-AAI
- Dove siamo oggi
- Cosa possiamo fare insieme

# Perché INFN-AAI

---

- AAI di sede
  - Una analisi dei Sistemi di Autenticazione ed Autorizzazione usati nelle varie sedi INFN, mostra una situazione estremamente diversificata
    - Praticamente tutti i Sistemi noti sono in uso
    - Praticamente nessuna sede ha di fatto una AAI (le poche “quasi-AAI” non sono usate per TUTTI i servizi)
- INFN-AAI
  - L’integrazione delle AAI di sede in una unica Infrastruttura nazionale, fornisce inoltre il supporto per applicazioni centralizzate, sia a livello nazionale che inter-sede (o per esperimento o gruppo)

# I requisiti

---

- Viene da sé, che una volta che basiamo su un unico sistema il funzionamento della Autenticazione e della Autorizzazione, diventano estremamente importanti due caratteristiche del sistema:
  - Affidabilità: il sistema deve poter garantire la coerenza dei dati
  - Disponibilità: i dati necessari per le operazioni di Autenticazione ed Autorizzazione, devono essere sempre disponibili.
  - Standardizzazione: un sistema basato su standard, non legato ad un unico “vendor”.

# I Vincoli

---

- Una delle peculiarità dell'INFN, quella di essere un unico ente ma composto da molte Unità Operative amministrativamente indipendenti, impone vincoli forti, nel momento in cui si inizia a pensare ad infrastrutture unitarie.
  - L'AAI dell'INFN deve poter fornire tutte le funzionalità tipiche di una Infrastruttura di questo tipo
  - L'AAI dell'INFN deve poter garantire l'autonomia “amministrativa” delle varie sedi, pur garantendo la fruibilità dei suoi “servizi” da parte di amministrazioni esterne.

# Le possibili soluzioni

---

- Requisiti e vincoli di questo tipo, sono soddisfatti da due tipi di soluzioni:
- Federazione di AAI
  - Una AAI in ogni sede, senza vincoli di sorta
  - Un sistema di federazione di AAI (Shibboleth)
- Albero di AAI
  - Una AAI in ogni sede, aderente ad un MODELLO COMUNE.
  - Una sovrastruttura unificatrice delle AAI di sede.

# Federazione di AAI

---

- Pro
  - Assoluta indipendenza delle varie sedi
- Contro
  - Complessità di implementazione
  - Richiede molte risorse in ogni sede
  - Fornisce solo Infrastruttura per Web applications (almeno per ora)

# Albero di AAI

---

- Pro

- Disegno, progettazione e definizione del modello comune fatto una volta per tutti i partecipanti
- Ridotto overhead
- Riproduce meglio la struttura logica dell'INFN, e si sposa bene con infrastrutture esistenti (Kerberos5)

- Contro

- Necessità di un coordinamento più stretto

# Le fasi del progetto

---

- “Nell’aria” già da dicembre 2006
  - Tutorial a Febbraio
  - Definito il modello comune
  - Kick-off meeting il 30 maggio
  - Approccio “industriale” (CDR, TDR) iniziato
  - Implementazione entro un paio d’anni

# Il modello comune

---

- Autenticazione Kerberos5
- Autorizzazione via Directory Service LDAP
- Infrastruttura nazionale di “cross-authentication” dei realm Kerberos5
- Directory Servers LDAP nazionali e di sede

# Situazione oggi

---

- CDR in fase di scrittura
- Verifica di alcuni aspetti importanti per la definizione dell'architettura dell'albero LDAP
  - Definizione del DIT per una migliore interoperabilità con Windows AD
  - Valutazione approfondita dei due modelli implementativi del Directory Service nazionale (centralizzato VS distribuito)
- In altre parole, oggi non possiamo fornire un insieme di specifiche per l'utilizzo della INFN-AAI (non esiste ancora) ma...

# Collaborazione

---

- E' sicuramente importante che nuove esigenze (come appunto gli strumenti di collaborazione per un esperimento, o proto-esperimento) tengano in conto che sta nascendo la INFN-AAI, e quindi non prendano direzioni incompatibili con quello che stiamo facendo (grazie a Mauro per questo meeting)
- INFN-AAI tenga in adeguata considerazione le esigenze dei nascenti gruppi, proto-esperimenti e quant'altro, in modo da non escluderli dal possibile utilizzo della nascente AAI