INFN-AAI

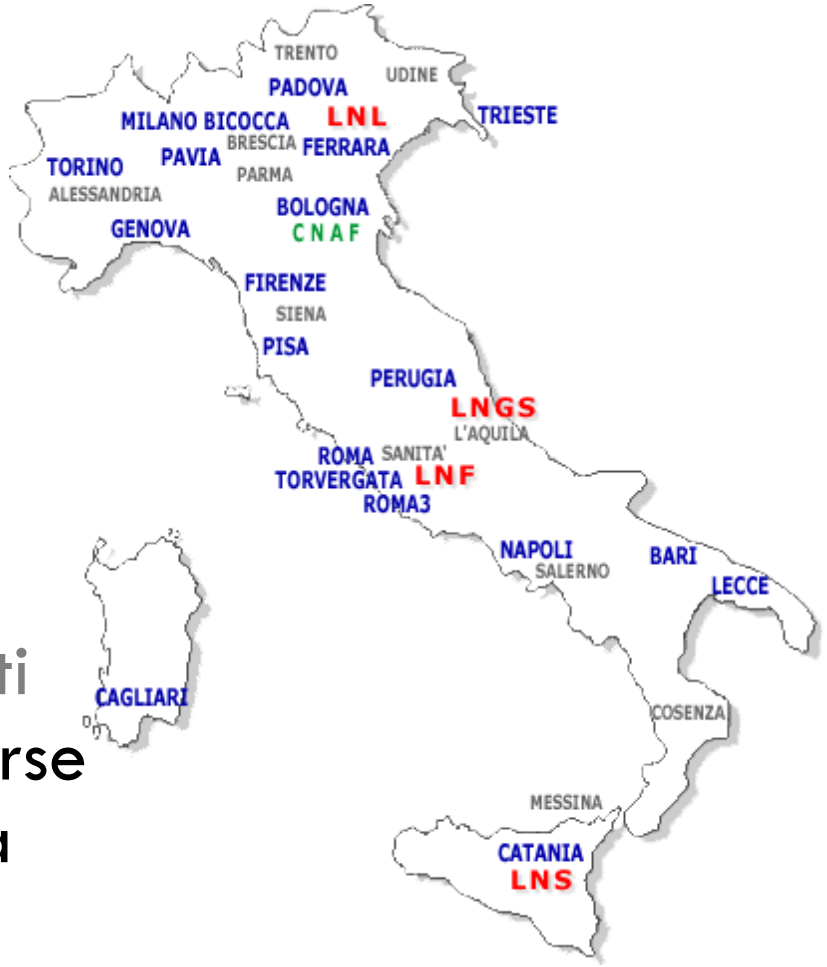
Una infrastruttura per uso amministrativo e scientifico

Agenda

- Presentazione dell'INFN
- Identità Digitali
- Architettura di INFN-AAI
- L'Identity Provider & le web applications
- INFN-AAI & il calcolo scientifico
- INFN-AAI & IDEM
- Prossimi passi

L'Istituto Nazionale di Fisica Nucleare

- Ufficio di Presidenza
- Amministrazione Centrale
- 4 Laboratori Nazionali
- 1 Centro Nazionale
- 19 Sezioni
- 11 Gruppi Collegati
- Sezioni e Gruppi Collegati spesso condividono le risorse con i Dipartimenti di Fisica



Tipologie di Utenti

- Dipendenti
  - Anche in senso lato (Borsisti, Contrattisti, Assegni di Ricerca, ecc. ecc.)
- Associati
  - Tipicamente dipendenti dei Dipartimenti di Fisica, ma non solo (ex dipendenti INFN in quiescenza, Borsisti INFN) che hanno un contratto di associazione con l'INFN
- Ospiti
  - In alcuni casi l'INFN accende contratti assicurativi (tipicamente nei Laboratori Nazionali)
- Visitatori

Scenario AAI pre INFN-AAI

- Ogni Unità Operativa dell'INFN gode di un elevato livello di autonomia
  - Direzione, Ufficio Amministrazione, Ufficio del Personale, Ufficio Acquisti, Servizio Calcolo & Reti, …
- Alla autonomia "amministrativa" è sempre corrisposta una autonomia "operativa"
- ~1 soluzione di AAI per ogni struttura

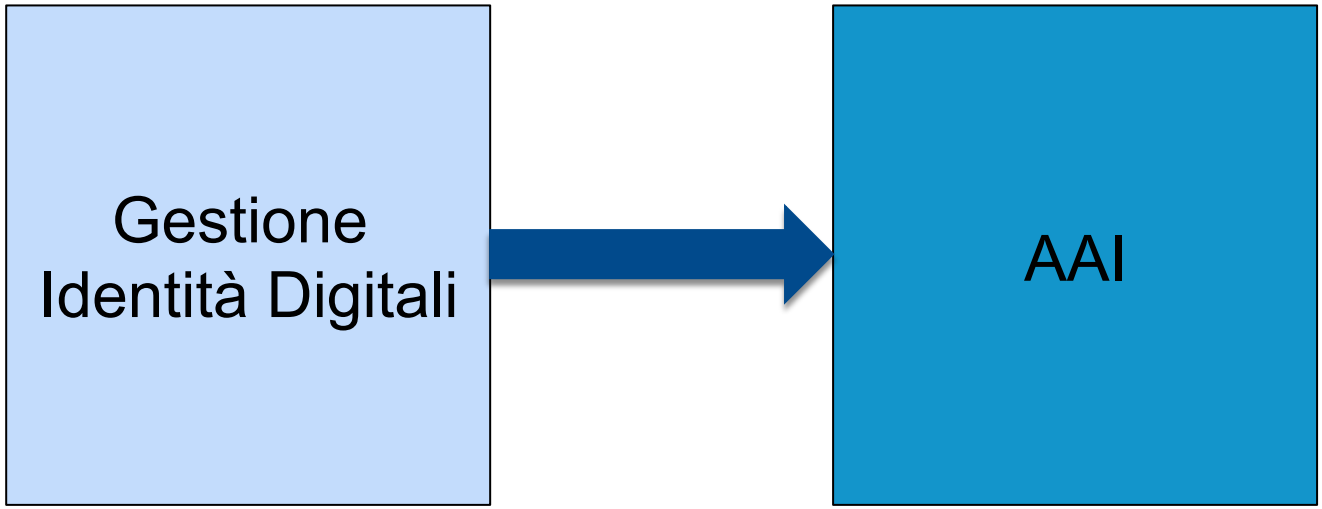
Servizi centralizzati

- Per soddisfare gli adempimenti istituzionali sono stati messi a punto un certo numero di servizi informatizzati accessibili via web, con DB utenti "locale".
- Servizi forniti da strutture differenti (AC, CNAF, LNF) si basano su DB utenti differenti

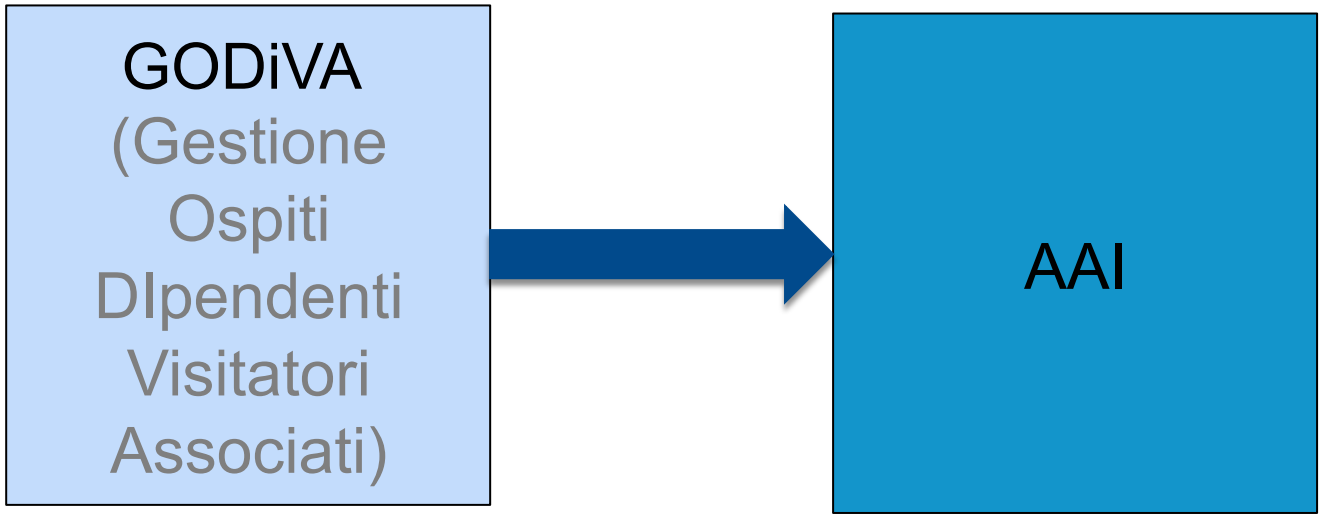
Due strade

- Una federazione di Unità Operative dell'INFN
  - Rispetta le autonomie delle strutture
  - Richiede una corretta gestione della AAI locale in federazione con le altre
- Soluzione unificatrice: INFN-AAI
  - Estensione logica (ed unificazione funzionale) delle AAI dei servizi centralizzati
  - Architetturalmente più elegante
  - Complessa da realizzare specialmente se si vuole garantire impatto minimo, rispetto delle autonomie delle strutture ed HA

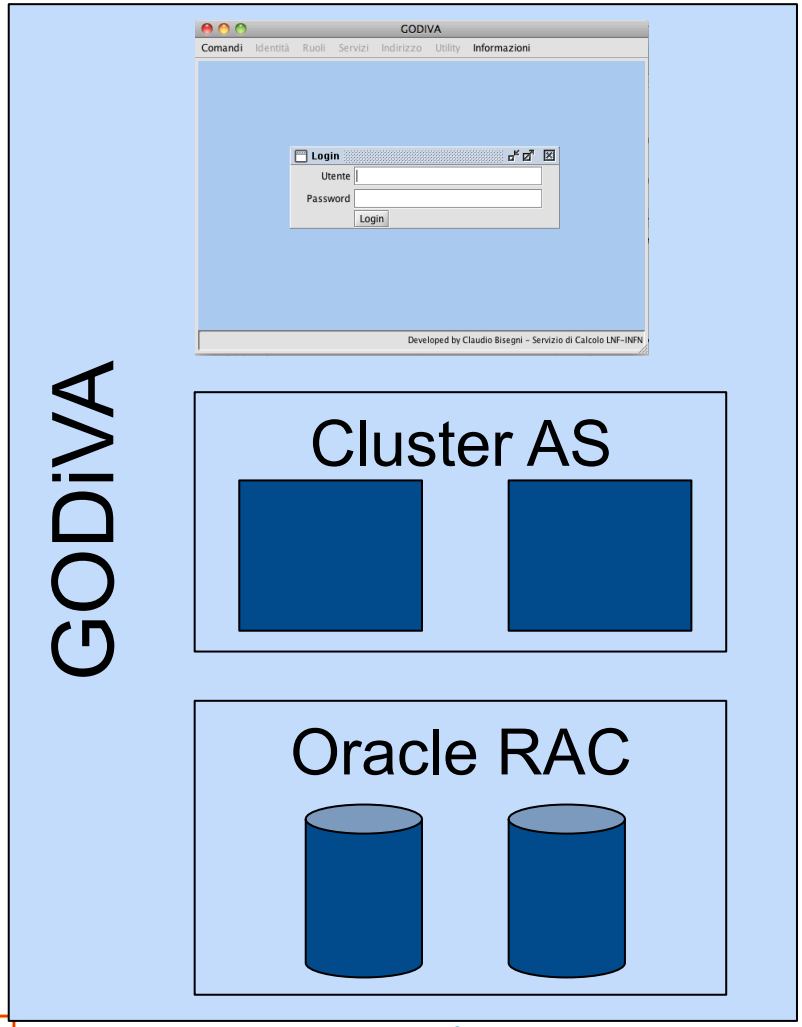
Architettura di INFN-AAI



Architettura di INFN-AAI

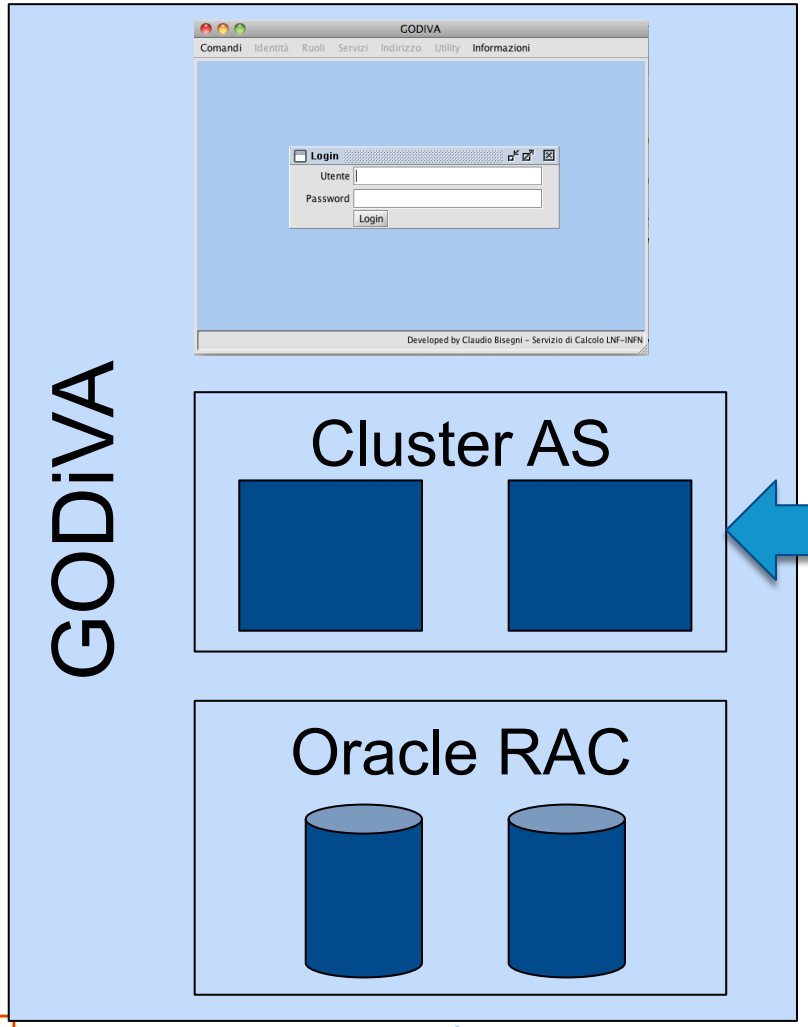


Architettura di INFN-AAI: GODiVA



- Applicazione a 3 livelli
- JAVA GUI & engine
- Cluster di Application Server
- Persistenza in Oracle Real Application Cluster
- Server @LNF
- (Disaster recovery @CNAF)

Architettura di INFN-AAI: GODiVA



- API ad uso delle altre applicazioni centralizzate (principalmente DataWeb)

ID: GODiVA

- Dipendenti
  - Importati direttamente dal sistema dello stipendiale che è autoritativo per questa categoria di utenti
- Associati
  - Gestito dalla web-app delle associazioni nativamente in GODiVA via API
- Ruolo legato al contratto e tenuto aggiornato da un "at-like job"
- Ospiti & Visitatori prossimamente (~gennaio 2012)

Arricchimento ID: GODiVA

- Organigrammi
  - Nell'INFN parallelamente all'organigramma istituzionale viene definito ogni anno un organigramma scientifico (partecipazione ad un esperimento)
  - Alla posizione all'interno di tale organigramma deve corrispondere un livello di privilegi sia di carattere amministrativo (accesso ai sistemi di gestione dei finanziamenti) che di carattere scientifico (accesso alle risorse fisiche o di calcolo)
  - GODiVA realizza tale corrispondenza associando all'ID il percorso nell'albero dell'organigramma:

```
isMemberOf: i:infn:le:csn1:atlas::resp:locale
```

INFN-AAI: Autenticazione

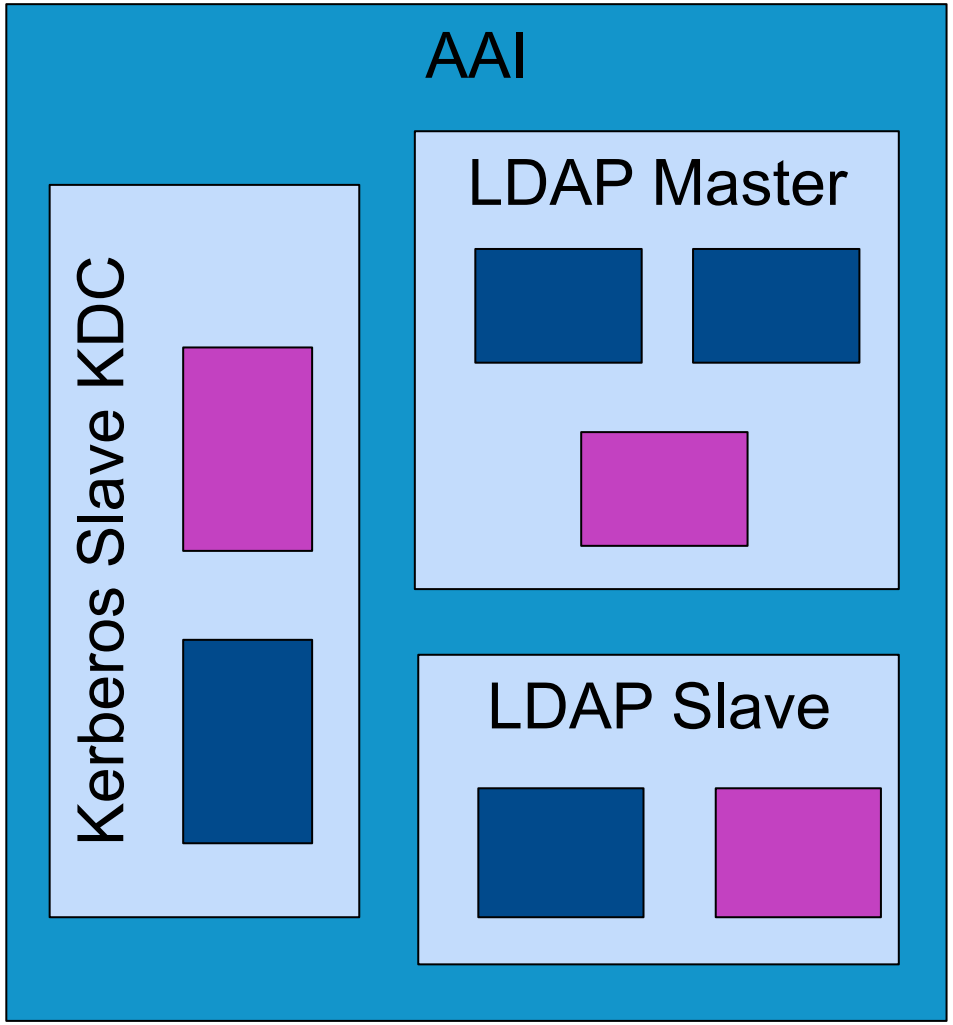
- Kerberos
  - I sistemi di Autenticazione di alcune sedi sono basate su Kerberos e le applicazioni utilizzate non ne possono fare a meno (AFS) la scelta è stata di fatto obbligatoria.
- username/password (anche Kerberos)
- Certificati X.509
- OTP

Architettura di INFN-AAI: AAI "core"

- Server LDAP 389 DS (RedHat Directory Server)
- 3 Server in configurazione MultiMaster
- 2 Server slave
- MultiREALM KDC

@CNAF

@LNF



389 Directory Server

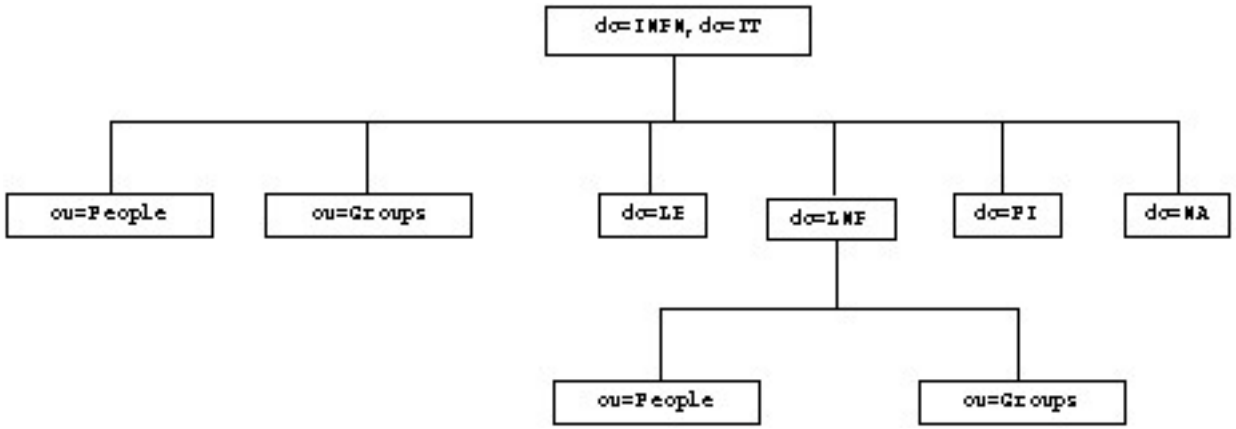
- Enterprise-class
- Multi Master
- Secure authentication and transport (SSLv3, TLSv1, and SASL)
- On-line, zero downtime, LDAP-based update of schema, configuration, management and in-tree Access Control Information (ACIs)
- Pluggable

389 DS Krb5 plug-in

- Per client LDAP kerberos-compliant, l'autenticazione Kerberos avviene attraverso il meccanismo SASL/ GSSAPI
- Per garantire l'accesso anche da client non kerberos-compliant si è sviluppato un plug-in che utilizza le credenziali kerberos trasmesse in un canale SSL

Minimo Impatto

- Dispiegamento graduale nelle varie sedi
  - Funzionalità complete per le sedi che hanno completato la migrazione
- DIT "misto"
  - contiene una parte "nazionale" insieme ai vari rami "locali"



OU=People,DC=infn,DC=IT

- La parte nazionale del DIT contiene le informazioni relative alle identità, arricchite dalle posizioni all'interno degli organigrammi ed informazioni relative all'account di sede

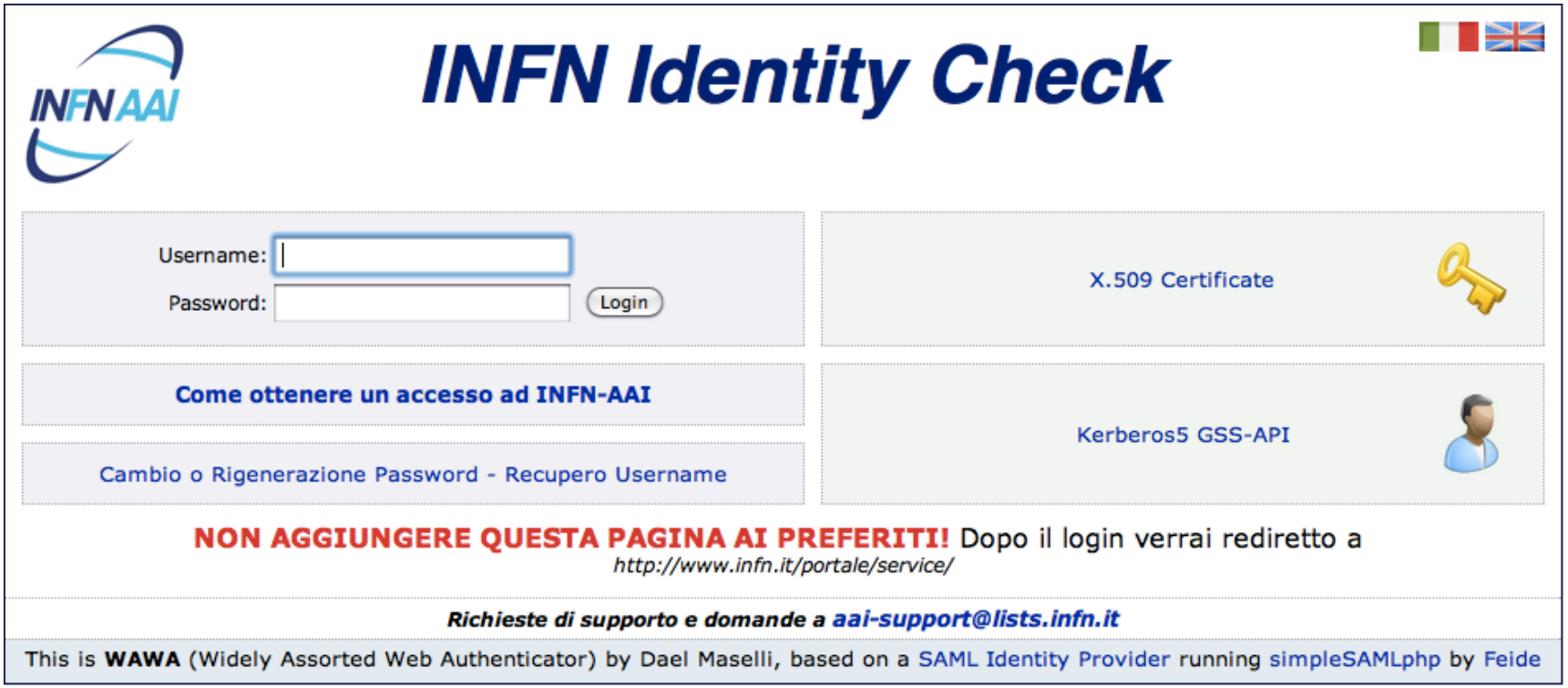
```
# f8d35e28-2532-43c8-989c-3faa58f5cba4, People, infn.it
dn: infnUUID=f8d35e28-2532-43c8-989c-3faa58f5cba4,ou=People,dc=infn,dc=it
uid: enrico
infnKerberosPrincipal: enrico@INFN.IT
mail: Enrico.M.V.Fasanelli@le.infn.it
l: le
eduPersonAffiliation: staff
eduPersonAffiliation: member
telephoneNumber: +39 0832 297442
.....
```

OU=People,DC=le,DC=infn,DC=IT

- La parte locale del DIT contiene le informazioni relative all'account di sede ed informazioni relative all'account nazionale

```
# 020f41f5-913a-425f-bb91-aaea40739ff7, People, le.infn.it
dn: infnUUID=020f41f5-913a-425f-bb91-aaea40739ff7,ou=People,dc=le,dc=infn,dc=it
infnLinkedUUID: f8d35e28-2532-43c8-989c-3faa58f5cba4
uid: enrico
infnKerberosPrincipal: enrico@INFN.IT
mail: Enrico.M.V.Fasanelli@le.infn.it
.....
```

WAWA

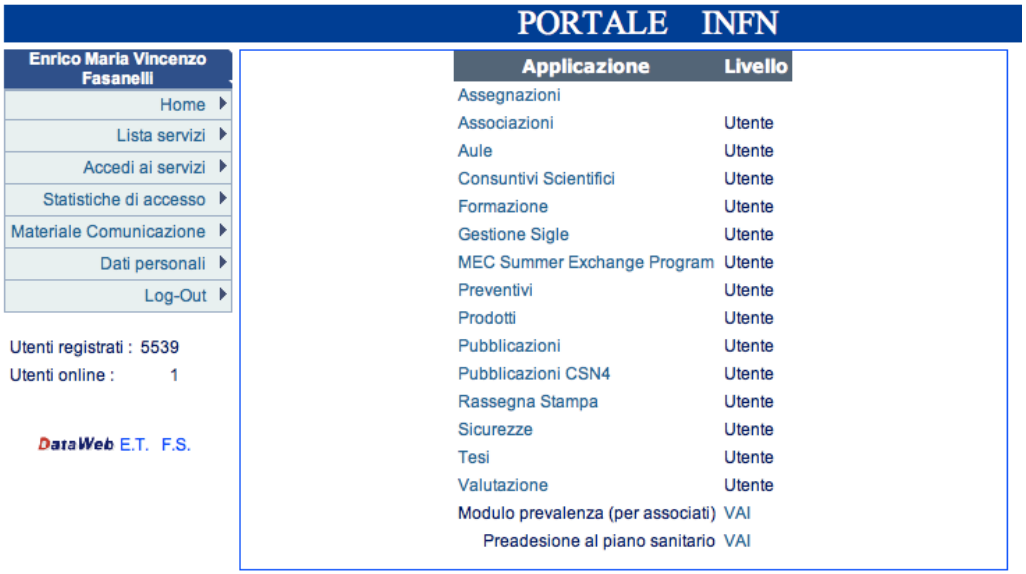

INFN Identity Check
Username:
Password:
Login
X.509 Certificate
Come ottenere un accesso ad INFN-AAI
Kerberos5 GSS-API
Cambio o Rigenerazione Password - Recupero Username
NON AGGIUNGERE QUESTA PAGINA AI PREFERITI! Dopo il login verrai rediretto a
http://www.infn.it/portale/service/
Richieste di supporto e domande a aai-support@lists.infn.it
This is WAWA (Widely Assorted Web Authenticator) by Dael Maselli, based on a SAML Identity Provider running simpleSAMLphp by Feide

WAWA

- SAML (simpeSAMLphp)
- Back-end LDAP (ramo nazionale)
- Kerberos/GSSAPI
  - Entry LDAP via kerberosPrincipal
- OTP (username & MOTP)
- Certificato X.509
  - Entry LDAP via e-mail del certificato

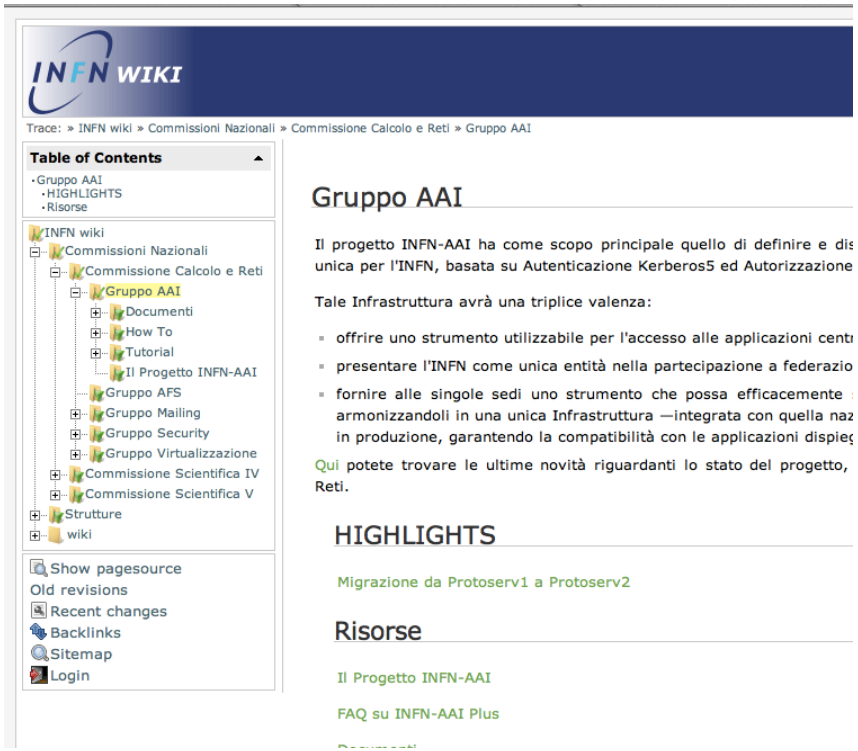
WAWA & Web Applications

- Portale INFN
  - Assegnazioni
  - Associazioni
  - Consuntivi Scientifici
  - Formazione
  - Preventivi
  - Pubblicazioni
  - Rassegna Stampa
  - Sicurezza
  - Tesi



WAWA & Web Applications

- Web Tools
  - Agenda
  - Wiki



WAWA & Web Applications

- Portale del Sistema Informativo
  - Missioni
  - Richieste di Acquisto
  - Report Gestionali
  - Presenze

Calcolo Scientifico

- Il goal di INFN-AAI è quello di consentire l'accesso alle risorse utilizzando le proprie credenziali, indipendentemente dal luogo dove sono collocate le risorse
- Per il calcolo scientifico questo significa in alcuni casi permettere il login interattivo su sistemi UNIX via username/password nazionali (le stesse usate in WAWA)
- Accesso a server opportunamente configurati, garantito dal possesso di "entitlement"
  - assegnato all'identità digitale
  - legato al progetto di ricerca di cui si fa parte ed ereditato in modo automatico dalla posizione nell'organigramma scientifico

thnucui.pi.infn.it

- Facility di calcolo del gruppo nucleare teorico
- Primo esempio di accesso a sistemi interattivi nazionali, utilizzando credenziali rilasciate dalla sede di appartenenza
- Entitlement assegnato direttamente alle Identità Digitali

```
urn:mace:terena.org:schac:UserStatus:it:infn.it
:clusternucleari
```

INFN-AAI & IDEM

- L'INFN ha già aderito ad IDEM e registrato un servizio.
- INFN-AAI ha da poco perfezionato la richiesta la registrazione dell'IdP (certificazione in corso)
- Ad oggi l'IdP INFN garantisce l'autenticazione di Dipendenti ed Associati.

INFN-AAI & IDEM: i prossimi passi

- Conclusione della certificazione dell'IdP ed utilizzo dei servizi in federazione
  - Certificati X.509 forniti da TERENA-TCS
  - GARR-VCONF
- Inclusione di Ospiti e Visitatori in GODiVA ed in INFN-AAI (con relativa revisione del DOPAU)

INFN-AAI & INFN: i prossimi passi

- Dispiegamento di INFN-AAI nelle sedi INFN
  - Accesso ai servizi locali via INFN-AAI
  - Completare la unificazione delle credenziali (Kerberos per tutti)
  - "Addomesticare" le applicazioni all'utilizzo degli entitlements per le autorizzazioni

INFN-AAI

Una infrastruttura per uso amministrativo e scientifico