INFN
Istituto Nazionale
di Fisica Nucleare

DOPAU – V.1.1 del 10 agosto 2011

Documento descrittivo del Processo di Accreditamento degli Utenti dell'Istituto Nazionale di Fisica Nucleare

Le informazioni fornite in questo documento sono accurate alla data del 10 agosto 2011

Indice

Revisioni

Data	Versione	Descrizione modifica	Autore
29 luglio 2011	1.0	Prima Versione Dipendenti ed Associati	Enrico M.V. Fasanelli Silvia Arezzini
10 agosto 2011	1.1	Aggiunta cardinalità utenti Aggiunto l'Indice	Enrico M. V. Fasanelli

Abbreviazioni

INFN	Istituto Nazionale di Fisica Nucleare
IAM	Identity and Access Management
GODiVA	Gestione Ospiti, DIpendenti, Visitatori ed Associati
AC	Amministrazione Centrale
AL	Gruppo collegato di Alessandria
AQ	Gruppo collegato dell'Aquila
BA	Sezione di Bari
BO	Sezione di Bologna
BS	Gruppo collegato di Brescia
CA	Sezione di Cagliari
CNAF	Centro Nazionale per la Ricerca e lo Sviluppo nelle Tecnologie Informatiche e Telematiche
CS	Gruppo collegato di Cosenza
CT	Sezione di Catania
FE	Sezione di Ferrara
FI	Sezione di Firenze
GE	Sezione di Genova
ISS	Gruppo collegato dell'Istituto Superiore di Sanità
LE	Sezione di Lecce
LNF	Laboratorio Nazionale di Frascati
LNGS	Laboratorio Nazionale del Gran Sasso
LNL	Laboratorio Nazionale di Legnaro
LNS	Laboratorio Nazionale del Sud
ME	Gruppo collegato di Messina
MI	Sezione di Milano
MIB	Sezione di Milano Bicocca
NA	Sezione di Napoli
PD	Sezione di Padova
PV	Sezione di Pavia
PG	Sezione di Perugia
PI	Sezione di Pisa
PR	Gruppo collegato di Parma
PRESID	Ufficio di Presidenza
ROMA1	Sezione di Roma
ROMA2	Sezione di Roma Tor Vergata
ROMA3	Sezione di Roma Tre
SA	Gruppo collegato di Salerno
SI	Gruppo collegato di Siena
TO	Sezione di Torino
TN	Gruppo collegato di Trento
TS	Sezione di Trieste
UD	Gruppo collegato di Udine

INFN
Istituto Nazionale
di Fisica Nucleare

Introduzione

L' Istituto Nazionale di Fisica Nucleare (INFN) conta 27 "Unità Organizzative" (20 Sezioni, 4 Laboratori Nazionali, 1 Centro Nazionale per la Ricerca e lo Sviluppo nelle Tecnologie Informatiche e Telematiche, 1' Ufficio di Presidenza e l'Amministrazione Centrale) che godono tutte di una elevata autonomia amministrativa. È inoltre presente in 11 sedi universitarie con i cosiddetti "gruppi collegati" (strutture che non hanno autonomia amministrativa, ma dipendono da altre sezioni o laboratori) per un totale di 38 sedi o punti di presenza in Italia.

Questa notevole parcellizzazione e le autonomie esistenti hanno fatto sì che la gestione delle Identità Digitali sia stata affrontata in modo unitario solo di recente all'interno del progetto INFN-AAI, che ha come scopo quello di fornire agli utenti dell'INFN un unico sistema di Autenticazione ed Autorizzazione valido sia per l'accesso ai servizi informatici delle sedi che a quelli nazionali nonché per l'accesso ai servizi federati attraverso le varie federazioni come ad esempio GARR-IDEM.

Per poter raggiungere il suo scopo, il progetto INFN-AAI ha dovuto affrontare le varie problematiche relative alla gestione delle Identità Digitali e le ha risolte producendo un Sistema Unificato per la Gestione delle Identità e dei Privilegi di Accesso (IAM o Identity and Access Management System).

Questo Sistema permette di gestire le Identità e gli attributi legati ai diritti di accesso (sia a servizi informatici che a strutture fisiche) per le quattro tipologie di utenti presenti nell'INFN (Dipendenti, Associati, Ospiti e Visitatori) ed è in produzione da circa un anno (esattamente dal 19 Agosto 2010) per due tipi di utenti: Dipendenti ed Associati. E' ancora in fase di sviluppo anche se in uno stato di avanzamento molto vicino al rilascio in produzione, per quello che riguarda la parte relativa alla gestione di Ospiti e Visitatori.

Non essendo ancora in produzione la gestione delle Identità Digitali di Ospiti e Visitatori, in questo documento verranno descritte le modalità di Accreditamento dei soli utenti gestiti attualmente: Dipendenti ed Associati INFN (sarà nostra cura produrre una versione aggiornata di questo DOPAU non appena sarà modificata la base di utenza gestita).

Gestore dell'accreditamento

Come anticipato gli utenti dell'INFN sono classificati in quattro categorie (Dipendenti, Associati, Ospiti e Visitatori) che si distinguono per la posizione giuridica dell'utente nei riguardi dell'INFN. In ognuna delle 27 sedi è presente personale dedicato all'identificazione ed alla registrazione di tutto il personale afferente alla sede stessa.

Per l'identificazione, non è previsto un ufficio ma una funzione che può venire assolta dall'Ufficio del Personale, dalle segreterie di Direzione, dal servizio Calcolo e Reti, in certi casi addirittura dalla guardiania (addirittura, nella stessa sede, possono esservi differenti uffici a seconda della categoria di utenti da identificare).

E' però certo che l'accesso di un qualunque utente, a qualsiasi titolo, nell'INFN viene registrato in maniera tale da permettere all'utente stesso di vedersi attribuita una identità digitale INFN univoca a livello di ente.

In particolare, per i Dipendenti e gli Associati, l'accreditamento e la verifica dell'identità viene effettuata di norma, rispettivamente dall'Ufficio del Personale e dall'ufficio di Direzione di ogni sede. Gli Ospiti sono invece accreditati presso gli Uffici Personale Esterno, mentre i Visitatori sono normalmente accreditati dal personale delle guardianie che controllano anche l'accesso fisico alle strutture (tipicamente ciò avviene nei laboratori) o da uffici dei Dipartimenti Universitari che ospitano la sede INFN (nelle sedi più piccole l'Ufficio del Personale e/o l'Ufficio Personale Esterno in genere coincidono con l'Ufficio di Presidenza).

Utenti gestiti

Il sistema di Gestione delle Identità Digitali dell'INFN è disegnato per garantire la gestione delle identità delle quattro categorie di utenti presenti nell'INFN: Dipendenti, Associati Ospiti e Visitatori.

Attualmente GODiVA (da Gestione Ospiti, DIpendenti, Visitatori ed Associati) è in produzione limitatamente alla gestione delle Identità Digitali dei soli Dipendenti ed Associati. Di conseguenza anche le funzionalità di Autenticazione e supporto per l'Autorizzazione di INFN-AAI sono limitate a queste due categorie di utenti.

La gestione delle Identità Digitali di Ospiti e Visitatori, in via di completamento, sarà messa in produzione nei prossimi mesi e sarà accompagnata da una versione aggiornata di questo DOPAU che comprenderà quindi anche la descrizione dei Processi di Accreditamento delle altre categorie di utenti.

Dipendenti INFN ed **Associati INFN** sono da considerarsi Staff. Entrambi godono di uno stato contrattuale ben definito nei confronti dell'INFN. Per i primi esiste un rapporto di lavoro (o comunque uno stato che prevede l'erogazione mensile di emolumenti o assimilabili). Per i secondi il rapporto contrattuale prevede l'utilizzo di risorse dell'ente, alla pari dei Dipendenti, in cambio di collaborazione nelle attività dell'Ente.

A titolo di esempio, di seguito sono riportate le tipologie di contratti in essere per Dipendenti INFN ed Associati INFN.

Dipendenti INFN

Personale Ricercatore, (Livelli I-III)
Personale Tecnologo (Livelli I-III)
Personale Collaboratore Tecnico degli Enti di Ricerca CTER (Livelli IV-VI))
Personale Operatore Tecnico degli Enti di Ricerca OTER (Livelli VII-X)
Personale Collaboratore di Amministrazione (Livelli IV-VII)
Personale Operatore di Amministrazione (Livelli VIII-X)
Personale a contratto (co.co.co, art. 2222, ecc. ecc.)
Assegnisti di Ricerca
Borsisti

Tabella 1: Tipologie di contratto per Dipendenti

Associati INFN

Scientifica Ricercatori/Professori Università	Tecnologica Contratti a tempo determinato 19
Scientifica Professori a Contratto	Tecnologica Ricercatori/Professori università
Scientifica Dipendenti altri enti	Tecnologica Professori a Contratto
Scientifica Istituti secondari	Tecnologica Altri Enti (laurea o diploma universitario)
Scientifica Enti stranieri (FAI)	Tecnologica Laurea Magistrale

Scientifica Enti stranieri	Tecnologica Borse INFN
Scientifica Consorzi Ricerca	Tecnologica Dottorandi, Borse non INFN e assegni
Scientifica Laureandi Magistrali	Tecnologica Borse Private
Scientifica Borse INFN	Tecnologica Consorzi ricerca
Scientifica Dottorandi, Borse non INFN e Assegni	Tecnologica Personale E.P.
Scientifica Borse Private	Borsisti INFN per Estero
Scientifica Specializzazione Fisica Sanitaria	Incarico di Collaborazione Tecnica
Scientifica Contratti a tempo determinato 19	Incarico di Ricerca attribuito dal Presidente
Scientifica Personale E.P.	Incarico di Ricerca scientifica
Scientifica Senior	Incarico di Ricerca tecnologica
Scientifica Master	Associazione Tecnica
Scientifica attribuita dal Presidente	Associazione Tecnica Senior

Tabella 2: Tipologie di contratto per Associati INFN

Mappatura degli utenti sulle affiliazioni IDEM

Per gli utenti che appartengono alle categorie "Dipendenti INFN" o "Associati INFN" l'affiliazione IDEM è quella tipica di utenti strutturati ossia:

```
eduPersonAffiliation: staff
eduPersonAffiliation: member
```

Cardinalità degli utenti gestiti

Il numero di Dipendenti INFN e quello di Associati INFN non varia sensibilmente nel corso degli anni, anche se ci possono essere delle piccole variazioni all'inizio dell'anno solare, periodo in cui si effettuano le nuove associazioni.

Alla data di scrittura di questo documento, il numero totale di utenti gestiti (somma di Dipendenti ed Associati) è pari a 5745.

Visione di insieme del processo di accreditamento degli utenti

Il Processo di Accreditamento degli Utenti si basa interamente sul sistema GODiVA attraverso il quale vengono gestite tutte le informazioni presenti nel DataBase Unificato (GODiVA-DB) che è il database autoritativo per le informazioni riguardanti gli Associati INFN e che prende le informazioni relative ai Dipendenti, direttamente dal relativo database autoritativo. Le informazioni presenti nel GODiVA-DB sono riportate anche in modo automatico (sincrono in caso di modifica manuale delle informazioni o attraverso delle operazioni programmate in caso di modifiche che dipendono dalle date (ad esempio la data di scadenza di un contratto) in opportuni attributi LDAP del sistema di Directory centrale dell'INFN che è il cuore dell'infrastruttura di Autenticazione ed Autorizzazione prodotta dal progetto INFN-AAI.

Per ogni Identità Digitale viene definito un Identificativo Universalmente Univoco UUID che rimane assegnato alla persona e che non verrà mai modificato né riassegnato in quanto la sua generazione automatica avviene attraverso le librerie di sistema che garantiscono l'univocità dei valori di UUID calcolati.

Esistono delle piccole differenze procedurali per l'accreditamento delle differenti tipologie di utenti. Nel seguito descriveremo in dettaglio i diversi processi di accreditamento per i Dipendenti INFN ed Associati INFN.

Il processo di accreditamento per i Dipendenti

L'accreditamento dei Dipendenti utilizza le procedure in essere presso la Direzione Affari del Personale dell'Amministrazione Centrale e gli Uffici del Personale delle varie sedi.

Il processo

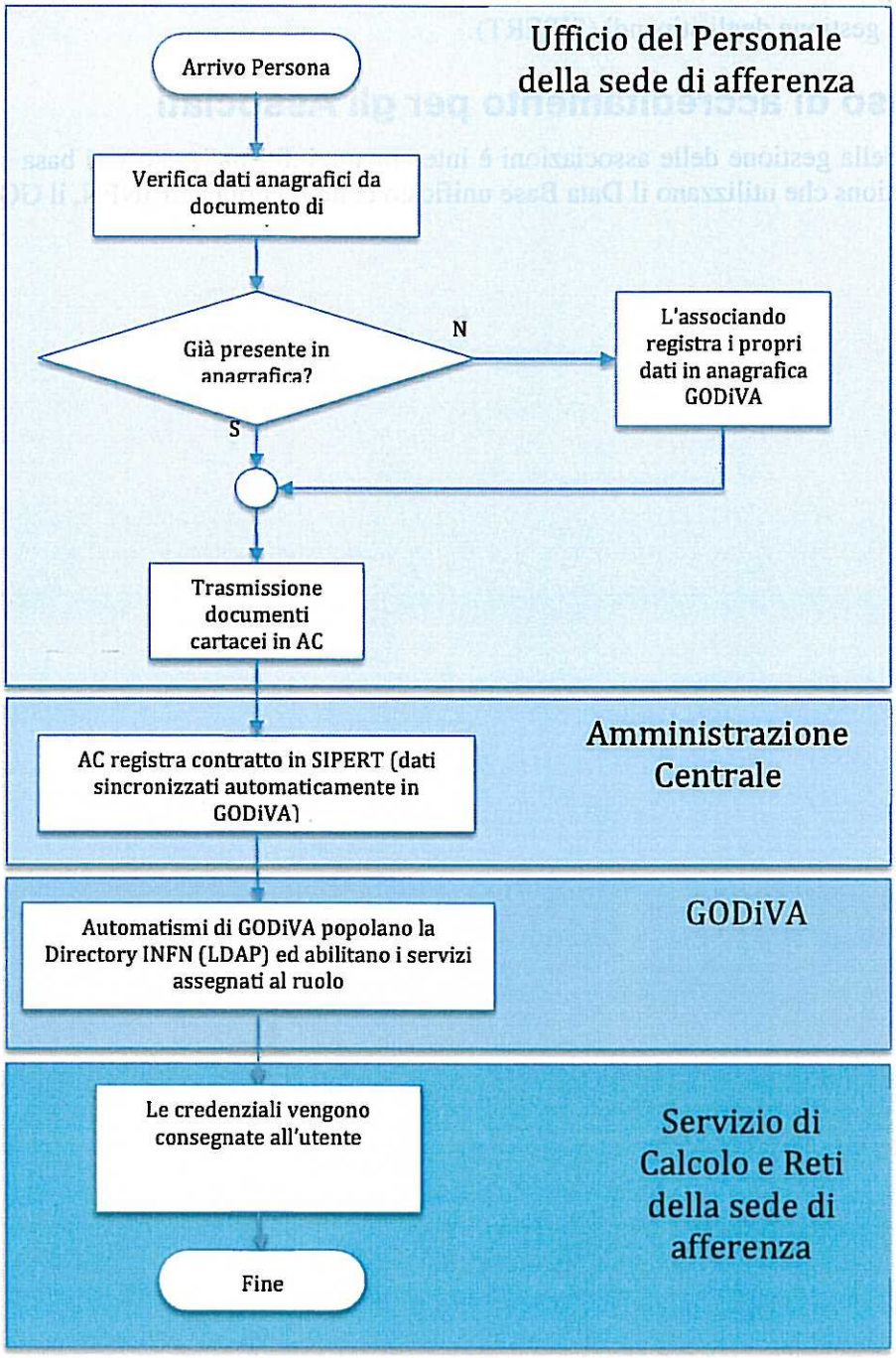

Figura 1: Il Processo di Accreditamento per Dipendenti

Modalità di riconoscimento della persona (Dipendente)

Al momento dell'assunzione il Dipendente deve recarsi presso l'Ufficio del Personale della sede presso la quale dovrà prestare servizio, munito di documento di riconoscimento (oltre alla

documentazione richiesta per perfezionare l'assunzione). La verifica dell'identità viene quindi effettuata "DE VISU" ed i dati del nuovo Dipendente vengono comunicati alla Direzione Affari del Personale dell'Amministrazione Centrale che provvede ad inserirli[1] nel DataBase utilizzato dal sistema per la gestione degli stipendi (SIPERT).

Il processo di accreditamento per gli Associati

Il workflow della gestione delle associazioni è interamente informatizzato e si basa su una serie di Web Applications che utilizzano il Data Base unificato delle Identità nell'INFN, il GODiVA-DB.

[1] L'inserimento dei dati nel DB di SIPERT può avvenire in modalità differenti a seconda che la persona sia stata o meno già censita nell'INFN. Nel caso di una persona già censita (i cui dati anagrafici sono quindi presenti all'interno del GODiVA-DB) i dati vengono presi –previa verifica di congruenza– dal GODiVA-DB. Altrimenti i dati vengono inseriti manualmente e questo processo genera un identificativo universalmente univoco (UUID) che verrà assegnato all'Identità Digitale.
I nuovi dati inseriti nel DB di SIPERT verranno poi importati attraverso procedure automatiche anche nel GODiVA-DB

Il Processo

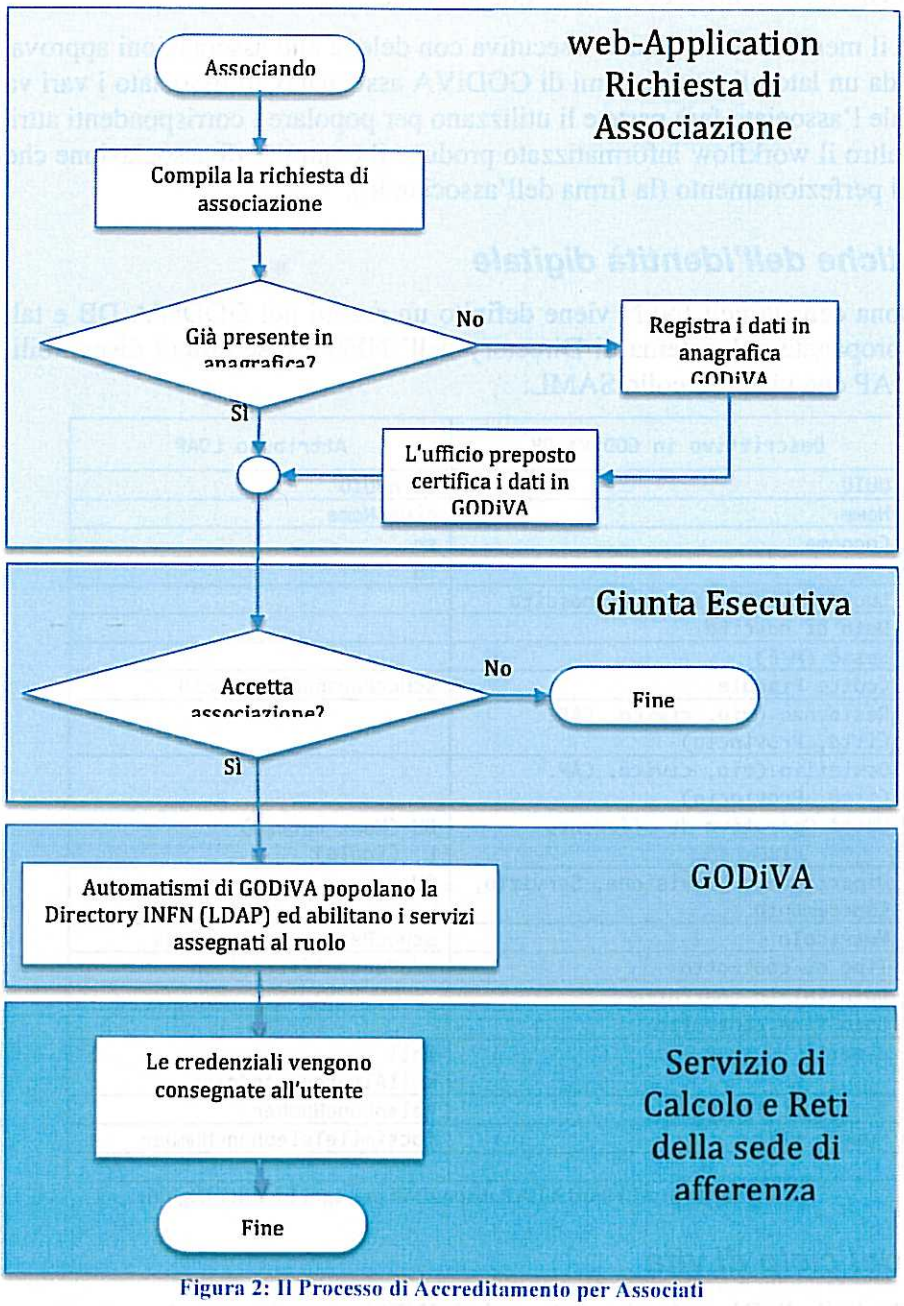

Figura 2: Il Processo di Accreditamento per Associati

Modalità di riconoscimento della persona (Associato)

Al momento della richiesta di associazione, l'associando inserisce i propri dati anagrafici e personali nel GODiVA-DB attraverso la form web di richiesta di associazione (ovvero recupera i propri dati dal GODiVA-DB, se già censito precedentemente).

Un apposito ufficio designato dal Direttore della sede (ad es. la segreteria di Direzione) valida i dati inseriti confrontandoli con un documento di riconoscimento dell'associando ed inoltra la richiesta per il successivo workflow approvativo che passa dal Direttore della Sezione o Laboratorio e dal membro della Giunta Esecutiva con delega alle associazioni.

Una volta che il membro della Giunta Esecutiva con delega alle associazioni approva la richiesta di associazione, da un lato gli automatismi di GODiVA assegnano all'associato i vari valori relativi ai gruppi del quale l'associato farà parte e li utilizzano per popolare i corrispondenti attributi dell'entry LDAP e dall'altro il workflow informatizzato produce il contratto di associazione che viene inviato alla sede per il perfezionamento (la firma dell'associando).

Caratteristiche dell'identità digitale

Per ogni persona censita nell'INFN viene definito un record nel GODiVA-DB e tali informazioni vengono poi propagate nel sistema di Directory dell'INFN e rese quindi disponibili a tutti sia via protocollo LDAP che via protocollo SAML.

Descrittivo in GODiVA-DB	Attributo LDAP
UUID	infnUUID
Nome	givenName
Cognome	sn
	cn
Luogo o Stato estero di nascita	
Data di nascita	
Sesso (M/F)	
Codice Fiscale	schacPersonalUniqueID
Residenza (via, civico, CAP, Città, Provincia)	
Domicilio (via, civico, CAP, Città, Provincia)	
Unità Operativa di afferenza	OU (Nome esteso) L (Sogla)
Dipartimento, Divisione, Servizio, Esperimento	OU
Matricola	schacPersonalUniqueCode
Tipo di contratto	eduPersonAffiliation
Data inizio contratto	
Data fine contratto	
e-mail	mail mailAlternateAddress
Numero di Telefono	telephoneNumber
Numero FAX	facsimileTelephoneNumber

Tabella 3: Attributi LDAP disponibili per ogni Identità Digitale

Gestione del ciclo di vita

Le Identità Digitali di Dipendenti ed Associati INFN sono legate al contratto (di lavoro o di associazione) e gli automatismi del sistema di gestione GODiVA garantiscono che gli attributi associati alle Identità Digitali nel GODiVA-DB ed alle corrispondenti entry in LDAP contengano i valori aggiornati in tempo reale. Questo avviene sia per gli attributi che contengono valori relativi ai ruoli istituzionali (come ad esempio `isMemberOf` o `OU`), che per i valori dell'attributo `eduPersonAffiliation` che contiene i valori dell'affiliazione IDEM.

Alla scadenza del contratto vengono modificati solo i valori degli attributi che definiscono lo stato della persona nei riguardi dell'INFN e viene lasciato inalterato il resto degli attributi dell'Identità Digitale che essendo legati alla persona, rimangono comunque validi.

Non è infatti prevista alcuna cancellazione di Identità Digitali, a meno di richieste esplicite di rimozione dei dati personali dal Data Base effettuate dall'intestatario.

Formato e regole delle credenziali

L'architettura di INFN-AAI prevede che a regime (ossia quando tutte le sedi utilizzeranno l'infrastruttura di Autenticazione Kerberos5) vengano utilizzate sia credenziali Kerberos5 (anche in modalità non nativa, attraverso la coppia kerberosPrincipalName/passwordKerberos) sia certificati X.509. È prevista anche, ma solo in futuro, l'implementazione di un meccanismo basato su coppie username/password-usa-e-getta (One Time Password) i cui dettagli saranno descritti, non appena il meccanismo verrà implementato, in una successiva versione di questo DOPAU.

Nel periodo di transizione oltre alle credenziali sopra elencate, e per le sole sedi che non utilizzano alcuna infrastruttura Kerberos5, viene mantenuto un sistema di autenticazione LDAP basato su coppia username/password.

Kerberos5

Nell'INFN sono in produzione alcune infrastrutture di Autenticazione Kerberos5 (INFN.IT, BA.INFN.IT, LE.INFN.IT, LNF.INFN.IT, LNGS.INFN.IT, MI.INFN.IT, PI.INFN.IT) che sono cross-autenticate tra di loro. Le sedi che non hanno implementato un proprio realm Kerberos5, utilizzeranno (alcune sedi lo utilizzano già) il realm nazionale INFN.IT la cui gestione, legata alla gestione della cella nazionale AFS infn.it, avviene in modalità condivisa attraverso WARC, uno strumento software fornito dal CASPUR (grazie ad un conta tratto di consulenza e collaborazione) atto a permettere la distribuzione dei ruoli di amministratore limitandoli ai principalKerberos di ogni singola sede.

INFN-AAI integra nella propria architettura le infrastrutture Kerberos5 esistenti e di conseguenza le operazioni di gestione delle credenziali Kerberos5 degli utenti sono a cura del singolo Servizio di Calcolo e Reti della sede a cui afferisce l'utente (o direttamente nel caso di realm Kerberos locale o attraverso lo strumento di gestione WARC come appena descritto).

Per poter collegare l'Identità digitale (e quindi la corrispondente entry LDAP) al principal Kerberos5, INFN-AAI ha esteso lo schema LDAP introducendo la Object Class infnPerson descritta in Appendice 1 nella quale è definito anche l'attributo `infnKerberosPrincipal` che contiene il valore del principal Kerberos5 (nel formato username@REALM.NAME) associato all'Identità Digitale[2]

[2] L'architettura di INFN-AAI prevede che ad ogni utente sia associato un unico principal Kerberos, ma per garantire compatibilità con le situazioni esistenti sono temporaneamente gestiti anche i casi in cui ad una Identità Digitale sono associati più principal Kerberos appartenenti a REALM differenti. In questi casi, se correttamente registrati, i principal Kerberos sono tutti contemporaneamente attivi e quindi INFN-AAI garantisce l'autenticazione attraverso uno qualunque di essi.

Certificati X.509 - PKI

Tutti i Dipendenti ed Associati INFN possono ottenere un certificato X.509 rilasciato dalla Autorità di Certificazione dell'INFN (INFN-CA https://security.fi.infn.it/CA) che si basa su una infrastruttura di Autorità di Registrazione (RA) distribuita in tutte le sedi dell'INFN. La INFN-CA rilascia certificati X.509 anche ad utenti non INFN per l'accesso a risorse GRID, ma il possesso di un tale certificato non è condizione sufficiente per essere autenticati attraverso l'infrastruttura di INFN-AAI. È necessario infatti che l'utente sia correttamente registrato all'interno del GODiVA-DB e che quindi esista una entry nell'LDAP di INFN-AAI il cui attributo `mail` (o eventualmente anche `alternateMailAddress`) contenga lo stesso valore contenuto all'interno del certificato X.509 rilasciato dalla INFN-CA.

L'autenticazione attraverso certificato X.509 avviene infatti grazie al mapping effettuato tra i valori dell'attributo `mail` (o `alternateMailAddress`) con il valore di `"email"` dell'`X509v3 Subject Alternative Name` presente nel certificato X.509.

Come tutti i certificati rilasciati dalla INFN-CA anche questi hanno una validità di dodici mesi e possono essere rinnovati direttamente dall'utente finale. Il processo di richiesta di rinnovo del certificato digitale richiede una conferma da parte dell'Autorità di Registrazione della sede a cui afferisce l'utente. La RA verifica che l'utente abbia diritto di ottenere un certificato rilasciato dalla INFN-CA ed ogni 5 anni deve verificare **de visu** l'identità dell'utente e la validità dei documenti presentati.

Username/Password LDAP

Per il solo periodo necessario a completare il dispiegamento di INFN-AAI nelle sedi e per i soli utenti che afferiscono a sedi che non hanno implementato alcun REALM Kerberos5, l'autenticazione in INFN-AAI avviene attraverso coppia username/password gestite attraverso i server LDAP. Queste credenziali sono, per loro natura, valide soltanto per autenticazione effettuata attraverso l'infrastruttura di INFN-AAI e sono gestite attraverso un form WEB con il quale l'utente può modificare o resettare la propria password. La nuova password può essere inserita direttamente dall'utente nel form dopo che il sistema ha verificato l'identità del richiedente attraverso un e-mail inviato all'indirizzo di posta elettronica indicato dall'utente, se tale indirizzo compare nella lista degli indirizzi di posta elettronica registrati in INFN-AAI nella sua entry.

Modalità di consegna delle credenziali

Ad esclusione del caso di coppia username/password LDAP sopra descritto, in cui l'utente gestisce in modo autonomo la modifica ed il recupero (nel senso di nuova impostazione) di credenziali smarrite, la consegna delle credenziali ed il recupero di credenziali smarrite avviene di persona da parte di personale dedicato nelle varie strutture dell'INFN: di norma presso il Servizio di Calcolo e Reti e/o presso gli Uffici del Personale.

Il sistema di autenticazione e autorizzazione interno

La maggior parte dei servizi informatici dell'INFN implementati a livello nazionale utilizzano l'infrastruttura di INFN-AAI per l'Autenticazione e l'Autorizzazione. Sia attraverso il protocollo SAML (INFN-AAI fornisce un Identity Provider SAML2) per i servizi WEB, che attraverso i protocolli Kerberos5 ed LDAP per i servizi non web.

In particolare i servizi WEB interni all'INFN che utilizzano INFN-AAI sono

- WIKI http://wiki.infn.it/
- Agenda http://agenda.infn.it/
- Prenotazione aule http://www.lnf.infn.it/aule
- Il Portale Utenti del Sistema Informativo e del Sistema di Rivelazione Presenze https://portale-sisinfo.infn.it:8888/
- Il portale dellINFN http://www.infn.it/portale/
- I siti di progetti/servizi/esperimenti definiti all'interno del sistema web multi-sito http://web.infn.it/ come ad esempio http://web.infn.it/aai
- I portali per l'accesso ai servizi GRID per i siti
  - applications.eu-decide.eu
  - applications.eumedgrid.eu
  - gisela-gw.ct.infn.it
  - gilda.ct.infn.it
  - gw.ct.infn.it
  - gweather.ct.infn.it
  - gwlib.ct.infn.it
  - indicate-gw.consorzio-cometa.it
  - liferay.ct.infn.it
  - ricevi.ct.infn.it
  - viralgrid.ct.infn.it
  - www.chain-project.eu
  - www.special-project.it

Mentre per quanto riguarda i servizi non-web, è in produzione la login interattiva alla Facility di Calcolo della comunità Nucleare teorica dell'INFN installata presso la sezione di Pisa.

Il sistema assegna ad ogni nuova identità un identificativo univoco di tipo UUID (Universal Unique Identifier version 4) che non viene mai riassegnato, tale identificativo viene utilizzato per calcolare l'attributo *eduPersonTargetedID*. L'attributo *eduPersonPrincipalName* invece viene calcolato concatenando il realm *@infn.it*.

Per alcuni servizi è disponibile la funzionalità di single-sign-on, il time-out può variare in base all'applicazione, da 8 a 24 ore.

Il sistema assegna ad ogni nuova identità un identificativo univoco di tipo UUID (Universal Unique Identifier version 4) che non viene mai riassegnato, tale identificativo viene utilizzato per calcolare l'attributo *eduPersonTargetedID*. L'attributo *eduPersonPrincipalName* invece viene calcolato concatenando il realm *@infn.it* allo username univoco all'interno dell'ente. Tali username vengono assegnati alle nuove identità e non vengono mai eliminate; di conseguenza *eduPersonPrincipalName* è univoco e mai riassegnato.

Per alcuni servizi è disponibile la funzionalità di *single-sign-on*. In caso l'utente non eseguisse autonomamente la procedura di logout logout, il sistema prevede un time-out che può variare in base all'applicazione compreso tra 8 e 24 ore.

Partecipazione ad altre federazioni

L'istituto Nazionale di Fisica Nucleare non partecipa ad altre federazioni.