Centro Elaborazione Dati Amministrativi

SEDE - BOLOGNA

Via P. Gobetti, 101
40129 BOLOGNA
P.I. 06895721006
Cod. Fisc. 97220210583
Ph.: +39 051 6399406 – 6399430
Fax +39 051 6399439
www.ced.inaf.it
Email: ced-staff@inaf.it

Processo Accreditamento Utenti

ISTITUTO NAZIONALE DI ASTROFISICA
(INAF)

Mauro Nanni

25 febbraio 2011

Protocollo: IRA-200-2011

Introduzione

Questo documento descrive le procedure di accreditamento degli utenti dei servizi informatici erogati dall'INAF a livello nazionale attraverso l' "**INAF identity provider**" (IDP-INAF).

Le singole strutture dell'INAF possiedono propri sistemi di accreditamento per l'utilizzo delle risorse di calcolo e dei servizi locali, Il sistema che qui viene descritto si riferisce ad un sistema di accreditamento appositamente predisposto per dare supporto a nuovi servizi a livello nazionale per l'INAF e per partecipare alla federazione **IDEM** del **Garr**.

Il nuovo IDP-INAF e' allestito presso il CED Amministrativo dell'INAF. Il CED e' collocato a Bologna presso l'Istituto di Radioastronomia di Bologna, fornisce supporto alle strutture territoriali per quello che riguarda l'utilizzo dei software amministrativi e di gestione del personale (CSA) e in particolare ospita sui propri server il database del personale, aggiornato settimanalmente a partire dai dati inviati dal Cineca, e l'archivio degli associati mantenuto dagli uffici centrali.

Nel seguito verranno indicati i criteri utilizzati per la gestione dell'utenza, le procedure seguite per l'accreditamento e la gestione delle identità digitali e l'organizzazione generale del servizio.

INAF ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

Centro Elaborazione Dati Amministrativi

SEDE - BOLOGNA

Via P. Gobetti, 101
40129 BOLOGNA
P.I. 06895721006
Cod. Fisc. 97220210583
Ph.: +39 051 6399406 – 6399430
Fax +39 051 6399439
www.ced.inaf.it
Email: ced-staff@inaf.it

Il sistema centralizzato di autenticazione

L'INAF non ha avuto, fino ad ora, un sistema centralizzato di autenticazione. L'occasione offerta dalla nostra partecipazione alla federazione IDEM e' quella di ripensare l'organizzazione dei servizi che richiedono la validazione degli utenti (cedolini stipendiali, accesso alla rete WiFi, alcuni processi di login, pagine web ad accesso ristretto, webmail, etc) per semplificarne l'utilizzo da parte di tutti i colleghi che operano a vario titolo presso l'Ente.

l'**Identity provider dell'INAF** e' basato su un server LDAP su cui saranno registrate le informazioni per l'accreditamento di tutti gli utenti secondo le regole che si vanno a descrivere nei prossimi capitoli. Il server LDAP funge da base di dati per un servizio RADIUS (EDU-Roam) ed un servizio SHIBBOLETH (IDEM) e per altri servizi che si andranno via via ad individuare.

Sull'IDP-INAF sono disponibili applicazioni web per gli utenti (tipicamente per il cambio della password) e per permettere interventi da remoto agli amministratori che operano presso le strutture. Gran parte delle informazioni dell' IDP-INAF verranno acquisite in via automatica dal database dell'anagrafica del personale e quindi si prevede un intervento molto limitato da parte degli amministratori di sistema.

L' infrastruttura di autenticazione sara' disponibile, con le dovute restrizioni, anche ai singoli Istituti/Strutture, ai quali verra' consentito l'accesso al proprio ramo dell'albero LDAP, per riutilizzare le credenziali anche sui sistemi afferenti alle reti locali delle strutture.

Procedura di accreditamento del personale

Il personale dell'INAF o che ne frequenta le strutture e' costituito da:

1 - Personale dipendente a tempo determinato ed indeterminato.(circa 1200)
2 - Collaboratori (Borsisti, Assegnisti, Contrattisti, etc) (circa 300)
3 - Associati e incaricati di ricerca. (circa 200)
4 - Personale in formazione (Laureandi, Dottorandi, PhD, etc) (circa 300)

INAF
ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

Centro Elaborazione Dati Amministrativi

SEDE - BOLOGNA

Via P. Gobetti, 101
40129 BOLOGNA
P.I. 06895721006
Cod. Fisc. 97220210583
Ph.: +39 051 6399406 – 6399430
Fax +39 051 6399439
www.ced.inaf.it
Email: ced-staff@inaf.it

Il personale indicato dalle voci 1-Personale e 2-Collaboratori viene assunto tramite concorso o selezione, ha un rapporto con l'Ente per un periodo lungo e ben definito, e viene gestito dagli uffici centrali e/o periferici che mantengono le informazioni anagrafiche sul sistema CSA del Cineca. Questo personale e' iscritto d'ufficio nel sistema di autenticazione attraverso una procedura automatica che va' a compilare/aggiornare settimanalmente i campi dei record LDAP.

Gli Associati e Incarichi di ricerca (voce 3) sono personale delle Universita' o di altri enti pubblici o privati, nazionali o stranieri che collaborano con INAF su specifici progetti di ricerca. Sono associati anche numerosi ricercatori e tecnici INAF in quiescenza, che hanno mantenuto rapporti di fattiva collaborazione con l'Ente. Per associarsi all'INAF e' necessario sottoporre la richiesta agli organi dirigenti dell'Ente che devono esprimere un parere favorevole. L'associatura ha una durata di 2 anni. Gli associati, provenendo in gran parte da Universita' o Enti di ricerca, potrebbero essere gia' accreditati a IDEM. Gli uffici centrali valuteranno quindi caso per caso se procedere con l'accreditamento sull'IDP-INAF degli Associati e degli "Incarichi di Ricerca".

Il Personale in formazione (voce 4) accede alle strutture ed ai servizi dell'INAF sotto la responsabilita' di un tutor che e' un dipendente a tempo indeterminato o un associato della struttura. Per ora non si ritiene necessario accreditare tutti gli studenti sull'IDP-INAF, in quanto questo non e' richiesto per l'utilizzo dei servizi locali delle strutture (calcolo, posta elettronica, WiFi, biblioteca) e si assume che gli studenti possano accreditarsi ai servizi IDEM presso la propria Universita'. Qualora si rendesse necessario l'accreditamento INAF si procedera' con l'inserimento manuale nel LDAP primario, oppure si puo' prevedere la creazione di LDAP secondari presso le strutture per interrogazioni in cascata.

Nel caso di Dipendenti, Collaboratori ed Associati esiste quindi una procedura definita per il riconoscimento e l'accettazione della persona a cui fa' seguito la registrazione dei dati anagrafici sul sistema CSA del Cineca. Settimanalmente questi dati sono trasferiti in un database del CED e sono utilizzati per aggiornare l'IDP-INAF in via automatica. Il processo di aggiornamento e accreditamento e' quindi sotto il controllo degli uffici amministrativi. Sara' poi compito dell'utente provvedere alla attivazione del account sull'Identity Provider generando una prima password provvisoria, che sara' inviata al proprio indirizzo e-mail. Al primo accesso sara' richiesto di impostare una propria password personale definitiva.

INAF ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

Centro Elaborazione Dati Amministrativi

SEDE - BOLOGNA

Via P. Gobetti, 101
40129 BOLOGNA
P.I. 06895721006
Cod. Fisc. 97220210583
Ph.: +39 051 6399406 – 6399430
Fax +39 051 6399439
www.ced.inaf.it
Email: ced-staff@inaf.it

Nel caso del personale in formazione sara' opportuno seguire una differente procedura che deve avvenire all'interno delle strutture alle quali essi afferiranno e viene operata direttamente dagli uffici amministrativi che gia' si occupano della verifica dei requisiti (assicurazioni, attestazione universitaria, etc) e provvedono alla consegna delle varie informative di prassi (sicurezza dei luoghi di lavoro, acceptable use policy, etc).

Successivamente il nuovo utente interagira' con il referente informatico locale che, valutate le esigenze, procedera' alla assegnazione delle credenziali. Tali credenziali saranno inserite mediante la compilazione di una pagina web che permette di inserire gli elementi significativi dell'account e in particolare Nome, Cognome, Codice Fiscale, Struttura di afferenza, Indirizzo di posta elettronica, oltre alla scadenza o altre informazioni addizionali. La pagina web sarà protetta da protocollo di cifratura TSL/SSL. L'account sara' poi attivato dall'utente che otterra' nella propria casella postale una password provvisoria.

Ogni utente otterra' un diverso identificativo. L'identificativo dell'utente (ID) sara' generato utilizzando uno schema del tipo *cognome<punto>nome* in caratteri minuscoli e lunghezza massima di 20 caratteri. Nel caso di nome e/o cognome doppio sara' utilizzato solo il primo di questi, mentre saranno eliminati tutti i caratteri speciali (accenti, apostrofi e spazi). Le omonimie saranno eliminate apponendo un numero al cognome. L'indirizzo di posta elettronica associato all'utente sara' la sua casella postale personale, di solito fornita dalla struttura di appartenenza. Si prevede di poter assegnare anche un indirizzo di posta elettronica (alias) costituito dall'identificativo associato al dominio **@inaf.it**.

L'attributo qualificante l'utente (Member/Staff/Student ...) sara' definito in funzione della tipologia di utente. Sara' mantenuto aggiornato a partire dagli archivi anagrafici del CED, o nel caso di personale in formazione con interventi manuali. Tutta la documentazione cartacea relativa all'utente, sara' gestita e custodita dalle amministrazioni delle differenti strutture.

Centro Elaborazione Dati Amministrativi

SEDE - BOLOGNA

Via P. Gobetti, 101
40129 BOLOGNA
P.I. 06895721006
Cod. Fisc. 97220210583
Ph.: +39 051 6399406 – 6399430
Fax +39 051 6399439
www.ced.inaf.it
Email: ced-staff@inaf.it

Caratteristiche dell'identità digitale

Le informazioni che sono attualmente registrate per ogni utente sono:

1 - Nome e Cognome
2 - Codice Fiscale
3 - Telefono
4 - Indirizzo di posta elettronica
5 - Afferenza organizzativa
6 – Scadenza dell'identita'

Di queste si renderanno pubbliche le informazioni strettamente necessarie a seconda delle applicazioni, il Codice Fiscale in particolare sara' reso disponibile solo a procedure amministrative che saranno eventualmente implementate da fornitori di servizi all'INAF. Solo Nome e Cognome e afferenza organizzativa sono da considerarsi informazioni totalmente pubbliche. In futuro si potrebbe decidere di aggiungere ulteriori campi.

Procedura di disattivazione degli utenti

La disattivazione delle utenze avverra' in maniera automatica oppure sara' fatta su richiesta dell'utente o del referente. La disattivazione automatica è conseguenza della scadenza della password al cessare del rapporto istituzionale con INAF.

Dal momento della cessazione ufficiale del rapporto tra INAF e l'utente del IDP sara' comunque garantito un periodo di tempo in cui la password continuera' ad essere attiva, la lunghezza del periodo dipendera' dal tipo di rapporto, in particolare:

1 - Personale dipendente a tempo determinato ed indeterminato.	2 Anni
2 - Collaboratori (Borsisti, Assegnisti, Contrattisti, etc)	1 Anno
3 - Associati e incaricati di ricerca. (circa 200)	1 Anno
4 - Personale in formazione (Laureandi, Dottorandi, PhD, etc)	90 Giorni

Il referente o lo stesso utente può richiedere esplicitamente la disattivazione ai gestori del servizio nel momento in cui dovesse ravvisare che non esistono piu' i requisiti per usufruire dei servizi che INAF mette a disposizione in forma diretta o indiretta.

INAF
ISTITUTO NAZIONALE DI ASTROFISICA
NATIONAL INSTITUTE FOR ASTROPHYSICS

Centro Elaborazione Dati Amministrativi

SEDE - BOLOGNA

Via P. Gobetti, 101
40129 BOLOGNA
P.I. 06895721006
Cod. Fisc. 97220210583
Ph.: +39 051 6399406 – 6399430
Fax +39 051 6399439
www.ced.inaf.it
Email: ced-staff@inaf.it

Gestione password e cessazione

L'utente puo' cambiare la password in ogni momento attraverso una interfaccia web, oppure, nel caso di smarrimento, generare una password provvisoria che sara' inviata alla casella postale. Nella attuale organizzazione non e' previsto che l'Identity provider INAF controlli anche l'accesso alla casella postale personale; se il servizio dovesse evolvere in futuro, prevedendo anche l'autenticazione dei servizi di posta elettronica, sarà necessario trovare una soluzione al problema della "password dimenticata".

L'indirizzo di posta elettronica registrato nel database LDAP dell'Identity provider e' quello segnalato alle amministrazioni nel momento in cui viene a istaurarsi il rapporto con INAF, e non puo' essere cambiato se non con comunicazione agli uffici amministrativi delle strutture presso cui si opera.

Nel caso che l'utenza sia scaduta o sia stata bloccata i gestori possono riabilitare l'account con una password a validita' temporale ridotta.

Dopo 3 anni dalla disattivazione l'account sara' cancellato definitivamente. Dopo di che quell'identificativo potra' essere utilizzato per un nuovo utente.

Partecipazione ad altre Federazioni

L'INAF attualmente non partecipa ad altre Federazioni.

Responsabile del processo di accreditamento

Il responsabile del processo di accreditamento e' la dott.essa **Barbara Neri** che opera presso il CED amministrativo dell'INAF (barbara@ced.inaf.it) e si occupa degli archivi anagrafici del personale.

Il Referente Amministrativo
INAF per IDEM
Mauro Nanni