Allegato per l'adesione ad IDEM

Documento descrittivo del processo di accreditamento degli utenti dell'Università Degli Studi di Firenze

Le informazioni fornite in questo documento sono accurate alla data del 30/03/2011

Sommario

Revisioni

Data	Versione	Descrizione Modifica	Autori
30/03/2011	1.0	Versione 1.0	Rosella, Ferrini

1) Abbreviazioni

AAI:	Authentication Authorization Infrastructure
AUP:	Acceptable User Policy
EDUROAM:	Educational Roaming
GARR:	Gestione Ampliamento Rete Ricerca
IDEM:	Identity Management
IDP:	Identity Provider
SP:	Service Provider
CSIAF:	Centro Servizi Informatici e Informativi dell'Ateneo
UNIFI:	Università degli Studi di Firenze

2) Gestore dell'accreditamento

L'accreditamento è gestito dalle seguenti strutture:

- **Area delle Risorse Umane**, per il personale Tecnico-Amministrativo, Docenti e Ricercatori.
- **Servizi alla Didattica e alla Ricerca dei Poli** per gli studenti immatricolati a qualsiasi titolo
- presso **UNIFI**, dottorati di ricerca, contratti di docenza, assegni di ricerca.
- **Presidenze delle Facoltà** per i docenti a contratto.
- **CSIAF**, per i soggetti che hanno titolo all'utilizzo dei servizi Internet e posta elettronica e applicativi erogati o gestiti dall'Università Unifi, a seguito di identificazione personale.
- L'accreditamento di co.co.co/pro viene gestito da CSIAF su richiesta delle varie strutture (Dipartimenti, Facoltà, Poli etc.)

La raccolta dei dati, il filtraggio e l'armonizzazione sono realizzati da CSIAF.
La gestione dell'accreditamento riguarda esclusivamente il ciclo di vita delle identità digitali mentre la definizione e la formalizzazione del rapporto di lavoro dell'individuo con l'ateneo ne è un prerequisito; il processo completo è descritto in dettaglio nei capitoli 6-9:
"Il processo di accreditamento per le diverse categorie di utenti".

3) Utenti gestiti

Tabella di dettaglio delle categorie di utenza classificate in ateneo

1	Professori Ordinari
2	Professori Associati
3	Docenti a contratto
4	Assistenti Universitari
5	Collaboratore esperto linguistico – Tesoro
6	Lettori madre lingua
7	Ricercatori Universitari
8	Ricercatori a tempo determinato - INPS
9	Ricercatori a tempo determinato – Tesoro
10	Personale tecnico ed amm.vo a tempo indeterminato
11	Personale tecnico ed amm.vo a tempo determinato – Tesoro
12	Addetti Ufficio Stampa
13	Dirigente
14	Dirigente a contratto
15	Incaricati esterni
16	Lavoratore autonomo
17	Non docenti a tempo determinato – INPS
18	Personale esterno che presta attività lavorativa presso l'Università Unifi – E
19	Titolari di assegno di ricerca - AS
20	Dottorandi - DT
21	Dottorandi SUM – SU
22	Studenti Master di 1° livello- M1
23	Studenti Master di 2° livello- M2
24	Studenti Lauree Specialistiche – LS
25	Studenti Lauree Magistrali – LM (comprensivi ciclo unico)
26	Studenti Scuole di Specializzazione – SP
27	Studenti Diploma di Laurea – DU (ad esaurimento)
28	Studenti corsi ante 509 + triennali 509 e 270 – LT
29	Studenti Corsi Singoli – (01 05 10 03 35 20 60 02 36)
30	Laureati di un qualunque corso di studi (LT LS LM M1 M2 SP DU)

4) Mappatura degli utenti sulle affiliazioni IDEM

Nella tabella seguente sono riportate le categorie mappate in IDEM e quindi a quali utenti viene dato l'accesso ai servizi della Federazione.

1	Professori Ordinari	Staff, Member
2	Professori Associati	Staff, Member
3	Docenti a contratto	Staff, Member
4	Assistenti Universitari	Staff, Member
5	Collaboratore esperto linguistico – Tesoro	Staff, Member
6	Lettori madre lingua	Staff, Member
7	Ricercatori Universitari	Staff, Member
8	Ricercatori a tempo determinato - INPS	Staff, Member
9	Ricercatori a tempo determinato – Tesoro	Staff, Member
10	Personale tecnico ed amm.vo a tempo indeterminato	Staff, Member
11	Personale tecnico ed amm.vo a tempo determinato – Tesoro	Staff, Member
12	Addetti Ufficio Stampa	Staff, Member
13	Dirigente	Staff, Member
14	Dirigente a contratto	Staff, Member
15	Incaricati esterni	Staff, Member
16	Lavoratore autonomo	Staff, Member
17	Non docenti a tempo determinato – INPS	Staff, Member
18	Personale esterno che presta attività lavorativa presso l'Università Unifi – E	Staff, Member
19	Titolari di assegno di ricerca - AS	Staff, Member
20	Dottorandi - DT	Staff, Member
21	Dottorandi SUM – SU	Member
22	Studenti Master di 1° livello- M1	Student, member
23	Studenti Master di 2° livello- M2	Student, Member
24	Studenti Lauree Specialistiche – LS	Student, Member
25	Studenti Lauree Magistrali – LM	Student, Member
26	Studenti Scuole di Specializzazione – SP	Student, Member
27	Studenti Diploma di Laurea – DU	Student, Member
28	Studenti corsi ante 509 + triennali 509 e 270 – LT	Student, Member
29	Studenti Corsi Singoli – (01 05 10 03 35 20 60 02 36)	Student
30	Laureati di un qualunque corso di studi (LT LS LM M1 M2 SP DU)	Student, Member

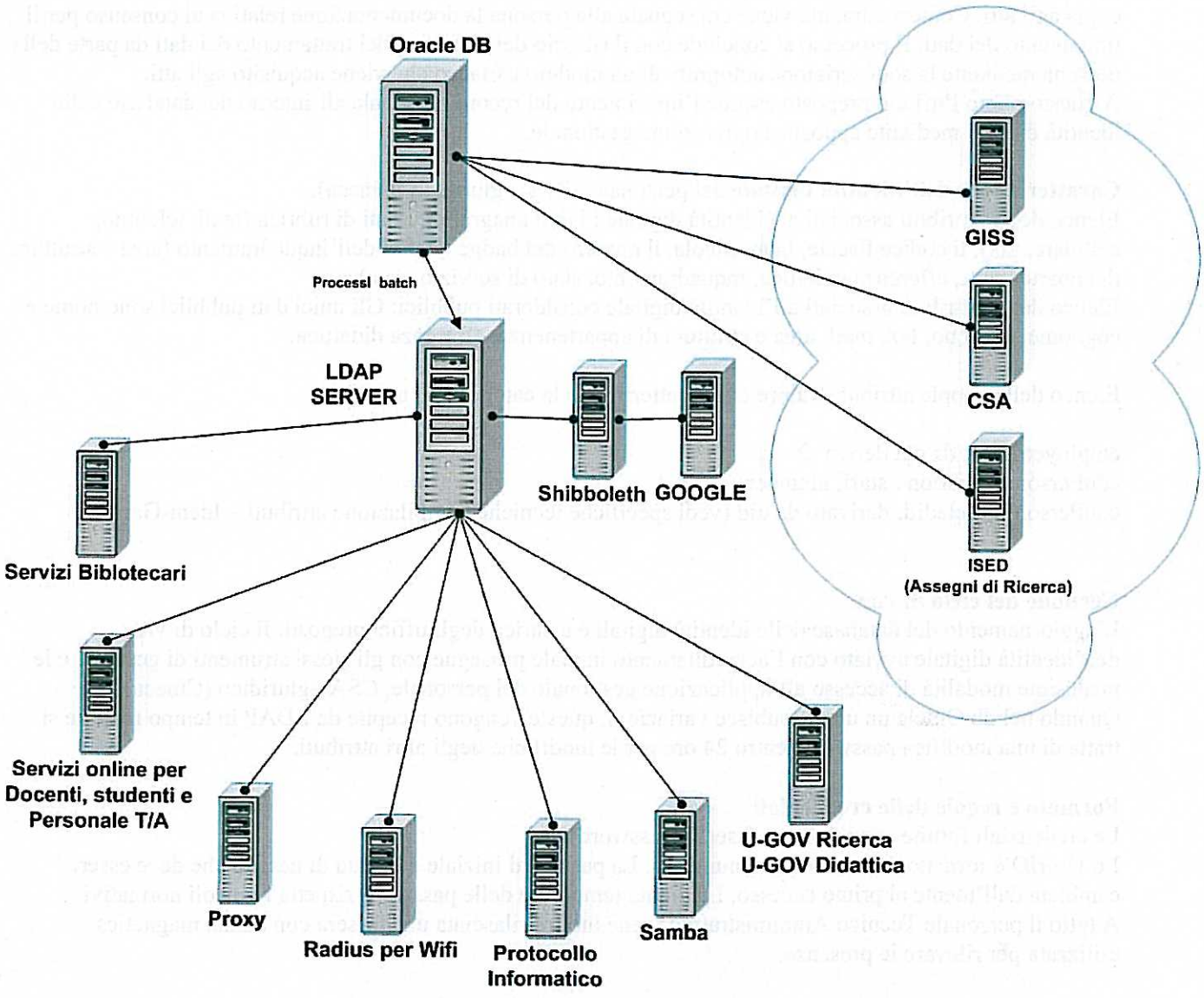
Tabella mappature delle macro categorie di utenza sulle affiliazioni IDEM

Cardinalità di massima delle categorie per affiliazione:

1) Staff 8552 utenti
2) Member 108233 utenti
3) Student 102354 utenti

5) Visione di insieme del processo di accreditamento utenti

La base dati degli utenti e le informazioni associate alle identità digitali vengono conservate all'interno di più database ORACLE gestiti tramite applicativi Web e software client-server.
Un insieme di procedure eseguite giornalmente effettua gli aggiornamenti (inserimenti, modifiche e cancellazioni) sul directory service LDAP, che alimenta a sua volta i servizi Shibboleth.
CSIAF ha sviluppato una serie di servizi online per l'accesso ai dati di studenti e personale tra cui anche i servizi di gestione delle credenziali che sono uniche per l'accesso a tutte le applicazioni esclusa la posta elettronica di tutte le categorie utenti tranne gli studenti.
Attraverso un servizio online di gestione degli accessi internet tramite Wifi è possibile assegnare credenziali per conferenze ed altri eventi di Ateneo direttamente su LDAP.
L'utente utilizza le proprie credenziali per accedere ai servizi online di Ateneo, per l'accesso alla rete dalle aule informatiche, dalle postazioni pubbliche dell'Ateneo e dalla propria abitazione, tramite servizio Proxy autenticato, per l'accesso alla rete internet tramite Wifi , attraverso il captive portal dei controller wireless , per l'accesso ai file server di Polo tramite server SAMBA. Tutte le tipologie di accesso si basano su LDAP per l'autenticazione centralizzata. Al momento, tra le principali applicazioni, vi sono la gestione del protocollo informatico, la gestione delle presenze, l'accesso VPN sicuro da reti esterne, i servizi bibliotecari, l'accesso alle banche dati, oltre a tutti i servizi online sviluppati per docenti (gestione esami, firma digitale, appelli etc), studenti (dati carriera, prenotazioni esami, piano di studi, E-learning Moodle etc), personale (consultazione presenze, U-GOV-didattica, U-GOVricerca, servizi di back office per gli studenti etc).
Il grafico seguente illustra il flusso dei dati.



6) Il processo di accreditamento per la categoria di utenti:

- Personale Tecnico Amministrativo a tempo determinato ed indeterminato
- Collaboratori tecnico amministrativi
- Lettori e Collaboratori linguistici
- Personale Docente e Ricercatore di ruolo e a contratto

Il processo
Struttura organizzativa di riferimento: Area Risorse Umane
Responsabile accreditamento: Responsabili di Uffici "Gestione del Rapporto di Lavoro del personale Tecnico Amministrativo e dei Collaboratori ed Esperti Linguistici ", " Gestione del Rapporto di Lavoro del personale Docente e Ricercatore".
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali delle categorie trattate in questo capitolo.

Modalità di riconoscimento della persona

Uffici di riferimento: Ufficio "Gestione del Rapporto di Lavoro del personale Tecnico Amministrativo e dei Collaboratori ed Esperti Linguistici " e Ufficio " Gestione del Rapporto di Lavoro del personale Docente e Ricercatore".
Modalità di riconoscimento della persona: avviene al momento dell'assunzione con la presenza fisica della persona presso l'ufficio preposto che effettua il controllo dei documenti d'identità personale e ne trattiene copia agli atti. Contestualmente viene consegnata alla persona la documentazione relativa al consenso per il trattamento dei dati. Il processo si conclude con il rilascio del consenso del trattamento dei dati da parte della persona mediante la sottoscrizione autografa di un modulo cartaceo che viene acquisito agli atti.
A questo punto l'ufficio preposto esegue l'inserimento del record personale all'interno del database delle identità digitali mediante apposita applicazione gestionale.

Caratteristiche dell'identità digitale del personale, CSA – giuridico (Cineca).
Elenco degli Attributi associati all'identità digitale : i dati anagrafici, i dati di rubrica (mail, telefono, cellulare, fax), il codice fiscale, la matricola, il numero del badge e i dati dell'inquadramento (area e struttura di appartenenza, afferenza didattica, inquadramento, stato di servizio, ecc.).
Elenco degli Attributi associati all'identità digitale considerati pubblici: Gli unici dati pubblici sono nome e cognome, telefono, fax, mail, area e struttura di appartenenza, afferenza didattica.

Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:

employeeType: da cui deriva →
eduPersonAffiliation : staff, member
eduPersonTargetedId: derivato da uid (vedi specifiche tecniche compilazione attributi – Idem-Garr)

Gestione del ciclo di vita
L'aggiornamento del database delle identità digitali è a carico degli uffici preposti. Il ciclo di vita dell'identità digitale avviato con l'accreditamento iniziale prosegue con gli stessi strumenti di gestione e le medesime modalità di accesso all'applicazione gestionale del personale, CSA –giuridico (Cineca).
Quando nel db Oracle un utente subisce variazioni, queste vengono recepite da LDAP in tempo reale se si tratta di una modifica password, entro 24 ore per le modifiche degli altri attributi.

Formato e regole delle credenziali
Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici. La password iniziale è la data di nascita che deve essere cambiata dall'utente al primo accesso. La durata temporale delle password rispetta i vincoli normativi.
A tutto il personale Tecnico Amministrativo viene inoltre rilasciata una tessera con banda magnetica utilizzata per rilevare le presenze.

Eventuale presenza di credenziali multiple per la stessa persona
Le credenziali multiple non interagiscono.

Modalità di consegna delle credenziali
Le credenziali sono comunicate al momento della presa in servizio.

Modalità di recupero delle credenziali smarrite
Per il recupero della password è prevista una procedura web basata su meccanismo di domanda/risposta e l'invio della password recuperata viene effettuato tramite mail (all'indirizzo di posta istituzionale).
Il reset della password può essere richiesto, tramite apposito modulo da compilare ed inviare firmato, all'ufficio preposto di CSIAF che ripristina la password originale al solo fine del primo accesso e successivo cambiamento password da parte dell'utente

Durata dell'accreditamento
Gli utenti di queste categorie sono accreditati per tutto il tempo in cui sussiste il rapporto di lavoro e da 2 fino ad un massimo di 4 anni, dalla cessazione del rapporto di lavoro per pensionamento, per l' accesso ad internet, posta elettronica e servizi bibliotecari.
I docenti Emeriti sono accreditati a vita.

Disabilitazione utente
Per le categorie caratterizzate da un rapporto di lavoro a termine la disabilitazione avviene in modo automatico alla data di fine rapporto impostata nel database utenti. Di norma questa data corrisponde alla scadenza del contratto.
Dall'avvenuta disabilitazione la persona non potrà più condurre con successo la procedura di autenticazione.

Cancellazione definitiva utente
Per le categorie caratterizzate da un rapporto di lavoro a tempo indeterminato o determinato non è prevista la cancellazione, in quanto i dati sono conservati nello storico.

7) Il processo di accreditamento per la categoria di utenti:

- Studenti
- Studenti Corsi Singoli
- Laureati

Il processo
Struttura organizzativa di riferimento: Servizi alla Didattica dei Poli e dell'Amministrazione centrale.
Responsabile accreditamento: Responsabile di Servizio "Servizi alla didattica e agli studenti" per ogni Polo e tramite i Servizi di "Segreteria studenti", Uffici "Post laurea" e "Master".
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali della categoria "Studenti" dell'ateneo.

Modalità di riconoscimento della persona
Ufficio di riferimento: Segreteria studenti.
Modalità di riconoscimento della persona: il riconoscimento avviene presso l'ufficio preposto con la presenza fisica della persona al momento dell'iscrizione al primo anno del corso di studi. In quell'occasione viene effettuato il controllo dei documenti d'identità personale e trattenuta copia agli atti. Contestualmente l'ufficio preposto ritira la documentazione relativa all'immatricolazione e al consenso per il trattamento dei dati personali attraverso la sottoscrizione autografa di un modulo cartaceo che viene acquisito agli atti. L'utente viene quindi inserito nel sistema di gestione delle carriere di GISS (KION).
Gli studenti che si immatricolano ricevono le credenziali dalla segreteria studenti salvo quelli che utilizzano il servizio "Immatricolazione online" che le ricevono via email , all'indirizzo di posta privato comunicato in fase di immatricolazione.

Caratteristiche dell'identità digitale
Elenco degli Attributi associati all'identità digitale: Tutti i dati dell'anagrafica, i dati della facoltà, del corso di laurea, dell'indirizzo di studi, dell'anno di corso, dello stato di avanzamento degli studi.
Elenco degli Attributi associati all'identità digitale considerati pubblici: Nessuno dato è pubblico.

Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:

employeeType: da cui deriva →
eduPersonAffiliation : student, member
eduPersonTargetedId: derivato da uid (vedi specifiche tecniche compilazione attributi – Idem-Garr)

Gestione del ciclo di vita
L'aggiornamento del database delle identità digitali è a carico dgli uffici preposti ed il ciclo di vita è pilotato dal sistema di gestione della carriera studenti GISS (KION). Gli strumenti di gestione e le modalità di accesso all'applicazione sono i medesimi del processo di attribuzione dell'identità digitale.

Formato e regole delle credenziali
Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici. La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri. La durata temporale delle password rispetta i vincoli normativi.

Eventuale presenza di credenziali multiple per la stessa persona
Le credenziali multiple non interagiscono.

Modalità di consegna delle credenziali
Le credenziali sono comunicate dall' Ufficio Segreteria Studenti al momento dell'immatricolazione dello studente o via e-mail se hanno utilizzato il servizio di immatricolazione on line.

Modalità di recupero delle credenziali smarrite

Per il recupero della password è prevista una procedura web basata su meccanismo di domanda/risposta e l'invio della password recuperata viene effettuato tramite mail all'indirizzo di posta registrato.
Il reset della password può essere richiesto agli uffici competenti (Segreterie studenti, Postlaurea, Master) che ripristinano la password originale al solo fine del primo accesso e successivo cambiamento password da parte dell'utente.

Durata dell'accreditamento
La durata dell'accreditamento e' indefinita.

Disabilitazione
Sono previsti due livelli di disabilitazione dell'identità digitale: il primo riguarda la gestione della carriera universitaria dello studente, il secondo riguarda l'accesso ai servizi di ateneo.
Il primo livello viene ereditato dalla base dati GISS e fornisce l'informazione se lo studente è in regola con il pagamento delle tasse e/o se si e' laureato.
Nel caso lo studente si sia laureato il passaggio di stato avviene automaticamente, dalla data di laurea, e viene mantenuto attivo in LDAP per tre (3) anni dalla data di laurea, garantendogli l'accesso ad internet, ai servizi di biblioteca e agli applicativi per la consultazione dei propri dati anagrafici e di carriera.
Lo studente che non è in regola con il pagamento delle tasse viene cancellato da LDAP il 30/06 dell'anno successivo all'anno dell'ultima iscrizione e viene reintegrato solo in seguito alla regolarizzazione del suo stato.
Il secondo livello di disabilitazione viene gestito dagli uffici preposti attraverso una specifica procedura applicativa. Come sopra, dall'avvenuta disabilitazione lo studente non potrà più condurre con successo la procedura di autenticazione ai servizi d'ateneo.
Lo studente del corso singolo gode dello stesso trattamento dello studente non laureato.

Cancellazione definitiva utente
Non è prevista la cancellazione definitiva di uno studente in quanto i dati sono conservati nello storico.

8) Il processo di accreditamento per la categoria di utenti:

- Docenti a contratto
- Assegnisti di ricerca
- Dottorandi

Il processo
Strutture organizzative di riferimento: "Facoltà", "Dipartimenti", "Uffici alla Ricerca e Relazioni Internazionali di Polo".
Responsabile accreditamento: Responsabile di Ufficio "Dottorato e Assegni di Ricerca", "Uffici alla Ricerca e Relazioni Internazionali di Polo", " Presidenze di Facoltà", "Direzione di Dipartimento".
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali delle categorie trattate in questo capitolo.

Modalità di riconoscimento della persona
Ufficio di riferimento: Ufficio "Dottorato e Assegni di Ricerca", Servizi alla Ricerca e Relazioni Internazionali di Polo", "Presidenze di Facoltà", "Dipartimenti".
Modalità di riconoscimento della persona: avviene al momento dell'assunzione con la presenza fisica della persona presso l'ufficio preposto che effettua il controllo dei documenti d'identità personale e ne trattiene copia agli atti.
Contestualmente viene consegnata alla persona la documentazione relativa al consenso per il trattamento dei dati. Il processo si conclude con il rilascio del consenso del trattamento dei dati da parte della persona mediante la sottoscrizione autografa di un modulo cartaceo che viene acquisito agli atti.
A questo punto l'ufficio preposto esegue l'inserimento del record personale all'interno del database delle identità digitali mediante apposite applicazioni di gestione delle carriere di ISED e CINECA-KION (GISS, U-GOVdidattica).

Caratteristiche dell'identità digitale
Elenco degli Attributi associati all'identità digitale: i dati anagrafici, i dati di rubrica (mail, telefono, fax), il codice fiscale, la matricola e i dati dell'inquadramento (area e struttura di appartenenza, afferenza didattica, inquadramento, stato di servizio, ecc.).
Elenco degli Attributi associati all'identità digitale considerati pubblici: Gli unici dati pubblici sono nome e cognome, telefono, fax, mail, area e struttura di appartenenza, afferenza didattica.

Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:

employeeType: da cui deriva →
eduPersonAffiliation : staff, member
eduPersonTargetedId: derivato da uid (vedi specifiche tecniche compilazione attributi – Idem-Garr)

Gestione del ciclo di vita
L'aggiornamento del database delle identità digitali è a carico degli uffici preposti. Il ciclo di vita dell'identità digitale avviato con l'accreditamento iniziale prosegue con gli stessi strumenti di gestione e le medesime modalità di accesso all'applicazione web di attribuzione dell'identità digitale.
Quando nel db Oracle un utente subisce variazioni, queste vengono recepite da LDAP in tempo reale se si tratta di una modifica password, entro 24 ore per gli altri attributi.

Formato e regole delle credenziali
Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici. . La password iniziale è la data di nascita che deve essere cambiata dall'utente al primo accesso. La durata temporale delle password rispetta i vincoli normativi.

Eventuale presenza di credenziali multiple per la stessa persona
Eventuali credenziali multiple non interagiscono.

Modalità di consegna delle credenziali
Le credenziali sono comunicate al momento della presa in servizio.

Modalità di recupero delle credenziali smarrite
Per il recupero della password è prevista una procedura web basata su meccanismo di domanda/risposta e l'invio della password recuperata viene effettuato tramite mail.
Il reset della password può essere richiesto da assegnisti e dottorandi all'ufficio preposto che ripristina la password originale al solo fine del primo accesso e successivo cambiamento password da parte dell'utente, mentre i docenti a contratto devono inviare via fax l'apposito modulo firmato all'ufficio preposto di CSIAF.

Durata dell'accreditamento
Per i docenti a contratto la scadenza è al 30/04 dell'anno successivo alla data di fine incarico.
Per i dottorandi la scadenza è uguale alla data di fine dottorato + 3 anni.
Per gli assegnisti è uguale alla data di fine carriera.

Disabilitazione utente
La disabilitazione avviene in modo automatico alla data di fine rapporto impostata nel database degli utenti, in base alle regole della durata di accreditamento.
Dal momento della disabilitazione la persona non potrà più condurre con successo la procedura di autenticazione.

Cancellazione definitiva utente
Per le categorie dei Docenti a contratto, Dottorandi e Assegnisti di Ricerca non è prevista la cancellazione, in quanto i dati sono conservati nello storico.

9) Il sistema di autenticazione e autorizzazione interno

Elenco delle applicazioni interne all'ateneo che utilizzano il sistema di gestione delle identità:

Applicazioni	SSO	LDAP
Accessi pubblici alla rete dati d'ateneo tramite wireless (attraverso un Portale web)		X
Accessi pubblici alla rete dati d'ateneo tramite proxy autenticato		X
Accessi sicuri in VPN da internet alla rete dati d'ateneo		X
Protocollo informatico		X
Servizi bibliotecari di consultazione e prestito		X
Piattaforma di E-Learning Moodle		X
Shibboleth	X	X
Servizi di posta elettronica/mailing list Studenti	X	X
CMS di Ateneo		X
Servizi online per studenti, personale docente /ricercatore, tecnici amm.		X
U-GOV didattica e U-GOV ricerca		X

Tabella delle applicazioni interne e relativo metodo di autenticazione.

Gli identificatori principali di ogni persona, una volta assegnati, sono univoci e secondo le direttive di IDEM non possono essere riutilizzati. La durata delle sessioni di autenticazione rispetta i valori di default di Shibboleth.

10) Partecipazione ad altre federazioni

L'Università degli Studi di Firenze partecipa alla Federazione Italiana Eduroam coordinata dal consortium GARR che ha lo scopo di facilitare l'accesso alla rete GARR agli utenti mobili delle organizzazioni partecipanti.
Lo scopo della doppia partecipazione alle federazioni Eduroam e IDEM-AAI è garantire che qualsiasi persona accreditata presso una delle organizzazioni federate anche a livello internazionale, possa accedere ad internet ed usufruire delle risorse federate connettendosi all'infrastruttura WiFi di una qualsiasi delle organizzazioni federate solamente con l'impiego delle credenziali fornite dalla propria organizzazione.
Per assicurare la piena mobilità a tutti coloro che hanno una "identità" ed assicurare l'accesso anche a tutti gli altri servizi che IDEM mette a disposizione è fondamentale condividere la medesima base dati d'identità digitali.