Documento descrittivo del processo di accreditamento degli utenti dell'Università del Salento

Le informazioni fornite in questo documento sono accurate alla data del 26/04/2011

Revisioni

Data	Versione	Descrizione modifica	Autore
27/10/2010	0.1	Bozza da IDEM - Modello DOPAU – V.0.4 del 2/12/2009	Antonio Campa
14/11/2010	0.2	Integrazione del documento a seguito di un incontro con il Responsabile del Servizio Elaborazione Dati	Antonio Campa, Ugo Barchetti, Anna Lisa Guido, Antonio Capodieci
01/12/2010	0.3	Completamento stesura Dopau	Ugo Barchetti, Anna Lisa Guido
18/03/2011	0.3	Adeguamento del server LDAP di Ateneo con gli attributi richiesti da IDEM	Ugo Barchetti, Antonio Marra
26/04/2011	0.4	Revisione del documento	Antonio Campa

INDICE

1 ABBREVIAZIONI 4
2 GESTORE DELL'ACCREDITAMENTO 4
3 UTENTI GESTITI 5
4 MAPPATURA DEGLI UTENTI SULLE AFFILIAZIONI IDEM 6
5 COMPONENTI E FASI DEL PROCESSO DI ACCREDITAMENTO DEGLI UTENTI 6
5.1. Anagrafica Unica e Codice Identificativo 6
5.2. Creazione di un'identità digitale 6
5.3. Allineamento LDAP_A – IDEM_LDAP 7
5.4. Propagazione delle password 7
5.5. Riconoscimento dell'utente 7
5.6. Formato e regole delle credenziali 8
5.7. Uso delle credenziali 8
5.8. L'Identity Provider (IdP) dell'Università del Salento 8
5.9. Visione d'insieme del processo di accreditamento 8
5.10. Modalità di consegna delle credenziali 9
5.11. Ciclo di vita dell'identità digitale 9
5.12. Caratteristiche e visibilità dell'identità digitale 9
6 IL PROCESSO DI ACCREDITAMENTO PER LA CATEGORIA DI UTENTI STUDENTE 10
7 IL PROCESSO DI ACCREDITAMENTO PER LA CATEGORIA DI UTENTI PERSONALE 10
8 IL SISTEMA DI AUTENTICAZIONE E AUTORIZZAZIONE INTERNO 11
9 PARTECIPAZIONE AD ALTRE FEDERAZIONI 11

Nota introduttiva

L'Università del Salento intende partecipare alla Federazione IDEM ("Federazione") ed utilizzare la tecnologia SAML di condivisione degli attributi relativi alle identità digitali, al fine di gestire l'accesso alle risorse on-line che possono essere rese disponibili all'interno della comunità IDEM.

L'Università del Salento, contestualmente all'adesione, fa proprio l'obiettivo della Federazione di sviluppare, nel tempo, degli standard per le organizzazioni al fine di assicurare che le asserzioni sugli attributi siano sufficientemente robuste e fidate per gestire l'accesso alle importanti risorse protette.

*Obiettivo di questo documento è quello di fornire agli altri Partecipanti alla Federazione asserzioni sugli attributi **autorevoli e accurate** e che ciascun Partecipante possa ricevere asserzioni sugli attributi in maniera **protetta** e nel rispetto dei **vincoli di privacy** imposti dalla Federazione o dalla fonte delle informazioni. Si intende, inoltre, rendere disponibili agli altri Partecipanti alla Federazione certe informazioni di base riguardanti il proprio sistema di **identity management**, incluse le informazioni relative agli attributi che vengono utilizzati per la Federazione.*

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono: (1) che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione e che (2) il sistema che emette le credenziali per gli utenti finali (per esempio userid/password, etc.) sia dotato di appropriate misure di gestione del rischio.

In caso di modifica delle procedure o informazioni descritte nel presente documento, esso dovrà essere prontamente aggiornato e trasmesso alla Federazione.

1 Abbreviazioni

DOPAU: Documento sul Processo di Accreditamento degli Utenti
IdP: Identity Provider
SP: Service Provider
SAML: Security Assertion Markup Language
IAM: Identity and Access Management
FIAM: Federated IAM
OSS: Open Source Software
SSO: Single Sign On
UMS: User Management System
LDAP: Lightweight Directory Access Protocol
LDAP_A: LDAP di Ateneo
IDEM LDAP: LDAP di affiliazione IDEM, sincronizzato all'LDAP di Ateneo

2 Gestore dell'accreditamento

L'accreditamento degli utenti abilitati all'accesso ai servizi informatici dell'Università del Salento è operativamente gestito dalle seguenti strutture dell'Ateneo:

- ***Ripartizione Didattica*** *per gli studenti immatricolati a qualsiasi titolo presso l'Università del Salento*
- ***Ripartizione Risorse Umane*** *per il personale e per tutti gli altri soggetti che stipulano con l'Università del Salento un contratto*
- ***Ripartizione Ricerca*** *per le aziende ed i referenti aziendali*
- ***Ripartizione Informatica*** *per tutto il personale e per tutti gli altri soggetti che hanno titolo all'utilizzo dei servizi Internet e posta elettronica erogati dall'Università del Salento.*

Le applicazioni di gestione delle identità digitali sono curate da:

- ***Area Sistemi*** *della Ripartizione Informatica* - è responsabile delle applicazioni che gestiscono il processo di accreditamento, registrazione, riconoscimento, assegnazione delle credenziali, mantenimento, disabilitazione, propagazione delle identità digitali nei directory server e della gestione e della sicurezza dei sistemi (database server e directory server LDAP_A) nei quali le identità digitali vengono conservate. L'Area Sistemi è articolata in *Servizio Elaborazione Dati*, *Servizio Sistemi Informativi* e *Servizio Web*.

- ***Area Infrastrutture*** *della Ripartizione Informatica* è responsabile della gestione dei servizi di autenticazione per IDEM e per EDUROAM e si articola in: *Servizio Dorsale di Rete* che cura l'IdP e l'architettura FIAM, in *Servizio Reti Locali e Telefonia* che cura l'infrastruttura EduRoam ed in *Servizio Posta Elettronica* che cura l'autenticazione ai servizi di posta elettronica e messaggistica.

3 Utenti gestiti

Allo scopo di razionalizzare e semplificare la gestione dell'accreditamento degli utenti sono state definite delle macrocategorie che raggruppano le categorie d'utenza con caratteristiche di appartenenza simili ed esigenze operative comuni. Gli utenti del sistema informativo dell'Università del Salento si possono, dunque, suddividere nelle tre seguenti macrocategorie:

- **Studente**
- **Personale**
- **Guest**

Tale suddivisione in macrocategorie è stata successivamente utilizzata per la mappatura degli utenti sulle affiliazioni IDEM.

La tabella seguente (Tabella 1) descrive i vari profili di utenza gestiti dall'Ateneo, per ognuno di essi indica la macrocategoria che l'Università del Salento assegna al profilo e la cardinalità indicativa dell'insieme di utenti per ciascuna categoria.

Profilo	Categoria	Cardinalità
Studenti iscritti di qualunque corso di studi	Studente	30.000
Studente Scuola di Dottorato/Specializzazione	Studente	
Laureato	Studente	
Docente strutturato	Personale	4.000
Docente a contratto	Personale	
Tecnico amministrativo strutturato (tempo indeterminato o determinato)	Personale	
Collaboratore tecnico amministrativo, alla didattica, alla ricerca	Personale	
Referenti di aziende stage e job placement	Guest	2.000
Candidato studente / Pre-immatricolato	Guest	

Tabella 1: Dettaglio dei profili di utenza classificati in Ateneo

Nella macrocategoria ***Studenti*** rientrano:

- Studenti iscritti ad un qualunque corso di studi di primo e secondo livello
- Dottorandi
- Studenti iscritti a Scuole di specializzazione
- Laureati che hanno avuto accesso al portale delle applicazioni per gli studenti

Nella macrocategoria ***Personale*** rientrano:

- Personale docente
- Ricercatori
- Personale tecnico/amministrativo a tempo indeterminato/determinato
- Collaboratori tecnico/amministrativi
- Collaboratori membri di commissioni
- Collaboratori alla didattica
- Collaboratori alla ricerca
- Assegnisti di ricerca
- Docenti a contratto

Nella macrocategoria ***Guest*** rientrano:

- Operatori di Aziende

- Studenti non ancora iscritti (che hanno completato la prima fase dell'iscrizione)

4 Mappatura degli utenti sulle affiliazioni IDEM

Nella seguente tabella sono riportate le macrocategorie mappate sulle affiliazioni IDEM alle quali viene garantito l'accesso ai servizi della Federazione.

	Valori dell'attributo eduPersonScopedAffiliation				
Macrocategoria	***Member***	***Staff***	***Student***	***Alum***	***Affiliate***
Studente	•		•		
Personale	•	•			
Guest (Referenti di Aziende)[1]	=	=	=	=	=

Tabella 2: Mappatura delle macroategorie sui profili IDEM

5 Componenti e fasi del processo di accreditamento degli utenti

5.1. Anagrafica Unica e Codice Identificativo

L'Università del Salento sta predisponendo un progetto di revisione delle modalità di gestione delle identità digitali del personale (interno ed esterno) e degli studenti finalizzato alla creazione di un anagrafica unica di Ateneo (**ANAGRAFICA_UNICA**) e di un sistema di credenziali unificato. Il Gruppo di Lavoro che è stato costituito (**GAU** – Gruppo Anagrafica Unica), ha l'obiettivo di definire un nuovo UMS e nuove procedure di accreditamento. In attesa della conclusione dei lavori del GAU, un directory server LDAP raccoglie le credenziali di tutti gli utenti censiti e le rende disponibili alle applicazioni. Gli utenti gestiti su tale server, provenienti da vari database, vengono distinti e consolidati tramite un Codice Identificativo (**UID - User ID**) che garantisce l'unicità dell'identità digitale a seguito di una verifica del Codice Fiscale dell'utente. Nonostante la presenza dello UID si è deciso, tuttavia, che ogni utente debba utilizzare le seguenti credenziali di accesso ai servizi informatici:

1. e-mail istituzionale (una delle e-mail istituzionali possedute dall'utente);
2. la password dell'account di accesso al servizio informatico attivato per prima dall'utente.

Con tale organizzazione viene pertanto gestita una sola password privata e personale con la quale ciascun utente dell'Università del Salento, già accreditato, può accedere ai servizi offerti dall'Ateneo ed ai *Service Provider* presenti nel contesto della federazione IDEM. Al momento non ci sono applicazioni che impiegano meccanismi di SSO .

5.2. Creazione di un'identità digitale

La registrazione di un'identità digitale può avvenire tramite tre distinte applicazioni che a loro volta alimentano altrettanti database distinti:

[1] La macrocategoria non è ancora stata abilitata ad accedere ad IDEM

- l'applicazione GISS/ESSE3, per i profili studenti e pre-immatricolati
- l'applicazione CSA/VISPER, per la macrocategoria Personale
- l'applicazione TIROCINI, per la macrocategoria Guest, profilo Referenti di aziende, stage e job placement.

Le identità digitali nascono nei vari database e, mediante script, vengono esportate, in maniera sincrona, sul sistema centrale LDAP di Ateneo (LDAP_A) che rappresenta, in questo modo ed a tutti gli effetti, un servizio di directory di anagrafica unica.
La credenziale unica (e-mail e password) viene registrata in LDAP_A dopo aver verificato la non esistenza nello stesso database di un'altra identità in possesso dello stesso Codice Fiscale. Laddove in LDAP_A fosse già presente un'altra identità con lo stesso Codice Fiscale, per quell'utente verranno mantenute le credenziali preesistenti aggiornando l'identità con gli ulteriori attributi.
L'attributo ***eduPersonScopedAffiliation*** viene creato secondo le regole di mappatura descritte nella precedente Tabella 2.
Il modello prevede, quindi, che le credenziali risiedano in quattro strutture dati: LDAP_A, DB GISS/ESSE3, DB VISPER e DB TIROCINI. Solo LDAP_A, generato consolidando gli altri 3 database, contiene le credenziali utili per i moduli di autenticazione delle applicazioni interne, per l'accesso ai servizi della federazione IDEM e potenzialmente per l'accesso alle future applicazioni in SSO (Single Sign On).
Per garantire maggiore sicurezza l'IdP è stato previsto che non dovrà accedere direttamente ad LDAP_A, ma ad una sua replica sincronizzata denominata IDEM_LDAP. Al momento, l'IdP accede ad una replica di LDAP_A denominata LDAP-pre.
Le identità digitali e le rispettive credenziali per l'accesso ai servizi di ***posta elettronica*** ed alla ***rete wireless*** sono mantenute in un differente database, derivato, per gran parte, dai database sopra riportati. Tale database, che contiene credenziali differenti dalle credenziali contenute in LDAP_A, non è oggetto di analisi di questa versione del documento (DOPAU), ma lo sarà nelle successive versioni e aggiornamenti a seguito di ulteriori analisi e accorpamenti che potranno essere effettuate o disposte dal gruppo di lavoro GAU.

5.3. Allineamento LDAP_A – IDEM_LDAP

Le identità digitali presenti in LDAP_A verranno automaticamente trasferite nel directory server LDAP di IDEM attraverso un meccanismo di sincronizzazione che, quando rileva variazioni sugli attributi di un identità in LDAP_A, le propaga nel directory server di IDEM.
Al momento è stato collegato all'IdP una copia dell'LDAP_A.

5.4. Propagazione delle password

Il meccanismo di generazione della password avviene indipendentemente nelle varie applicazioni in cui l'identità digitale è creata ed insiste nei vari database di pertinenza. Il cambio della password può essere effettuato via web dall'utente dal portale VISPER per la categoria Personale e dal portale degli Studenti per la categoria Studenti. Per la categoria GUEST, profilo referenti esterni, le password sono assegnate e modificate dalle strutture preposte. Qualora per l'utente venisse creato l'account su VISPER, la relativa password avrebbe priorità sulle altre nel meccanismo di definizione della credenziale unica per IDEM.

5.5. Riconoscimento dell'utente

Il riconoscimento dell'utente, in generale, può avvenire in maniera diretta, contestualmente al rilascio delle credenziali presso l'ufficio competente, oppure in maniera indiretta, contestualmente al rilascio delle credenziali se ciò avviene via web.

5.6. Formato e regole delle credenziali

Le credenziali di autenticazione sono costituite da indirizzo e-mail e password.

1) indirizzo e-mail: uno degli indirizzi e-mail istituzionali posseduti dall'utente (nome.cognome@unisalento.it oppure matricola@studenti.unisalento.it).
2) password: sequenza di almeno 6 caratteri alfanumerici.

5.7. Uso delle credenziali

Le credenziali uniche associate alla persona possono essere utilizzate nei contesti di autenticazione federata IDEM e per le applicazioni interne. Al momento non sono stati configurati Service Provider di ateneo che facciano uso delle credenziali IDEM.

5.8. L'Identity Provider (IdP) dell'Università del Salento

L'Identity Provider (IdP) dell'Università del Salento è basato su Shibboleth su infrastruttura OSS. L'IdP sarà collegato al directory server LDAP di Ateneo (LDAP_A) tramite LDAP_IDEM e da quest'ultimo preleverà gli attributi delle identità.

5.9. Visione d'insieme del processo di accreditamento

La figura seguente descrive il flusso di accreditamento, la propagazione dell'identità digitale dai database fino a giungere al directory server di Ateneo ed indica poi i canali di autenticazione degli utenti.

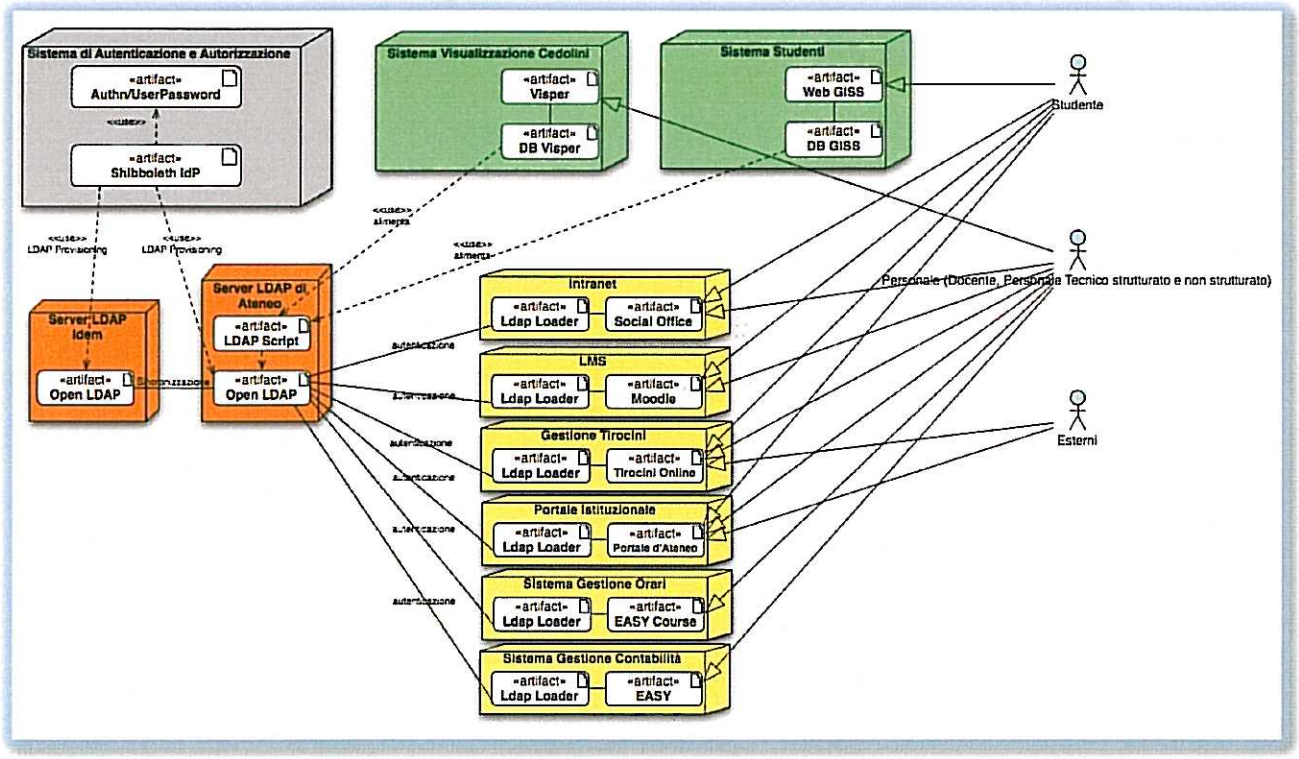

Figura 1: Modello dei flussi di accreditamento dell'utenza

5.10. Modalità di consegna delle credenziali

La consegna delle credenziali allo ***studente*** (la prima volta o in caso di dimenticanza) prevede soltanto la modalità via web, in modalità self-service.

La consegna delle credenziali al ***personale*** prevede due modalità:

- la prima volta: alla ricezione di una lettera via posta ordinaria, all'atto del primo stipendio
- ad ogni variazione o in caso di dimenticanza: via web in modalità self-service.

5.11. Ciclo di vita dell'identità digitale

Il modello con credenziali unificate prevede che un'identità digitale abbia il seguente ciclo di vita:

1. l'identità digitale e la relativa credenziale viene creata in ciascun database applicativo;
2. tramite script si popola l'LDAP_A con le nuove identità e con le nuove password;
3. ogni variazione sugli attributi anagrafici dell'identità digitale in LDAP_A sarà automaticamente propagata sul directory server LDAP collegato all'IdP;
4. ogni variazione legata all'attivazione/disattivazione di un profilo su LDAP_A genera opportunamente l'attributo eduPersonScopedAffiliation.

Alla macrocategoria Guest è stato deciso di non assegnare per il momento alcun valore all'attributo eduPersonScopedAffiliation.

5.12. Caratteristiche e visibilità dell'identità digitale

Per le identità della macrocategoria Personale e per una parte delle identità della macrocategoria Guest sono visibili in modo pubblico sul portale di Ateneo le informazioni relative a Nome, Cognome,

Telefono ufficio, Mail istituzionale. Per la categoria Studenti nessun attributo dell'identità è pubblicamente accessibile sul sito di Ateneo.
L'identità digitale presente in LDAP_A è caratterizzata oltre che dagli attributi anagrafici di base anche da: mail istituzionale, mail personali, eventuale telefono interno.

6 Il processo di accreditamento per la categoria di utenti Studente

Lo studente può entrare a far parte degli utenti dell'ateneo esclusivamente mediante iscrizione online. L'iscrizione online avviene in due fasi: (1) una prima fase in cui lo studente effettua una preiscrizione, inserisce i propri dati e si assegna delle credenziali per una casella di posta temporanea e non è abilitato ad altri servizi, ed (2) una seconda fase, che si conclude al pagamento delle tasse, in cui l'utente completa la preiscrizione e riceve l'abilitazione ad accedere a tutti i servizi. A conclusione della prima fase online viene rilasciata l'identità digitale dello studente ma lo stesso è classificato nella macrocategoria GUEST. Al termine della seconda fase lo studente immatricolato potrà usufruire di servizi messi a disposizione dall'Ateneo e viene cambiata la macrocategoria di appartenenza da GUEST a Studente.
Gli attributi che costituiscono l'identità digitale dello studente sono: ***Nome, Cognome, indirizzo, e-mail istituzionale, matricola studente, categoria di appartenenza, UID e password.***
Le credenziali utilizzate per l'accesso sono l'e-mail istituzionale, assegnata automaticamente, e la password scelta dallo stesso studente via web in fase di immatricolazione.
In caso di smarrimento della password lo studente può richiedere l'invio della nuova password.
Gli identificatori principali dell'identità digitale sono: UID, che identifica in maniera univoca l'utente nell'LDAP_A, eduPersonPrincipalName, eduPersonScopedAffiliation e eduPersonTargetedID e quest'ultimo identifica in maniera univoca l'utente nel rilascio dell'identità digitale all'interno dell'IdP.

7 Il processo di accreditamento per la categoria di utenti Personale

Il personale entra a far parte degli utenti dell'ateneo potenzialmente nel momento in cui avviene il pagamento del primo stipendio. L'identità digitale viene, infatti, rilasciata in occasione del pagamento dello stipendio ed in tale occasione sono spedite le credenziali all'utente attraverso la posta ordinaria. L'ufficio preposto alla creazione dell'identità digitale è l'Ufficio Stipendi.
Una volta che l'utente ha ricevuto le credenziali egli può accedere a tutti i servizi messi a sua disposizione.
Gli attributi che costituiscono l'identità digitale del personale sono: ***Nome, Cognome, indirizzo, e-mail istituzionale, matricola dipendente, categoria di appartenenza, UID e password.***
Le credenziali utilizzate per l'accesso sono l'e-mail istituzionale e la password assegnata in prima istanza dall'ufficio preposto alla creazione dell'identità digitale. La modifica della password può essere effettuata online dal personale attraverso il portale VISPER. È possibile che il personale appartenga anche alla categoria studente ed in tal caso potrà utilizzare indifferentemente come userID una delle e-mail istituzionali assegnate a lui.
In caso di smarrimento della password il personale può richiedere l'invio della nuova password sul suo indirizzo e-mail istituzionale.
Gli identificatori principali dell'identità digitale sono UID, che identifica in maniera univoca l'utente nel LDAP_A, eduPersonPrincipalName, eduPersonScopedAffiliation e eduPersonTargetedID e quest'ultimo identifica in maniera univoca l'utente nel rilascio dell'identità digitale all'interno dell'IdP.

8 Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione delle identità descritto in questo documento viene utilizzato per alimentare i sistemi di autenticazione e autorizzazione di numerose applicazioni interne tra cui alcune sono riportate in Figura 1. Tale sistema è per buona parte indipendente dal sistema di autenticazione e autorizzazione per i servizi di posta elettronica e per l'accesso al wireless.
Gli identificatori principali di ogni persona, come "UID" o eduPersonTargetedID, sono univoci una volta assegnati.

9 Partecipazione ad altre federazioni

L'Università del Salento partecipa alla federazione EDUROAM attraverso la quale gli studenti possono accedere ai servizi WIFI presso gli Atenei federati.