Documento descrittivo del processo di accreditamento degli utenti dell' Università degli Studi di Urbino "Carlo Bo"

Revisioni 1
Gestore dell'accreditamento 2
Utenti gestiti 2
B2B / Servizi 3
Mappatura degli utenti sulle affiliazioni IDEM 3
Visione di insieme del processo di accreditamento degli utenti 4
Il processo di accreditamento per la categoria di utenti STAFF 5
Il processo 5
Modalità di riconoscimento della persona 5
Caratteristiche dell'identità digitale 5
Gestione del ciclo di vita 6
Formato e regole delle credenziali 6
Eventuale presenza di credenziali multiple per la stessa persona 6
Modalità di consegna delle credenziali 6
Modalità di recupero delle credenziali smarrite 6
Modalità di gestione smarrimento smartcard/token 6
Durata dell'accreditamento 6
Disabilitazione utente 6
Cancellazione definitiva utente 6
Rischi specifici associati alla categoria di utenti 7
Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard) 7
Il processo di accreditamento per la categoria di utenti Student 7
Il processo 7
Modalità di riconoscimento della persona 7
Caratteristiche dell'identità digitale 7
Gestione del ciclo di vita 8
Formato e regole delle credenziali 8
Eventuale presenza di credenziali multiple per la stessa persona 8
Modalità di consegna delle credenziali 8
Modalità di recupero delle credenziali smarrite 8
Modalità di gestione smarrimento smartcard/token 8
Durata dell'accreditamento 9
Disabilitazione utente 9
Cancellazione definitiva utente 9
Rischi specifici associati alla categoria di utenti 9
Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard) 9
Il sistema di autenticazione e autorizzazione interno 7

Revisioni

Data	Versione	Descrizione modifica	Autore
23/12/2009	2.0	Bozza	
		Bozza	
		Rilasciato	

Gestore dell'accreditamento

Il processo di accreditamento degli utenti che afferiscono all'Università degli studi di Urbino fa riferimento a seconda delle classi di utenti al **Servizio Front-Office** o al **Servizio Risorse Umane.** La custodia delle credenziali e' affidata al **Sistema Informatico di Ateneo.** Le responsabilità per il conferimento e la gestione delle credenziali degli utenti sono assegnate dal Direttore Amministrativo ai responsabili dei servizi indicati.

Utenti gestiti

Sono di seguito elencate tutte le categorie e le tipologie in esse comprese delle identità gestite dall'Università degli Studi di Urbino incluse nel *"Regolamento per la gestione e l'utilizzo della rete di Ateneo":*

Dipendenti (strutturati – rapporto di lavoro subordinato a tempo indeterminato/determinato)

Personale docente;
Ricercatori;
Personale tecnico/amministrativo;
CEL;

Studenti

Studenti iscritti ad un qualunque corso di studi di primo o secondo livello, Master, Scuole di Specializzazione, Corsi di Perfezionamento e Aggiornamento;
Dottorandi;
Studenti Erasmus;
Studenti iscritti in Atenei e frequentanti corsi presso il nostro;

Altre tipologie

Collaboratori tecnico/amministrativi (Co.Co.Co.);
Collaboratori alla ricerca (Borsisti);
Assegnisti di ricerca;
Docenti a contratto;
Partecipanti a progetti di ricerca;

Ospiti

Convegnisti;

Ex utenti

Utenti appartenenti ad una delle categorie sopraindicate che hanno cessato i rapporti con l'Ateneo relativamente alla categoria in cui erano incardinati;

L'accesso ai servizio della Federazione (inclusione nell'IdP) viene dato a tutte le categorie ad eccezione degli Ospiti e degli Ex utenti

B2B / Servizi

Non previsti

Mappatura degli utenti sulle affiliazioni IDEM

Member

Dipendenti & Altre Tipologie

Personale docente;
Ricercatori;
Personale tecnico/amministrativo;
CEL;

Collaboratori tecnico/amministrativi (Co.Co.Co.);
Collaboratori alla ricerca (Borsisti);
Assegnisti di ricerca;
Docenti a contratto;
Partecipanti a progetti di ricerca;

Studenti

Studenti iscritti ad un qualunque corso di studi di primo o secondo livello, Master, Scuole di Specializzazione, Corsi di Perfezionamento e Aggiornamento;
Dottorandi;
Studenti Erasmus;
Studenti iscritti in Atenei e frequentanti corsi presso il nostro;

Staff

Dipendenti & Altre Tipologie

Personale docente;
Ricercatori;
Personale tecnico/amministrativo;
CEL;

Collaboratori tecnico/amministrativi (Co.Co.Co.);
Collaboratori alla ricerca (Borsisti);
Assegnisti di ricerca;
Docenti a contratto;

Partecipanti a progetti di ricerca;

Student

Studenti

Studenti iscritti ad un qualunque corso di studi di primo o secondo livello, Master, Scuole di Specializzazione, Corsi di Perfezionamento e Aggiornamento;
Dottorandi;
Studenti Erasmus;
Studenti iscritti in Atenei e frequentanti corsi presso il nostro;

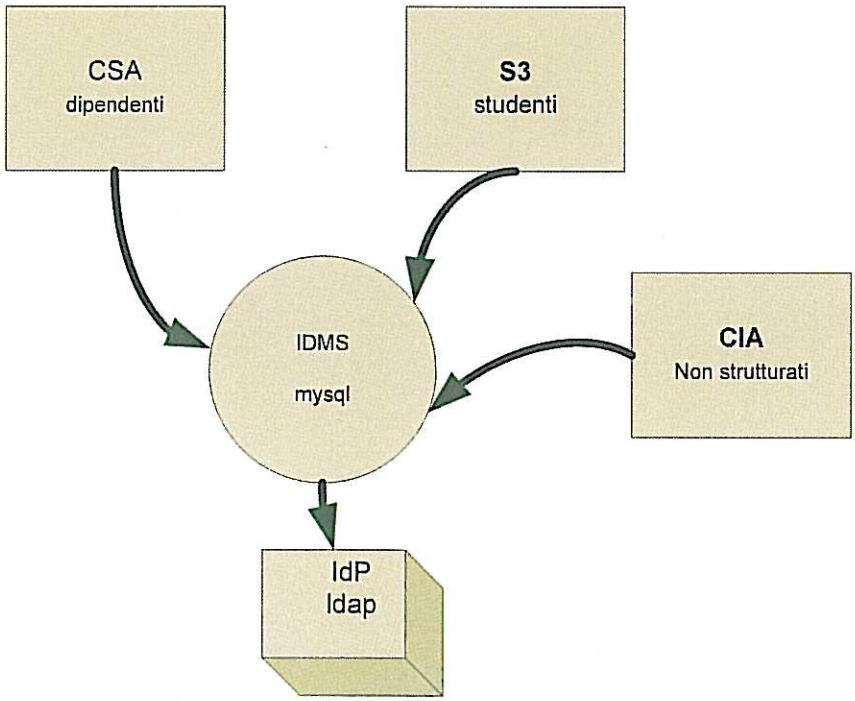
Alum

Laureati di un qualunque corso di studi/ dottorato/ master

Affiliate (Ospiti)

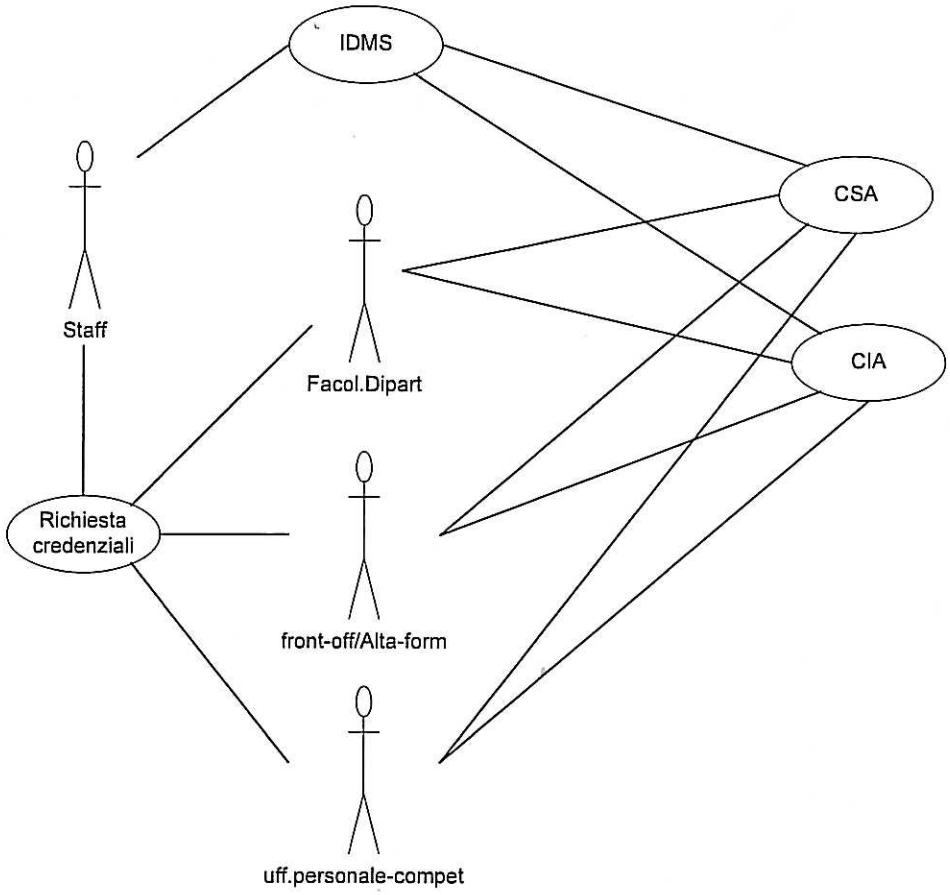
Convegnisti

Visione di insieme del processo di accreditamento degli utenti



Il processo di accreditamento per la categoria di utenti STAFF

Il processo



Modalità di riconoscimento della persona

La persona si presenta all'ufficio preposto:
Risorse Umane –Ufficio Personale competente
Front Office-Ufficio Alta Formazione
Presidenza di Facolta'/Direzione di Dipartimento- IdProvisioning)
dove viene riconosciuta tramite valido documento di identita'.

Caratteristiche dell'identità digitale

All'identita' digitale vengono associati i seguenti attributi nelle procedure CSA e IdProvisioning (CIA):

Cognome, Nome, Codice Fiscale, Lingua preferita, Posizione organizzativa, Titolo personale, Unità operativa di afferenza , Indirizzo di posta, Affiliazione, Diritto accesso risorse, UserID, Password.

Vengono considerati pubblici e forniti a chi ne faccia richiesta gli attributi specificati come obbligatori dalla Federazione

Gestione del ciclo di vita

Le modifiche effettuate sulle procedure CSA e IdProvisioning (CIA) si propagano all'IdP
(CSA->MySQL->LDAP)
(IdProvisioning CIA->MySQL->LDAP).

Formato e regole delle credenziali

Le credenziali utilizzate nell'organizzazione sono del tipo, userID/password.

La validità della password viene allineata alle disposizione di legge (6 mesi).

Eventuale presenza di credenziali multiple per la stessa persona

Non previste.

Modalità di consegna delle credenziali

Dopo l'identificazione presso l'ufficio competente viene notificata all'utente la userid nome.cognome (casi di omonimia sono risolti con l'accodamento di un numero progressivo al nome utente).
L'utente digita personalmente la propria password.

Modalità di recupero delle credenziali smarrite

Ritorno all'ufficio personale competente dove viene inserita la nuova password.

Modalità di gestione smarrimento smartcard/token

Non previste

Durata dell'accreditamento

Mantenuto nella classe in oggetto sino al cambiamento della categoria.

Disabilitazione utente

Disabilitazioni asincrone dopo un intervallo di tempo di 6 mesi dalla cessazione del rapporto istituzionale.
Vengono annullate le credenziali mentre si mantengono le identità digitali.
Ulteriore caso di disabilitazione immediata in caso di mancata osservanza delle policy di utilizzo dei servizi.

Cancellazione definitiva utente

Mai

Rischi specifici associati alla categoria di utenti

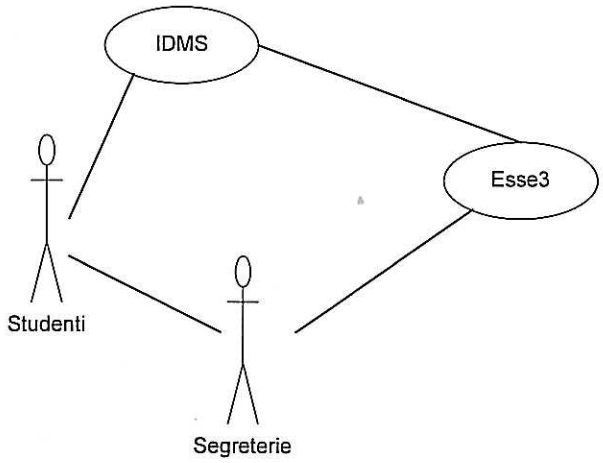
Nessuno

Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)

Non prevista

Il processo di accreditamento per la categoria studenti

Il processo



Modalità di riconoscimento della persona

La persona si presenta alla segreteria studenti competente (servizio Front Office) dove viene riconosciuta tramite valido documento di identita' durante il processo di formalizzazione dell'immatricolazione.

Caratteristiche dell'identità digitale

All'identita' digitale vengono associati i seguenti attributi nella procedura Esse3:

Cognome, Nome, Codice Fiscale, Lingua preferita, Corso di laurea, Titolo personale, Parità tasse , Indirizzo di posta, Affiliazione, Diritto accesso risorse, UserID, Password

Vengono considerati pubblici e forniti a chi ne faccia richiesta gli attributi specificati come obbligatori dalla Federazione

Gestione del ciclo di vita

Le modifiche effettuate sulla procedura Esse3 si propagano all'IdP (Esse3->MySQL->LDAP).
Nel caso di uscita trasferimento in ALUM

Formato e regole delle credenziali

Le credenziali utilizzate nell'organizzazione sono del tipo, userID/password.

La validità della password viene allineata alle disposizione di legge (6 mesi).

Eventuale presenza di credenziali multiple per la stessa persona

Non previste.

Modalità di consegna delle credenziali

In caso di preimmatricolazione online:

vengono automaticamente generate dalla procedura userid e password. Queste saranno utilizzabili solo all'interno della procedura di immatricolazione online fino alla formalizzazione della stessa. Da quel momento le credenziali gia' in possesso del soggetto vengono validate per l'accesso agli altri servizi disponibili per la categoria.

In caso di immatricolazione allo sportello:

la persona si presenta alla segreteria competente (servizio Front Office) e dopo la formalizzazione dell'immatricolazione gli vengono consegnate la userid e la password su supporto cartaceo dal personale preposto.

iniziale-nome.cognome (casi di omonimia sono risolti con numerazione progressiva dopo l'userid)
L'utente ritira personalmente la sua password iniziale che dovrà poi essere modificata tramite apposita procedura online

Modalità di recupero delle credenziali smarrite

Ritorno alla segreteria di riferimento dove viene inserita la nuova password.
Attraverso procedura online di recupero password una nuova password viene inviata all'indirizzo di posta elettronica comunicato in fase di immatricolazione.

Modalità di gestione smarrimento smartcard/token

Non previste

Durata dell'accreditamento

Mantenuto nella classe in oggetto sino al cambiamento della categoria.

Disabilitazione utente

Disabilitazioni tutte asincrone dopo un intervallo di tempo di 3 mesi.
Vengono annullate le credenziali mentre si mantengono le identità digitali.
Ulteriore caso di intervento in caso di mancata osservanza delle policy.

Cancellazione definitiva utente

Mai

Rischi specifici associati alla categoria di utenti

Nessuno

Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)

Non Prevista

Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione delle identita' viene utilizzato per tutte le applicazioni interne disponibili eccetto:
Gestione Presenze
Protocollo Informatico

Gli identificatori principali di ogni persona, come "net ID," eduPersonPrincipalName, o eduPersonTargetedID, sono univoci una volta assegnati; per ora non vengono riutilizzati.

Partecipazione ad altre federazioni

Non previsto