UNIVERSITÀ DEGLI STUDI DI PADOVA

CENTRO DI CALCOLO DI ATENEO

Documento descrittivo del Processo di Accreditamento degli Utenti

dell'Università degli Studi di Padova

DOPAU 2010

Revisioni

Versione	Data emissione	Descrizione modifiche	Autore
1.0	22-02-2010	Primo rilascio	S.Zanmarchi

Indice

1 INTRODUZIONE....3
2 GESTORE DELL'ACCREDITAMENTO....3
3 UTENTI GESTITI....3
4 MAPPATURA DEGLI UTENTI SULLE AFFILIAZIONI IDEM....4
5 VISIONE DI INSIEME DEL PROCESSO DI ACCREDITAMENTO....5
6 L'ACCREDITAMENTO PER LA CATEGORIA @STUDENTI.UNIPD.IT....6
6.1 MODALITÀ DI RICONOSCIMENTO DELLA PERSONA E CONSEGNA DELLE CREDENZIALI....6
6.2 GESTIONE DEL CICLO DI VITA E DURATA DELL'ACCREDITAMENTO....7
6.3 FORMATO E REGOLE DELLE CREDENZIALI....7
6.4 EVENTUALE PRESENZA DI CREDENZIALI MULTIPLE PER LA STESSA PERSONA....8
6.5 DISABILITAZIONE UTENTE....8
6.6 RECUPERO DELLE CREDENZIALI SMARRITE....8
6.7 RISCHI SPECIFICI ASSOCIATI ALLA CATEGORIA DI UTENTI....9
7 L'ACCREDITAMENTO PER LA CATEGORIA @UNIPD.IT....9
7.1 MODALITÀ DI RICONOSCIMENTO DELLA PERSONA E CONSEGNA DELLE CREDENZIALI....9
7.2 GESTIONE DEL CICLO DI VITA E DURATA DELL'ACCREDITAMENTO....9
7.3 FORMATO E REGOLE DELLE CREDENZIALI....10
7.4 EVENTUALE PRESENZA DI CREDENZIALI MULTIPLE PER LA STESSA PERSONA....10
7.5 DISABILITAZIONE UTENTE....11
7.6 RECUPERO DELLE CREDENZIALI SMARRITE....11
7.7 RISCHI SPECIFICI ASSOCIATI ALLA CATEGORIA DI UTENTI....11
8 PARTECIPAZIONE AD ALTRE FEDERAZIONI....11

1 Introduzione

L'Università di Padova partecipa alla Federazione Idem mediante lo stesso Shibboleth IdP utilizzato per i propri SP interni. Le credenziali di accesso (username e password) coincidono con l'indirizzo e la password della posta elettronica istituzionale.
Alcuni servizi interni posti sotto Single Sign On vengono tuttavia forniti, con altre credenziali, anche ad utenti sprovvisti di posta elettronica istituzionale (ad es. resposabili di tirocinio, ex studenti, preimmatricolati,...).
Inoltre la stessa casella di posta elettronica istituzionale viene sia data a dipendenti di altre organizzazioni (ad es. convenzioni con biblioteche) che, per un certo lasso di tempo, concessa anche agli utenti che hanno cessato il loro rapporto con l'Ateneo.
In tutti questi casi tuttavia, pur superando l'utente la fase di autenticazione, l'Attribute Authority non ne fornisce ai SP aderenti alla Federazione alcun attributo.
Questo documento descrive quindi in maniera schematica solo il processo di accreditamento in atto in Ateneo per gli utenti mappati sulle affiliazioni di Idem.

2 Gestore dell'accreditamento

Il processo di accreditamento è alquanto rigido, poiché l'Ateneo non concede, per questioni di immagine, l'utilizzo di una casella di posta isttuzionale ad utenti che non soddisfino precisi requisiti di afferenza.
Responsabile dell'assegnazione, del mantenimento e della cancellazione delle caselle di posta istituzionale, come pure del funzionamento dell'IdP è il Centro di Calcolo di Ateneo.

3 Utenti gestiti

Gli utenti sono divisi in due macrocategorie:

1. Utenti aventi diritto alla mail istituzionale di tipo @unipd.it, gestiti dal mail server di Ateneo, implementato presso il Centro di Calcolo, che ha quindi controllo diretto sugli account e sulle interfacce web di gestione della password:

   - *Personale docente (ordinari, associati, ricercatori)*
   - *Docenti a contratto*
   - *Affidamenti di docenza a esterni*
   - *Collaboratori alla didattica e alla ricerca*
   - *Borsisti*

- *Stagisti*
- *Assegnisti di ricerca*
- *Assistenti*
- *Cultori della materia*
- *Dirigenti*
- *Personale tecnico/amministrativo a tempo indeterminato/determinato*
- *Bibliotecari in convenzione*
- *CEL (lettori)*
- *Tutor l.170*
- *Collaboratori Co.co.co.*
- *Volontario servizio civile nazionale*

2. Utenti aventi diritto alla mail istituzionale di tipo @studenti.unipd.it con servizio fornito da Cineca. Cineca gestisce il mail server, ma effettua l'autenticazione verso uno slave LDAP server, allineato real-time al master server LDAP di autenticazione, contenente username e password, in esercizio presso il Centro di Calcolo, che ha quindi pieno controllo sugli account e sulle interfacce web di gestione della password:

   - *Studenti delle lauree di base e specialistiche*
   - *Studenti iscritti a Master*
   - *Studenti iscritti a Dottorato di Ricerca*
   - *Studenti in Mobilità Internazionale*
   - *Studenti laureati o diplomati*

4 Mappatura degli utenti sulle affiliazioni Idem

Solo alcuni utenti afferenti alle due macrocategorie sopra descritte vengono attualmente mappati sulle affiliazioni Idem.
Come accennato nell'introduzione, l'Attribute Authority mappa sulle affiliazioni soltanto alcune categorie di utenti in possesso di casella di posta istituzionale di Ateneo. Si tratta in ogni caso di persone che hanno ancora attiva una carriera da studente (inclusi i post lauream) o da dipendente. Quando la carriera cessa non vengono più mappati, indipendentemente dal loro eventuale diritto a conservare la casella di posta istituzionale per un certo lasso di tempo.
La tabella descrive gli utenti mappati.

Utente	Valori di *eduPersonAffiliation*				
	member	staff	student	alumn	affiliate

ordinari, associati, ricercatori	✓	✓			
docenti a contratto	✓	✓			
collaboratori a didattica e a ricerca	✓	✓			
assegnisti di ricerca	✓	✓			
assistenti	✓	✓			
dirigenti	✓	✓			
personale tecnico/amministrativo	✓	✓			
lettori (CEL)	✓	✓			
tutor legge 170	✓	✓			
volontario servizio civile nazionale	✓				
studenti lauree base/specialistiche	✓		✓		
master	✓		✓		
dottorandi	✓	✓	✓		

Tab. 1: mappatura utenti-affiliazioni

5 Visione di insieme del processo di accreditamento

In figura viene illustrato in maniera estremamente schematizzata l'infrastruttura connessa all'IdP di Ateneo. In verde la parte relativa all'autenicazione, in azzurro quella relativa al prelievo degli attributi.
Le password vengono gestite (processi di prima attivazione, cambio password, recupero password) dagli utenti tramite interfacce web. Il provisioning verso il server LDAP di autenticazione è in tempo reale.
Gli attributi vengono letti dalla Attribute Authority dell'IdP direttamente dai database dei sistemi gestionali dei dipendenti (Giada) e degli studenti (Esse3) mediante viste dedicate.
È proprio la logica di creazione di queste viste che consente di mappare granularmente le affiliazioni Idem solo per alcune prescelte categorie di utenti con carriera aperta e in possesso di mail istituzionale. Gli utenti che non soddisfano questi criteri non vengono mappati.

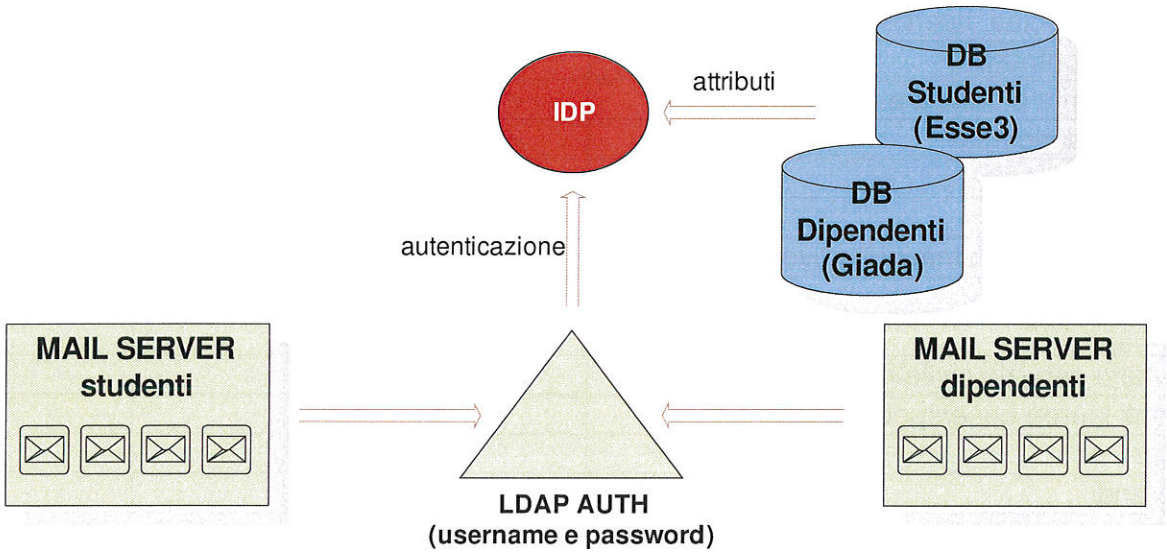

Fig 1: visione schematica dell'infrastrutura di SSO

È stato recentemente compiuto uno sforzo si normalizzazione nell'assegnazione degli indirizzi di posta agli utenti. Gli utenti contenuti nel database del gestionale delle risorse umane (Giada) hanno tutti indirizzo istituzionale di tipo @unipd.it, quelli contenuti nel gestionale degli studenti (Esse3) hanno invece indirizzo di tipo @studenti.unipd.it.
Vi sono ancora dei casi di incrocio (as es i post lauream prima del 2009 hanno mail di tipo @unipd.it), ma sono figure ad esaurimento.

6 L'accreditamento per la categoria @studenti.unipd.it

6.1 Modalità di riconoscimento della persona e consegna delle credenziali

Ci sono vari Servizi (Servizio Concorsi e Carriere Docenti, Servizio Ricerca, Segreterie Studenti, Mobilità Internazionale, ecc.) preposti all'accettazione degli utenti - a seconda della diverse carriere che stanno per intraprendere - e al loro inserimento nel sistema gestionale Esse3.
Il riconoscimento dell'utente avviene sempre in seguito alla presentazione di un documento d'identità valido. In alcuni casi (collaboratori alla ricerca e alla didattica, cultori della materia, docenti a contratto) il riconoscimento non viene fatto direttamente dai Servizi, ma dai presidi di Facoltà e direttori di Dipartimento, che inviano ai Servizi la richiesta di accettazione via fax.
Contestualmente all'inserimento di questi utenti nel sistema gestionale Esse3, effettuato da personale d'Ateneo, viene loro generato l'indirizzo di posta istituzionale di tipo

@studenti.unipd.it. La comunicazione all'utente dell'indirizzo avviene mediante stampa su supporto cartaceo.
Se l'utente ha già una casella di posta di tipo @studenti.unipd.it (ad es. laureati presso l'Ateneo di Padova che si iscrivono ad un dottorato), la mantiene insieme alla password, e utilizza queste credenziali per accedere ai vari SP.
Se l'utente non ha già una casella di posta di tipo @studenti.unipd.it (ad es. un nuovo immatricolato, o un laureato in altra sede che inizia una carriera post lauream) gli viene anche indicato il sito dove attivarla e il codice di attivazione.
L'operazione web di attivazione della casella consiste nella scelta della password di propria preferenza e dell'insieme di domande multiple a risposta segreta per il recupero della password.
Terminata l'operazione la casella di posta istituzionale è attiva e le credenziali sono da subito utilizzabili per accedere ai servizi sotto Single Sign On.

6.2 Gestione del ciclo di vita e durata dell'accreditamento

Gli utenti afferenti alla categoria @studenti.unipd.it conservano le credenziali di accesso (username e password) per sempre.
Le credenziali non vengono mai rimosse dal server LDAP di autenticazione, l'autenticazione è sempre possibile, e il controllo degli accessi viene demandato alle applicazioni accedute mediante l'invio degli attributi (carriera aperta/chiusa, in regola con le tasse, ecc..).
Ad esempio il servizio di posta è accedibile per ulteriori 12 mesi dalla chiusura della carriera o dall'ultimo pagamento regolare delle tasse, mentre l'accesso al servizio informativo studenti è garantito per sempre (sola visualizzazione della carriera), come pure l'accesso ai servizi di Stage.
La mappatura sulle affiliazioni Idem avviene però solo quando la carriera è aperta.

Se lo stesso utente ricomincia una nuova carriera, gli viene riasseganato lo stesso indirizzo di posta.
Il centro di Calcolo mantiene lo storico degli indirizzi di posta istituzionale assegnati, evitandone la riassegnazione futura ad altri utenti.

6.3 Formato e regole delle credenziali

Lo username coincide con la casella di posta istituzionale ed è formato secondo l'algoritmo nome.cognome[.n]@studenti.unipd.it.
Eventuali omonimie vengono quindi risolte aggiungendo un numero progressivo (ad es. mario.rossi.9@studenti.unipd.it).

Non è consentito all'utente, se non come eccezione, il cambio della casella di posta assegnatagli.

La password dev'essere di almeno 8 caratteri, contenere almeno una maiuscola, un numero e un carattere speciale: (punto), (due punti), (punto e virgola),(meno).
La password comunque scade dopo 3 mesi ed è imposto il non riutilizzo della password precedente.
Se l'utente si ricorda di cambiarla per tempo, la procedura di cambio password richiede la conoscenza della vecchia.
Se l'utente la lascia scadere dovrà invocare la procedura di recupero password e rispondere alle domande la cui risposta aveva dato in fase di attivazione della casella.

6.4 Eventuale presenza di credenziali multiple per la stessa persona

Non sono possibili credenziali multiple di tipo @studenti.unipd.it. Nel caso di più carriere aperte (sono possibili alcuni incroci tra carriere pre e post lauream) l'utente riceve infatti lo stesso indirizzo di posta.
Sono invece possibili e frequenti credenziali multiple @studenti.unipd.it e @unipd.it, ad es. per dipendenti che siano anche studenti.
Il limite delle credenziali multiple è che l'insieme degli attributi dell'utente può variare a seconda delle credenziali utilizzate, ad ed la matricola (da studente o da dipendente), o la mappatura sulle affiliazioni Idem

6.5 Disabilitazione utente

L'utente non viene cancellato dal server di autenticazione. Se è necessario disabilitarlo gli viene impostata la password a valore a lui ignoto ed inibita la procedura di recupero password.

6.6 Recupero delle credenziali smarrite

L'utente può recuperare le credenziali smarrite:

- via web, mediante risposta alle domande segrete impostate in fase di attivazione della casella di posta
- presentandosi in segreteria con un documento d'identità valido

6.7 Rischi specifici associati alla categoria di utenti

Gli ex studenti possono accedere ad alcuni servizi di Ateneo posti sotto SSO, ad esempio al sistema informativo studenti, per accedere in sola visione alla loro carriera, o al servizio stage e tirocini. Si è deciso che tali utenti possano accedere presentando il codice fiscale come credenziale di autenticazione. Questi utenti non vengono quindi attualmente mappati nella affiliazione Alumn di Idem, poiché il codice fiscale è una credenziale di autenticazione debole.

In LDAP di autenticazione non vengono mai rimosse username e password. Verrà a breve introdotta una procedura periodica di controllo per rimuovere gli utenti deceduti.

Il timeout della sessione dell'IdP è attualmente di 2 ore, ma verrà probabilmente portato a mezz'ora, secondo le raccomandazioni di Idem.

7 L'accreditamento per la categoria @unipd.it

7.1 Modalità di riconoscimento della persona e consegna delle credenziali

Come per gli utenti della categoria @studenti.unipd.it, anche per quelli di questa categoria, molto meno numerosa, vi sono dei Servizi (Servizio Concorsi e Carriere Docenti, Servizio Relazioni Sindacali) preposti all'accettazione e all'inserimento nel sistema gestionale delle risorse umane Giada.
Il riconoscimento dell'utente avviene sempre alla firma del contratto, dietro presentazione di un documento d'identità valido
Alcuni giorni dopo la firma del contratto l'utente chiama gli operatori del Centro di Calcolo che gli comunicano l'indirizzo di posta istituzionale assegnato, il codice di attivazione e l'url dove effettuare l'attivazione della casella.
L'operazione web di attivazione della casella consiste nella scelta della password di propria preferenza e dell'insieme di domande multiple a risposta segreta per il recupero della password.
Terminata l'operazione la casella di posta istituzionale è attiva e le credenziali sono da subito utilizzabili per accedere ai servizi sotto Single Sign On.

7.2 Gestione del ciclo di vita e durata dell'accreditamento

Gli utenti afferenti alla categoria @unipd.it conservano le credenziali di accesso fino a quando è loro concessa la posta di ateneo: a carriera aperta e per un certo lasso di tempo dopo la chiusura (4 anni e mezzo per i docenti, 1 anno per gli altri).

Durante questo periodo l'autenticazione è sempre possibile, e il controllo degli accessi viene demandato alle applicazioni accedute mediante l'invio degli attributi.
La mappatura sulle affiliazioni Idem avviene però solo quando la carriera è aperta.

Se lo stesso utente ricomincia una nuova carriera, gli viene riasseganato lo stesso indirizzo di posta.
Il centro di Calcolo mantiene lo storico degli indirizzi di posta istituzionale assegnati, evitandone la riassegnazione futura ad altri utenti.

7.3 Formato e regole delle credenziali

Lo username coincide con la casella di posta istituzionale ed è formato secondo l'algoritmo nome.cognome@studenti.unipd.it.
Eventuali omonimie vengono risolte non mediante aggiunta di numerico progressivo, ma secondo la regola del buon senso (ad es. m.rossi@unipd.it), quando l'utente telefona al Centro di Calcolo per sapere l'indirizzo che gli è stato assegnato.
Non è in seguito consentito all'utente, se non come eccezione, il cambio della casella di posta scelta..

La password dev'essere di almeno 8 caratteri, contenere almeno una maiuscola, un numero e un carattere speciale: (punto), (due punti), (punto e virgola),(meno).
La password comunque scade dopo 3 mesi ed è imposto il non riutilizzo della password precedente.
Se l'utente si ricorda di cambiarla per tempo, la procedura di cambio password richiede la conoscenza della vecchia.
Se l'utente la lascia scadere dovrà invocare la procedura di recupero password e rispondere alle domande la cui risposta aveva dato in fase di attivazione della casella.

7.4 Eventuale presenza di credenziali multiple per la stessa persona

Sono ancora possibili credenziali multiple di tipo @unipd.it, ma è in atto una procedura di normalizzazione per portarle ad una sola.
Sono invece possibili e frequenti credenziali multiple @studenti.unipd.it e @unipd.it, ad es. per dipendenti che siano anche studenti.
Il limite delle credenziali multiple è che l'insieme degli attributi dell'utente può variare a seconda delle credenziali utilizzate, ad ed la matricola (da studente o da dipendente), o la mappatura sulle affiliazioni Idem

7.5 Disabilitazione utente

L'utente non viene cancellato dal server di autenticazione. Se è necessario disabilitarlo gli viene impostata la password a valore a lui ignoto ed inibita la procedura di recupero password.

7.6 Recupero delle credenziali smarrite

L'utente può recuperare le credenziali smarrite:

- via web, mediante risposta alle domande segrete impostate in fase di attivazione della casella di posta
- presentandosi ad un ufficio preposto con un documento d'identità valido

7.7 Rischi specifici associati alla categoria di utenti

Vi è un lieve rischio di furto di identità dovuto al meccanismo di consegna delle credenziali: una persona a conoscenza del meccanismo, e che sapesse che qualcuno ha appena firmato un contratto, potrebbe telefonare al Centro di Calcolo e impersonificarlo.
Si ritiene basso il rischio perché, se anche succedesse, l'interessato verrebbe subito a saperlo quando telefona per l'attivazione della casella.
In futuro il sistema di assegnazione delle credenziali verrà reso contestuale alla firma del contrato, eliminando il rischio.

Il timeout della sessione dell'IdP è attualmente di 2 ore, ma verrà probabilmente portato a mezz'ora, secondo le raccomandazioni di Idem.

8 Partecipazione ad altre federazioni

L'ateneo non partecipa attualmente ad altre federazioni.