Documento descrittivo del processo di accreditamento degli utenti

Università di Pisa

Le informazioni fornite in questo documento sono accurate alla data: ottobre 2011

Gestore dell'accreditamento

Il processo di accreditamento è gestito dalle seguenti strutture:

- **Area Reclutamento e Amministrazione del Personale**: per il personale che ha stipulato un contratto di collaborazione o insegnamento con l'Università di Pisa (CSA);
- **Area Servizi per la Didattica**: per gli studenti immatricolati a qualsiasi titolo presso l'Università di Pisa (ESSE3);
- **Centri di Spesa (Facoltà, Dipartimenti, Biblioteche, Poli Didattici,..)**: per tutti i soggetti che hanno rapporto di lavoro con le stesse;
- **Servizio Reti e Fonia Serra:** per tutti i soggetti che hanno esigenze "istituzionali" di accesso ai servizi

La raccolta dei dati, il filtraggio e l'armonizzazione sono in capo al **Servizio Reti e Fonia Serra**.

Utenti Gestiti

Personale

Gli utenti gestiti dall' **Area Reclutamento a Amministrazione del Personale:**

- docenti;
- ricercatori;
- personale T/A a tempo determinato e indeterminato;
- titolari di assegni di ricerca;
- collaboratori co.co.co, co.co.pro.

Studenti

Gli utenti gestiti dall' **Area Servizi per la Didattica:**

- studenti dei corsi di laurea (di base, specialistiche);
- dottorandi;
- specializzandi;
- studenti dei master.

Nota: gli sudenti erasmus verranno gestiti a breve con modalità analoghe.

Esterni

Gli utenti gestiti dai **Centri di Spesa** periferici:

- ospiti temporanei;
- rapporti di lavoro assimilabili al personale interno;
- studenti erasmus.

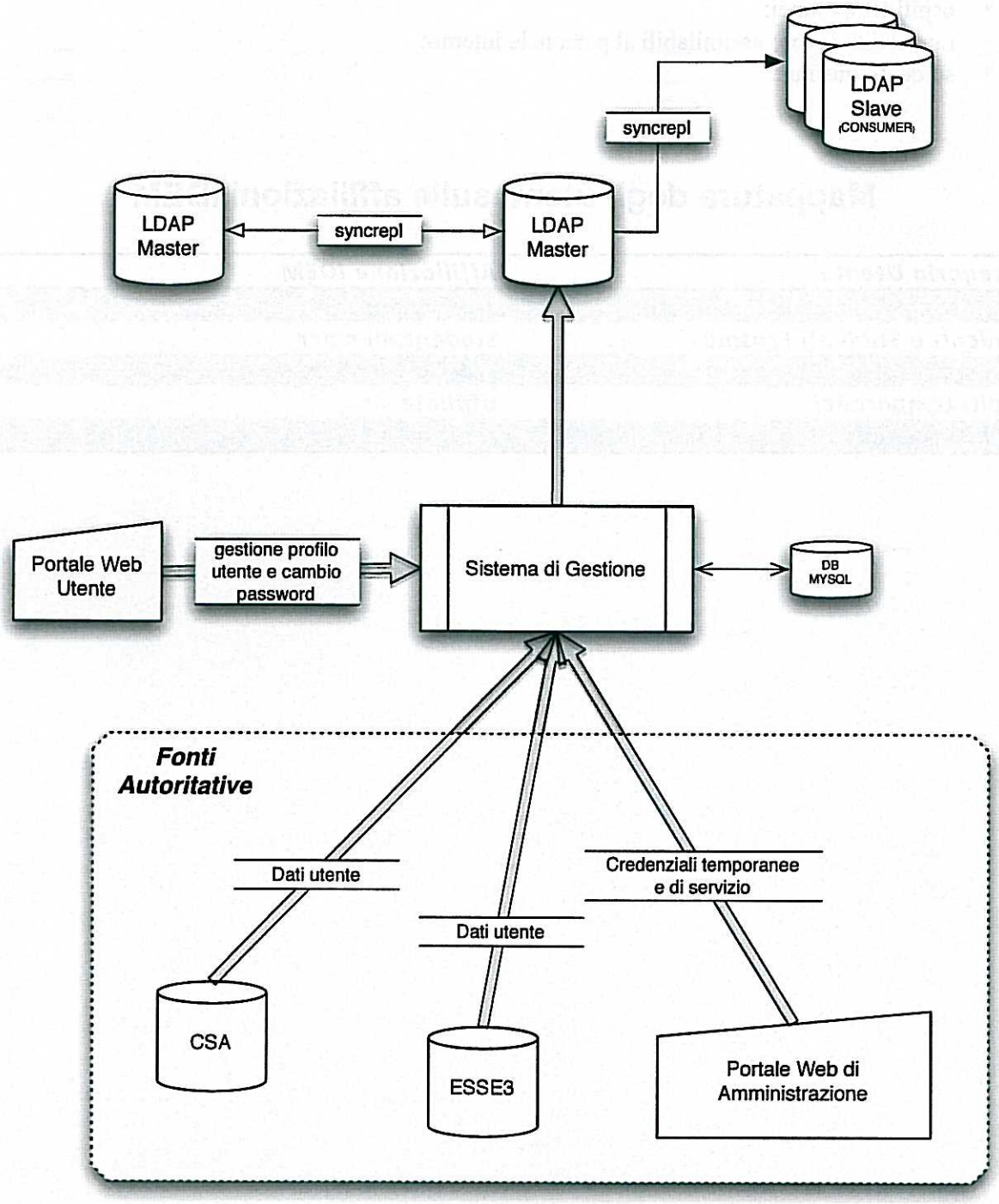
Mappatura degli utenti sulle affiliazioni IDEM

Categoria Utente	*Affiliazione IDEM*
Tutte le categorie del Personale	*staff,member*
Studenti e Studenti Erasmus	*student,member*
Dottorandi	*staff,student,member*
Ospiti temporanei	*affiliate*
Esterni assimilabili al personale interno	*staff,member*

Visione d'insieme del processo di accreditamento utenti

Architettura

La figura seguente descrive il flusso dati relativo alla creazione delle credenziali utente:



Il Sistema di Gestione è una collezione di procedure sviluppate in casa alimentato dalle fonti autoritative che si occupa di creare e mantenere aggiornato il Directory. Le procedure di

trattamento dei dati autoritativi provenienti da CSA e ESSE3 sono regolamentate mediante cron con frequenza giornaliera e oraria rispettivamente.

Le modifiche richieste tramite il ***Portale di Amministrazione*** e il ***Portale Utente*** sono invece gestite in tempo reale.

Fonti autoritative

CSA: database dell' **Area Reclutamento a Amministrazione del Personale;**
ESSE3: database dell'**Area Servizi per la Didattica;**
Portale di Amministrazione: applicativo sviluppato in casa per la gestione delle credenziali.

Uso delle credenziali

Attualmente le credenziali sono utilizzate per i seguenti servizi:

- posta elettronica;
- gestione presenze;
- gestione cedolino;
- accesso rete autenticata (wired e wireless);
- siti web che prevedono accesso autenticato (tipicamente mediante plugin ldap dei cms utilizzati);
- servizio VPN centralizzato;
- piattaforme di E-Learning Moodle e Claroline.

Sono in fase di perfezionamento i seguenti servizi:

- servizi bibliotecari di consultazione e prestito;
- fax server centralizzato.

Il processo di accreditamento per la categoria di utenti: personale

Il processo

Gli uffici coinvolti nella gestione delle identità di questa categoria sono quelli **dell'Area Reclutamento e Amministrazione del Personale**. Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali per la categoria trattata.

Modalità di riconoscimento della persona

Presenza fisica negli uffici preposti e riconoscimento tramite documento d'identità e codice fiscale.

Caratteristiche dell'identità digitale

- 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.).
- attributi associati all'identità digitale considerati **pubblici**: nome e cognome, telefono, fax, mail, area e struttura di appartenenza, afferenza didattica.

Gestione del ciclo di vita

L'aggiornamento del database delle identità digitali è a carico degli uffici preposti. Ogni modifica portata nel **DB CSA** viene elaborata da ***Sistema di Gestione*** durante la notte seguente. Quando il rapporto con l'Ateneo cessa il ***Sistema di Gestione*** registra su ldap lo stato "fuoriruolo" e la "data di cessazione". La entry rimane in ldap per 18 mesi.

Formato e regole delle credenziali

Le credenziali fornite sono una coppia 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. Non sono attualmente presenti meccanismi per l'obbligo programmatico di cambio password.

A tutti i dipendenti viene inoltre rilasciata una tessera con banda magnetica utilizzata per rilevare le presenze.

Eventuale presenza di credenziali multiple per la stessa persona

Non vengono rilasciate credenziali multiple.

Modalità di consegna delle credenziali

Le credenziali sono consegnate brevi manu dall'ufficio gestore alla persona in busta chiusa.

Sono in corso di perfezionamento procedure per la semplificazione di questo processo mediante creazione di token di attivazione spediti agli interessati via e-mail ad un indirizzo esterno fornito dall'utente in fase di registrazione del rapporto di lavoro.

Modalità di recupero delle credenziali smarrite

La riemissione della password e dello userid possono essere ottenute contattando l'ufficio preposto.

È in fase di completamento la semplificazione di queste procedure mediante servizi web. Per la riemissione della password l'utente deve preventivamente fornire alcune informazioni aggiuntive tramite il ***Portale Utente*** che permettono al ***Sistema di Gestione*** di identificarlo in modo univoco. Per lo userid smarrrito sarà sufficiente fornire via web il proprio codice fiscale.

Modalità di gestione smarrimento smartcard/token

Non sono attualmente utilizzate.

Durata dell'accreditamento

Gli utenti sono accreditati per tutto il tempo in cui sussiste il rapporto di lavoro e fino a 18 mesi oltre la "data di cessazione", descritta nel paragrafo ***Gestione del ciclo di vita.***

Disabilitazione utente

Non è gestita.

Cancellazione definitiva utente

Un utente è cancellato da ldap dopo che sono scaduti tutti i suoi incarichi e per ciascun incarico scaduto sono decorsi i tempi di conservazione previsti.

Rischi specifici associati alla categoria di utenti

La correttezza dei dati presenti in ldap dipende da operazioni manuali di gestione della fonte autoritativa. Per evitare possibili inconsistenze sono previste periodiche verifiche incrociate dei dati ldap e i dati contenuti nel db del sistema di gestione del personale.

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

Nessuna.

Il processo di accreditamento per la categoria di utenti: studenti

Il processo

Gli uffici coinvolto nella gestione delle identità di questa categoria sono quelli dell'**Area Servizi per la Didattica**. Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento delle identità digitali per la categoria trattata.

Modalità di riconoscimento della persona

Presenza fisica negli uffici preposti e riconoscimento tramite documento d'identità e codice fiscale.

Caratteristiche dell'identità digitale

- attributi associati all'identità digitale: dati anagrafici, i dati della facoltà, del corso di laurea, dell'indirizzo di studi, dell'anno di corso, dello stato di avanzamento degli studi.
- attributi associati all'identità digitale considerati **pubblici**: nessuno.

Gestione del ciclo di vita

L'aggiornamento del database delle identità digitali è a carico degli uffici preposti. Ogni modifica portata nel **DB ESSE3** viene elaborata da ***Sistema di Gestione*** durante l'ora seguente.

Il ciclo di vita è pilotato dalle variazioni dei dati nel sistema di gestione degli studenti esse3. Dopo la chiusura della carriera dello studente la entry rimane in ldap per 18 mesi.

In caso di rinuncia o trasferimento ad altro ateneo la entry viene cancellata immediatamente da ldap.

Infine, in caso di mancato pagamento delle tasse universitarie la entry rimane in ldap per 18 mesi.

Formato e regole delle credenziali

Le credenziali fornite sono una coppia 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. Non sono attualmente presenti meccanismi per l'obbligo programmatico di cambio password.

Eventuale presenza di credenziali multiple per la stessa persona

In alcuni casi particolari è prevista la generazione di due identità digitali. Si tratta degli studenti dottorandi e degli studenti di master. Questi utenti hanno un'identità digitale con validità

permanente per la carriera universitaria ed un'identità digitale con validità determinata per il solo periodo di durata del corso di dottorato o di master.

Modalità di consegna delle credenziali

Le credenziali **ESSE3** vengono consegnate dalla segreteria all'atto di immatricolazione. Le stesse credenziali vengono automaticamente create su ldap dopo al massimo 1 ora.

Modalità di recupero delle credenziali smarrite

La riemissione della password e dello userid possono essere ottenute contattando la **Segreteria Studenti**. I dati ldap vengono automaticamente sincronizzati entro1 ora dalla variazione su ESSE3.

Modalità di gestione smarrimento smartcard/token

Non sono attualmente utilizzate.

Durata dell'accreditamento

Gli studenti sono accreditati per tutto il tempo in cui resta aperta la loro carriera nel sistema di gestione ESSE3.

Disabilitazione utente

Non è gestita.

Cancellazione definitiva utente

Non è prevista la cancellazione dell'identità digitale di uno studente da sistema ESSE3. Una entry è cancellata da ldap dopo che sono trascorsi 18 mesi dalla chiusura della carriera su ESSE3.

Rischi specifici associati alla categoria di utenti

Le password della credenziale per l'accesso ai servizi di Ateneo è la stessa utilizzata da ESSE3 e da tutti i servizi studenti.

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

Nessuna.

Il processo di accreditamento per la categoria di utenti: esterni

Il processo

Gli uffici coinvolto nella gestione delle identità di questa categoria sono i referenti per le credenziali nelle strutture periferiche (dipartimenti, facoltà, Poli didattici) e nell'Amministrazione Centrale. Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento delle identità digitali per la categoria trattata.

Modalità di riconoscimento della persona

Presenza fisica negli uffici preposti e riconoscimento tramite documento d'identità e codice fiscale.

Caratteristiche dell'identità digitale

- attributi associati all'identità digitale: i dati anagrafici, codice fiscale, struttura di affiliazione, data di scadenza dell'incarico
- attributi associati all'identità digitale considerati **pubblici**: nessuno

Gestione del ciclo di vita

I dati per la creazione delle credenziali vengono spediti via fax dai referenti al **Servizio Reti e Fonia Serra.** Il responsabile del servizo usa il ***Portale di Amministrazione*** per l'aggiornamento del sistema, che viene fatto in tempo reale.

Formato e regole delle credenziali

Vedi categoria *Personale*.

Eventuale presenza di credenziali multiple per la stessa persona

Vedi categoria *Personale*.

Modalità di consegna delle credenziali

Gli utenti devono presentarsi muniti di documento di riconoscimento al **Servizio Reti e Fonia Serra** dove vengono loro consegnate le credenziali in busta chiusa.

È in fase di perfezionamento una procedura web, analoga a quella prevista dalla categoria *Personale*, che permetterà ai referenti di consegnare le credenziali in modo autonomo eliminando i tempi di attesa per l'inoltro del fax e la successiva elaborazione della richiesta.

Modalità di recupero delle credenziali smarrite

Vedi categoria *Personale*.

Modalità di gestione smarrimento smartcard/token

Non sono attualmente utilizzate.

Durata dell'accreditamento

Fino alla conclusione del rapporto di lavoro. Scaduto tale termine la entry viene immediatamente rimossa da ldap.

Disabilitazione utente

Non è gestita.

Cancellazione definitiva utente

Dopo 3 mesi dalla conclusione del rapporto di lavoro.

Rischi specifici associati alla categoria di utenti

Non si evidenziano rischi specifici.

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

Nessuna.

Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione crea identificatori utente univoci che non possono essere riutilizzati. La tendenza attuale è quella di utilizzare il Directory di Ateneo, basato su openldap, quale sistema principale di autenticazione. Per il futuro il progetto è quello di aderire a IDEM e di proporre l'IdP per l'autenticazione federata quale meccanismo di SSO per tutte le applicazioni interne.

Per quanto riguarda la sicurezza sono state adottate le buone pratiche di gestione dei server linux quali aggiornamenti del sistema operativo, patch di sicurezza, comunicazioni crittografate. Infine, per le impostazioni dei timeout e la terminazione delle sessioni sono stati utilizzati i valori di default di Shibboleth.

Partecipazione ad altre federazioni

L'università di Pisa non partecipa attualmente ad altre federazioni. È in progetto l'adesione alla confederazione ***EDUROAM***, coordinata dal ***Consortiun GARR***.