Documento descrittivo del processo di accreditamento degli utenti

Università di Modena e Reggio nell'Emilia

27 novembre 2009

1 Gestore dell'accreditamento

L'accreditamento è gestito dalle strutture decentrate: segreterie studenti per gli studenti, ufficio personale per i dipendenti, centri, dipartimenti e facoltà per coloro che hanno rapporti con le stesse.

La raccolta dei dati, il filtraggio e l'armonizzazione è in capo ai Servizi informatici (gestionali, statistica, web, identity management), della Direzione pianificazione, valutazione e formazione.

2 Utenti gestiti

2.1 Personale dipendente

Sono gli utenti i cui dati provengono dall'ufficio risorse umane. Sono:

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

2.2 Studenti

Sono gli utenti i cui dati provengono dalle segreterie studenti.

- studenti delle lauree di base e specialistiche;
- dottorandi;
- specializzandi;
- studenti dei master.

2.3 Esterni

Sono gli utenti identificati dalle strutture periferiche:

Descrizione	Affiliation
rapporti che richiedono il solo accesso alla rete	affiliate
rapporti assimilabili allo studente	student,member
rapporti assimilabili al docente (supplente, contrattista, ecc...)	employee,member

Tabella 1: Ruoli esterni e loro mappatura nelle affiliation

3 Mappatura degli utenti interni sulle affiliazioni

Descrizione	Affiliation
Personale non docente	staff,employee,member
Lettore di madre lingua	staff,employee,member
Collaboratori linguistici (td INPDAP)	staff,employee,member
Primi dirigenti	employee,member,student
Ricercatori Universitari	faculty,employee,member
Dottorandi	employee,member,student
Professori Associati	faculty,employee,member
Assegnisti di ricerca	employee,member
Assistenti universitari	faculty,employee,member
Professori Ordinari	faculty,employee,member
Non docenti a tempo det-Tesoro	staff,employee,member
Dirigente a contratto	staff,employee,member
Dirigente	staff,employee,member
Collaboratori ed esperti linguistici	staff,employee,member

Tabella 2: Ruoli dei dipendenti e loro mappatura nelle affiliation

Per la mappatura degli esterni si veda la tabella 1 a pagina 2.

4 Visione d'insieme del processo di accreditamento

Le credenziali utente (numero del badge di riconoscimento e la coppia di valori nome utente/password) sono immagazzinati su un cluster openldap che contiene solo dati che dipendono da altre fonti. In altre parole, la perdita del cluster ldap rappresenta un downtime dei servizi di autenticazione ma è possibile rigenerare i dati dalle fonti originarie come prima del disastro.

I dati dalle fonti autoritative sono processati offline tutte le notti. La procedura genera un file ldif che viene applicato come diff al server ldap per avere i dati aggiornati.

L'unico dato aggiornato in tempo reale su ldap è la password utente che, per la necessità di non avere dati che risiedano solo su ldap, è salvata anche su un db mysql.

Oltre al cluster openldap esistono diversi server openldap replica in modalità syncrepl per aumentare la disponibilità.

4.1 Fonti dati autoritative

- db delle segreterie studenti (Esse3);
- db dell'ufficio risorse umane (CSA);
- db degli esterni (software sviluppato *in house* PI);
- db dei contatti telefonici e delle mail (software sviluppato *in house* mailamdin); i dati telefonici sono immessi dall'utente;
- db delle password e degli username;
- file di testo per gli eduPersonEntitlement.

4.2 Integrazione e inserimento in ldap

Il compito del programma di integrazione e inserimento in ldap è correlare i dati della stessa persona per generare uno o più entry ldap. La chiave di correlazione è il codice fiscale.

Esistono due tipi di entry ldap (differenziate dallo schema): *unimoreDipendente* e *unimoreStudente*. Se un utente è sia studente che dipendente ha due entry. Se un utente ha profili multipli (dipendente che ha incarichi in diverse strutture o dipendente che fornisce anche servizi esterni o fornitore esterno per più strutture) ha comunque una sola entry che contiene gli attributi provenienti dai vari incarichi.

Questo programma gestisce anche lo spazio degli username. Gli studenti hanno una username puramente numerica (es: *50000*) che coincide con il loro numero tessera. I dipendenti hanno una username che non può essere puramente numerica e che è salvata nel db degli username/passwd.

Per nessun motivo gli username vengono riassegnati ad utenti diversi in qunato viena mantenuta una banca dati degli username già utilizzati.

4.3 Uso delle credenziali

Gli utenti fanno uso delle credenziali principalmente per:

- autenticazioni shibboleth (vari servizi web interni all'Ateneo);

- autenticazioni dirette su ldap (autenticazioni pam per linux, autenticazioni radius per la navigazione, accesso wi-fi tramite captive portal, ...);
- accesso ai domini samba;
- controllo accesso che richiede il passaggio della tessera magnetica (parcheggi, accesso alle biblioteche);
- e per tutti i servizi che richiedono autenticazione che sono in continua crescita.

5 Il processo di accreditamento per il personale dipendente

5.1 Panoramica

L'ufficio coinvolto nella gestione delle identità del personale è l'ufficio risorse umane che inserisce l'utente nel db del personale:

5.2 Modalità di riconoscimento della persona

Documento d'identità e codice fiscale.

5.3 Caratteristiche dell'identità digitale

Oltre ai dati anagrafici (schema inetOrgPerson), ai dati posix (posixAccont) e samba (sambaAccount) sono presenti i dati di rubrica (mail, telefono, fax), il codice fiscale, la matricola, la tessera, il numero del badge e i dati dell'inquadramento (struttura di appartenza, afferenza didattica, inquadramento – ad es: `D2` –, stato di servizio – `in servizio`, `cessato`, ecc –, e diversi altri della stessa natura).

Gli unici dati pubblici sono nome e cognome, telefono, fax, mail, struttura di appartenenza, afferenza didattica e stato di servizio.

5.4 Gestione del ciclo di vita

Quando nel db CSA un utente subisce variazioni, queste vengono recepire da ldap il giorno successivo.

Se la variazione riguarda la cessazione (pensione, dimissioni o simili) in LDAP viene aggiornato lo stato come `Non piu' in rapporto con l'Universita'`. Quando un dipedente cessa per qualunque motivo viene aggiunto un attributo `unimoredatacessazione`, e la entry rimane in ldap per sei mesi.

5.5 Formato e regole delle credenziali

A tutti i dipendenti viene rilasciata una tessera con banda magnetica e una coppia username/password.

Nel 2010 verrà stabilito l'obbligo del cambio password ogni sei mesi. Al cambiamento verrà verificata la lunghezza minima della password a 8 caratteri.

5.6 Eventuale presenza di credenziali multiple per la stessa persona

Le credenziali multiple (tessera con banda magnetica e una coppia username/password) servono per servizi diversi e non interagiscono.

5.7 Modalità di consegna delle credenziali

Dopo l'assunzione il dipendente si connette a un sito web che, richiesti codice fiscale e numero di matricola, permette la scelta dello username. Fino alla scelta dell'username all'utente viene associata una entry che non ha possibilità si autenticarsi su nessun servizio salvo quelli che usano la sola tessera magnetica (parcheggi, accessi ai tornelli delle strutture).

Lo username è scelto dall'utente tra quelli liberi nello spazio dei nomi.

La password iniziale fino al primo cambio password è il numero di matricola.

5.8 Modalità di recupero delle credenziali smarrite

Tutti i dipendenti hanno anche un account di posta. La posta autentica gli utenti su un db autonomo da ldap ma mantenuto sincronizzato. Uno dei requisiti per non rompere il sincronismo è che un utente con account di posta debba cambiare la password nel sito web della posta che inoltra la passwd a ldap (il viceversa non è vero).

Il reset della password per la posta (che quindi implica anche il reset della password ldap) avviene con richiesta per fax agli incaricati. La nuova password è il codice fiscale dell'utente in maiuscolo.

5.9 Modalità di gestione smarrimento smartcard/token

Gli utenti possono avere un badge con banda magnetica con o senza smartcard per la firma digitale con validità legale.

In caso di smarrimento è revocato il precedente ed emesso una nuovo; se risulta smarrito un badge con smartcard si gestisce in aggiunta il processo di revoca presso l'ente erogatore (Infocamere).

5.10 Durata dell'accreditamento

I dipendenti sono accreditati per tutto il tempo in cui sussiste il rapporto di lavoro e fino a sei mesi oltre la scadenza risultante dal db dell'ufficio risorse umane.

5.11 Disabilitazione utente

Non è gestita.

5.12 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 mesi di policy di conservazione (6 mesi per tutti i ruoli dipendenti)

5.13 Rischi specifici associati alla categoria utenti

- credenziali iniziali prevedibili (numero di matricola). Questo rischio si chiude al primo cambio password;
- dopo la scadenza la entry resta in ldap per sei mesi con una marcatura poco evidente.

5.14 Interoperabilità tra credenziali deboli e eventuali credenziali forti (smartcard)

Non esistono servizi che possono accettare username/password oppure smartcard. I servizi usano l'una o l'altra.

6 Il processo di accreditamento per gli studenti

6.1 Panoramica

L'ufficio responsabile è la segreteria studenti.

6.2 Modalità di riconoscimento della persona

Documenti e tesserino del codice fiscale.

6.3 Caratteristiche dell'identità digitale

Oltre ad anagrafica, posixAccount e sambaAccount nello schema *unimoreStudente* ci sono i dati della facoltà, corso di laurea, indirizzo di studio, anno di corso situazione di in corso/fuori corso ecc.

Nessuno di questi dati è pubblico. Per gli studenti neppure le informazioni anagrafiche sono pubbliche.

6.4 Gestione del ciclo di vita

Il ciclo di vita è pilotatq dalle variazioni dei dati nel sistema di gestione degli studenti esse3.

6.5 Formato e regole delle credenziali

Stesse dei dipendenti.

6.6 Eventuale presenza di credenziali multiple per la stessa persona

Idem come i dipendenti; nelle torrette gli studenti usano badge e password.

6.7 Modalità di consegna delle credenziali

All'iscrizione insieme al libretto. La password iniziale è la stessa dell'accesso al sistema esse3, che ha un'autenticazione autonoma dall'identity management di ateneo. Nel 2010 verrà introdotto l'obbligo del cambio password ogni sei mesi.

6.8 Modalità di recupero delle credenziali smarrite

È possibile resettare la password ldap alla password di esse3 che a sua volta può essere variata in presenza agli sportelli di segreteria.

6.9 Modalità di gestione smarrimento token

Richiesta alla segreteria studenti.

6.10 Durata dell'accreditamento

In caso di cessazione o trasferimento ad altro ateneo l'utente è cancellato da ldap dal giorno successivo; in caso di conseguimento del titolo di studio l'utente resta in ldap per tre anni. La affiliation non cambia ad *alum.* Viene aggiunto un attributo per tenere traccia di questo evento.

6.11 Disabilitazione utente

Non è prevista.

6.12 Cancellazione definitiva utente

Dopo tre anni dal conseguimento del titolo l'utente è cancellato da ldap.

Dal giorno successivo alla cessazione o per altri motivi, al trasferimento in uscita l'utente è cancellato da ldap.

6.13 Rischi specifici associati alla categoria utenti

- La possibilità di resettare la password a quella di esse3;
- dopo la scadenza la entry resta in ldap per tre anni con una marcatura poco evidente.

7 Il processo di accreditamento per gli esterni

7.1 Panoramica

Gli esterni sono accreditati dalla struttura presso cui hanno il titolo che conferisce loro l'accesso all'identity management di ateneo.

Ogni struttura (dipartimento, centro, facoltà ecc.) nomina uno o più incaricati all'identificazione che possono identificare il personale esterno. Per l'identificazione l'esterno deve produrre un documento, il codice fiscale e il titolo per l'inserimento.

L'incaricato all'identificazione inserisce l'identità dell'esterno e vi associa uno o più incarichi (che quindi possono essere multipli perché un utente può essere esterno per più strutture).

Gli incarichi devono avere una scadenza, che coincide con quella del titolo dell'inserimento e che non può essere maggiore di tre anni.

Se si tratta del primo incarico, l'utente riceve un PIN con il quale può scegliere la username in una form web (è richiesto anche il codice fiscale). Fino alla scelta della username l'utente è nel limbo (vedi i dipendenti).

7.2 Modalità di riconoscimento della persona

Documenti e codice fiscale.

7.3 Caratteristiche dell'identità digitale

Oltre ai soliti dati degli schemi inetOrgPerson, posixAccount e sambaAccount sono valorizzati alcuni attributi dello schema *unimoreDipendente* con le indicazioni del ruolo dell'utente e della struttura presso cui è affiliato. Un attributo che è sempre presente per gli esterni è la data di scadenza dell'incarico, che permette di stabilire se un incarico è scaduto.

7.4 Gestione del ciclo di vita

Come al solito segue le variazioni dei dati nel db.

7.5 Formato e regole delle credenziali

Sono le stesse dei dipendenti.

7.6 Eventuale presenza di credenziali multiple per la stessa persona

Idem come i dipendenti.

7.7 Modalità di consegna delle credenziali

Al momento dell'identificazione: PIN e compilazione di una form web.

7.8 Modalità di recupero delle credenziali smarrite

Se l'utente ha un account di posta dell'ateneo segue la stessa procedura dei dipendenti, altrimenti è possibile resettare la password al PIN iniziale con richiesta all'ufficio gestione delle identità.

7.9 Modalità di gestione smarrimento smartcard/token

Idem come i dipendenti.

7.10 Durata dell'accreditamento

Dipende dalla policy che a sua volta dipende dal ruolo. È prevista la presenza per un periodo di 6 mesi a decorrere dalla cessazione.

7.11 Disabilitazione utente

Non è prevista.

7.12 Cancellazione definitiva utente

Dopo che sono passati i mesi di policy di mantenimento dell'ultimo incarico, l'utente è cancellato da ldap.

7.13 Rischi specifici associati alla categoria utenti

- Dopo la scadenza la entry resta in ldap con una marcatura poco evidente.

8 Il sistema di autenticazione e autorizzazione interno

Gli username sono univoci e non possono essere riutilizzati neppure in tempi diversi.

Pur con numerosi compromessi, la tendenza ad autenticare le più varie applicazioni sul sistema di gestione delle identità di ateneo è fortissima ed

impedisce di completare un loro censimento completo. Ad esempio ci sono almeno una ventina di Shibboleth-SP interni.

Questo ateneo mira ad impiegare nell'accesso ad IDEM lo stesso IdP che usa per le autenticazioni interne. Gli aspetti chiave della sicurezza dello IdP sono il rispetto delle buone pratiche di gestione dei server Linux, la lettura della mailing list degli utenti Shibboleth, l'aggiornamento del server alle ultime versioni.

Per quel che riguarda le impostazioni dei timeout e la terminazione delle sessioni non si è modificato il valore predefinito dell'installazione Shibboleth.

9 Partecipazione ad altre federazioni

Oltre all'uso interno questo ateneo usa Shibboleth per autenticare i propri utenti con servizi gestiti esternamente:

- ER-GO (azienda diritto allo studio);
- Comune di Reggio nell'Emilia per la navigazione wi-fi nella città;
- google apps per la posta degli studenti;
- Metalib – software di ricerca bibliografica;
- DataManagement per il software Sebina Open Library.

Nessuno di questi servizi è una federazione propriamente detta perché si tratta di accordi bilaterali.