DOCUMENTO DESCRITTIVO DEL PROCESSO DI ACCREDITAMENTO DEGLI UTENTI DELL'UNIVERSITÀ DEGLI STUDI DI MILANO-BICOCCA

Le informazioni fornite in questo documento sono accurate alla data del 05/07/2010

ABBREVIAZIONI

Si abbrevierà con "Università" il nome completo dell'Università degli Studi di Milano-Bicocca.

Per indicare l'Area del Personale verrà utilizzato l'acronimo AdP.
L'Area Segreteria Studenti sarà abbreviata in AS.
L'Area Sistemi Informativi d'ora innanzi sarà abbreviata con SI.

GESTORE DELL'ACCREDITAMENTO

L'assegnazione, il mantenimento e la cancellazione delle identità digitali degli utenti sono gestite a seconda della tipologia d'utenza dall'Area del Personale, dall'Area Segreteria Studenti, dai singoli dipartimenti, o dai Referenti Informatici dei vari dipartimenti; e dall'Area Sistemi Informativi in maniera trasversale a tutte le aree precedenti.

UTENTI GESTITI

In seguito vengono elencate e descritte tutte le categorie di utenti gestite dall'Università. Esse sono divise in tre macro-categorie (Utenti, Studenti, Ospiti).

Per ogni categoria è stata riportata la cardinalità, che per natura è dinamica, al momento della stesura del documento; e l'affiliazione IDEM.

PERSONALE TECNICO, AMMINISTRATIVO E DOCENTE

- Assegnista di ricerca (279) - staff, member
- Collaboratore esterno identificato (432) – affiliate
- Cultore della materia (9) – staff, member
- Docente a contratto (93) – staff, member
- Collaboratore ex strutturato (54) – nessuna affiliazione
- Tutor (27) – staff, member
- Professore ordinario (220) – staff, member
- Professore straordinario (29) – staff, member
- Professore associato (53) – staff, member
- Professore associato confermato (207) – staff, member
- Ricercatore (161) – staff, member
- Ricercatore confermato (253) – staff, member
- Ricercatore a tempo determinato (12) – staff, member
- Assistente ordinario (2) – staff, member
- Tecnico-amministrativo (692) – staff, member
- Tecnico-amministrativo distaccato da altra amministrazione (4) – staff, member
- Tecnico-amministrativo a tempo determinato (50) – staff, member
- Dirigente (4) – staff, member
- Direttore amministrativo (1) – staff, member
- Dirigente a tempo determinato (1) – staff, member

- Collaboratore ed esperto linguistico in lingua madre (7) – staff, member
- Borsista (0) - member
- Collaborazione coordinata continuativa (0) – staff, member
- Esercitatore (0) – staff, member

Esistono inoltre 667 account "di servizio", ciascuno delle quali ha una entry completa in LDAP e una relativa casella di posta elettronica. Essi hanno accesso a un insieme limitato di servizi d'Ateneo e sono utilizzati in molti casi da più persone (condividendo la password).

Per quanto riguarda questi account lo IdP non rilascia alcun attributo.

È anche presente la categoria "Collaboratore esterno non identificato" (459 unità), si tratta di entry in via di dismissione che sono state registrate in passato usando forme di verifica dell'identità debole o nulla, per le quali, similmente agli account di servizio, lo IdP non rilascia nessun attributo dopo l'autenticazione.

STUDENTI

- Ambito di Mobilità (Erasmus) (894) - student, member
- Ambito di Mobilità: Accordi bilaterali (0) - student, member
- Corso di Aggiornamento (12) - student, member
- Corso di Formazione (188) - student, member
- Corso di Perfezionamento (335) - student, member
- Corso Singolo (302) – student, member
- Corso di Diploma (3) - student, member – immatricolazione non più attiva
- Corso di Dottorato (995) - student, staff, member
- Diploma Universitario (191) - student, member – immatricolazione non più attiva
- Corso di Laurea – vecchio ordinamento quadriennale e quinquennale (4509) - student, member
- Corso di Laurea (32944) - student, member
- Corso di Laurea Specialistica a ciclo unico (5 anni) (72) - student, member
- Corso di Laurea Specialistica a ciclo unico (6 anni) (441) - student, member
- Corso di Laurea Magistrale (4158) - student, member
- Laurea Magistrale Ciclo Unico 5 anni (2173) - student, member
- Laurea Magistrale Ciclo Unico 6 anni (369) - student, member
- Corso di Laurea Specialistica (5658) - student, member
- Master di Primo Livello (640) - student, member
- Master di Secondo Livello (239) - student, member
- Scuola di Specializzazione (360) - student, staff, member
- Scuola di Specializzazione (5 anni) (100) – student, staff, member
- Scuola di Specializzazione (6 anni) (4) - student, staff, member

OSPITI

Gli ospiti sono persone esterne all'Università, con la quale hanno rapporti solo per brevi periodi di tempo (il caso più frequente è quello dei partecipanti a convegni o altre manifestazioni temporanee, che hanno bisogno di accedere alla rete Wi-Fi dell'Università).

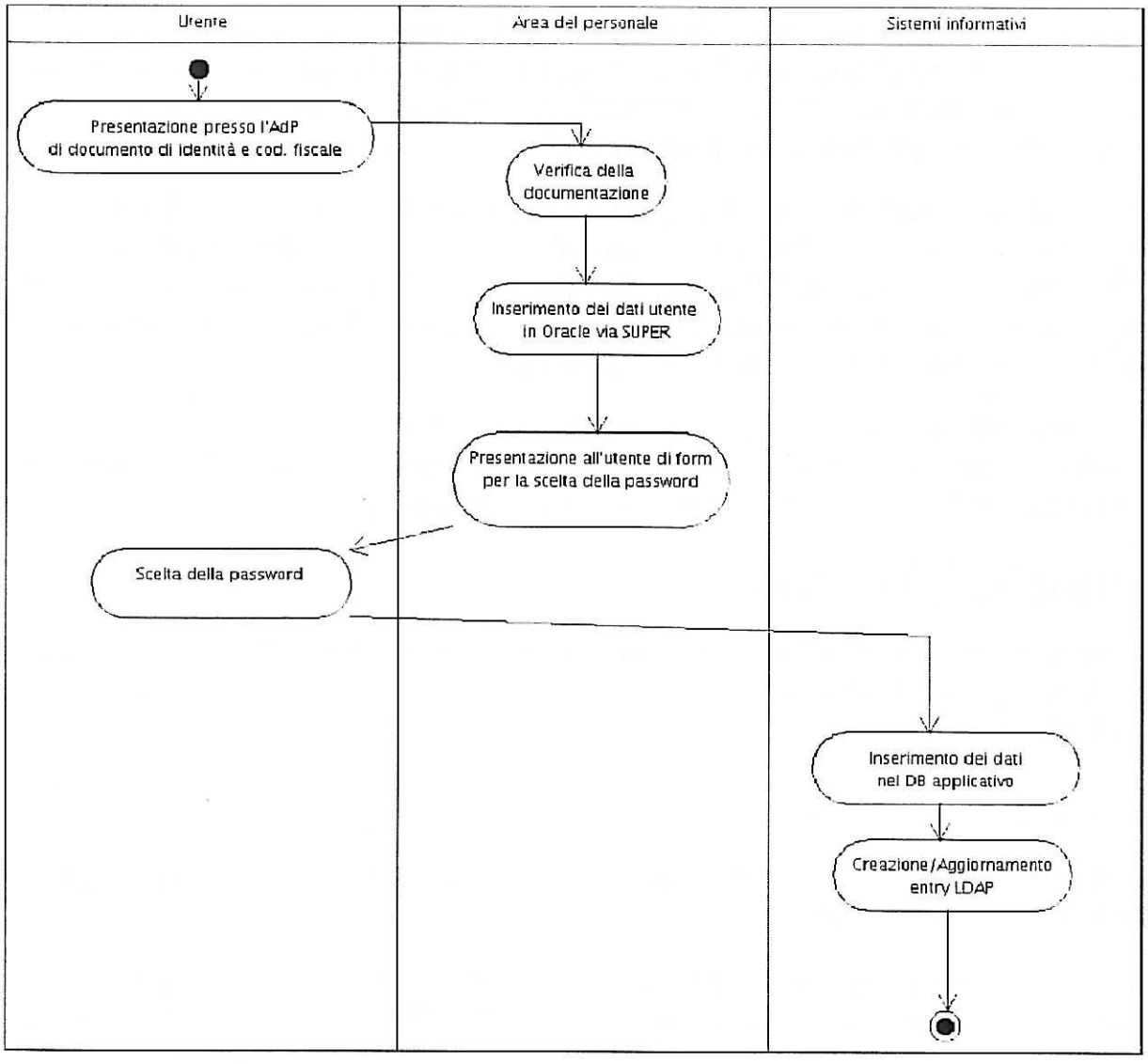
Al momento della stesura di questo documento sono presenti dodici entry ospite. L'affiliazione prevista per IDEM è quella di "affiliate" come stabilito dal documento ST-A.

DESCRIZIONE DEL PROCESSO DI ACCREDITAMENTO DEGLI UTENTI

I processi di accreditamento sono macroscopicamente differenti per quanto riguarda le diverse tipologie di personale (strutturato e non strutturato), gli studenti, e gli ospiti.

IL PROCESSO DI ACCREDITAMENTO PER IL PERSONALE STRUTTURATO

Di seguito viene descritto il processo di accreditamento per le seguenti categorie: Assegnista di ricerca, Borsista, Collaborazione Coordinata Continuativa, Tecnico-Amministrativo, Tecnico-Amministrativo distaccato da altra amministrazione, Dirigente, Direttore Amministrativo, Collaboratore ed esperto linguistico in lingua madre, Tecnico amministrativo a tempo determinato, Professore ordinario, Professore straordinario, Professore associato, Professore associato confermato, Ricercatore, Assistente ordinario, Ricercatore confermato, Ricercatore a tempo determinato.



Schema 1:Il processo di accreditamento per il personale strutturato

MODALITÀ DI RICONOSCIMENTO DELLA PERSONA

Al momento della presa di servizio, il nuovo dipendente si reca presso l'Ufficio dell'AdP per la registrazione.

Il dipendente viene identificato dal personale dell'AdP presentando un documento di identità in corso di validità e il proprio codice fiscale.

CREAZIONE E CARATTERISTICHE DELL'IDENTITÀ DIGITALE

I dati anagrafici e quelli relativi alla posizione del nuovo assunto vengono inseriti nell'infrastruttura informatica dell'Università dal personale dell'AdP attraverso l'applicativo "SUPER Anagrafica" (il quale si appoggia a un DB Oracle). Al momento della creazione dei record nel DB, le informazioni vengono trasferite in un secondo DB (SQL Server) sul quale viene generato lo username che il nuovo utente utilizzerà per l'accesso alla maggior parte dei servizi dell'Ateneo.

Le caratteristiche associate all'identità digitale sono il nome, il cognome, il numero di matricola, il numero di telefono, l'email, il codice fiscale e il rapporto di lavoro della persona. Inoltre sono associate le informazioni relative alla funzione della persona e sono specificati il dipartimento e la struttura di afferenza.

Le informazioni suddette sono conservate sul DB associato a SUPER, sul DB degli applicativi Web dei Sistemi Informativi, e sul sistema di autenticazione LDAP. La password viene generata sul DB applicativo dei Sistemi Informativi e dopo il trasferimento su LDAP (che avviene in maniera asincrona ogni minuto) viene rimossa dal DB, perciò ne esiste una sola copia sulla directory LDAP.

I dati considerabili pubblici (ed effettivamente pubblicati sulla rubrica online d'Ateneo, accessibile a chiunque) sono il nome e cognome dell'utente, il suo ruolo e la struttura di afferenza, l'indirizzo e-mail e il numero di telefono dell'ufficio.

GESTIONE DEL CICLO DI VITA

Nel caso di cambiamenti del rapporto di lavoro della persona con l'Università, la posizione viene aggiornata dal personale dell'AdP; le modifiche vengono propagate fino alla entry LDAP.

FORMATO E REGOLE DELLE CREDENZIALI

Le principali credenziali dell'utente sono costituite una coppia userID/password, tali credenziali non hanno scadenza.

A ciascun utente che ne faccia richiesta via Web autenticandosi con la coppia userID/password suddetta viene rilasciato un certificato X509 dalla validità di un anno.

EVENTUALE PRESENZA DI CREDENZIALI MULTIPLE PER LA STESSA PERSONA

Nella circostanza in cui la stessa persona sia un dipendente dell'Università e contemporaneamente sia uno studente essa avrà due distinte credenziali, con l'eccezione dei dottorandi.

MODALITÀ DI CONSEGNA DELLE CREDENZIALI

La password iniziale viene scelta personalmente dall'utente recandosi nell'Ufficio dell'AdP dove gli/le verrà presentato un form Web accessibile solo al personale AdP autenticato.

Il cambio della password è effettuato direttamente dall'utente accedendo via HTTPS alla propria pagina personale.

MODALITÀ DI RECUPERO DELLE CREDENZIALI SMARRITE

Le credenziali smarrite non possono essere recuperate ma solo resettate. Ci sono due modalità per chiedere il reset della password. Nella prima l'utente invia un fax ai SI segnalando la richiesta, allegando un documento di identità e specificando un recapito (telefonico o email) presso cui ricevere la password nuova.

In alternativa l'utente si presenta presso il personale informatico del proprio dipartimento; quest'ultimo effettua il riconoscimento dell'utente e invia la richiesta di cambio password ai sistemi informativi. Essi comunicano la password al referente che la comunica a sua volta all'utente finale.

DURATA DELL'ACCREDITAMENTO

L'identità digitale rimane attiva fintanto che continua il rapporto di lavoro dell'Utente con l'Università.

DISABILITAZIONE UTENTE

Alla scadenza dei contratti la categoria assegnata all'identità digitale dell'utente viene cambiata in "collaboratore ex strutturato". Esso mantiene ancora un numero di servizi attivi, tra cui la posta elettronica e la possibilità di consultare i cedolini.

CANCELLAZIONE DEFINITIVA UTENTE

L'identità digitale di un utente non viene mai cancellata dalle basi di dati.

La entry viene eliminata dalla directory LDAP (e quindi all'utente viene negato l'accesso ai servizi) trenta giorni dopo la disattivazione dell'utente, a meno che non si tratti di un ex docente, in qual caso la entry rimane attiva a tempo indeterminato.

INTEROPERABILITÀ TRA CREDENZIALI DEBOLI (USERNAME+PWD) ED EVENTUALI CREDENZIALI FORTI (SMARTCARD)

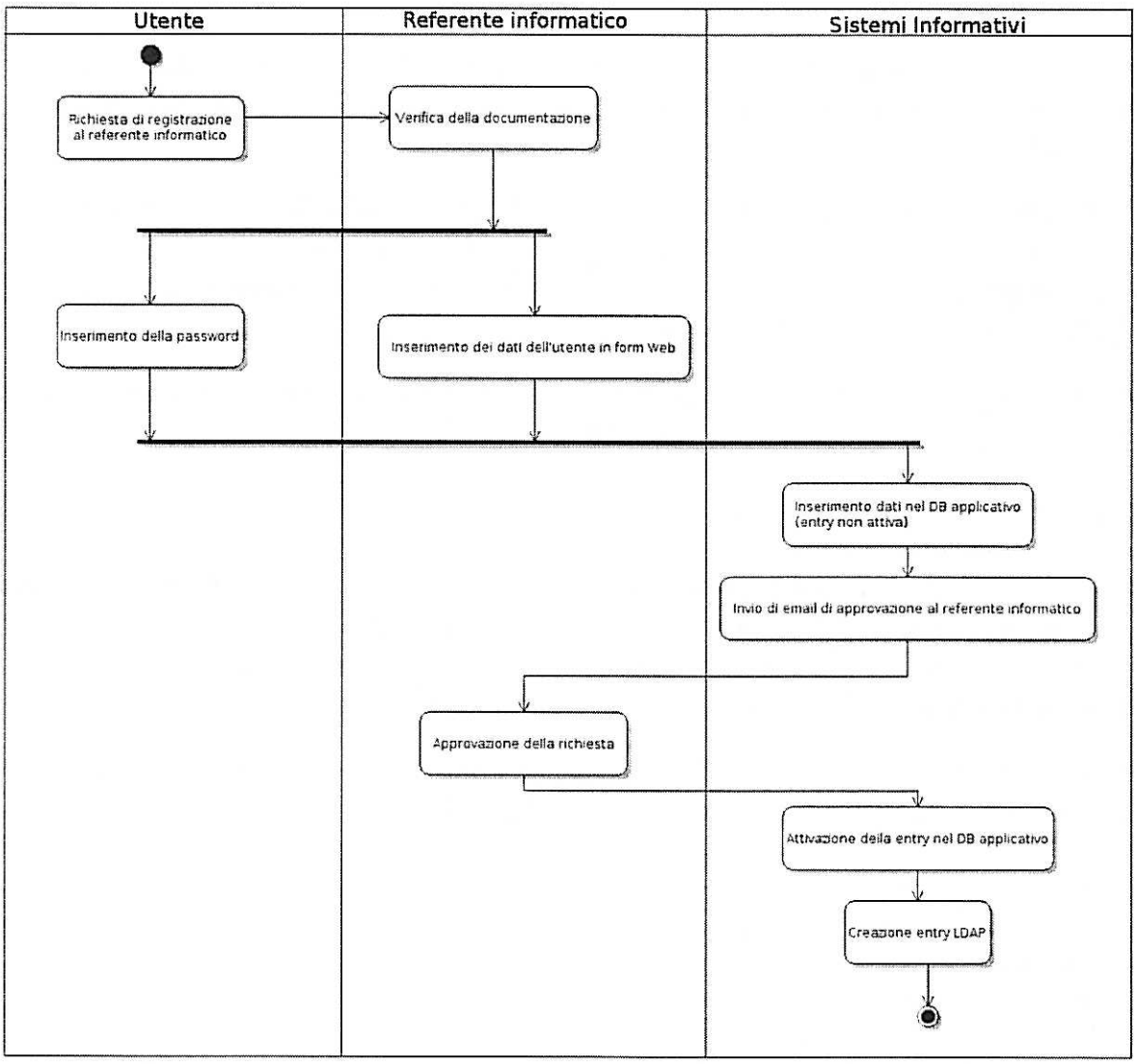
La combinazione userID/password viene usata per accedere alla pagina di generazione di un certificato X.509 e della relativa chiave privata. Il certificato è utilizzato per accedere alla rete WiFi d'Ateneo.

IL PROCESSO DI ACCREDITAMENTO PER IL PERSONALE NON STRUTTURATO

Di seguito viene descritto il processo di accreditamento per le categorie: Collaboratore esterno, Cultore della materia, Docente a contratto, Esercitatore, Tutor.

La responsabilità della registrazione degli utenti appartenenti alle categorie suddette ricade sul personale informatico dell'area (o dipartimento) di appartenenza del registrando.

MODALITÀ DI RICONOSCIMENTO DELLA PERSONA



Schema 2:Il processo di accreditamento per il personale non strutturato

Il dipendente viene identificato dal referente informatico della struttura di appartenenza presentando un documento di identità in corso di validità e il proprio codice fiscale.

CREAZIONE E CARATTERISTICHE DELL'IDENTITÀ DIGITALE

I dati anagrafici e quelli relativi alla posizione del nuovo assunto vengono inseriti in una pagina cifrata con HTTPS e non autenticata.

Il referente informatico inserisce nel form i dati anagrafici, l'area di appartenenza e la categoria dell'utente.

La password viene scelta dall'utente e inserita nel medesimo form in presenza del referente informatico. L'invio dei dati attraverso il form causa la creazione della entry nella base di dati applicativa (MS SQL). L'utente è marcato come "non attivo". Il sistema di registrazione invia contestualmente un'email al referente informatico del dipartimento presso cui è stato inserito l'utente.

Se il referente risponde con un'email di approvazione, l'utente viene marcato come "attivo" e viene creata la entry nella directory LDAP; ovvero gli/le vengono abilitati tutti i servizi.

Le informazioni sull'utente si trovano nel DB MS SQL e nella directory LDAP, in alcuni casi in maniera univoca su una sola delle risorse oppure ridondate su entrambe. Per quanto concerne la password, una volta trasferita su LDAP (la sincronizzazione avviene ogni minuto) essa viene rimossa dal DB.

I dati pubblici sono il nome e cognome dell'utente, il suo ruolo e la struttura di afferenza, l'indirizzo e-mail e il numero di telefono dell'ufficio.

GESTIONE DEL CICLO DI VITA

Nel caso di cambiamenti del rapporto di lavoro della persona con l'Università, la posizione viene aggiornata dall'area di competenza (vale a dire che verrà gestita dall'Area del Personale secondo la procedura sopra descritta se la persona diventa strutturata). Se la persona rimane non strutturata non viene presa nessuna misura.

La dismissione viene effettuata dal referente informatico seguendo una procedura analoga a quella descritta per la creazione dell'utente.

FORMATO E REGOLE DELLE CREDENZIALI

Le principali credenziali dell'utente sono costituite una coppia userID/password, tali credenziali non hanno scadenza.

A ciascun utente che ne faccia richiesta via Web autenticandosi con la coppia userID/password suddetta viene rilasciato un certificato X509 dalla validità di un anno.

EVENTUALE PRESENZA DI CREDENZIALI MULTIPLE PER LA STESSA PERSONA

Nella circostanza in cui la stessa persona sia un dipendente dell'Università e contemporaneamente sia uno studente essa avrà due distinte credenziali, con l'eccezione dei dottorandi.

MODALITÀ DI CONSEGNA DELLE CREDENZIALI

La password viene scelta personalmente dall'utente al momento della sua registrazione come indicato sopra.

Il cambio della password è effettuato direttamente dall'utente accedendo via HTTPS alla propria pagina personale.

MODALITÀ DI RECUPERO DELLE CREDENZIALI SMARRITE

Le credenziali smarrite non possono essere recuperate ma solo resettate. Ci sono due modalità per chiedere il reset della password, nella prima l'utente invia un fax ai SI segnalando la richiesta, allegando un documento di identità e specificando un recapito (telefonico o email) presso cui ricevere la password nuova.

In alternativa l'utente si presenta presso il personale informatico del proprio dipartimento; quest'ultimo riconosce l'utente e invia la richiesta di cambio password ai sistemi informativi. Essi comunicano la password al referente che la comunica a sua volta all'utente finale.

DURATA DELL'ACCREDITAMENTO

L'identità digitale rimane attiva fintanto che continua il rapporto di lavoro dell'Utente con l'Università.

DISABILITAZIONE UTENTE

Alla scadenza dei contratti la categoria assegnata all'identità digitale dell'utente viene cambiata in "collaboratore ex strutturato". Esso mantiene ancora un numero di servizi attivi, tra cui la posta elettronica e la possibilità di consultare i cedolini, per trenta giorni.

CANCELLAZIONE DEFINITIVA UTENTE

L'identità digitale di un utente non viene mai cancellata dalle basi di dati.

La entry viene eliminata dalla directory LDAP (e quindi all'utente viene negato l'accesso ai servizi) trenta giorni dopo la disattivazione dell'utente.

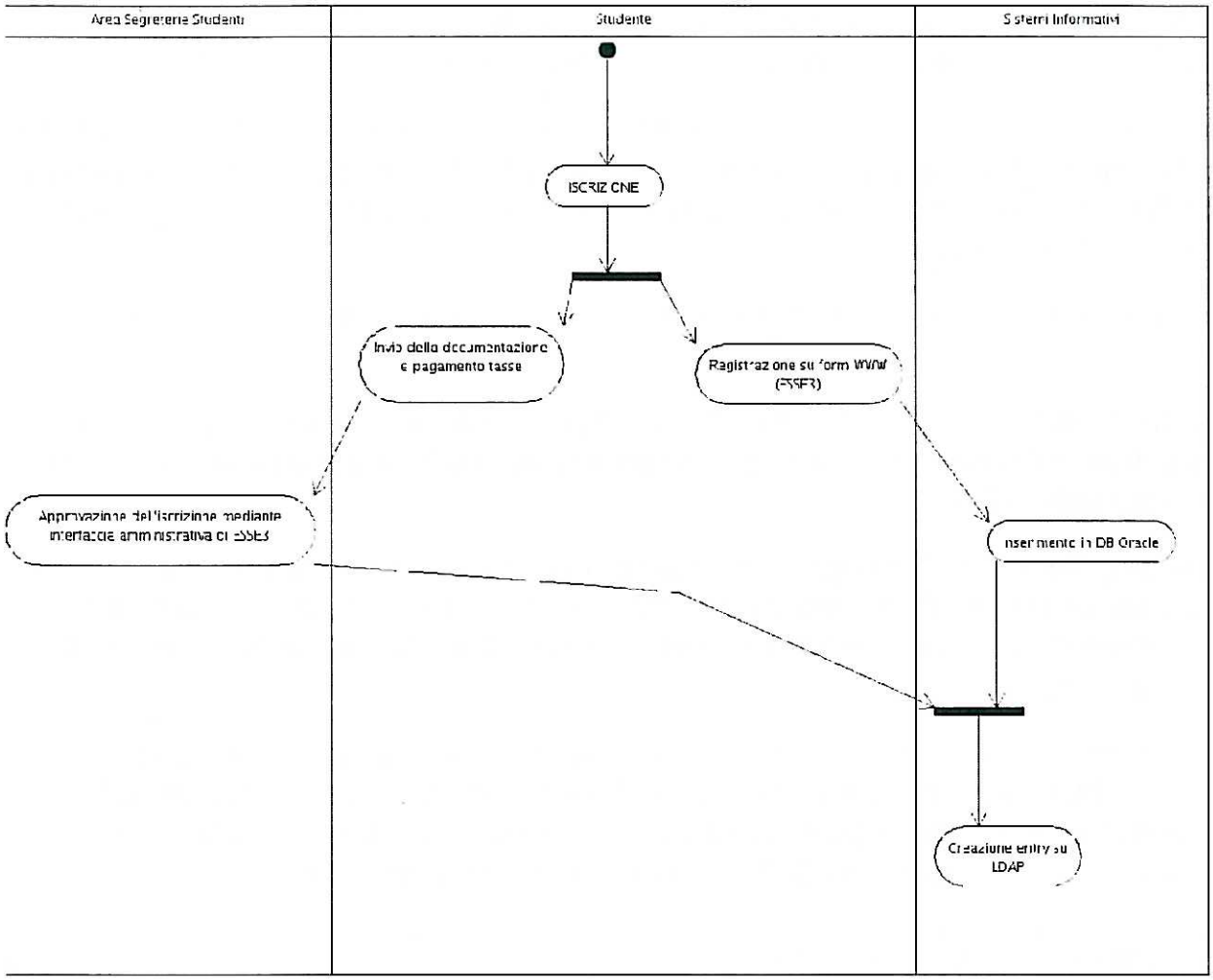
INTEROPERABILITÀ TRA CREDENZIALI DEBOLI (USERNAME+PWD) ED EVENTUALI CREDENZIALI FORTI (SMARTCARD)

La combinazione userID/password viene usata per accedere alla pagina di generazione di un certificato X.509 e della relativa chiave privata. Il certificato è utilizzato per accedere alla rete WiFi d'Ateneo.

IL PROCESSO DI ACCREDITAMENTO PER GLI STUDENTI

L'accreditamento e la gestione delle identità digitali degli studenti è gestita dall'Area Segreteria Studenti.

MODALITÀ DI RICONOSCIMENTO DELLA PERSONA



Schema 3: Il processo di accreditamento per gli studenti

Lo studente registrando inserisce i propri dati nell'applicativo ESSE3 in maniera autonoma via Internet, utilizzando un formulario Web.

La produzione del libretto universitario da parte delle segreterie studenti avviene dopo la ricezione da parte delle stesse di una fotocopia della carta di identità e del codice fi-

scale dello studente; tuttavia, l'identità digitale viene creata (e i servizi informatici vengono abilitati) come conseguenza del solo pagamento del modello MAV, come descritto in seguito.

CREAZIONE E CARATTERISTICHE DELL'IDENTITÀ DIGITALE

Il registrando inserisce personalmente i propri dati anagrafici, il codice fiscale e eventuali recapiti facoltativi (posta elettronica, numero di telefono, numero di FAX)

in una pagina web accessibile pubblicamente (all'indirizzo http://s3w.si.unimib.it/esse3/Anagrafica/Registrazione.d

Il sistema genera una password "one shot" e la presenta all'utente nella stessa pagina web. Se l'utente ha specificato un indirizzo di posta elettronica personale tra i recapiti facoltativi, la password "one shot" verrà inviata a questo indirizzo. Al primo login gli verrà imposto di cambiarla.

Fino a questo momento, l'identità digitale dell'utente risiede esclusivamente su ESSE3.

Dopo che l'utente ha effettuato la domanda di partecipazione ad un corso di studio ovvero di immatricolazione, viene generato un bollettino MAV per il pagamento della prima rata universitaria.

Solo in seguito al corretto pagamento della prima rata, l'entry dello studente viene inserita nella directory LDAP e per quella entry vengono abilitati tutti i servizi ordinari per gli studenti (accesso ai SIFA, posta elettronica, WiFi d'Ateneo, accesso alle biblioteche digitali).

Le informazioni dell'utente immatricolato si trovano in ESSE3 (che si appoggia a una base di dati Oracle) e nella directory LDAP d'Ateneo; in alcuni casi in maniera univoca su una sola delle risorse oppure ridondate su entrambe. La password risiede su entrambe e viene propagata da ESSE3 a LDAP in caso di aggiornamento.

GESTIONE DEL CICLO DI VITA

La richiesta di cambio di facoltà viene effettuata autonomamente dallo studente presso l'interfaccia web di ESSE3. In seguito la domanda va formalizzata con un documento cartaceo e con il pagamento di una tassa. Se la richiesta viene approvata l'identità digitale dell'utente viene aggiornata su ESSE3 e la modifica viene riportata su LDAP.

Similmente, il record di uno studente che diventi dottorando viene aggiornato su ESSE3 e le informazioni relative alla sua posizione vengono propagate su LDAP.

Se il rapporto dell'utente con l'università cambia da quello di studente a quello di dipendente (ovvero se la persona rientra in una delle categorie descritte nelle sezioni precedenti), verrà creato un nuovo account secondo le procedure già descritte.

FORMATO E REGOLE DELLE CREDENZIALI

Le principali credenziali dell'utente sono costituite una coppia userID/password, tali credenziali non hanno scadenza.

A ciascun utente che ne faccia richiesta via Web autenticandosi con la coppia userID/password suddetta viene rilasciato un certificato X509 dalla validità di un anno.

Agli studenti viene inoltre fornita una smart card utilizzabile per l'accesso fisico alla biblioteca e ai parcheggi dell'Ateneo.

EVENTUALE PRESENZA DI CREDENZIALI MULTIPLE PER LA STESSA PERSONA

Nella circostanza in cui la stessa persona sia un dipendente dell'Università e contemporaneamente sia uno studente essa avrà due distinte credenziali, con l'eccezione dei dottorandi.

MODALITÀ DI CONSEGNA DELLE CREDENZIALI

Al momento della registrazione dell'utente presso ESSE3, il sistema genera una password one-shot e la mostra via Web all'utente (se questi ha inserito tra i recapiti anche un indirizzo di posta elettronica, la password gli verrà inviata anche per email).

Il cambio della password è effettuato direttamente dall'utente accedendo via HTTPS alla propria pagina personale.

MODALITÀ DI RECUPERO DELLE CREDENZIALI SMARRITE

Le credenziali smarrite non possono essere recuperate ma solo resettate. Attraverso l'interfaccia web di ESSE3 l'utente effettua la richiesta di reset della password. Il sistema richiede all'utente di identificarsi inserendo il proprio numero di matricola e il codice fiscale. Quindi genera una nuova password e la invia alla casella di posta elettronica specificata in fase di registrazione.

Se l'utente non ha specificato un indirizzo di posta elettronica personale, dovrà presentarsi presso le segreterie studenti con un apposito modulo e presentando la propria carta di identità (in alternativa, è possibile far pervenire il modulo e una copia della carta di identità via fax o via posta cartacea).

DURATA DELL'ACCREDITAMENTO

Agli studenti che si laureano viene mantenuto l'account (con tutti i servizi abilitati) per tre anni.

Agli studenti che decidano di cessare formalmente il loro rapporto con l'Ateneo verrà mantenuto abilitato l'account per un anno di tempo dal momento della cessazione.

CANCELLAZIONE DEFINITIVA UTENTE

L'identità digitale di un utente non viene mai cancellata dalla base di dati di ESSE3.

La entry viene eliminata dalla directory LDAP (e quindi all'utente viene negato l'accesso ai servizi) trascorso il periodo di tempo indicato nel paragrafo precedente.

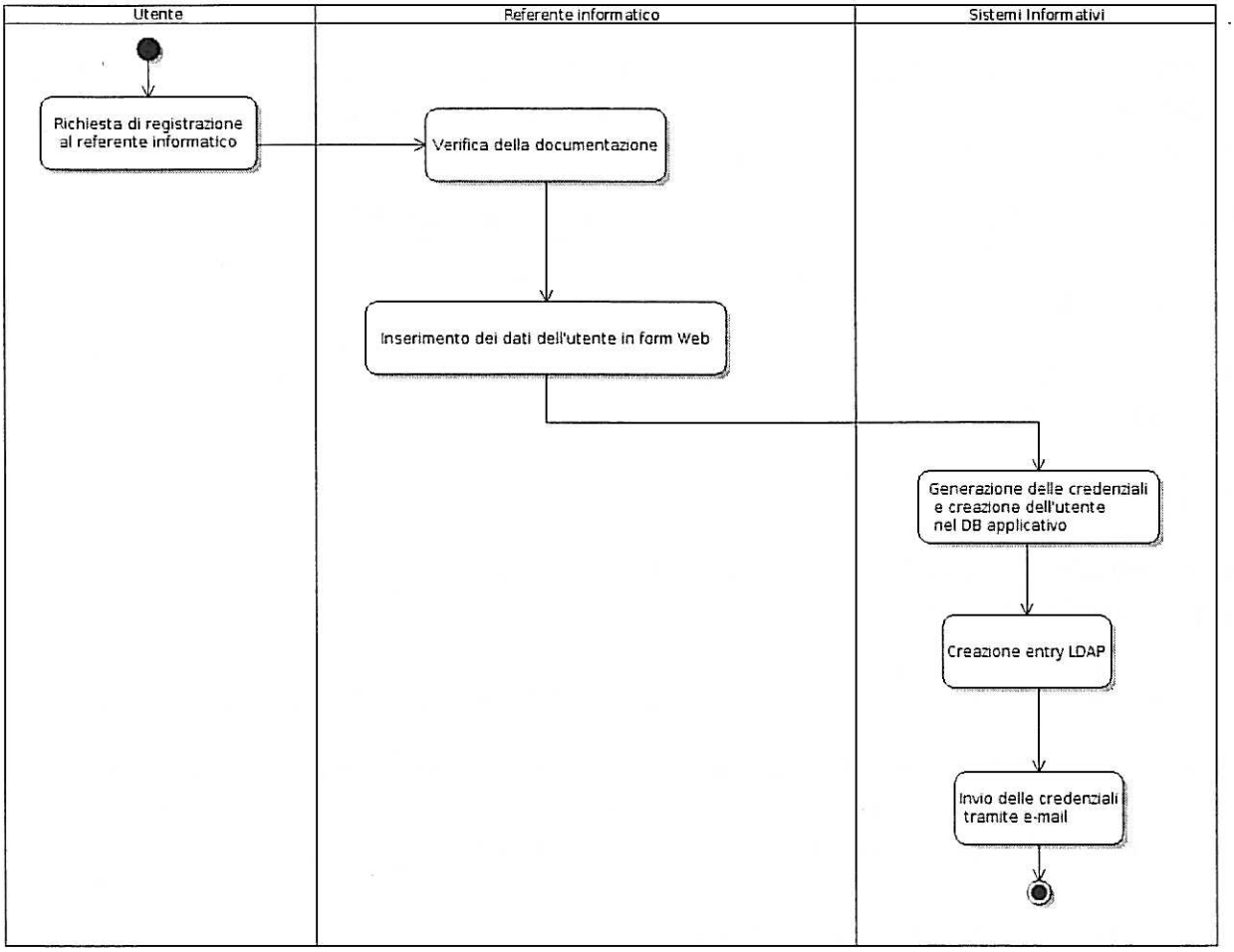
INTEROPERABILITÀ TRA CREDENZIALI DEBOLI (USERNAME+PWD) ED EVENTUALI CREDENZIALI FORTI (SMARTCARD)

La combinazione userID/password viene usata per accedere alla pagina di generazione di un certificato X.509 e della relativa chiave privata. Il certificato è utilizzato per accedere alla rete WiFi d'Ateneo. I tre tipi di credenziali non sono interoperabili. Per l'accesso a IDEM verrà utilizzata la sola combinazione userID/password.

IL PROCESSO DI ACCREDITAMENTO PER GLI OSPITI

Gli ospiti vengono registrati dal personale informatico dell'area (o dipartimento) di appartenenza del registrando.

MODALITÀ DI RICONOSCIMENTO DELLA PERSONA



Schema 4: Il processo di accreditamento per gli ospiti

Il dipendente viene identificato dal referente informatico della struttura di appartenenza presentando un documento di identità in corso di validità e il proprio codice fiscale.

CREAZIONE E CARATTERISTICHE DELL'IDENTITÀ DIGITALE

I dati anagrafici e quelli relativi alla posizione del nuovo assunto vengono inseriti in una pagina cifrata con HTTPS e autenticata, accessibile solo ai referenti informatici.

Il referente verifica i documenti del registrando e inserisce nel form i dati anagrafici, stabilisce la validità delle credenziali (cinque oppure dieci giorni) e indica l'indirizzo di

posta elettronica presso cui inviarle; le credenziali vengono generate in maniera automatica e mandate all'indirizzo email specificato.

Se l'utente ha modo di consultare la propria posta elettronica attraverso un accesso di rete autonomo, il referente indicherà un indirizzo personale dell'utente e le credenziali verranno inviate direttamente a quest'ultimo. Viceversa, il referente specificherà il proprio indirizzo email, e successivamente comunicherà le credenziali a voce al registrando.

Le informazioni sull'utente si trovano nel DB MS SQL e nella directory LDAP. Per quanto concerne la password, una volta trasferita su LDAP (la sincronizzazione avviene ogni minuto) essa viene rimossa dal DB.

Nessuno dei dati dell'utente viene reso pubblico in alcun modo.

GESTIONE DEL CICLO DI VITA

La dismissione delle credenziali avviene automaticamente al termine della loro validità scelta all'atto della generazione (cinque o dieci giorni).

FORMATO E REGOLE DELLE CREDENZIALI

Le credenziali dell'utente rilasciate attraverso questa procedura sono costituite una coppia userID/password.

EVENTUALE PRESENZA DI CREDENZIALI MULTIPLE PER LA STESSA PERSONA

Gli ospiti potrebbero avere eccezionalmente (qualora il referente ne facesse richiesta) sia le credenziali del tipo userID/password che un certificate X.509 (utilizzabile esclusivamente per l'accesso alla rete wireless con autenticazione 802.1X).

MODALITÀ DI CONSEGNA DELLE CREDENZIALI

Il nome utente e la password vengono generate casualmente e inviati all'indirizzo di posta elettronica specificato al momento della registrazione.

L'utente può cambiare la propria password autenticandosi presso una pagina HTTPS (il cui URL viene comunicato nella stessa email in cui vengono inviate le credenziali).

MODALITÀ DI RECUPERO DELLE CREDENZIALI SMARRITE

Le credenziali smarrite non possono essere recuperate. In caso di smarrimento, il referente procederà alla dismissione delle credenziali smarrite e alla generazione di una nuova coppia userID/password.

DURATA DELL'ACCREDITAMENTO

Le credenziali hanno una validità di cinque oppure dieci giorni.

DISABILITAZIONE E CANCELLAZIONE DEFINITIVA UTENTE

Al termine della validità delle credenziali, il record dell'utente viene eliminato dalla directory LDAP. Ne viene mantenuta traccia sui database applicativi.

IL SISTEMA DI AUTENTICAZIONE E AUTORIZZAZIONE INTERNO

Il sistema di gestione delle identità viene utilizzato per autenticare l'utenza presso la quasi totalità dei servizi d'Ateneo. In tutti gli scenari le credenziali vengono trasmesse attraverso protocolli cifrati. Nella fattispecie, i servizi accessibili mediante autenticazione centralizzata sono:

Posta elettronica e quarantena (archivio separato dei messaggi di spam)

Accesso ai servizi d'Ateneo (consultazione dei cedolini, ecc)

Accesso remoto a Internet via modem

Consultazione della biblioteca digitale

Accesso ai servizi per gli studenti (certificazioni, presentazione di piani di studio, ecc)

Inoltre le credenziali vengono utilizzate per richiedere la generazione di un certificato digitale e relativa chiave privata, il quale è a sua volta utilizzabile come credenziale di accesso alla rete WI-FI di Ateneo (con autenticazione e cifratura WPA2-Enterprise).

L'accesso ai servizi Web con l'eccezione della Webmail è fornito utilizzando CAS come soluzione di Single Sign-On; il server IdP dell'Università è già predisposto per utilizzare il sistema CAS attuale come Login Handler di Shibboleth. La durata delle sessioni di SSO gestite da CAS è di due ore.

Il sistema CAS prevede la possibilità di effettuare il Single Sign-Out, mantenendo traccia di tutte le applicazioni accedute dall'utente e inviando un postback a tutte le applicazioni quando viene fatta esplicita richiesta di logout presso uno dei servizi acceduti via CAS. È sempre possibile terminare tutte le sessioni aperte chiudendo il browser.

Gli identificatori principali (uid, ecc) di ogni persona sono univoci una volta assegnati e non vengono mai riassegnati. Dopo la dismissione dell'identità digitale di una persona, se la medesima rientra a fare parte a qualunque titolo dell'Università, le viene assegnato un identificativo differente.

È in corso di implementazione la procedura di rassegnazione del medesimo identificatore principale basato sul riconoscimento della persona tramite codice fiscale.

PARTECIPAZIONE AD ALTRE FEDERAZIONI

L'Università partecipa alla federazione Eduroam.