

Procedure di accreditamento degli utenti
(Università di Parma)

Marco Panella
(Settore Innovazione Tecnologie Informatiche)

15 dicembre 2008

Indice

1	L'Università di Parma	5
1.1	Cenni storici	5
1.1.1	Server a directory	5
1.1.2	Servizio di autenticazione centralizzata	6
1.1.3	Progetto IDEM	6
1.2	Macro-categorie di persone	6
1.2.1	Il personale strutturato	6
1.2.2	Gli studenti	6
1.2.3	Altre categorie	7
1.3	Organigramma dell'Ateneo di Parma	7
1.3.1	Strutture per la didattica e la ricerca	7
1.3.2	Strutture tecnico-amministrative	8
1.4	Ruolo del sistema informativo	8
1.4.1	CIA	9
1.4.2	CSA	9
1.4.3	U-GOV Didattica	9
1.4.4	GISS	9
1.5	Tipologie di persone	10
1.5.1	Dipendenti strutturati	10
1.5.2	Contrattisti e borsisti	10
1.5.3	Studenti	11
1.5.4	Fornitori esterni	12
1.5.5	Ospiti	12
2	Personale strutturato	14
2.1	Accreditamento	14
2.2	Rilascio credenziali	14
2.2.1	Fornitura dei dati CSA	15
2.2.2	Altri dati	15
2.3	Modifica credenziali	15
2.4	Modifica attributi	16
2.5	Cessazione	16

3	Contrattisti e borsisti	17
3.1	Accreditamento	17
3.1.1	Assegnisti di ricerca	17
3.1.2	Professori a contratto	17
3.1.3	Non docenti a tempo determinato	18
3.1.4	Borsisti	18
3.1.5	Altro	18
3.2	Rilascio credenziali	18
3.3	Modifica credenziali	18
3.4	Modifica attributi	19
3.5	Cessazione	19
4	Studenti	20
4.1	Accreditamento	20
4.1.1	Studenti di corsi di primo e secondo livello	20
4.1.2	Studenti di master	21
4.1.3	Studenti di scambio	21
4.1.4	SSIS	21
4.1.5	Dottorandi	22
4.1.6	Specializzandi	22
4.2	Creazione credenziali	22
4.3	Modifica credenziali	22
4.4	Modifica attributi	23
4.5	Cessazione	23
5	Altre persone	24
5.1	Accreditamento	24
5.2	Rilascio credenziali	24
5.3	Modifica credenziali	24
5.4	Modifica attributi	25
5.5	Cessazione	25
6	Sviluppi futuri	26
6.1	Database centrale	26
6.1.1	Certificati digitali	26
6.1.2	Progetto 2009 per l'autenticazione	26
6.2	Sistema di autenticazione	26
6.2.1	Controllo scadenza password o account	26
6.2.2	Self-reset password	27
6.3	Gestione di altre categorie	27
6.3.1	Future matricole	27
6.3.2	Ditte esterne	27
6.4	Modifica procedure di accreditamento	28

6.4.1	Professori a contratto	28
6.4.2	Studenti	28
6.4.3	Ospiti	28

DRAFT

Elenco delle tabelle

1.1	Ruoli dei dipendenti strutturati	11
1.2	Ruoli dei dipendenti non strutturati	11

DRAFT

Elenco delle figure

1.1 Organigramma della struttura amministrativa	13
---	----

DRAFT

Capitolo 1

L'Università di Parma

Le Università hanno il compito di elaborare e promuovere la conoscenza scientifica e di diffondere e trasmettere il sapere.

Per perseguire queste finalità primarie le Università si avvalgono di svariate tipologie di persone in ruoli didattici, di ricerca o di supporto tecnico-amministrativo.

La molteplicità di compiti differenti rende le Università dei mondi complessi; non solo per il numero di persone che la frequentano ma anche per la varietà di ruoli che esse ricoprono.

Grazie alle nuove tecnologie informatiche ed ad una organizzazione del lavoro adeguata, l'erogazione di servizi informatici può portare diversi vantaggi.

Essi richiedono due passi preliminari: che la persona che accede si faccia riconoscere e che alla stessa persona siano assegnati i permessi associati con la sua identità digitale.

Lo scopo dell'uso di sistemi di autenticazione e autorizzazione è garantire la sicurezza dei sistemi e la protezione dei dati personali degli utenti.

1.1 Cenni storici

Il nucleo centrale del sistema di autenticazione centralizzato nasce per la gestione del servizio di posta elettronica.

Nel 2000 si inizia a fornire un indirizzo di posta elettronica ufficiale al personale strutturato.

1.1.1 Server a directory

Nel 2002 l'Ateneo si appoggia a CINECA per fornire un indirizzo a tutti gli studenti dell'Ateneo; il servizio prevede che le informazioni per l'accesso siano mantenute su server a directory, compatibili con il protocollo LDAP: l'Ateneo gestisce internamente il server LDAP master.

Sfruttando questa esperienza, all'inizio del 2004 anche il nuovo server di posta per la gestione degli indirizzi del personale e degli ospiti si appoggia al medesimo server per l'autenticazione.

Nel corso del 2004 i due server, quello per il personale e quello per gli studenti, sono riuniti in un unico server.

Dal 2004 sono in continuo aumento i servizi che si appoggiano all'autenticazione centralizzata e quindi le categorie di persone censite nel sistema.

1.1.2 Servizio di autenticazione centralizzata

Contemporaneamente all'installazione del nuovo server di posta, si inizia a parlare di sistemi di autenticazione centralizzata anche per i servizi web.

Viene perciò installato il server Central Authentication Service (CAS)¹ che consente l'autenticazione secondo il modello Single Sign On².

1.1.3 Progetto IDEM

Dal 2007, l'Università di Parma partecipa al progetto pilota IDEM³, promosso dal *Consortium GARR*⁴ per la creazione di una federazione di autenticazione e autorizzazione ai servizi in rete.

I vantaggi di un sistema IAM federato sono molteplici; i costi iniziali di progettazione e standardizzazione sono ripagati nel medio-lungo periodo.

1.2 Macro-categorie di persone

1.2.1 Il personale strutturato

I dipendenti dell'Ateneo sono divisi tra docenti, ricercatori e personale tecnico-amministrativo.

I tecnici amministrativi sono a loro volta suddivisi in aree professionali: amministrativa, tecnica, socio-sanitaria e bibliotecaria.

1.2.2 Gli studenti

La categoria di dimensioni più consistente è quella degli studenti, suddivisi principalmente per tipologia di corso frequentato.

Le tipologie di corso (di primo, secondo o terzo livello) possono distinguersi in:

¹<http://www.ja-sig.org/products/cas/>

²All'interno di una singola sessione di lavoro, è sufficiente una sola operazione di autenticazione per avere accesso a tutti i servizi per i quali si è abilitati.

³<http://www.idem.garr.it>

⁴<http://www.garr.it>

primo livello laurea triennale e master di primo livello

secondo livello laurea magistrale, laurea specialistica, laurea specialistica a ciclo unico, master di secondo livello

terzo livello specializzazione, perfezionamento, dottorato di ricerca

Sono inoltre offerti corsi di perfezionamento post-laurea, rivolti anche a persone che già lavorano (secondo il modello detto *lifelong learning*).

Una seconda distinzione è operabile in base al fatto che lo studente sia iscritto direttamente all'Ateneo o se invece sia gestito amministrativamente da altri Atenei e frequenti l'Ateneo di Parma in virtù di accordi di vario genere.

1.2.3 Altre categorie

Comprendono persone non incardinate stabilmente nelle strutture dell'Ateneo e quindi definite *non strutturate*.

Le tipologie sono molteplici: sono persone con un contratto a tempo determinato con compiti specifici e differenziati.

Tra di essi si distinguono i professori a contratto (per la didattica), gli assegnisti di ricerca e i borsisti (per la ricerca) ovvero ospiti (ad esempio docenti di altri Atenei in visita).

Molte aziende hanno stabili rapporti con gli Atenei sia nelle vesti di fornitori sia di partner in progetti di ricerca o didattica (es. tirocini di formazione o di orientamento).

Un'altra categoria di persone che deve interagire con i servizi in rete degli Atenei sono gli studenti delle superiori che intendono iscriversi l'anno successivo, al fine di compilare domande di beneficio ovvero di partecipazione ai concorsi per i corsi a numero chiuso.

1.3 Organigramma dell'Ateneo di Parma

1.3.1 Strutture per la didattica e la ricerca

Il Corso di laurea è alla base delle strutture didattiche d'Ateneo; la Facoltà racchiude più corsi di laurea e costituisce la struttura didattica per eccellenza.

Ogni Corso di Laurea è gestito da un Consiglio i cui componenti sono i docenti che tengono un insegnamento afferente a quel Corso.

Le Facoltà dell'Università di Parma sono undici; è stato costituito un Comitato Ordinatore per la dodicesima Facoltà (Scienze Politiche).

Ogni Facoltà prevede un ufficio di presidenza, il cui personale è stato recentemente incardinato in Staff all'Area *Didattica*.

Il Dipartimento è la struttura base per la ricerca ed ha autonomia finanziaria rispetto all'Ateneo.

L'organizzazione di un dipartimento prevede una segreteria amministrativa e uno o più unità organizzative di laboratorio.

I Dipartimenti dell'Università di Parma sono quarantadue.

1.3.2 Strutture tecnico-amministrative

La struttura amministrativa dell'Ateneo prevede la suddivisione in aree dirigenziali, settori e servizi.

Le aree dirigenziali sono sei, come da figura 1.1.

A capo di un'Area è posto un Dirigente che coordina le attività dei Settori assegnati.

Durante la riorganizzazione del 2005, il Servizio *Analisi e sviluppo delle procedure*, afferente al Settore *Informatico Servizi Amministrativi* (SISA) con competenza sullo sviluppo del sistema informativo, è stato scorporato e le persone che vi afferivano sono state poste in staff ai Dirigenti.

A fine 2006 il Centro di Calcolo Elettronico, struttura di supporto informatico alla ricerca e alla didattica, è stato trasformato in Settore *Innovazione Tecnologie Informatiche* (SITI).

Nello stesso momento il personale afferente alle Presidenze di Facoltà è stato organizzato in staff al Dirigente dell'Area *Didattica*.

1.4 Ruolo del sistema informativo

Le informazioni delle persone sono memorizzate nel sistema informativo, che permette l'accentramento delle modifiche in una base dati unica di tutte le informazioni rilevanti e la distribuzione dei permessi di accesso a tutti coloro che fanno uso di queste informazioni.

Il sistema informativo ha ormai assunto compiti importanti nell'erogare servizi online; fino a poco tempo fa invece si poteva limitare a registrare le informazioni rilevanti per le attività amministrative.

Questo è il motivo per cui l'Ateneo di Parma utilizza tre applicativi separati per gli ambiti della contabilità (chiamato CIA), delle risorse umane (chiamato CSA) e della didattica (chiamato GISS).

Da qualche tempo è stato acquistato il programma per la gestione della programmazione didattica (U-GOV SIADI), che viene utilizzato dalle presidenze di facoltà anche per registrare le cosiddette "coperture didattiche" degli insegnamenti presenti nel piano di studio.

1.4.1 CIA

Il programma Contabilità Integrata d'Ateneo (CIA) è utilizzato per tutta la gestione della contabilità dell'Ateneo, sia delle strutture di ricerca (che hanno una parziale autonomia finanziaria) sia delle strutture amministrative.

In esso sono registrati le anagrafiche dei fornitori esterni, dei borsisti e dei professori a contratto.

L'area dirigenziale di riferimento è quella della *Contabilità*.

1.4.2 CSA

Il programma Carriere e Stipendi d'Ateneo (CSA) è utilizzato per registrare le anagrafiche e i dati di carriera del personale.

In esso sono presenti i dati del personale strutturato e non strutturato.

Ad ognuno è associato un ruolo.

In CSA sono presenti anche i dati anagrafici dei professori a contratto; essi però non hanno un ruolo ma solo un incarico di docenza. Questo perchè i dati anagrafici sono inseriti dalle presidenze di facoltà ma CSA non gestisce le fasi relative alla firma del contratto e quindi all'avvenuto inserimento in ruolo del docente.

L'area dirigenziale di riferimento è quella delle *Risorse Umane*, ma il sistema CSA è usato anche dal Settore *Stipendi ed Emolumenti al personale esterno* (dipendente dall'area Contabilità).

1.4.3 U-GOV Didattica

Il Ministero richiede che, a fini di monitoraggio e trasparenza, la programmazione didattica sia deliberata con ampio anticipo (entro maggio).

Recentemente, le Facoltà sono chiamate a deliberare, con maggiore anticipo rispetto al passato, anche le coperture. Questo determina la necessità di anticipare anche le decisioni in merito all'eventuale necessità di docenti a contratto.

Il programma è utilizzato per gestire i regolamenti didattici, l'offerta formativa e le coperture degli incarichi didattici. Inoltre si definiscono le regole e i limiti che gli studenti devono tenere presenti nel variare i propri piani di studi.

Gli uffici di riferimento sono le presidenze di Facoltà, che seguono anche quasi tutto l'iter relativo ai concorsi per docenti a contratto; l'ultimo passo, cioè la firma vera e propria, è a carico del servizio *Affidamenti e Contratti* del Settore *Personale docente* dell'Area Risorse Umane.

1.4.4 GISS

Il programma GISS è usato per gestire i dati anagrafici e le carriere degli studenti.

L'area dirigenziale di riferimento è quella della *Didattica*.

1.5 Tipologie di persone

Le persone possono essere impegnate in uno o più ambiti di attività, a causa del ruolo che rivestono o perché ricoprono più ruoli.

Le principali macro categorie di persone sono:

dipendenti strutturati sono docenti e non docenti, assunti a tempo indeterminato e i loro dati sono gestiti esclusivamente dall'ufficio personale;

contrattisti e borsisti sono persone che assumono un ruolo interno all'Ateneo per un tempo determinato e i cui dati sono gestiti da uffici differenti, in base alla specifica tipologia;

studenti sono persone iscritte all'Ateneo per conseguire un titolo di studio e i cui dati sono gestiti da uffici appartenenti all'Area Didattica;

ospiti sono coloro che non risultano censiti dal sistema informativo ma che comunque rivestono un ruolo all'interno dell'Ateneo.

Ognuna di queste categorie è formata da diverse tipologie di persone. Esse possono avere ruoli differenti e ogni servizio deve trattarle in modo diverso.

Le persone sono perciò associate ad un codice che identifica il ruolo ricoperto.

Una ulteriore distinzione è possibile in base all'ufficio che effettua l'inserimento dei dati nel sistema informativo.

Alcune persone possono essere accreditati da più uffici contemporaneamente; l'esempio classico è quello del dipendente che si iscrive ad un corso di laurea.

Caso ancora più particolare è quello degli specializzandi perché è il ruolo che automaticamente li rende sia dipendenti (ricevono un assegno mensile) sia studenti.

1.5.1 Dipendenti strutturati

In questa categoria ricadono tutti i dipendenti a tempo indeterminato, siano essi docenti, ricercatori o non docenti.

Nel sistema CSA ogni tipologia è identificata da una sigla (vedi tabella 1.1): queste persone sono censite esclusivamente dall'ufficio personale.

1.5.2 Contrattisti e borsisti

A questa categoria fanno riferimento tutti i dipendenti a tempo determinato: siano essi tecnici-amministrativi, titolari di assegno di ricerca oppure docenti a contratto.

I Dirigenti e il personale non docente a tempo determinato sono trattati dall'ufficio personale come i dipendenti strutturati; le altre tipologie sono invece gestite dall'ufficio stipendi (SP e BS) o servizio borse e dottorati (PE, inquadramento 100 06).

PO	Professori ordinari
PA	Professori associati
RU	Ricercatori
ND	Non docenti a tempo indeterminato
AS	Assistenti universitari (ruolo ad esaurimento)
CL	Collaboratori linguistici
D8	Dirigenti

Tabella 1.1: Ruoli dei dipendenti strutturati

I professori a contratto sono invece privi di ruolo nel sistema CSA, ma i loro dati anagrafici sono presenti perché prelevati dai dati relativi alle coperture didattiche nel sistema SIADI per la programmazione didattica.

DC	Dirigenti a contratto
NM	Non docenti a tempo determinato
PE	Assegnisti di ricerca
SP	Specializzandi
BS	Borsisti
-	Professori a contratto

Tabella 1.2: Ruoli dei dipendenti non strutturati

In CSA sono presenti anche molte altre persone che non ricoprono però ruoli d'interesse per l'Ateneo: ad esempio l'ufficio stipendi censisce gli eredi dei dipendenti nel caso vadano erogate ulteriori emolumenti.

1.5.3 Studenti

In questa categoria rientrano tutti gli studenti dei corsi di laurea (triennale, magistrale, specialistica), dei corsi di specializzazione, dei master (primo o secondo livello), dei corsi di dottorato.

Anche gli studenti SSIS e gli studenti iscritti tramite programmi di scambio con l'estero fanno parte di questa categoria.

Solo dall'anno accademico 2008-2009 il database GISS conterrà anche le informazioni degli studenti di dottorato e di quelli di scambio con l'estero. Anche gli studenti SSIS avrebbero dovuto essere inseriti ma il blocco di questo tipo di Scuola da parte del Ministero ha interrotto il progetto di inclusione.

1.5.4 Fornitori esterni

Nel sistema della contabilità sono gestite le anagrafiche di tutti i fornitori o di coloro che percepiscono dei compensi o dei rimborsi non regolari (professori a contratto, studenti, ecc).

1.5.5 Ospiti

In questa categoria ricadono tutte le persone che non rientrano nelle categorie precedenti.

Dipartimenti, facoltà e strutture amministrative sono frequentate da molte tipologie di persone che nessun ufficio è chiamato ad inserire in sistema informativo: alcune tipologie di borsisti, tutor di master, persone pagate con fondi di ricerca e studenti di corsi di perfezionamento cui non viene assegnata una matricola.

Anche gli studenti che si iscrivono per sostenere l'esame di corsi singoli non sono immatricolati regolarmente.

DRAFT

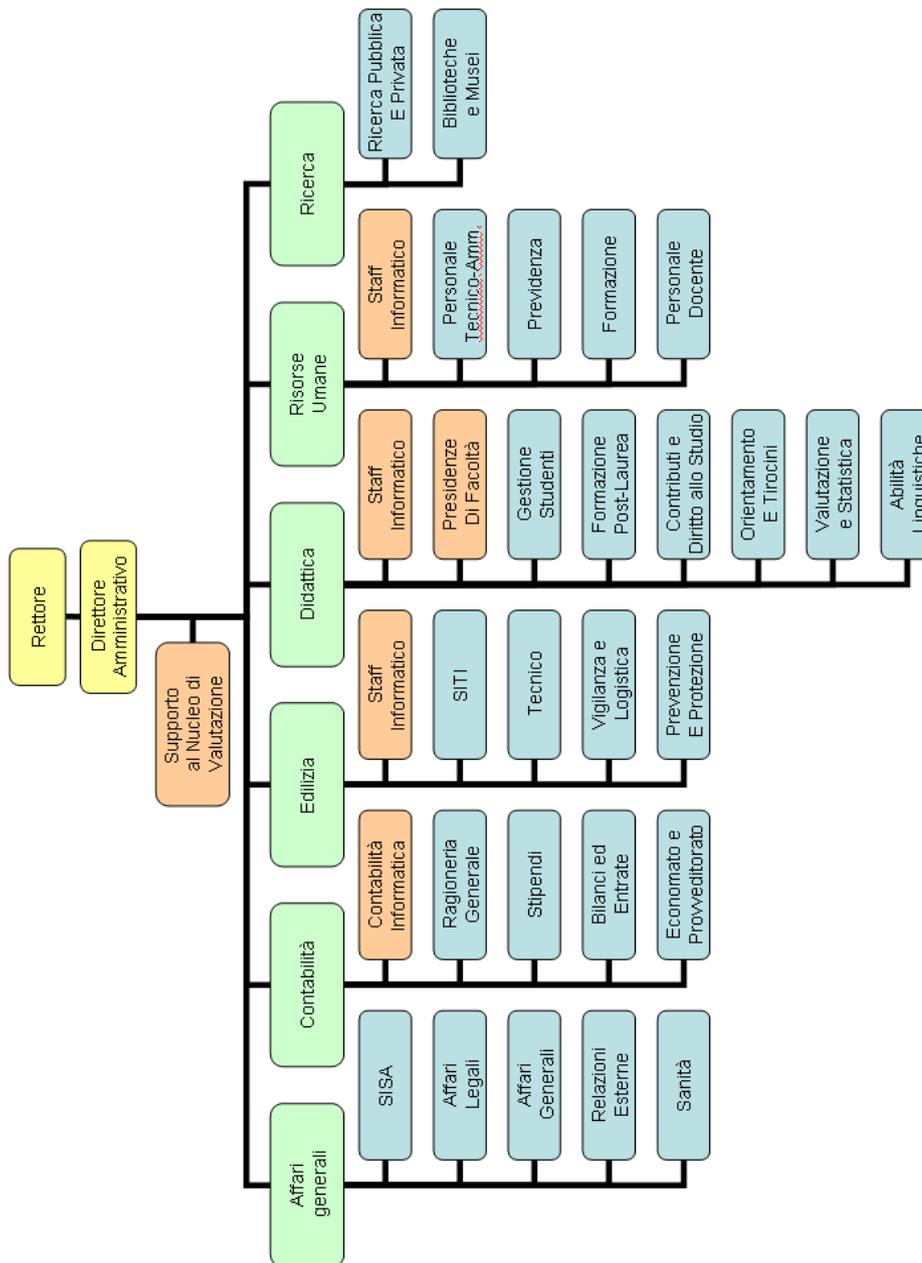


Figura 1.1: Organigramma 2005-2008 della struttura amministrativa (in azzurro i Settori, in arancione le strutture di Staff).

Capitolo 2

Personale strutturato

Con la dizione *personale strutturato* si intendono i docenti e i non docenti a tempo indeterminato.

Per gestire questa categoria di persone il sistema applicativo utilizzato è CSA di CINECA.

2.1 Accreditamento

L'assunzione avviene a seguito di pubblico concorso.

I tecnici-amministrativi dichiarati vincitori del concorso sono chiamati a firmare il contratto presso l'Area delle Risorse Umane.

Per quanto riguarda i docenti, dopo l'espletamento della procedura di valutazione comparativa e la chiamata deliberata dal Consiglio di Facoltà, prendono servizio consegnando i relativi documenti presso l'Area Risorse Umane.

Una volta firmato il contratto, i dati del personale strutturato sono registrati in CSA e la responsabilità di tutti i controlli è ad opera dei Settori *Personale docente* o *Personale tecnico-amministrativo* (entrambi dell'Area Risorse Umane, ognuno per la propria parte).

CSA contiene i dati anagrafici e tutte le informazioni dettagliate relative ad eventuali passaggi giuridici ed economici effettuati all'interno del rapporto di lavoro.

2.2 Rilascio credenziali

I dati anagrafici sono inviati al Settore *Innovazione Tecnologie Informatiche* dell'Area *Edilizia* dove sono generati gli indirizzi email seguendo il modello

*nome.cognome@unipr.it*¹ e il file per il caricamento dei dati nel database a directory.

2.2.1 Fornitura dei dati CSA

I dati sono per il momento esportati tramite client CSA dallo staff informatico dell'Area *Risorse umane* e inviati al Settore *Innovazione Tecnologie Informatiche* via posta elettronica sotto forma di file in formato DBase.

Il trasferimento avviene tipicamente tra l'8 e il 12 di ogni mese, poiché la quantità di variazioni giornaliere è insufficiente a giustificare una maggiore frequenza.

L'accesso diretto ai dati tramite la vista *SGE.INTERVALLI.PLUS*, presente sul database U-GOV, renderà disponibile tutte le informazioni necessarie con maggiore celerità.

2.2.2 Altri dati

Il personale del Settore *Innovazione Tecnologie Informatiche* usa Access per caricare i dati in un database relazionale e, tramite programmi PHP, genera l'indirizzo ufficiale di posta del tipo *nome.cognome@unipr.it*².

Lo stesso programma genera l'uid (utilizzato sui sistemi *nix per determinare la proprietà dei file - e utilizzato anche per altri servizi) di 8 caratteri (3 lettere iniziali del nome, 3 lettere iniziali del cognome e 2 cifre casuali³), genera l'uid-Number (equivalente numerico dell'uid) e quindi genera l'identità digitale della persona.

Il SITI si incarica poi di inviare alla persona le credenziali (mail, uid, password) in busta chiusa presso la sede della struttura di appartenenza.

2.3 Modifica credenziali

Gli utenti possono modificare autonomamente la password attraverso una pagina web protetta da SSL. Il certificato in uso è autofirmato, ma è già stato richiesto un certificato SCS.

Le password scadono ogni 180 giorni.

Se l'utente dimentica la password o lascia passare 200 giorni dall'ultimo cambio, il sistema non permette più di accedere ai servizi (neppure a quello di cambio password) e l'utente deve rivolgersi al Servizio *Supporto ai servizi internet* del Settore *Innovazione Tecnologie Informatiche* dell'Area *Edilizia*.

¹Le omonimie sono trattate facendo precedere un numero distintivo prima del segno della chiocciola.

²In caso di omonimie con indirizzi esistenti viene aggiunto un numero prima della chiocciola.

³Usate per evitare duplicati.

La modalità di richiesta è l'invio di un fax prestampato allegando una fotocopia di un documento di identità.

2.4 Modifica attributi

Come ricordato nei paragrafi precedenti, tutti i mesi sono inviate le informazioni relative ai dipendenti attivi.

Per differenza con l'elenco del mese precedente, tramite procedure analoghe a quelle usate per la generazione degli account, il Settore *Innovazione Tecnologie Informatiche* modifica le informazioni relative a eventuali trasferimenti, promozioni, riassunzioni, ecc.

2.5 Cessazione

Per il momento non viene mai effettuata la cancellazione dell'account del personale strutturato.

Viene registrata la cessazione modificando il valore degli attributi *stato*, *lista-posta* e di quelli relativi all'affiliazione appartenenti all'objectclass *eduPerson*.

Capitolo 3

Contrattisti e borsisti

Non rappresentano una categoria omogenea perché diversi sono gli uffici responsabili dell'accREDITAMENTO e diverso è il trattamento dei dati per il rilascio delle credenziali.

Per la maggior parte le informazioni relative a queste persone sono gestite tramite CSA.

3.1 AccredITAMENTO

3.1.1 Assegnisti di ricerca

Dopo aver superato una valutazione comparativa, i vincitori delle selezioni per assegnisti di ricerca sono chiamati dal Servizio *Assegni di ricerca* del Settore *Personale docente* dell'Area *Risorse umane*.

Questo ufficio si preoccupa di inserire le informazioni relative agli assegnisti nel sistema CSA.

3.1.2 Professori a contratto

Le procedure di accREDITAMENTO sono differenti (e sono più coinvolte le facoltà che l'Area Risorse Umane):

1. il Consiglio di Facoltà decide di coprire con contratto un insegnamento nel limite del budget deciso dal Senato Accademico;
2. la Facoltà espleta le procedure di concorso: pubblicazione del bando, valutazione comparativa per titoli dei curriculum vitae dei candidati;
3. il personale della *Presidenza di Facoltà* inserisce i dati relativi alla copertura didattica nel programma *SIADI* (U-GOV programmazione didattica);

4. il Servizio *Affidamenti e Contratti* del Settore *Personale Docente* riceve la documentazione e chiama i docenti per la firma del contratto.

Per il momento, sono trattati come gli strutturati, ma il trasferimento dei loro dati al Settore *Innovazione Tecnologie Informatiche* avviene con evidente ritardo rispetto sia all'inizio del contratto sia, soprattutto, all'inizio delle attività didattiche. Infatti nel sistema informativo non è contemplata la gestione dell'evento relativo alla firma del contratto.

Questo vale solo per i professori a contratto che coprono insegnamenti ufficiali nei corsi di laurea.

I professori a contratto dei corsi di perfezionamento e di alcuni master sono pagati direttamente con il budget del corso, tramite fondi di dipartimento. I dati di queste persone non sono quindi gestiti tramite il sistema informativo.

3.1.3 Non docenti a tempo determinato

Per il tempo di durata del contratto queste persone sono gestiti come dipendenti strutturati.

I loro dati sono quindi trattati con le procedure previste al capitolo precedente.

3.1.4 Borsisti

A queste persone non viene assegnato un account con modalità automatiche, ma possono essere riceverlo come Ospite.

3.1.5 Altro

Altre categorie sono trattate come Ospiti.

3.2 Rilascio credenziali

I dati dei professori a contratto (di facoltà) e degli assegnisti di ricerca sono inviati al SITI insieme ai dati del personale strutturato.

Le altre persone ricadono sotto la categoria Ospiti.

3.3 Modifica credenziali

Gli utenti possono modificare autonomamente la password attraverso una pagina web protetta da SSL. Il certificato in uso è autofirmato, ma è già stato richiesto un certificato SCS.

Le password scadono ogni 180 giorni.

Se l'utente dimentica la password o lascia passare 200 giorni dall'ultimo cambio, il sistema non permette più di accedere ai servizi (neppure a quello di cambio password) e l'utente deve rivolgersi al Servizio *Supporto ai servizi internet* del Settore *Innovazione Tecnologie Informatiche* dell'Area *Edilizia*.

La modalità di richiesta è l'invio di un fax prestampato allegando una fotocopia di un documento di identità.

3.4 Modifica attributi

Non sono previste modifiche automatiche ai dati di queste persone, tranne che per i dipendenti tecnico-amministrativi.

3.5 Cessazione

Non è prevista la cessazione degli account relativi a queste persone.

Come per gli strutturati sono modificati i dati relativi allo *Stato* e gli attributi dell'objectclass *eduPerson* nel caso del personale gestito tramite CSA.

Capitolo 4

Studenti

Gli studenti sono persone iscritte ad uno dei corsi che l'Ateneo organizza per il conseguimento di un titolo.

Il sistema applicativo utilizzato per il trattamento dei loro dati è GISS di KION-CINECA.

4.1 Accredитamento

Gli studenti sono accreditati dalle segreterie studenti di Facoltà, dipendenti dal Settore *Gestione Studenti* dell'Area *Didattica*.

4.1.1 Studenti di corsi di primo e secondo livello

La procedura di immatricolazione si svolge in quattro fasi¹:

1. lo studente stampa i moduli necessari dal sito, li compila e li porta in segreteria, dove riceve il modulo da consegnare in banca per il pagamento della prima rata delle tasse. I documenti necessari sono:

- domanda di iscrizione
- fotocopia del codice fiscale o tessera sanitaria
- fotocopia di un documento di identità
- ricevuta del versamento della prima rata

2. lo studente paga la prima rata delle tasse in banca²

¹È stato co-finanziato il progetto presentato per il bando ministeriale ICT4U, nel quale è previsto un servizio di immatricolazione online.

²Solo Cassa di Risparmio di Parma e Piacenza

3. lo studente torna in segreteria con la ricevuta del pagamento. Mentre lo studente è presente, la segreteria inserisce i principali dati anagrafici e di carriera in GISS, recuperandoli dalla domanda di immatricolazione e gli consegna le credenziali appena generate dal sistema GISS;
4. la segreteria inserisce le informazioni mancanti o corregge quelle errate (questa operazione potrebbe portare alla generazione di un indirizzo di posta differente) e finalizza l'operazione di immatricolazione.

4.1.2 Studenti di master

I master non sono tutti gestiti dalle Facoltà; alcuni sono gestiti con fondi di dipartimento.

In questo secondo caso gli studenti non si iscrivono presso le segreterie studenti, ma presso la segreteria organizzativa del master, costituita presso il dipartimento. I dati di queste persone sono trattati come quelle degli Ospiti.

Nel caso di master di facoltà, essi sono studenti a tutti gli effetti.

4.1.3 Studenti di scambio

Dal 2008-2009 gli studenti sono inseriti dal Servizio *Scambi Didattici Internazionali* nel sistema GISS e i loro dati trattati come gli altri studenti.

Fino all'anno accademico 2007-2008, gli studenti *incoming* compilavano un *application form* preparato dal Settore *Innovazione Tecnologie Informatiche*.

I dati erano poi inseriti nel server di autenticazione tramite programma scritto in linguaggio php e utilizzato dal personale del *Servizio Scambi Didattici Internazionali* del Settore Gestione Studenti dell'Area *Didattica*.

Gli stessi dati erano usati per alimentare un database Access per la gestione amministrativa.

L'indirizzo mail personale dello studente e una password casuale costituivano le credenziali; il foglio che le conteneva era stampato e consegnato allo studente.

4.1.4 SSIS

Nell'anno accademico 2008-2009 il primo anno della scuola SSIS non è stato attivato e quindi non è stato necessario rilasciare nuove credenziali.

Fino all'anno accademico 2007-2008, la procedura prevedeva il passaggio di un file excel contenente i dati degli studenti SSIS dal Servizio *Specializzazioni* del Settore *Formazione Post-Laurea* dell'Area *Didattica* al Settore *Innovazione Tecnologie Informatiche*.

I dati erano trattati e esportati in formato CSV³ e usati per aggiornare il server a directory tramite programma scritto in linguaggio perl.

L'indirizzo mail personale dello studente o l'indirizzo nel formato *nome.cognome@ssispr.unipr.it* e una password casuale costituivano le credenziali. Alla segreteria didattica erano inviate le lettere da consegnare agli specializzandi nel corso delle prime lezioni.

4.1.5 Dottorandi

Dall'anno accademico 2008-2009 l'ufficio utilizza GISS e anche ai dottorandi viene fornito un account seguendo la procedura studenti.

Fino all'anno accademico 2007-2008, la procedura prevedeva il passaggio di un file excel contenente i dati degli studenti SSIS dal Servizio *Borse di Studio e Dottorati* del Settore *Formazione Post-Laurea* dell'Area *Didattica* al Settore *Innovazione Tecnologie Informatiche*.

4.1.6 Specializzandi

Il Servizio *Specializzazioni* del Settore *Formazione Post-Laurea* utilizza GISS, come le segreterie studenti.

I dati sono quindi gestiti in modo analogo a quelli degli studenti.

4.2 Creazione credenziali

La creazione delle credenziali avviene una volta che lo studente ha pagato la prima rata delle tasse e contestualmente all'inserimento dei dati in GISS (punto 3 della procedura).

La medesima sera una procedura batch estrae i dati dal database GISS e li inserisce in un file di testo di tipo CSV (il separatore di campo è però il segno di due punti).

Nel file sono contenuti tutti i dati necessari alla gestione dei servizi.

Alcune procedure bash+perl in automatico generano il file ldif per popolare il server master LDAP.

4.3 Modifica credenziali

Gli utenti possono modificare autonomamente la password attraverso una pagina web protetta da SSL. Il certificato in uso è autofirmato, ma è già stato richiesto un certificato SCS.

³Comma Separated Value, formato di file che prevede che i dati siano in formato tabellare e che i campi siano separati da virgole.

Se l'utente dimentica la password, deve rivolgersi al Servizio *Supporto ai servizi internet* del Settore *Innovazione Tecnologie Informatiche* dell'Area *Edilizia*.

La modalità di richiesta prevede la compilazione di un modulo elettronico con i dati minimi di cui lo studente è a conoscenza (matricola, indirizzo di posta e codice fiscale). Il modulo prodotto è un file PDF contenente una password casuale che deve essere stampato, firmato e inviato via fax allegando una fotocopia di un documento di identità.

4.4 Modifica attributi

Ogni sera, oltre al file contenente i dati dei nuovi iscritti, è inviato anche un file contenente i dati modificati degli studenti già iscritti.

Gli attributi sono modificati utilizzando delle procedure bash+perl simili a quelle usate per la creazione.

4.5 Cessazione

La cessazione della casella di posta elettronica, due anni dopo l'ultima iscrizione, non comporta la cancellazione dal server LDAP, ma solo lo spostamento ad altro ramo.

La decisione del Consiglio di Amministrazione è motivata dai risparmi finanziari⁴ del servizio di posta CINECA (0,5 euro a casella).

Gli attributi modificati sono *Stato*, *datafine*⁵, *anno*⁶, *categoria* e quelli relativi all'affiliazione appartenenti all'objectclass *eduPerson*.

⁴L'eventuale passaggio ad un fornitore gratuito renderà inutile questa misura

⁵Data della laurea, che nel caso di rinuncia non è valorizzata.

⁶Corrisponde all'ultimo anno in cui è stata pagata la prima rata delle tasse universitarie.

Capitolo 5

Altre persone

Di questa categoria fanno parte tutti coloro che non sono censiti nel sistema informativo o che non è previsto siano accreditati in modo automatico (per esempio, i borsisti).

5.1 Accreditamento

Queste persone sono accreditate da un dipendente strutturato, che fa richiesta di un account per questa persona.

5.2 Rilascio credenziali

Le informazioni richieste sono minime: nome, cognome, tipo di incarico e scadenza del rapporto con l'Ateneo.

Le credenziali sono inviate al dipendente strutturato che ha controfirmato la richiesta come responsabile.

In alcuni casi è generato un indirizzo di posta elettronica di Ateneo, nel formato *nome.cognome@nemo.unipr.it* mentre in altri l'account è generato facendo uso dell'indirizzo personale dell'utente. In questo secondo caso gli indirizzi personali devono essere forniti dal dipendente che richiede la generazione degli account.

5.3 Modifica credenziali

Gli utenti possono modificare autonomamente la password attraverso una pagina web protetta da SSL. Il certificato in uso è autofirmato, ma è già stato richiesto un certificato SCS.

Le password scadono ogni 180 giorni.

Se l'utente dimentica la password o lascia passare 200 giorni dall'ultimo cambio, il sistema non permette più di accedere ai servizi (neppure a quello di cambio

password) e l'utente deve rivolgersi al Servizio *Supporto ai servizi internet* del Settore *Innovazione Tecnologie Informatiche* dell'Area *Edilizia*.

La modalità di richiesta è l'invio di un fax prestampato allegando una fotocopia di un documento di identità.

5.4 Modifica attributi

Non è prevista alcuna modifica automatica agli attributi di questi account.

5.5 Cessazione

Alla data della scadenza, contenuta nel campo *shadowExpire*, l'utente non potrà più autenticarsi al servizio di posta elettronica.

DRAFT

Capitolo 6

Sviluppi futuri

6.1 Database centrale

6.1.1 Certificati digitali

L'art. 64 del Codice dell'Amministrazione Digitale (d.lgs. 7 marzo 2005, n.82 e s.m.i.) prevede che la carta d'identità elettronica e la carta nazionale dei servizi costituiscano strumenti di identificazione per i servizi erogati in rete dalle pubbliche amministrazioni centrali.

Per mantenersi al passo sarebbe opportuno adeguare il sistema di autenticazione affinché permetta l'accesso anche tramite certificati digitali X.509.

In particolare sarebbe necessario stabilire una procedura per associare ogni certificato che si potrebbe presentare al sistema con una identità digitale.

6.1.2 Progetto 2009 per l'autenticazione

Presupposto logico della possibilità di autenticarsi con certificati X.509 è che ad ogni persona sia associata una ed una sola identità digitale.

Al contrario sarebbe necessario che o una persona possieda tanti certificati quante sono le identità (ma i certificati non sono intercambiabili e utilizzabili a piacere) o che alcune identità possano identificarsi solo con username e password.

6.2 Sistema di autenticazione

6.2.1 Controllo scadenza password o account

Per decisione progettuale del produttore, l'attuale sistema di identificazione (Central Authentication Server) non gestisce la scadenza della password dell'account né quella dell'account.

Sarebbe opportuno imporre la verifica di tali parametri prima di consentire l'accesso ai servizi online. Un cambio più frequente della password è infatti garanzia di una maggiore sicurezza.

Il controllo della scadenza dell'account permetterebbe di impedire l'accesso ai servizi a coloro che non hanno più rapporti con l'Ateneo senza doverli forzatamente cancellare dal sistema.

6.2.2 Self-reset password

Attualmente le procedure di recupero password prevedono l'invio di un fax, allegando fotocopia di un documento di identità.

Per diminuire l'intervento del servizio Supporto ai Servizi Internet potrebbe essere opportuno consentire il recupero della password tramite sistemi automatici.

Questo diminuirebbe la sicurezza del sistema ma consentirebbe un miglior utilizzo di risorse umane con competenze medio-alte.

6.3 Gestione di altre categorie

Attualmente non sono gestite centralmente l'assegnazione delle password ad alcune categorie di persone.

6.3.1 Future matricole

Per varie ragioni gli Atenei raccolgono dati di studenti che non sono ancora immatricolati, ad esempio i candidati che partecipano ai concorsi per l'accesso ai corsi di laurea a numero chiuso.

Per loro natura i bandi per l'accesso ai benefici regionali (alloggio, borsa di studio, ecc.) si chiudono molto in anticipo sulle scadenze per le immatricolazioni all'Ateneo. In questo caso è possibile che lo studente si registri al sito dell'ente regionale per il diritto allo studio (operazione necessaria per compilare la domanda online) con dati inesatti e quindi differenti rispetto a quelli dell'immatricolazione.

Se i dati non sono esattamente uguali, è necessaria una faticosa operazione manuale per associare i dati dei due diversi inserimenti.

Se la registrazione fosse univoca, al futuro studente potrebbero essere fornite le credenziali all'interno del sistema di autenticazione centralizzata dell'Ateneo. In questo modo le informazioni sarebbero facilmente associabili ad una stessa persona.

6.3.2 Ditte esterne

Per il momento non esiste la necessità di rilasciare delle credenziali a tutti i fornitori esterni in quanto tali.

D'altra parte, gli studenti possono acquisire crediti formativi svolgendo attività pratiche (stage o tirocinio) in strutture anche esterne all'Ateneo.

Ogni tirocinio prevede un responsabile aziendale che segue lo studente nelle sue attività e che, alla fine del tirocinio, procede ad una valutazione del comportamento e dei risultati conseguiti.

In questo caso al personale dell'azienda si assegna un account per fornire il necessario accesso al sistema dei tirocini.

6.4 Modifica procedure di accreditamento

6.4.1 Professori a contratto

Il sistema informativo non gestisce l'evento "firma del contratto" (che comunque avviene dopo l'inizio dell'attività didattica), cosicché all'inizio del semestre è impossibile sapere con certezza se la persona chiamata dalla Facoltà a coprire un insegnamento ha effettivamente preso servizio.

Le credenziali sarebbero però necessarie prima di iniziare l'attività didattica (ad esempio per predisporre l'ambiente relativo al corso nelle applicazioni per il blended learning) ovvero per compilare i programmi dei corsi e le altre informazioni necessarie per rispettare i requisiti di trasparenza (D.M. 31 ottobre 2007, n. 544 e D.D. n. 61 del 10 giugno 2008).

Per questo è opportuno un maggiore coinvolgimento delle Presidenze di Facoltà nella consegna delle credenziali e nella gestione delle identità digitali di queste persone.

6.4.2 Studenti

Nel dicembre 2008, l'Università di Parma è risultata assegnataria di un contributo per il bando "Campus Digitali" del Ministero dell'Università e della Ricerca.

All'interno del progetto era obbligatorio prevedere la realizzazione di due servizi online minimi, uno dei quali è relativo all'immatricolazione degli studenti via web.

Questo cambia notevolmente le modalità con cui sono raccolte le informazioni sugli studenti e avrà un sicuro impatto anche sul processo di accreditamento per questa categoria di persone.

6.4.3 Ospiti

La procedura di accreditamento ospiti è attualmente attivata su richiesta di qualunque dipendente strutturato.

Il controllo dell'identità della persona è perciò delegato al dipendente strutturato che fa richiesta.

Sarebbe opportuno un sistema coordinato con una organizzazione appositamente costituita di persone delegate ad effettuare la richiesta di account a cui le persone ospiti possono rivolgersi.

In questo modo sarebbe possibile un migliore controllo dell'identità dell'ospite che necessita dell'account (potendo anche verificare se già è dotato di account dell'Università perché ricopre altri ruoli).

DRAFT