UNIVERSITA' DEGLI STUDI DI PAVIA
Area Sistemi Informativi
Via Ferrata, 1 - 27100 PAVIA - C.F. 80007270186 - P.I. 00462870189 - Tel. 0382985900 - Fax 0382985915

Documento descrittivo del processo di accreditamento degli utenti

Revisioni

Data	Versione	Descrizione modifica	Autore
05/03/2010	1.0	Versione definitiva	M. Alicanti – C. Venturini

Abbreviazioni

AD: Area della Didattica
AP: Area del Personale
ASI: Area Sistemi Informativi
CELL: Applicativo Collaboratori Esperti Linguistici di Lingua madre
CSA: Applicativo Carriere e Stipendi di Ateneo
DPS: Documento Programmatico della Sicurezza
ERASMUS: European Community Action Scheme for the Mobility of University Students
Esse3: Applicativo Servizi e Segreteria Studenti
IdP: Identity Provider
IRET: Incarichi Retribuiti
PAE: Procedura Accreditamento Esterni
PF: Presidenza di Facoltà
SIDRO:Sistema Informativo Dottorati di Ricerca On-line
U-Gov: University-Governance
URP: Ufficio Relazioni con il Pubblico
WiFi: Wireless Fidelity

Gestore dell'accreditamento

La struttura che sovraintende globalmente al processo di accreditamento degli utenti è l'Area Sistemi Informativi (ASI), la quale, a seguito dei differenti percorsi di riconoscimento/accreditamento previsti per le diverse categorie di utenti, delega alcune funzioni gestionali all'Area del Personale (AP), all'Area Didattica (AD) e alle Presidenze di Facoltà (PF).
La gestione, la disabilitazione e la cancellazione delle identità digitali avvengono in modo completamente automatico, l'assegnazione in generale è automatica ad eccezione della categoria ospiti per la quale è effettuata manualmente.

Utenti gestiti

Staff

Questa categoria è inclusa nell'IdP ed è costituita da circa 3170 utenti.

Professori ordinari
Professori associati
Professori a contratto
Ricercatori
Assegnisti di ricerca
Dirigenti
Personale tecnico-amministrativo
Personale tecnico-amministrativo a tempo determinato
Collaboratori ed esperti linguistici
Collaboratori Coordinati Continuativi
Volontari servizio civile

Student

Questa categoria è inclusa nell'IdP ed è costituita da circa 28.000 utenti.

Studenti iscritti a corsi di primo e secondo livello
Dottorandi
Specializzandi
Master

Alumn

Questa categoria non è inclusa nell'IdP.

Laureati di un qualunque corso di studi/ dottorato/ master

Affiliate

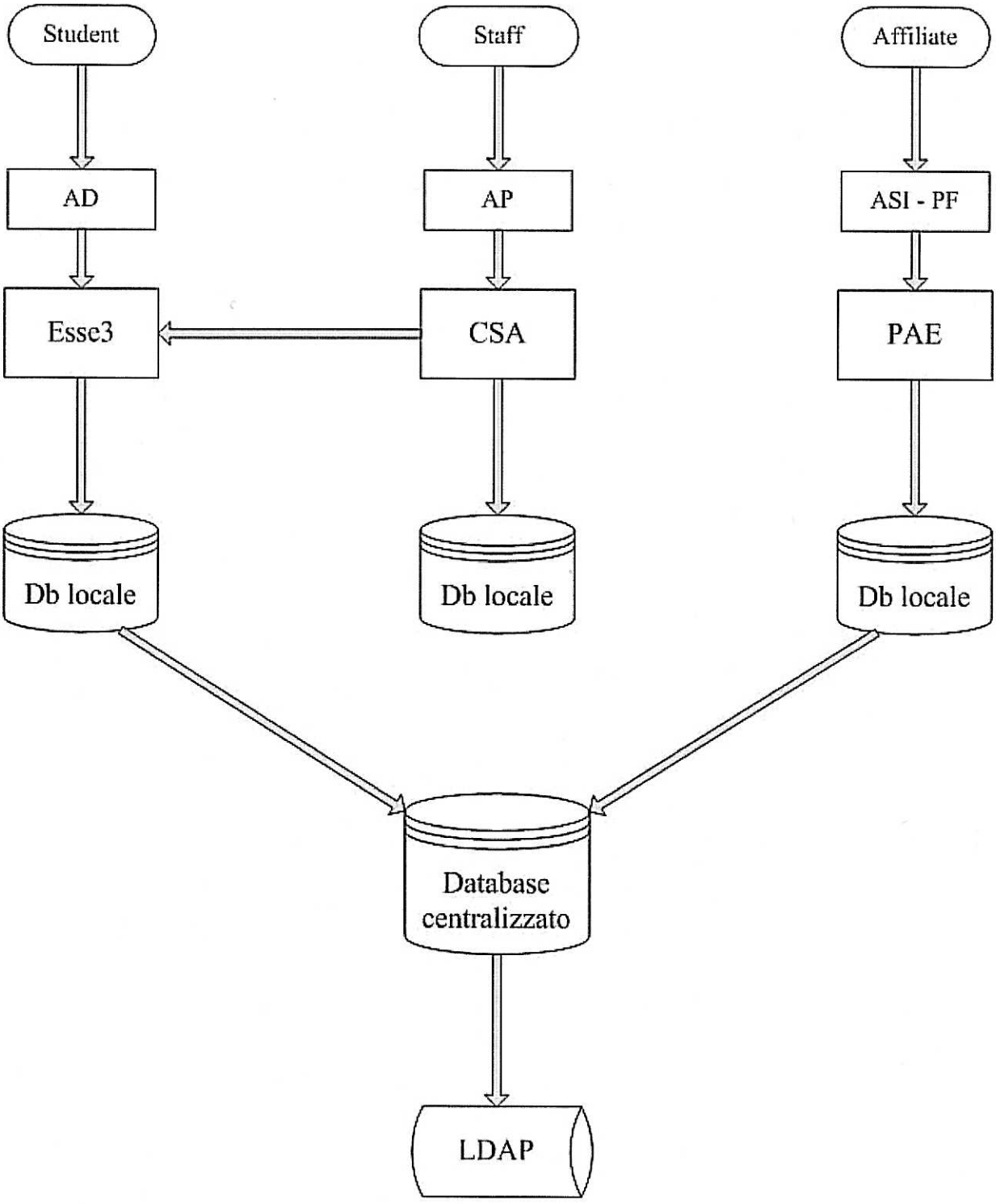
Questa categoria è inclusa nell'IdP ed è costituita da circa 345 utenti.

Visitatori
Operatori di aziende
Convegnisti

Mappatura degli utenti sulle affiliazioni IDEM

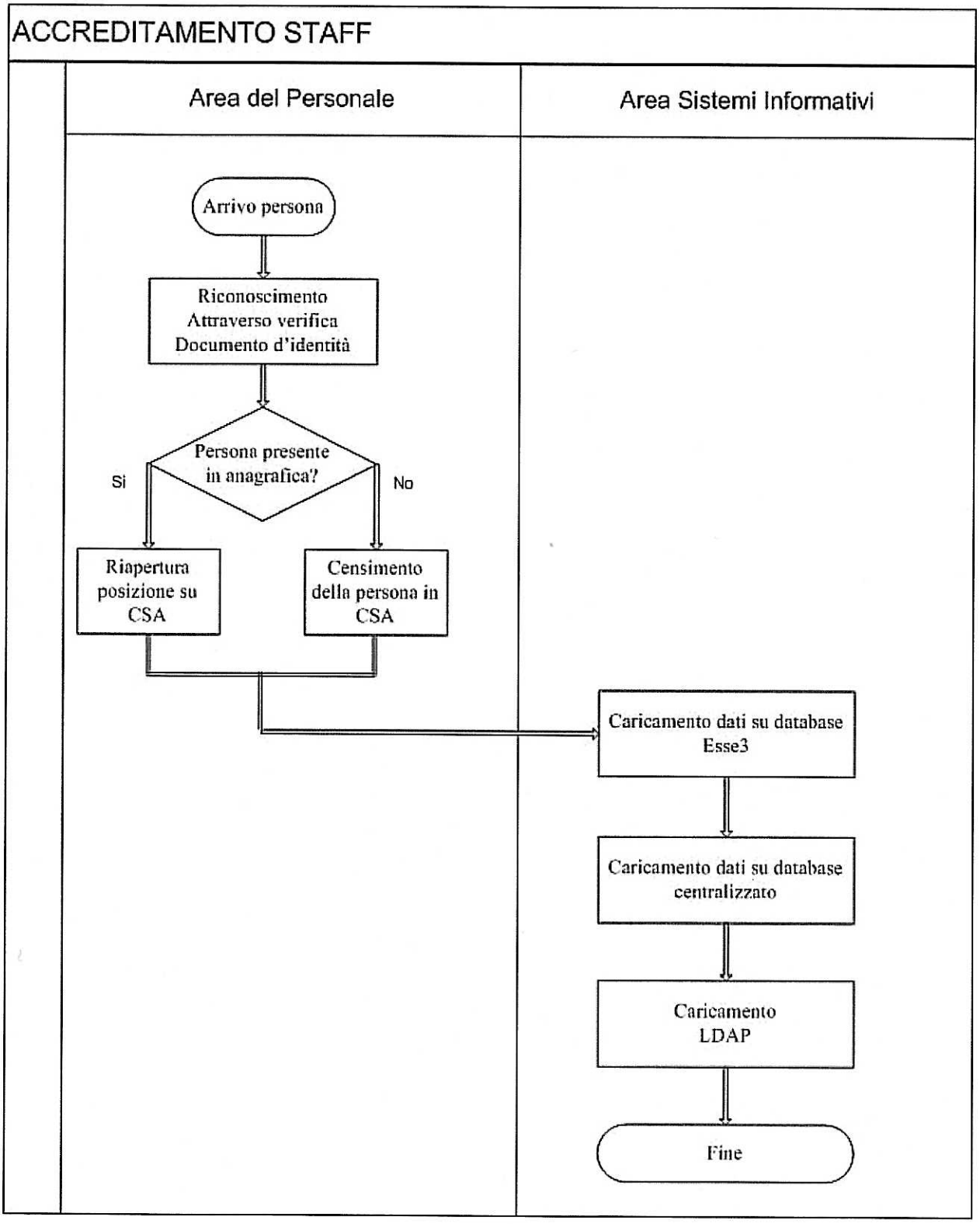
Professori ordinari	staff, member
Professori associati	staff, member
Professori a contratto	staff, member
Ricercatori	staff, member
Assegnisti di ricerca	staff, member
Dirigenti	staff, member
Personale tecnico-amministrativo	staff, member
Personale tecnico-amministrativo a tempo determinato	staff, member
Collaboratori ed esperti linguistici	staff, member
Collaboratori Coordinati Continuativi	staff, member
Volontari servizio civile	staff, member
Studenti iscritti a corsi di primo e secondo livello	student, member
Dottorandi	student, member
Specializzandi	student, member
Master	student, member
Visitatori	affiliate
Operatori di aziende	affiliate
Convegnisti	affiliate

Visione di insieme del processo di accreditamento degli utenti



Il processo di accreditamento per la categoria di utenti Staff

Il processo



Modalità di riconoscimento della persona

Il processo di verifica dell'identità del personale strutturato avviene all'atto dell'assunzione ed è effettuato dall'AP. L'Ufficio incaricato accerta l'identità mediante la verifica di un documento di riconoscimento in corso di validità e registra i dati anagrafici attraverso l'applicativo CSA. In modo automatico i dati relativi al nuovo assunto vengono trasmessi all'applicativo Esse3 che genera le relative credenziali che successivamente confluiscono nel database centralizzato da cui viene popolato LDAP.

Caratteristiche dell'identità digitale

Ad ogni identità digitale vengono associati, come minimo, l'insieme di attributi elencati nella tabella che segue.

Attributi	Attributo Pubblico (si/no)
Nome	Sì
Cognome	Sì
Codice fiscale	No
Matricola dipendente	No
Email	Sì
Password	No
Nome completo	Sì
Ruolo	Sì

Gestione del ciclo di vita

L'aggiornamento di una identità digitale avviene a seguito di cambio ruolo o dimissioni della persona. In particolare la modifica effettuata nel database di CSA genera l'aggiornamento automatico del database delle identità digitali.

Formato e regole delle credenziali

Le credenziali sono costituite da username e password, lo username coincide con il codice fiscale.
La password iniziale viene generata dall'applicativo Esse3, ha lunghezza minima di 8 caratteri ed è costituita da caratteri alfanumerici.
Non vengono utilizzate credenziali elettroniche di tipologia diversa.

Eventuale presenza di credenziali multiple per la stessa persona

Non è previsto il rilascio di credenziali multiple ad una singola persona.

Modalità di consegna delle credenziali

Le credenziali non vengono consegnate all'atto dell'accreditamento, un nuovo membro dello staff entra in possesso della propria password mediante la procedura on-line "Cambio password servizi di Ateneo" selezionando l'opzione "Dimenticato password" ed inserendo il proprio codice fiscale. Effettuata l'operazione, l'utente riceve la password personale mediante messaggio di posta elettronica inviato alla sua casella istituzionale. Il messaggio contiene inoltre l'invito a modificare immediatamente la parola chiave utilizzando l'opzione "Cambio password" dalla medesima procedura on-line. In questo caso la procedura richiederà

l'introduzione di codice fiscale, vecchia password, nuova password e conferma nuova password.

Modalità di recupero delle credenziali smarrite

Non è possibile recuperare una password smarrita in quanto le stesse vengono conservate criptate, pertanto, in caso di credenziale dimenticata, è necessario richiedere la generazione di una nuova password mediante la procedura on-line "Cambio password servizi di Ateneo" selezionando l'opzione "Dimenticato password" ed inserendo il proprio codice fiscale. Effettuata l'operazione, l'utente riceve la password personale mediante messaggio di posta elettronica inviato alla sua casella istituzionale. Il messaggio contiene inoltre l'invito a modificarla immediatamente utilizzando l'opzione "Cambio password" dalla medesima procedura on-line. In questo caso la procedura richiederà l'introduzione di codice fiscale, vecchia password, nuova password e conferma nuova password.

Modalità di gestione smarrimento smartcard/token

Non è al momento previsto il rilascio di smartcard/token.

Durata dell'accreditamento

L'accreditamento in generale non ha scadenza. Fa eccezione il personale dimissionario e il personale a contratto. Nel primo caso l'accreditamento scade 6 mesi dopo la data di fine rapporto, nel secondo coincide con la scadenza del contratto.

Disabilitazione utente

Gli utenti di questa categoria, in generale, non vengono disabilitati, fanno eccezione:

- i dimissionari che vengono disabilitati 6 mesi dopo la data di fine rapporto;
- il personale a contratto che viene disabilitato alla scadenza del contratto.

Cancellazione definitiva utente

La cancellazione di un utente dal repository delle credenziali è contemporanea alla sua disabilitazione, tutti i dati restano tuttavia nel database dell'applicativo di origine.

Rischi specifici associati alla categoria di utenti

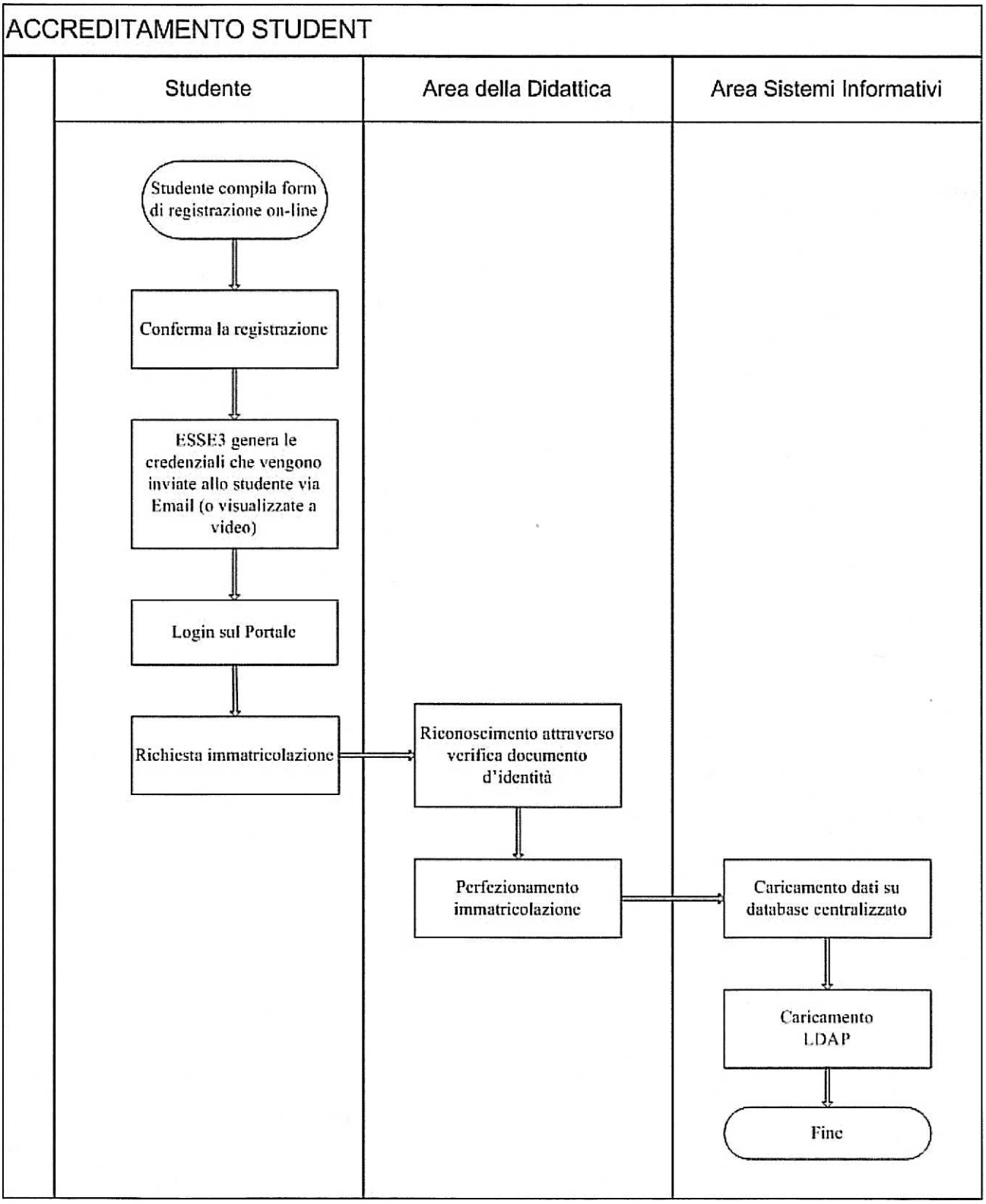
Il procedimento di creazione dell'identità digitale e quindi delle relative credenziali è scandito da passaggi burocratici/gestionali rigidi che non permettono l'introduzione di variazioni non controllate, inoltre, la mancanza di consegna/invio delle credenziali su supporto cartaceo evita che persone diverse dall'assegnatario, per motivi istituzionali o di altro genere, vengano a conoscenza delle stesse.
Inoltre, gli utenti di questa categoria, all'assunzione, vengono adeguatamente formati circa i procedimenti che caratterizzano le diverse attività universitarie, fra essi i regolamenti e le politiche di sicurezza, e periodicamente ricevono specifiche informative volte a ricordare/aggiornare le norme di sicurezza adottate dall'Ateneo nelle quali sono comprese anche le regole e le raccomandazioni relative alle credenziali.

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

Non è previsto il rilascio/utilizzo di credenziali forti e di conseguenza non esiste interazione con le credenziali deboli adottate.

Il processo di accreditamento per la categoria di utenti Student

Il processo



Modalità di riconoscimento della persona

Il riconoscimento di uno studente presso l'Università di Pavia avviene all'atto del perfezionamento dell'immatricolazione. Lo studente deve recarsi all'apposito sportello dell'AD ove il personale preposto procede al riconoscimento mediante verifica di documento d'identità in corso di validità e termina la procedura d'immatricolazione.
A questo punto, le credenziali create dall'applicativo Esse3 nella fase di registrazione on-line preventivamente effettuata dallo studente, vengono trasferite al database centralizzato da cui viene popolato LDAP.
Il riconoscimento degli studenti ERASMUS che hanno preventivamente ricevuto conferma di iscrizione avviene all'atto della registrazione. Lo studente deve recarsi presso l'AD ove l'ufficio preposto procede al riconoscimento mediante verifica di un documento di identità, conclude la procedura di iscrizione e contestualmente attraverso la procedura on-line Procedura Accreditamento Esterni (PAE) assegna le credenziali di accesso ai servizi definiti per tale profilo per il periodo di permanenza presso l'Ateneo.

Caratteristiche dell'identità digitale

Attributi	Attributo Pubblico (si/no)
Nome	Sì
Cognome	Sì
Codice fiscale*	No
Matricola studente	No
Email	Sì
Password	No
Nome completo	Sì
Corso di laurea	No
Facoltà	No
Ruolo	Sì

* Nel caso di studenti stranieri che non dispongano di codice fiscale, lo stesso viene sostituito da uno Username alfanumerico di lunghezza massima pari a 16 caratteri.

Gestione del ciclo di vita

L'aggiornamento di una identità digitale avviene a seguito di cambio di ruolo, di Facoltà, di Corso di laurea o di rinuncia. In particolare la modifica effettuata nel database di Esse3 genera l'aggiornamento del database delle identità digitali. Per gli studenti ERASMUS non sono previsti cambi di stato e di conseguenza non vengono effettuati aggiornamenti.

Formato e regole delle credenziali

Le credenziali per gli studenti di ogni ordine iscritti all'Università di Pavia sono costituite da username e password, lo username coincide con il codice fiscale, la password viene generata dall'applicativo Esse3, ha lunghezza di 8 caratteri ed è costituita da caratteri alfanumerici.
Le credenziali degli studenti ERASMUS sono costituite da username e password, lo username coincide con il codice fiscale se lo studente lo possiede, in caso contrario viene scelto all'atto della registrazione uno username alfanumerico di lunghezza compresa fra 8 e 16 caratteri. La password costituita da almeno 8 caratteri alfanumerici viene sempre scelta dallo studente all'atto della registrazione.

Non vengono utilizzate credenziali elettroniche di tipologia diversa.

Eventuale presenza di credenziali multiple per la stessa persona

Non è previsto il rilascio di credenziali multiple ad una singola persona.

Modalità di consegna delle credenziali

Una persona che intende diventare studente dell'Università di Pavia deve innanzitutto collegarsi alla pagina Matricole presente sul sito Web dell'Università ed effettuare la procedura di registrazione.
Svolta l'operazione, l'applicativo Esse3 provvede a rilasciargli una password che gli consente esclusivamente di operare sui dati inseriti in fase di registrazione e non gli permette di accedere a nessun servizio differente. Questa password, conservata su una tabella di appoggio, viene inviata all'indirizzo di posta elettronica indicato dal futuro studente o visualizzata al termine della registrazione sullo schermo del computer utilizzato in caso di Email mancante.
Il futuro studente deve poi perfezionare l'immatricolazione recandosi all'apposito sportello dell'AD ove il personale preposto procede al riconoscimento mediante verifica di documento d'identità in corso di validità e termina la procedura d'immatricolazione.
A questo punto le credenziali rilasciate allo studente nella fase di registrazione vengono trasferite da Esse3 al database centralizzato da cui viene popolato il repository LDAP.
Un percorso differente viene seguito dagli studenti stranieri che partecipano al programma ERASMUS, essi infatti, nel periodo che intercorre fra la richiesta e la conferma di iscrizione non dispongono di credenziali. Una volta ricevuta conferma di iscrizione, lo studente deve recarsi presso l'AD ove l'ufficio preposto procede al riconoscimento mediante verifica di un documento di identità, conclude la pratica di iscrizione e contestualmente attraverso la procedura on-line PAE assegna le credenziali di accesso ai servizi definiti per tale profilo per il periodo di permanenza presso l'Ateneo.

Modalità di recupero delle credenziali smarrite

Non è possibile recuperare una password smarrita in quanto le stesse vengono conservate criptate. Qualora uno studente dimentichi la propria password ha la possibilità di richiedere la generazione di una nuova password mediante la procedura on-line "Cambio password servizi di Ateneo" selezionando l'opzione "Dimenticato password" ed inserendo il proprio codice fiscale/username. Effettuata l'operazione, l'utente riceverà la password personale mediante messaggio di posta elettronica inviato alla sua casella istituzionale o alla casella segnalata all'atto dell'accreditamento mediante procedura PAE per gli studenti ERASMUS. Il messaggio contiene inoltre l'invito a modificarla immediatamente utilizzando l'opzione "Cambio password" dalla medesima procedura on-line. In questo caso la procedura richiederà l'introduzione di codice fiscale/username, vecchia password, nuova password e conferma nuova password.

Modalità di gestione smarrimento smartcard/token

Non è prevista l'assegnazione di smartcard/token.

Durata dell'accreditamento

L'accreditamento perdura per due anni dopo il termine della carriera universitaria. In caso il termine sia dovuto a rinuncia agli studi, la validità cessa alla data della rinuncia stessa.

L'accreditamento degli studenti ERASMUS ha termine allo scadere della loro permanenza presso l'Ateneo.

Disabilitazione utente

L'utente viene disabilitato due anni dopo il termine del corso di studi prescelto ad eccezione degli studenti rinunciatari le cui credenziali vengono disabilitate alla data della rinuncia stessa. Gli studenti ERASMUS vengono disabilitati allo scadere della loro permanenza presso l'Ateneo.

Cancellazione definitiva utente

La cancellazione di un utente dal repository delle credenziali è contemporanea alla sua disabilitazione, tutti i dati restano tuttavia nel database dell'applicativo di origine.

Rischi specifici associati alla categoria di utenti

Nel tempo non si sono riscontrate particolari criticità nel processo di riconoscimento/accreditamento degli utenti di questa categoria, siano essi studenti dell'Università di Pavia che ERASMUS. Per quanto riguarda questi ultimi, va precisato che il personale preposto al rilascio delle credenziali attraverso procedura manuale è incaricato del trattamento di dati personali e di conseguenza rispetta, anche in termini di riservatezza, quanto previsto dalla legge 196/03.
Mediante queste credenziali tutti gli studenti accedono alla rete wired e wireless d'Ateneo e di conseguenza a tutti i servizi loro dedicati, compresi quelli resi disponibili attraverso IDEM, le transazioni svolte via rete sono registrate e i log vengono archiviati.

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

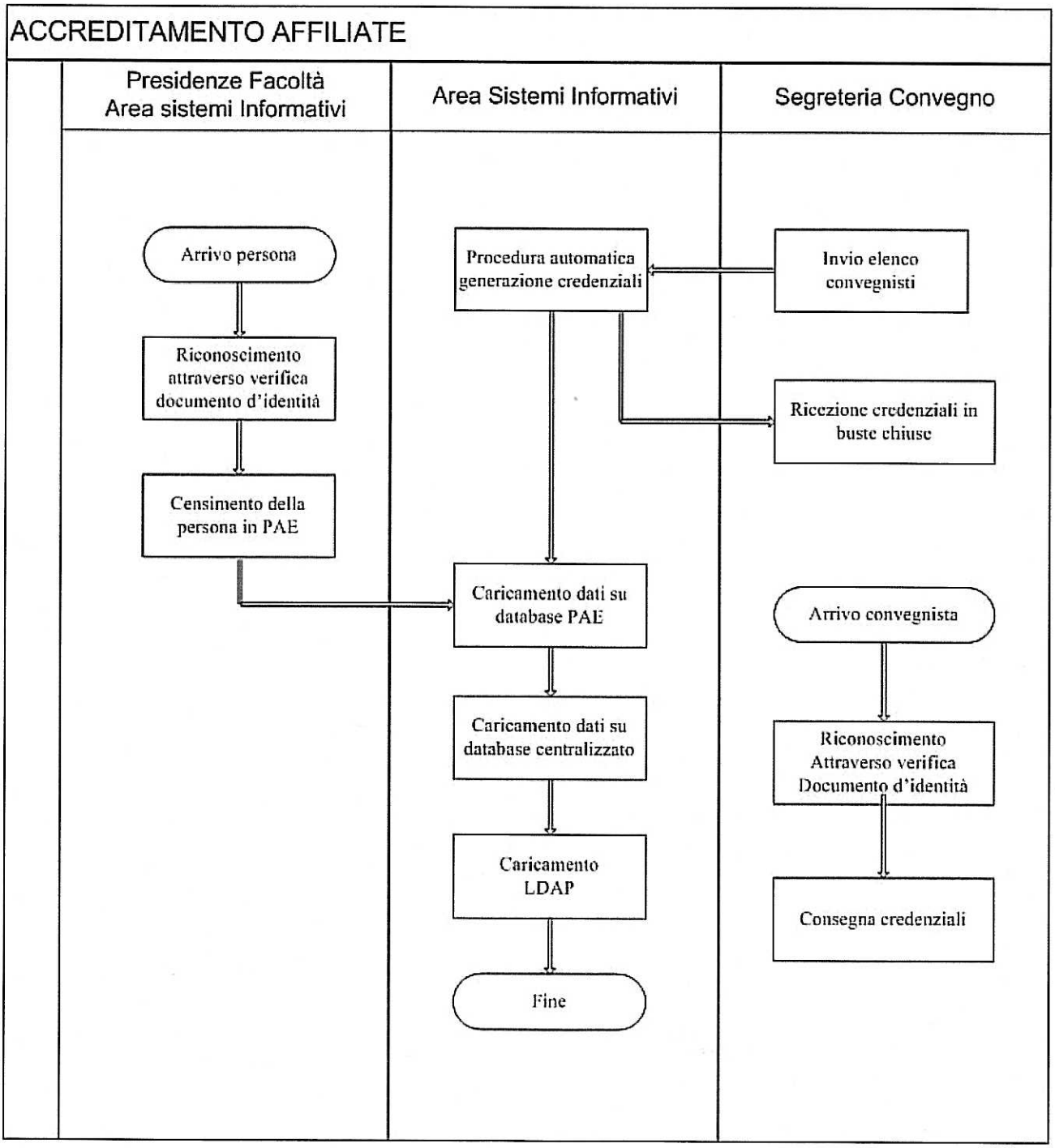
Non è previsto il rilascio/utilizzo di credenziali forti e di conseguenza non esiste interazione con le credenziali deboli adottate.

Il processo di accreditamento per la categoria di utenti Alumn

Attualmente non è prevista l'assegnazione di identità digitali agli Alumni.

Il processo di accreditamento per la categoria di utenti Affiliate

Il processo



Modalità di riconoscimento della persona

Il riconoscimento viene in generale effettuato, mediante documento d'identità, dalla Presidenza di Facoltà (PF) a cui temporaneamente l'ospite afferisce a vario titolo o dall'ASI qualora la persona afferisca a Uffici dell'Amministrazione centrale.
Fanno eccezione i partecipanti a convegni che vengono riconosciuti, mediante documento d'identità, dalla segreteria del convegno all'atto della registrazione.
L'attribuzione di una identità digitale avviene mediante l'apposito applicativo on-line PAE accessibile ai soli uffici autorizzati all'accreditamento. La procedura popola un proprio database dal quale, con cadenza giornaliera, vengono estratti i dati da inserire nel database centralizzato su cui si basa l'aggiornamento del repository LDAP.

Caratteristiche dell'identità digitale

Attributi	Attributo Pubblico (si/no)
Nome	Sì
Cognome	Sì
Codice fiscale/Username	No
Email*	Sì
Password	No
Nome completo	Sì
Ruolo	Sì

*L'attributo non è significativo per i convegnisti.

Gestione del ciclo di vita

L'aggiornamento di una identità digitale avviene a seguito di cambio ruolo o scadenza del rapporto con l'Università. In particolare la modifica effettuata nel database di registrazione genera l'aggiornamento del database centralizzato e quindi di quello delle identità digitali.

Formato e regole delle credenziali

Le credenziali sono costituite da username e password, in generale lo username coincide con il codice fiscale della persona, mentre la password viene scelta dall'ospite all'atto dell'accreditamento e deve avere lunghezza minima di 8 caratteri e rispettare le norme di sicurezza vigenti in Ateneo relativamente a questo attributo. Qualora l'ospite non sia in possesso di codice fiscale anche lo username verrà scelto dall'ospite stesso ed avrà lunghezza compresa fra 8 e 16 caratteri alfanumerici.
Fanno eccezione le credenziali assegnate ai partecipanti a convegni che vengono generate automaticamente da apposita procedura e caricate nel database dell'applicazione PAE, in questo caso lo username è una combinazione del nome del congresso e di un progressivo numerico, mentre la password è costituita da 8 caratteri ed è creata applicando un algoritmo alle generalità del partecipante.
Non vengono utilizzate credenziali elettroniche di tipologia diversa.

Eventuale presenza di credenziali multiple per la stessa persona

Non è previsto il rilascio di credenziali multiple ad una singola persona.

Modalità di consegna delle credenziali

In generale è l'ospite ad indicare una password, quindi non c'è meccanismo di consegna.
Relativamente ai convegni, le credenziali vengono consegnate ai partecipanti in busta chiusa dalla segreteria dell'evento.

Modalità di recupero delle credenziali smarrite

Non è possibile recuperare una password smarrita in quanto le stesse vengono conservate criptate. Qualora un ospite dimentichi la propria parola chiave, può richiedere la generazione di una nuova password mediante la procedura on-line "Cambio password servizi di Ateneo" selezionando l'opzione "Dimenticato password" ed inserendo il proprio codice fiscale. Effettuata l'operazione, l'utente riceverà la password personale mediante messaggio di posta elettronica inviato alla casella indicata all'atto dell'accreditamento mediante la procedura PAE. Il messaggio contiene inoltre l'invito a modificarla immediatamente utilizzando l'opzione "Cambio password" dalla medesima procedura on-line. In questo caso la procedura richiederà l'introduzione di codice fiscale, vecchia password, nuova password e conferma nuova password.
La procedura non è disponibile ai partecipanti a convegni in quanto l'attributo Email non viene considerato significativo poiché non sempre è disponibile.

Modalità di gestione smarrimento smartcard/token

Non è previsto il rilascio di smartcard/token.

Durata dell'accreditamento

La durata dell'accreditamento coincide esattamente con il periodo di presenza dell'ospite presso l'Ateneo.

Disabilitazione utente

La disabilitazione delle credenziali avviene automaticamente alla scadenza del rapporto con l'Ateneo.

Cancellazione definitiva utente

La cancellazione di un utente dal repository delle credenziali è contemporanea alla sua disabilitazione, i relativi dati rimangono nel database dell'applicativo di accreditamento per un periodo limitato.

Rischi specifici associati alla categoria di utenti

Unitamente alle credenziali gli ospiti ricevono un documento in lingua italiana e inglese contenente le regole da rispettare nell'utilizzo dei servizi messi a loro disposizione e le raccomandazioni riguardanti la riservatezza delle credenziali assegnate.

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

Non è previsto il rilascio/utilizzo di credenziali forti e di conseguenza non esiste interazione con le credenziali deboli adottate.

Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione delle identità descritto nelle precedenti pagine viene utilizzato da numerose applicazioni e servizi. La tabella seguente ne presenta l'elenco accompagnato da una breve descrizione.

Applicativo/Servizio	Descrizione
Esse3	Applicativo Servizi e Segreteria Studenti (es. piani di studio, carriere, certificati, ecc.)
U-Gov didattica	Applicativo per la programmazione dell'offerta didattica ad uso delle Facoltà.
U-Gov ricerca	Catalogo informatico centralizzato che raccoglie tutti i prodotti della ricerca dei docenti dell'Università di Pavia contiene i prodotti del Sistema Informativo della Ricerca (SIR) e dei Siti Docenti Ministeriali dei ricercatori dell'Ateneo.
ERASMUS	Applicativo per richiedere l'ammissione all'omonimo progetto.
ProxyBib	Applicativo di accesso alle riviste on-line.
Organi collegiali	Applicativo di gestione dei documenti degli Organi collegiali
Curricula	Applicativo per la gestione dei curricula del personale.
DPS	Applicativo per la gestione e l'aggiornamento del DPS.
SIDRO	Applicativo per la gestione dei dottorati di ricerca.
CSA-web	Applicativo per la consultazione di stipendi e CUD del personale
WiFi	Servizio di accesso alla rete wireless d'Ateneo.
URP	Applicativo per la gestione dei contatti con il pubblico.
CELL	Applicazione per la gestione delle attività di docenza dei Collaboratori Esperti Linguistici.
IRET	Applicativo per la gestione degli incarichi esterni retribuiti del personale docente.

Gli identificatori principali di ogni persona, come "net ID," eduPersonPrincipalName, o eduPersonTargetedID, una volta assegnati, sono univoci. Al momento non è previsto l'utilizzo in altri ambiti.

Partecipazione ad altre federazioni

L'Università di Pavia attualmente non partecipa ad altre Federazioni di Autenticazione e Autorizzazione.