Documento descrittivo del processo di accreditamento degli utenti dell'Università degli Studi di Bologna

Le informazioni fornite in questo documento sono accurate alla data del 23/07/2010

Revisioni

Data	Versione	Descrizione modifica	Autore
29/06/10	0.1	Bozza	Cristian Mezzetti
19/07/10	0.2	Bozza	Cristian Mezzetti, Aldo Schiavina
23/07/10	1.0	Rilascio	Enrico Lodolo, Cristian Mezzetti, Aldopaolo Palareti, Aldo Schiavina, Graziano Zucchini, Elisabetta Papini

Abbreviazioni

Ce.S.I.A. - Centro per lo Sviluppo e Gestione dei Servizi Informatici di Ateneo.
APOS – Area Personale Tecnico Amministrativo, Organizzazione e Sviluppo.
AFORM – Area della Formazione.
ADOC – Area dei Servizi al Personale Docente e Ricercatore.
ASAN – Area della Sanità.
ARIC – Area della Ricerca.
DIRI – Dipartimento Amministrativo Relazioni Internazionali.
ARCA – Area dei Contratti e degli Appalti.
DSA – Directory Service d'Ateneo.
Sito DSA – Applicativo Web per la gestione delle credenziali e il self-provisioning di dati anagrafici e contatti.
Web Personale – Applicativo Web per la gestione delle informazioni di carriera relative al personale dipendente.
GISS-BO – Applicativo per la gestione delle informazioni di carriera relative agli studenti.
AlmaWelcome - Servizio di iscrizione all'offerta formativa dell'Università di Bologna.
Anagrafica Unica – Database centrale che raccoglie tutte le identità dell'ateneo.
PEC – Posta Elettronica Certificata.
AlmaEsami – Applicativo Web per la verbalizzazione degli esami sostenuti dagli studenti.
InfoCert – Ente certificatore per la firma digitale utilizzato dall'Università di Bologna

Gestore dell'accreditamento

Gestore dell'accreditamento è il servizio DSA del Ce.S.I.A. Ad esso sono affidate le operazioni di assegnazione, mantenimento e cancellazione delle identità digitali dell'Università di Bologna.

Utenti gestiti

Staff

Personale docente: Docenti, ricercatori e assimilati (Professori straordinari, Professori ordinari. Professori ordinari fuori ruolo, Professori associati non confermati, Professori associati confermati, Professori associati fuori ruolo, Ricercatori non confermati, Ricercatori confermati, Assistenti).
Docenti a contratto: docenti con un contratto per la copertura di attività didattica
Personale tecnico-amministrativo: personale tecnico-amministrativo a tempo determinato e indeterminato.
Personale TA abilitato CONSIP: responsabili amministrativi dotati di certificati digitali per gli acquisti sul mercato elettronico CONSIP (sottoinsieme del personale TA).
Personale TA abilitato PEC: sottoinsieme del personale TA con accesso alla posta elettronica certificata, tramite certificato di autenticazione appositamente rilasciato.
Registration Authorization Officer (RAO): delegati per il rilascio di certificati digitali (sottoinsieme personale TA).
Contrattisti: titolari di assegni di ricerca, borse di studio, contratti di collaborazione di vario genere.
Accreditati interni: ospiti a vario titolo dell'ateneo, svolgono la loro attività prevalentemente presso i locali dell'Università.

Categoria utente	Accesso all'Identity Provider (IdP)	Cardinalità
Personale docente	Sì	4000
Docenti a contratto	Sì	6500
Personale tecnico-amministrativo	Sì	4000
Personale TA abilitato CONSIP	No	250
Personale TA abilitato PEC	No	10
Registration Authorization Officer	No	20
Contrattisti	Sì	5000
Accreditati interni	Sì	2500
Ricercatore dell'Alma Mater	Sì	0
Professore dell'Alma Mater	Sì	1

Il *personale TA abilitato CONSIP*, il *personale TA abilitato PEC* e i *Registration Authorization Officer* non hanno accesso all'IdP in quanto tali ma in quanto membri del *personale tecnico-amministrativo*.

Student

Dottorandi – Iscritti ad un corso di dottorato.

Studenti incoming attivi – Studenti provenienti da scambio internazionale che stanno svolgendo un periodo di studio presso l'Università.

Medici in formazione specialistica – Iscritti alle scuole di specializzazione mediche.
Laureati frequentatori – Studenti post-laurea che frequentano i locali dell'Università per un periodo (massimo 1 anno) di approfondimento di studio e/o ricerca.
Studenti attivi – Studenti che hanno perfezionato l'iscrizione e in regola con il pagamento delle tasse.
Studenti non attivi – Studenti che hanno perfezionato l'iscrizione ma non sono in regola con il pagamento delle tasse.

Categoria utente	Accesso all'Identity Provider (IdP)	Cardinalità
Dottorandi	Sì	10000
Studenti incoming attivi	Sì	2000
Medici in formazione specialistica	Sì	600
Laureati frequentatori	Sì	100
Studenti attivi	Sì	90000
Studenti non attivi	Sì	40000

Alumn

Studenti cessati con titolo: studenti laureati per i quali le credenziali continuano a funzionare. La cardinalità è data dalla differenza fra gli studenti che hanno perfezionato l'iscrizione (circa 260.000) e gli studenti attivi.
Studenti incoming cessati – Studenti provenienti da scambio internazionale che hanno concluso il periodo di studio presso l'Università.

Categoria utente	Accesso all'Identity Provider (IdP)	Cardinalità
Studenti cessati con titolo	Sì	130000
Studenti incoming cessati	Sì	8000

Affiliate

Studenti preiscritti – Studenti la cui iscrizione non è ancora perfezionata.
Referenti gestionali esterni – Referenti di organizzazioni esterne per l'attivazione e la gestione di convenzioni tra le stesse organizzazioni e l'Università.
Accreditati esterni – ospiti a vario titolo dell'ateneo, svolgono la loro attività prevalentemente all'esterno delle strutture dell'Università.
Ospiti per convegni – ospiti temporanei, accreditati solo per la durata dei convegni ospitati dalle strutture dell'ateneo.
Altri dipendenti cessati – dipendenti a vario titolo (escluso il *Personale docente*) il cui rapporto di lavoro è terminato, ai quali non sono ancora state eliminate le credenziali.

Categoria utente	Accesso all'Identity Provider (IdP)	Cardinalità
Studenti preiscritti	No – verso i servizi esposti dalla Federazione	140000
Referenti gestionali esterni	No – verso i servizi esposti dalla Federazione	6000
Accreditati esterni	No – verso i servizi esposti dalla Federazione	350
Ospiti per convegni	No – verso i servizi esposti dalla Federazione	N/A
Personale docente cessato	Sì	800
Altri dipendenti cessati	Sì	900

Le categorie di utenti sopra descritte per le quali è stato indicato *"No – verso i servizi esposti dalla Federazione"*, potrebbero avere accesso all'identity provider solo per servizi interni all'Università ma non per servizi esterni federati.

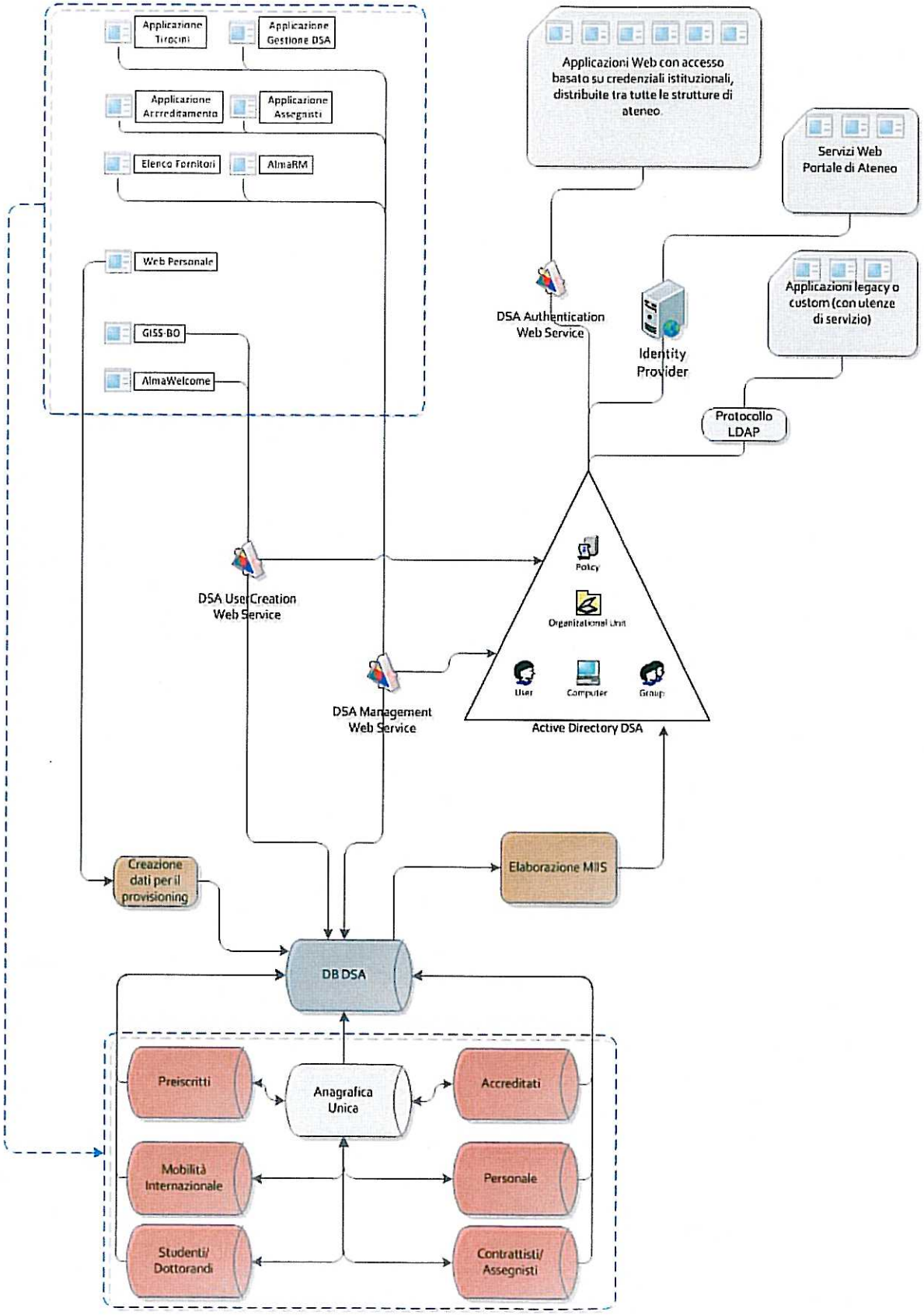
B2B / Servizi

Le utenze associate ai servizi sono gestite in modo autonomo dalle strutture che ne hanno necessità. Le credenziali possono essere create in una Organizational Unit assegnata alla struttura attraverso operazioni manuali (agendo direttamente sugli oggetti della directory). Per ogni struttura che ne fa richiesta è creata la OU e sono identificati degli amministratori responsabili della gestione delle identità di servizio.
Allo stesso modo sono gestite le credenziali di alcuni utenti, privilegiati dal punto di vista della directory (Enterprise Admins e Domain Admins), che di norma hanno un'utenza separata da quella personale per le operazioni di amministrazione.

Mappatura degli utenti sulle affiliazioni IDEM

Ruolo	EduPersonScopedAffiliation
Personale docente	staff, member
Ricercatore dell'Alma Mater	staff, member
Professore dell'Alma Mater	staff, member
Docenti a contratto	staff, member
Personale tecnico-amministrativo	staff, member
Personale TA abilitato CONSIP	N/A
Registration Authorization Officer	N/A
Personale TA abilitato PEC	N/A
Contrattisti	staff, member
Accreditati interni	staff, member
Personale docente cessato	affiliate, member
Altri dipendenti cessati	affiliate, member
Dottorandi	student, staff, member
Studenti incoming attivi	student, member
Medici in formazione specialistica	student, staff, member
Laureati frequentatori	student, member
Studenti attivi	student, member
Studenti non attivi	student, member
Studenti cessati con titolo	alumn, member
Studenti incoming cessati	alumn, member

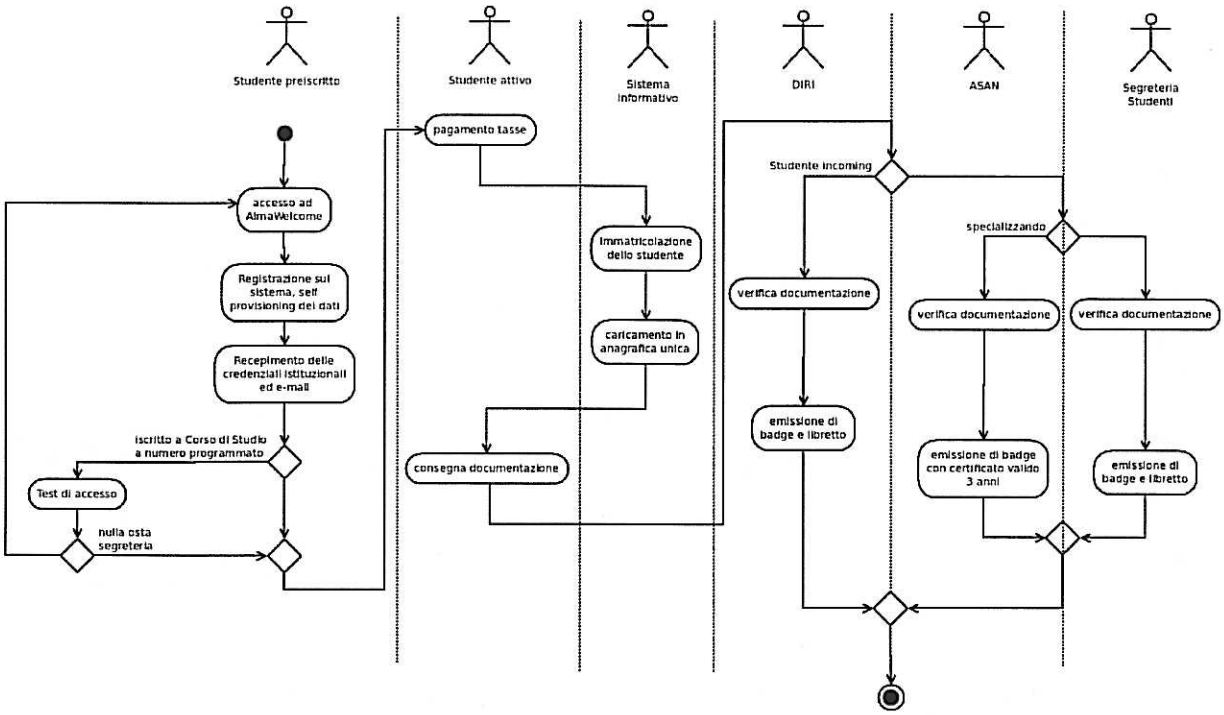
Visione di insieme del processo di accreditamento degli utenti



Il diagramma presenta tutti gli elementi coinvolti nella creazione e uso delle credenziali istituzionali. Le applicazioni riportate in alto a sinistra rappresentano gli strumenti gestionali a disposizione delle strutture per la creazione e la modifica dei dati legate alle identità digitali degli utenti.
Le modifiche apportate e i nuovi inserimenti sono accolti dai diversi DB centralizzati, raccordati attraverso il DB dell'Anagrafica Unica. La creazione delle credenziali avviene solamente tramite web service (DSA User Creation oppure DSA Management) o con la preparazione dei dati delle utenze, create successivamente in un'unica soluzione.
Per il processo di creazione delle credenziali è necessario un DB di appoggio (DB DSA) che ha il compito di raccogliere e normalizzare i dati. A partire da queste informazioni le elaborazioni giornaliere di MIIS (Microsoft Identity Information Server) aggiornano e integrano le informazioni contenute in Active Directory (che sono aggiornate anche tramite i web service di cui sopra per garantire la sincronia nella creazione degli utenti).
I dati della directory sono utilizzati da tutte le applicazioni web dell'ateneo che forniscano accesso tramite credenziali istituzionali. Ogni applicazione deve utilizzare il web service DSA Authentication, il cui accesso è registrato e profilato per ogni struttura richiedente avente diritto.
Per alcuni servizi legacy l'autenticazione è ancora basata sullo scambio di informazioni via protocollo LDAP, mentre per i servizi più recenti è disponibile l'identity provider con il supporto per il Single Sign-On.

Il processo di accreditamento per la categoria di utenti "Studenti"

Il processo



Modalità di riconoscimento della persona

Lo *studente attivo* al momento della consegna dei documenti è identificato dalla segreteria di riferimento tramite accertamento di documento d'identità, di cui vengono registrati gli estremi.

Caratteristiche dell'identità digitale

Attributi associati alla categoria Studente (o Studente incoming)

- Nome (pubblico)
- Cognome (pubblico)
- UPN (pubblico)
- Indirizzo email (pubblico)
- Matricola (pubblico)
- Luogo di nascita (non pubblico)
- Codice Fiscale (non pubblico)
- Sesso (non pubblico)

- Data di nascita (non pubblico)
- Indirizzo (non pubblico)
- Indirizzo e-mail secondario (non pubblico)
- PUK (non pubblico)
- Domanda personalizzata per reset password (non pubblico)
- Risposta alla domanda per reset password (non pubblico)

Gestione del ciclo di vita

Le modifiche alla carriera dello studente sono gestite tramite lo strumento gestionale GISS-BO, in dotazione alle Segreterie Studenti. Ogni modifica al profilo dello studente è immesso nei database centralizzati e recepito dalla directory.
Lo studente ha la possibilità di modificare autonomamente i dati anagrafici tramite l'uso di AlmaWelcome.

Formato e regole delle credenziali

Le credenziali fornite agli studenti sono composte da un nome utente, formato in genere utilizzando il nome e cognome della persona, a cui è associato un codice alfanumerico (PUK) generato casualmente in modo automatico. Al primo accesso l'utente è obbligato a cambiare la password e impostare una domanda e una risposta personalizzate da usare per un eventuale recupero di credenziali smarrite.
La password deve rispettare queste regole:

- avere una lunghezza compresa tra 6 e 16 caratteri;
- utilizzare i seguenti tipi di caratteri: lettere maiuscole, lettere minuscole, cifre, questi caratteri speciali (` ~ ! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /);
- non deve contenere né il nome, né il cognome;
- non deve contenere spazi.

I *medici in formazione specialistica* ricevono inoltre smartcard con certificato di sottoscrizione (per la firma digitale) a cui è associato un PIN, da utilizzare per la firma del contratto di lavoro.
La smartcard è emessa dal *Registration Authorization Officer* dell'Ufficio Scuole di Specializzazione Mediche (ASAN), in seguito all'identificazione del medico.

Eventuale presenza di credenziali multiple per la stessa persona

I *medici in formazione specialistica* ricevono oltre al nome utente e password anche un certificato digitale per la firma del contratto specifico della categoria.

Possono esistere identità digitali duplicate per credenziali molto vecchie legate a precedenti gestioni in cui non era ancora stata introdotta l'Anagrafica Unica, oppure in seguito a errori operativi. Quando si individuano queste situazioni individuate le identità in eccesso vengono eliminate.

Modalità di consegna delle credenziali

Le credenziali sono assegnate dal sistema di iscrizione (AlmaWelcome) al momento del pagamento. Fintanto che lo *studente preiscritto* non ha consegnato i documenti per l'iscrizione e la Segreteria Studenti non ha accertato l'identità, le credenziali consentono solamente l'accesso ad AlmaWelcome e alla posta elettronica studenti, per consentire il ricevimento di comunicazioni.
Una volta accertata l'identità dello studente, le credenziali acquistano piena capacità di autorizzazione.

In casi eccezionali è la Segreteria Studenti o l'HelpDesk di AlmaWelcome a consegnare le credenziali.

Modalità di recupero delle credenziali smarrite

Le credenziali smarrite sono recuperabili tramite l'uso dei servizi web AlmaWelcome e sito DSA. Tramite essi è possibile rispondere alla domanda personalizzata impostata al momento dell'iscrizione, riportando così la password al codice alfanumerico originariamente impostato dal sistema (PUK), consentendo la successiva modifica da parte dello studente (obbligatoria).
Lo studente può anche rivolgersi all'HelpDesk di AlmaWelcome che ha la possibilità di resettare la password al PUK iniziale.
Nel caso sia stato smarrito il PUK, lo studente può rivolgersi alla Segreteria di riferimento o all'HelpDesk di AlmaWelcome.

Modalità di gestione smarrimento smartcard/token

In caso di smarrimento della smartcard il *medico in formazione specialistica* deve consegnare una dichiarazione di smarrimento all'Ufficio Scuole di Specializzazione Mediche (ASAN), il *RAO* operante presso lo sportello effettua la revoca del certificato associato all'utente e l'emissione di un nuovo badge con certificato associato.

Durata dell'accreditamento

Le credenziali per studenti non hanno scadenza.

Il certificato usato dai *medici in formazione specialistica* è valido per 3 anni (durata prevista dei certificati di sottoscrizione InfoCert).

Disabilitazione utente

Lo studente che non è più iscritto a un corso di studi, sia per la naturale conclusione del percorso formativo sia per un'eventuale interruzione degli studi, assume lo stato di *studente cessato*.
L'attribuzione dello stato avviene in contemporanea al cambio di condizione.
L'utenza e le credenziali tuttavia non sono disabilitate, anche se sono soggette a revoche di autorizzazioni (es. eliminato accesso a portale studenti e alla rete wireless di ateneo).

Nel caso dei *medici in formazione specialistica*, pur non essendovi revoca dell'utenza e delle credenziali, la smartcard col certificato viene ritirata e revocata dal RAO subito dopo la firma sul contratto dell'ultimo anno di specializzazione.

Cancellazione definitiva utente

Gli utenti della categoria studenti non sono soggetti a cancellazione definitiva, salvo il caso di individuazione di identità duplicate.

Rischi specifici associati alla categoria di utenti

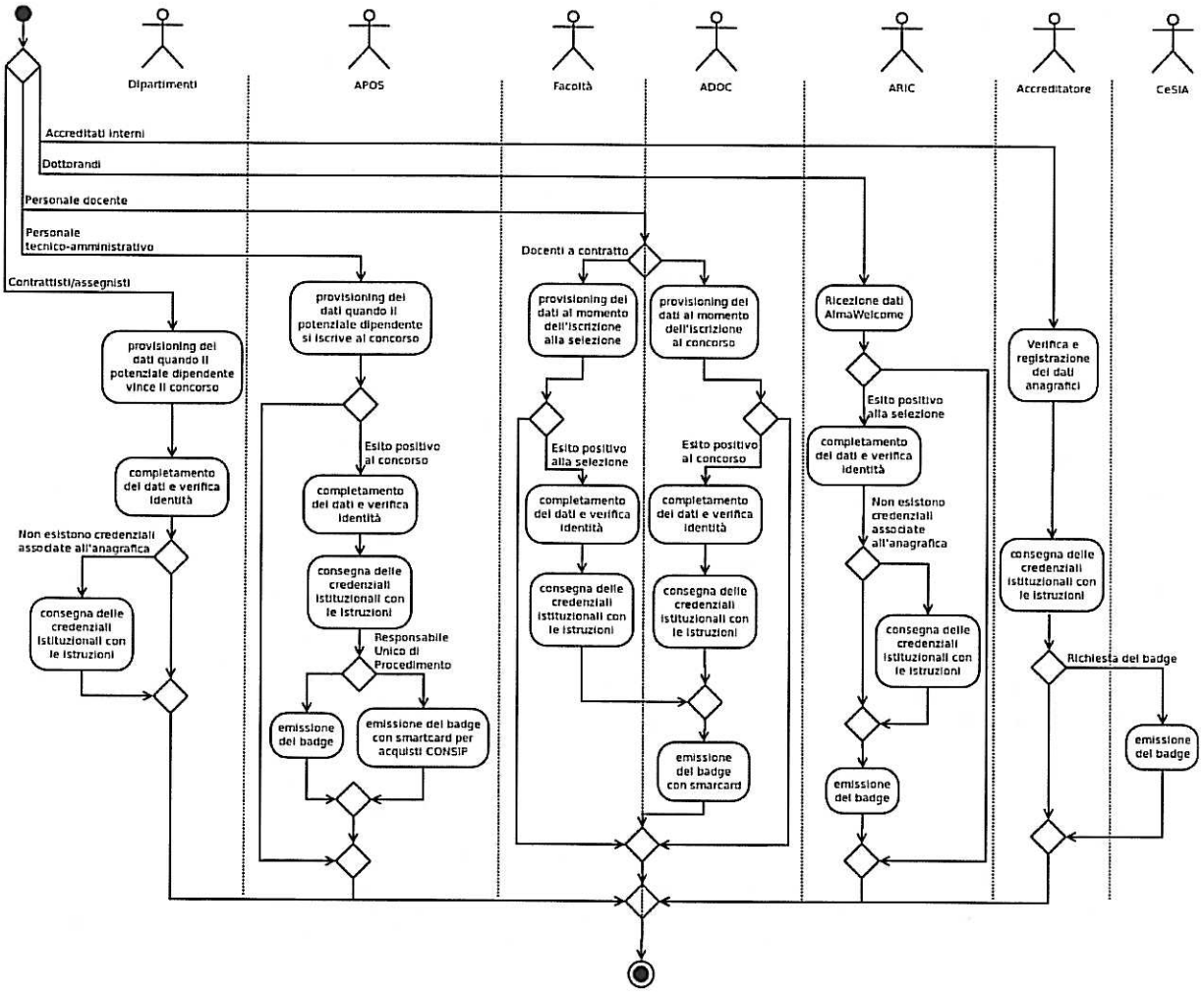
Non si registrano rischi specifici legati alla categoria.

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

La categoria non ha accesso a servizi che coinvolgano contemporaneamente credenziali deboli e credenziali forti.

Il processo di accreditamento per la categoria di utenti "Dipendenti"

Il processo



Modalità di riconoscimento della persona

Il dipendente è soggetto alla verifica dell'identità al momento del perfezionamento della posizione, solo in seguito alla verifica sono consegnate le credenziali. Fa eccezione la categoria *dottorandi* la cui gestione ha punti in comune sia con studenti che con dipendenti.

I *dottorandi* sono soggetti alla preiscrizione tramite AlmaWelcome, così come gli studenti. Quando la posizione è perfezionata vengono create dal sistema nuove credenziali della categoria dipendenti.

Gli *accreditati interni* sono collaboratori a vario titolo dell'ateneo (es. consulenti) che svolgono le proprie attività prevalentemente presso l'Università. La verifica e la registrazione delle credenziali

avvengono da parte di un dipendente con l'autorizzazione di accreditatore. Qualsiasi dipendente che faccia richiesta al CeSIA e dichiari di aver preso visione delle linee guida del servizio può diventare accreditatore.

Caratteristiche dell'identità digitale

Attributi associati alla categoria Dipendente

- Nome (pubblico)
- Cognome (pubblico)
- UPN (pubblico)
- Indirizzo email (pubblico)
- Matricola (pubblico)
- Ruolo (pubblico)
- Telefono (pubblico)
- Luogo di nascita (non pubblico)
- Codice Fiscale (non pubblico)
- Sesso (non pubblico)
- Data di nascita (non pubblico)
- Indirizzo (non pubblico)
- Indirizzo e-mail secondario (non pubblico)
- PUK (non pubblico)
- Domanda personalizzata per reset password (non pubblico)
- Risposta alla domanda per reset password (non pubblico)

Gestione del ciclo di vita

Le modifiche alla carriera del dipendente sono gestite tramite gli strumenti gestionali specifici (*Web Personale, applicazione gestione Assegnisti*) per i singoli ruoli , in dotazione ad APOS, ADOC e Dipartimenti. Ogni modifica al profilo del dipendente è immesso nei database centralizzati e recepito dalla directory.
I recapiti principali del dipendente (sede di servizio, residenza e domicilio) vengono modificati tramite l'applicazione di gestione del personale dalle aree amministrative competenti (APOS, ADOC).
Alcuni dei recapiti del dipendente (numeri telefono, indirizzi e-mail) possono essere modificati in modo autonomo tramite il sito DSA.

Nel caso dei *dottorandi* le modifiche avvengono tramite lo strumento gestionale GISS-BO da ARIC, gli aggiornamenti sono poi recepiti dalla directory.

Nel caso degli *accreditati interni* le poche modifiche previste al profilo sono effettuabili dall'accreditatore tramite l'applicativo web per l'accreditamento.

Formato e regole delle credenziali

Le credenziali fornite ai dipendenti (e *accreditati interni*) sono composte da un nome utente ed un codice alfanumerico (PUK) generato casualmente in modo automatico. Al primo accesso l'utente è obbligato a cambiare la password e impostare una domanda e una risposta personalizzate da usare per un eventuale recupero di credenziali smarrite.
La password deve rispettare queste regole:

- deve essere cambiata ogni 6 mesi (ogni 3 mesi se attraverso le credenziali vengono trattati dati sensibili o giudiziari) ed essere diversa da quella attualmente in uso;
- avere almeno 8 caratteri;
- comprendere almeno due tra i seguenti tipi di caratteri: lettere maiuscole, lettere minuscole, numeri, caratteri speciali;
- non deve contenere né il nome, né il cognome, né la data di nascita.

Il *personale docente* e i *docenti a contratto* ricevono inoltre una smartcard con certificato di sottoscrizione (per la firma digitale) a cui è associato un PIN, da utilizzare per la firma dei verbali di esame e dei registri delle lezioni. Il certificato è emesso dai *RAO* di ADOC e del CeSIA.
Al termine del rapporto di collaborazione con l'ateneo la smartcard dev'essere consegnata alla struttura di riferimento dove il certificato viene revocato dal *RAO*.

Gli appartenenti al sottoinsieme *Personale TA abilitato CONSIP* ricevono una smartcard con certificato di sottoscrizione (per la firma digitale) a cui è associato un PIN, da utilizzare per effettuare acquisti sul mercato elettronico. Dopo aver ricevuto la richiesta di abilitazione dal personale TA interessato, l'Area dei Contratti e degli Appalti verifica la documentazione comprovante e segnala la delega di responsabilità ad APOS, che provvede a emettere la smartcard con certificato valido 3 anni (validità standard dei certificati InfoCert) per gli acquisti sul mercato elettronico.

Gli appartenenti al sottoinsieme *Personale TA abilitato PEC* ricevono inoltre una smartcard con certificato di autenticazione a cui è associato un PIN, per l'accesso alla posta elettronica certificata per una struttura. Il certificato ha validità 3 anni (durata standard dei certificati InfoCert)..
L'emissione della smartcard è affidata ai *RAO* operanti presso il CeSIA.

Gli appartenenti alla categoria *Registration Authorization Officer* sono soggetti a formazione InfoCert e alla verifica delle nozioni necessarie a garantire la corretta gestione dei certificati. In seguito alla formazione sono dotati di smartcard InfoCert che permette di emettere e revocare certificati digitali.

Tutti i rinnovi di certificato al momento sono gestiti direttamente dai *RAO*.

Eventuale presenza di credenziali multiple per la stessa persona

In seguito a errori operativi o per situazioni precedenti alla creazione dell'Anagrafica Unica, si possono avere casi di duplicazione delle credenziali. Al verificarsi della condizione viene operata una fusione delle identità digitali, conservando i dati maggiormente aggiornati o significativi.

Modalità di consegna delle credenziali

Le credenziali sono stampate con un procedimento automatico dalle strutture di riferimento allo specifico ruolo (APOS, ARIC, ADOC, accreditatore) e consegnate in busta chiusa assieme alle istruzioni per la corretta gestione dell'identità digitale.
Le credenziali degli *accreditati interni* possono essere inviate all'interessato anche tramite email dal sistema di accreditamento.
La consegna avviene successivamente alla verifica dell'identità della persona.

Al momento della consegna delle credenziali viene emesso il certificato digitale per le categorie che ne hanno necessità. Oltre alla smartcard l'utente riceve una busta cieca contenente il PUK ed il PIN associati, le operazioni di cambio PIN e reset al PUK si effettuano con l'uso dell'applicazione multipiattaforma fornita da InfoCert.

Modalità di recupero delle credenziali smarrite

Le credenziali smarrite sono recuperabili attraverso il sito DSA. Tramite esso è possibile rispondere alla domanda personalizzata impostata al momento dell'attivazione delle credenziali, riportando così la password a quella originariamente impostata dal sistema (PUK), consentendo la successiva modifica da parte del dipendente.

Modalità di gestione smarrimento smartcard/token

In caso di smarrimento del badge con certificato digitale il dipendente deve presentare dichiarazione di smarrimento alla struttura di riferimento. Il vecchio certificato viene quindi revocato ed emesso un sostituto.

Durata dell'accreditamento

Le credenziali degli *accreditati interni* sono valide 1 anno, eventualmente prorogabili un anno alla volta da un accreditatore. Per le altre categorie la validità è pari alla durata del rapporto di collaborazione.

Ricercatori e Professori che decidano di andare in pensione prima del limite massimo, hanno la facoltà di richiedere la qualifica di *Ricercatore dell'Alma Mater* e *Professore dell'Alma Mater*. La qualifica permette ai docenti a cui viene riconosciuta di continuare a utilizzare i sistemi informativi dell'Università fino al raggiungimento del limite massimo di età pensionabile.

Disabilitazione utente

Il personale docente che non ha più in essere un rapporto di collaborazione con l'ateneo assume lo stato di *personale docente cessato*, i dipendenti non docenti al verificarsi delle stesse condizioni assumono lo stato di *altri dipendenti cessati*. L'attribuzione dello stato avviene in contemporanea al cambio di condizione.

L'utenza e le credenziali sono soggette a disabilitazione a seconda della specifica categoria:

- *personale docente*: al momento non è prevista la disabilitazione delle credenziali;
- *personale tecnico-amministrativo*: dopo un mese dalla conclusione del rapporto di lavoro le credenziali vengono disabilitate;
- *registration authorization officer*: fatte salve le regole del *personale tecnico-amministrativo*, devono consegnare al CeSIA la smartcard (il cui certificato viene revocato) al momento della conclusione del rapporto;
- *personale TA abilitato CONSIP*: fatte salve le regole del *personale tecnico-amministrativo*, devono consegnare ad APOS la smartcard (il cui certificato sarà revocato) al momento della conclusione del rapporto;
- *contrattisti*: dopo un mese dalla scadenza del contratto le credenziali vengono disabilitate (il meccanismo non è ancora in essere);
- *dottorandi*: dopo 6 mesi dalla scadenza del dottorato le credenziali vengono disabilitate (il meccanismo non è ancora in essere);
- *accreditati interni*: allo scadere di ogni mese viene inviata comunicazione agli accreditatori con accreditati in scadenza e agli accreditati scaduti da meno di un mese, della necessità del rinnovo nel caso le credenziali siano ancora necessarie. Dopo un mese da questa. comunicazione le credenziali vengono disabilitate nel caso non sia stato prodotto un rinnovo
-

Cancellazione definitiva utente

Gli utenti della categoria non sono soggetti a cancellazione definitiva, salvo il fatto che venga identificata un'utenza duplicata.

Rischi specifici associati alla categoria di utenti

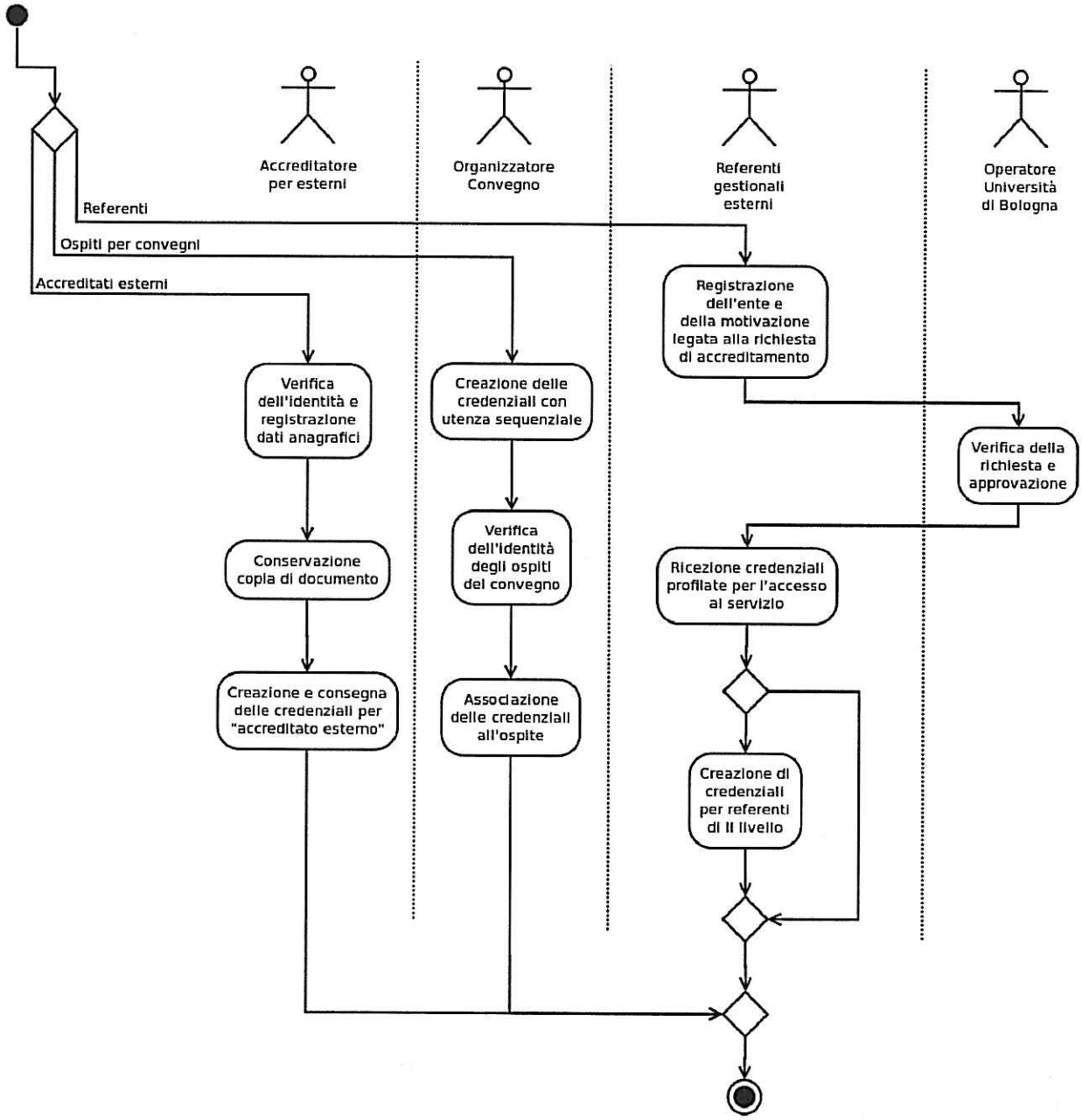
Il *personale tecnico-amministrativo* che occupa un ruolo dove è necessario gestire dati sensibili rappresenta una categoria le cui credenziali sono particolarmente delicate.

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

L'unico caso di interazione tra credenziali deboli e forti si verifica per la categoria docenti. Il servizio per la registrazione elettronica degli esami (AlmaEsami) richiede infatti l'accesso tramite credenziali, mentre la firma dei verbali avviene con certificato digitale.

Il processo di accreditamento per la categoria di utenti "Esterni"

Il processo



Modalità di riconoscimento della persona

L'*accreditato esterno* è soggetto alla verifica dell'identità da parte dell'accreditatore, quest'ultimo si occupa anche di registrare i dati anagrafici e conservare copia del documento di identità. La verifica avviene al momento della creazione delle credenziali, consegnate direttamente dall'accreditatore in busta chiusa o tramite l'applicativo di accreditamento.

Gli *ospiti per convegni* sono una categoria nata dall'esigenza di offrire il servizio di connessione wireless a utenze effimere. Per questa categoria gli organizzatori dei convegni sono incaricati di verificare l'identità degli ospiti, utilizzare un applicativo web per la creazione dell'insieme di utenti necessario (con utenza anonima sequenziale) e registrare la corrispondenza tra l'identità e l'utenza creata dal sistema automatico e assegnata al momento del riconoscimento.

I *referenti gestionali esterni* sono identificati attraverso i dati anagrafici e il codice fiscale che l'utente immette al momento della registrazione della propria organizzazione. Al termine di questo passo il *referente gestionale esterno* riceve le credenziali, le autorizzazioni consentono però di accedere al solo servizio di registrazione in modo da controllare lo stato di avanzamento della pratica. Una volta effettuata la registrazione dell'organizzazione un operatore dell'Università (l'attore esatto dipende dal tipo di convenzione) verifica la richiesta e procede all'approvazione. Necessaria alla conclusione dell'iter è la firma del rappresentante legale dell'organizzazione esterna. In seguito all'approvazione l'utente può usare le credenziali per accedere ai soli servizi per cui è stata approvata la convenzione.

Caratteristiche dell'identità digitale

Attributi associati alla categoria Esterni

- Nome (pubblico)
- Cognome (pubblico)
- UPN (pubblico)
- Luogo di nascita (non pubblico)
- Codice Fiscale (non pubblico)
- Sesso (non pubblico)
- Data di nascita (non pubblico)
- Indirizzo (non pubblico)
- Indirizzo e-mail secondario (non pubblico)
- PUK (non pubblico)
- Domanda personalizzata per reset password (non pubblico)
- Risposta alla domanda per reset password (non pubblico)

Gestione del ciclo di vita

Le modifiche ai profili dei *referenti gestionali esterni* sono gestite tramite meccanismi interni agli applicativi web che li coinvolgono. Ogni modifica al profilo dell'esterno è immesso nei database centralizzati e recepito dalla directory.

Nel caso degli *ospiti per convegni* non sono previste modifiche all'utenza vista la velocità con cui vengono disabilitate le credenziali.

Nel caso degli *accreditati esterni* le poche modifiche previste al profilo sono effettuabili dall'accreditatore tramite l'applicativo web per l'accreditamento.

Formato e regole delle credenziali

Il formato e le regole a cui sono soggette le credenziali di questa categoria sono le stesse della categoria Dipendenti.

Solo per gli o*spiti per convegni* l'utenza ha la particolare forma data dal nome del convegno e numero progressivo.

Eventuale presenza di credenziali multiple per la stessa persona

Escludendo il caso degli *ospiti per convegni*, la mutevolezza delle collaborazioni può portare a casi di duplicazione delle credenziali, al verificarsi della condizione è operata una fusione delle identità digitali, conservando i dati maggiormente aggiornati o significativi.

Modalità di consegna delle credenziali

Le credenziali degli *ospiti per convegni* sono consegnate dagli organizzatori in busta chiusa in seguito alla verifica dell'identità e all'assegnazione dell'utenza.
Per gli *accreditati esterni* la consegna può avvenire sia in modalità diretta in busta chiusa da parte dell'accreditatore, sia via email sfruttando l'applicativo per l'accreditamento.
I *referenti gestionali esterni* ricevono le credenziali via email oppure attraverso un documento riassuntivo in formato PDF al momento della registrazione.

Modalità di recupero delle credenziali smarrite

Eccezion fatta per gli *ospiti per convegni*, le credenziali smarrite sono recuperabili tramite l'uso dei servizi AlmaWelcome e sito DSA. Tramite essi è possibile rispondere alla domanda personalizzata impostata al momento dell'iscrizione, riportando così la password a quella originariamente impostata dal sistema (PUK), consentendo la successiva modifica da parte dell'utente.

Modalità di gestione smarrimento smartcard/token

Per la categoria non è previsto l'utilizzo di smartcard.

Durata dell'accreditamento

Le credenziali degli *accreditati esterni* sono valide per un periodo massimo di 1 anno, durata minore è definibile al momento dell'accreditamento o del rinnovo.

Un accreditatore ha la possibilità di rinnovare le credenziali ripetutamente per un periodo di tempo sempre di durata massima di un anno.

Gli *ospiti per convegni* hanno credenziali la cui durata è estremamente ristretta (pari a qualche giorno), limitata alla durata del convegno a cui partecipano.
Le credenziali dei *referenti gestionali esterni* non hanno al momento una scadenza assegnata in quanto il rapporto con gli enti convenzionati è di natura sporadica ma ripetuta in un arco temporale molto dilatato.

Disabilitazione utente

L'utenza e le credenziali sono soggette a disabilitazione a seconda della specifica categoria:

- *ospiti per convegni*: non sono soggette a disabilitazione ma sono direttamente eliminate;
- *accreditati esterni*: allo scadere di ogni mese viene inviata comunicazione agli accredita tori con accreditati in scadenza e agli accreditati scaduti da meno di un mese della necessità del rinnovo nel caso le credenziali siano ancora necessarie. Dopo un mese da questa comunicazione le credenziali vengono disabilitate nel caso non sia stato prodotto un rinnovo;
- *referenti gestionali esterni*: allo stato attuale non vengono disabilitati.

Cancellazione definitiva utente

Solo la categoria *ospiti per convegni* è soggetta a cancellazione definitiva. L'effettiva cancellazione avviene successivamente al termine del convegno (la durata viene definita al momento della creazione delle credenziali).

Rischi specifici associati alla categoria di utenti

Non si registrano rischi specifici legati alla categoria.

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

Per la categoria non è previsto l'utilizzo di credenziali forti.

Il sistema di autenticazione e autorizzazione interno

Il sistema di autenticazione e autorizzazione descritto è utilizzato per tutte le applicazioni interne all'organizzazione.

Nel contesto dell'accesso ai servizi federati gli identificatori eduPersonPrincipalName ed eduPersonTargetedID sono univoci una volta assegnati.

L'identity provider è stato progettato ricercando la separazione dei servizi e la continuità del servizio. Il sistema è costituito da un componente pubblico (Federation Proxy) e uno protetto (Federation Server), adibiti rispettivamente all'autenticazione degli utenti e alla comunicazione con DSA per la generazione degli attributi degli utenti.
La sessione autenticata ha una durata di 8 ore, all'interno dell'intervallo l'utente può accedere in modo trasparente ai servizi che supportano il Single Sign-On. Da ognuno dei servizi è possibile attivare la procedura di uscita (Single Logout) che causa la fine della sessione autenticata per ogni servizio a cui l'utente ha acceduto.

Partecipazione ad altre federazioni

L'Università di Bologna non partecipa per il momento ad altre federazioni. È intenzione dell'Università di Bologna partecipare al sistema fedERa, la federazione degli enti locali della Regione Emilia-Romagna.