Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione

Le informazioni fornite in questo documento sono accurate alla data del 06/05/2010.

Il presente documento, denominato DOPAU, aggiornato alla data del 05-06-2010, in versione 1.0 è sottofirmato dal referente organizzativo dott. Andrea Mongera

Revisioni

Data	Versione	Descrizione modifica	Autore
06/05/2010	0.5	Redazione iniziale	Maurizio Festi

Nota introduttiva

La partecipazione alla Federazione IDEM ("Federazione") abilita l'organizzazione partecipante ("Partecipante") ad utilizzare la tecnologia di Shibboleth di condivisione degli attributi relativi alle identità per gestire l'accesso alle risorse on-line che possono essere rese disponibili all'interno della comunità IDEM. Un obiettivo della Federazione è quello di sviluppare, nel tempo, degli standard per le organizzazioni al fine di assicurare che le asserzioni sugli attributi che vengono scambiate siano sufficientemente robuste e fidate per gestire l'accesso ad importanti risorse protette. Con la crescita della fiducia interna, la Federazione spera che i Partecipanti alla fine possano fidarsi dei sistemi di identity management e dei sistemi di gestione di accesso alle risorse degli altri partecipanti come si fidano dei propri.

Fondamentalmente ci si aspetta dai Partecipanti che essi forniscano agli altri Partecipanti asserzioni sugli attributi autorevoli e accurate e che ciascuno riceva asserzioni sugli attributi protette e nel rispetto dei vincoli di privacy imposti dalla Federazione o dalla fonte delle informazioni. Per raggiungere tale obiettivo IDEM richiede che ogni Partecipante renda disponibile agli altri Partecipanti certe informazioni di base riguardanti il proprio sistema di identity management, incluse le informazioni relative agli attributi che vengono utilizzati per la Federazione.

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono: (1) che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione e che (2) il sistema che emette le credenziali per gli utenti finali (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) sia dotato di appropriate misure di gestione del rischio (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.)

Il Documento DOPAU prodotto dal Partecipante DEVE contenere le informazioni elencate nel presente modello.

In caso di modifica delle procedure o informazioni descritte nel documento, esso DEVE essere prontamente aggiornato e ne deve essere data comunicazione alla Federazione.

Abbreviazioni

Abbrev.	Descrizione
ADA	Anagrafica di Ateneo
DSISTI	Direzione Sistemi Informativi Servizi e Tecnologie Informatiche
PTA	Personale Tecnico Amministrativo
PDR	Personale Docente e Ricercatore
SIRIUM	Modulo SAP-HR adattato alla gestione dello stato giuridico di PTA, PDR e alla gestione dei contratti della didattica.
ESSE3	Sistema informativo per la gestione della didattica e della carriera degli studenti
ADELINE	Applicazione SAP per la gestione dei contratti di lavoro occasionali o continuativi
IDP	Identity provider Shibboleth
SP	Service provider Shibboleth

Glossario

Termine	Significato
Dati identificativi minimi	Insieme di attributi che identifica univocamente una persona: nome,cognome,data di nascita, nazione di nascita, luogo di nascita, sesso
Identità digitale	Rappresentazione digitale di una persona, identificata univocamente da un ID_ADA e di dati identificativi minimi ad esso associati
Account di Ateneo	Coppia username/password associata ad una identità digitale di una persona che permette di autenticarsi per accedere ai servizi informatici di Ateneo
RUP-ruolo persona	Classificazione dei ruoli delle persone in Ateneo, intesi come indicazione di "che cosa una persona fa"
PPE-posizione personale	Associazione tra un'identità digitale di una persona, un RUP-ruolo persona, ed un periodo di validità: indica che cosa una determinata persona fa in Ateneo e per quanto tempo
RUO-ruolo organizzativo	Classificazione del ruolo di una persona in un unità organizzativa, es: responsabile, afferente.
POR-posizione organizzativa/istituzionale	Relazione tra una PPE-posizione personale ed un ruolo organizzativo all'interno di un'unità organizzativa
Sistema di Business	Sistema informatico, normalmente di tipo ERP, che supporta le attività di business specifiche di un'area dell'Ateneo.

Gestore dell'accreditamento

La gestione delle Identità Digitati dell'Ateneo è in carico alla Direzione Sistemi Informativi Servizi e Tecnologie Informatiche [DSISTI].
La direzione DSISTI gestisce le informazioni relative alle Identità di Ateneo e coordina i processi di accreditamento e di rilascio delle credenziali di ateneo (Account di Ateneo), alcuni dei quali sono in carico a strutture delle altre direzioni di Ateneo.
Tutte le identità sono tracciate attraverso il sistema Anagrafica Di Ateneo [ADA] che:

- garantisce un'unica identità per ogni persona;
- associa le credenziali (Account di Ateneo) all'identità della persona che le possiede;
- integra le informazioni relative alle persone presenti nelle varie applicazioni dell'Ateneo, sintetizzando quelle ritenute rilevanti alla gestione delle Identità e degli Account di Ateneo;
- traccia la durata del rapporto tra persona e Ateneo;
- caratterizza gli Account di Ateneo associando gli opportuni attributi e ruoli corrispondenti all'attività della persona in Ateneo.

Il responsabile della base dati di ADA è il dirigente della DSISTI.

Utenti gestiti con mappatura sulle affiliazioni IDEM

La ***Tabella 1: Elenco dei ruoli degli utenti gestiti con affiliazione IDEM*** elenca i ruoli associati agli utenti gestiti in UNITN con la relativa affiliazione IDEM.
E'previsto che ogni persona, di conseguenza ogni Account di Ateneo, possa avere più di un ruolo valido contemporaneamente.
La durata di un Account di Ateneo assegnato ad una persona è in relazione alla durata del o dei ruoli ad essa associati. In linea generale, un Account di Ateneo viene disattivato qualche tempo dopo la cessazione dell'ultimo ruolo associato alla persona.
Il periodo di estensione della validità di un Account di Ateneo oltre la data di fine del ruolo è specifica del ruolo stesso, va da pochi giorni, a qualche mese.

ID del ruolo	Descrizione del ruolo	Affiliazione IDEM	Significato del ruolo	Fonte del ruolo	Gestito in ADA
FACREG001	Professore straordinario	member;staff	Professore con qualifica straordinario	SIRIUM	VERO
FACREG002	Professore ordinario	member;staff	Professore con qualifica ordinario	SIRIUM	VERO
FACREG003	Professore associato	member;staff	Professore con qualifica di associato	SIRIUM	VERO
FACREG004	Ricercatore	member;staff	Ricercatore	SIRIUM	VERO
FACREG005	Collaboratore linguistico	member;staff	Personale che svolge mansioni di collaboratore linguistico	SIRIUM	VERO
FACADD001	Docente a contratto	member;staff	Professore esterno titolare di corso in UNITN in virtù della firma di un contratto	SIRIUM	VERO
FACADD003	Professore da altra universita	member	Docente proveniente da altra Università (supplenza in didattica o in ricerca)	SIRIUM	VERO
FACADD004	Esercitatore	member;staff	Persona che svolge attività di esercitatore a contratto	SIRIUM	VERO

ID del ruolo	Descrizione del ruolo	Affiliazione IDEM	Significato del ruolo	Fonte del ruolo	Gestito in ADA
FACADD005	Collaboratore di ricerca	member,staff	Collaboratore di ricerca (co.co.co/pro ricerca)	GESTIONE CONTRATTI (ADELINE)	VERO
FACADD006	Collaboratore di ricerca post doc	member,staff	Collaboratore di ricerca titolare di assegno di ricerca post doc	GESTIONE CONTRATTI (ADELINE)	VERO
FACADD007	Titolare di borsa in ambito ricerca	member	Studente che svolge attività di ricerca a seguito dell'ottenimento di una borsa di ricerca	SEGRETERIE DI DIPARTIMENTO	VERO
FACADD008	Stagista della ricerca	affiliate	Studente UNITN che svolge uno stage obbligatorio all'interno dell'Università	SEGRETERIE DI DIPARTIMENTO	VERO
FACADD009	Tutor	member,staff	contrattista per tutoraggio (supporto didattica)	SIRIUM	VERO
FACADD010	Visiting professor	member,staff	Professore molto qualificato (fama internazionale, marie curie, ecc.) RECLUTATO in ambito DIDATTICA con contratto pagato da un ente esterno (Endowed) (es. borsa marie curie, FSE, San Michele, Irst, ecc.)	SIRIUM	VERO
FACADD011	Collaboratore linguistico a contratto	member,staff	Personale che svolge mansioni di collaboratore linguistico a contratto	SIRIUM	VERO
FACADD012	Visiting research professor	member,staff	Professore molto qualificato (fama internazionale, marie curie, ecc.) RECLUTATO in ambito RICERCA (dipartimenti) con contratto pagato da un ente esterno (Endowed) (es. borsa marie curie, FSE, San Michele, Irst, ecc.)	SEGRETERIE DI DIPARTIMENTO	VERO
FACLOC001	Docente	member,staff	Docente che arriva in ADA in prima battuta direttamente da ESSE3 ed è in attesa di vedersi attribuito il suo ruolo persona dettagliato (es. professore a contratto) da SIRIUM, in attesa viene chiamato "docente" in maniera generica	ESSE3	VERO
FACLOC002	Professore ospite		Docente che insega in corsi di facoltà diverse da quella a cui afferisce (per finire il monte ore attribuitogli e non eaurito all'interno della sua facoltà). In queste facoltà è definito "Professore ospite"	ESSE3	VERO

ID del ruolo	Descrizione del ruolo	Affiliazione IDEM	Significato del ruolo	Fonte del ruolo	Gestito in ADA
STUUGR001	Studente di corso di LT	member,student	Studente che frequenta i Corsi di Laurea triennale (LT)	ESSE3	VERO
STUGRA001	Studente di corso di LS/LM	member,student	Studente che frequenta i Corsi di Laurea Specialistica/Laurea magistrale(LS/LM)	ESSE3	VERO
STUGRA002	Studente di Corso di MU1	member,student	Studente che frequenta i Corsi di Master Universitario 1° livello (CMU1); sono corsi di perfezionamento scientifico o di alta formazione	ESSE3	VERO
STUGRA003	Studente di Corso LS/LM a ciclo unico	member,student	Studente che frequenta i Corsi di Master Universitario 1° livello (CMU1); sono corsi di perfezionamento scientifico o di alta formazione	ESSE3	VERO
STUPGR001	Dottorando	member,staff,student	Studente di Corso di Dottorato di Ricerca (CDR)	ESSE3	VERO
STUPGR002	Specializzando	member,staff,student	Studente di Corso di Specializzazione (CS)	ESSE3	VERO
STUPGR003	Studente di Corso di MU2	member,student	Studente di Corso di Master Universitario di 2° livello (CMU2)	ESSE3	VERO
STUPGR004	Dottorando ospite	member	Studente di Scuola di Dottorato di Ricerca esterno a UNITN ospitato presso le strutture unitn (non è gestito in ESSE3)	UFFICIO DOTTORATI	VERO
STUPGR005	Dottorando in cotutela incoming	member,student	Studente di Scuola di Dottorato di Ricerca ospite in UNITN grazie a accordo di cotutela con altra università (è gestito in ESSE3 poiché afferisce a un corso)	ESSE3	VERO
STUPOR001	Studente ante riforma	member,student	Studente iscritto a un corso di laurea del vecchio ordinamento	ESSE3	VERO
STUOTH001	Studente di altra università	student	Studente proveniente da altra università per motivi vari	ESSE3	VERO
STUOTH002	Studente corso singolo	member,student	Studente che frequenta un corso singolo	ESSE3	VERO
STUOTH003	Studente formazione permanente	member,student	Studente che frequenta un corso singolo	ESSE3	VERO
STUOTH004	Altro studente	member,student	Altra tipologia di studente	ESSE3	VERO

ID del ruolo	Descrizione del ruolo	Affiliazione IDEM	Significato del ruolo	Fonte del ruolo	Gestito in ADA
ALUUGR001	Laureato di corso di LT		Ex studente che ha frequentato i Corsi di Laurea triennale (LT)	ESSE3	FALSO
ALUGRA001	Laureato di corso di LS/LM		Ex studente che ha frequentato i Corsi di Laurea Specialistica/Laurea magistrale (LS/LM)	ESSE3	FALSO
ALUGRA002	Laureato con master di 1° livello		Ex studente che ha frequentato i Corsi di Master Universitario 1° livello (CMU1)	ESSE3	FALSO
ALUGRA003	Laureato di corso di LS/LM a ciclo unico		Ex studente che ha frequentato i Corsi di Master Universitario 1° livello (CMU1)	ESSE3	FALSO
ALUPGR001	Dottore di ricerca		Ex studente di Corsi di Dottorato di Ricerca (CDR)	ESSE3	FALSO
ALUPGR002	Specialista		Ex studente di Corso di Specializzazione (CS)	ESSE3	FALSO
ALUPGR003	Laureato con master di 2° livello		Ex studente di Corso di Master Universitario di 2° livello (CMU2)	ESSE3	FALSO
ALUPOR001	Laureato ante riforma LT		Ex studente laureato vecchio ordinamento	ESSE3	FALSO
ALUOTH001	Laureato<motivo>		Laureato (casi particolari ad honorem, equipollenza ecc)	ESSE3	FALSO
ALUOTH002	Ex studente		Ex studente laureato	ESSE3	FALSO
PTAREG001	Personale tecnico	member;staff	Personale che svolge mansioni di tipo tecnico	SIRIUM	VERO
PTAREG002	Personale amministrativo	member;staff	Personale che svolge mansioni di tipo amministrativo	SIRIUM	VERO
PTAREG003	Dirigente	member;staff	Personale che ricopre un ruolo dirigenziale	SIRIUM	VERO
PTAREG004	Assistente	member;staff	Personale che svolge mansioni di assistenza al responsabile di 1° livello	SIRIUM	VERO
PTAADD001	Consulente	affiliate	Professionista che collabora con una struttura a seguito della stipula di un contratto di consulenza (partita IVA)	GESTIONE CONTRATTI (ADELINE)	VERO
PTAADD002	Collaboratore esterno	member;staff	Professionista che collabora con una struttura a seguito della firma di un contratto di Collaboraz. (Coord.e Cont./a progetto)	GESTIONE CONTRATTI (ADELINE)	VERO
PTAADD003	Stagista area TA	affiliate	Studente UNITN che svolge uno stage all'interno dell'Università	SEGRETERIE DI DIPARTIMENTO;SEGRETERIE DI FACOLTA;SEGRETERIE DI 1° LIVELLO	VERO

ID del ruolo	Descrizione del ruolo	Affiliazione IDEM	Significato del ruolo	Fonte del ruolo	Gestito in ADA
PTAADD004	Altro personale TA	member;staff	Altro personale TA	SEGRETERIE DI 1° LIVELLO	VERO
PTAADD005	Dirigente a contratto	member;staff	Professionista che ricopre un ruolo dirigenziale a seguito della firma di un contratto di Collaboraz. (Coord e Cont./a progetto)	GESTIONE CONTRATTI (ADELINE)	VERO
PTAADD006	Assistente a contratto	member;staff	Professionista che svolge mansioni di assistenza al responsabile di 1° livello a seguito della firma di un contratto di Collaboraz. (Coord e Cont./a progetto)	GESTIONE CONTRATTI (ADELINE)	VERO
OTHEXT001	Rappresentante istituzionale	member;staff	Persone che hanno a che fare con l'Ateneo solamente in qualità di rappresentanti istituzionali (es: presidente del CDA)	ORGANI COLLEGIALI	VERO
OTHEXT002	Stagista esterno all'Ateneo	affiliate	Studente esterno a UNITN che svolge uno stage all'interno dell'Università (es: studente di superiori che viene a fare uno stage in UNITN)		FALSO
OTHEXT003	Ospite	affiliate	Figure varie: Congressisti, Assistenza tecnica esterna, Ospiti occasionali	SEGRETERIE DI DIPARTIMENTO;SEGRETERIE DI FACOLTA;SEGRETERIE DI 1° LIVELLO	VERO
OTHEXT004	Altri esterni	affiliate	Persone che non sono in nessuna delle categorie sopra elencate ma che hanno a che fare con l'Ateneo		VERO
FACADD013	Ricercatore a progetto	member;staff	Persona che svolge attività di ricerca a medio lungo termine ma non di ruolo	SIRIUM	VERO
FACADD014	Professore ordinario a tempo determinato	member;staff	Docente a contratto equiparato ad un docente ordinario	SIRIUM	VERO
FACADD015	Relatore convegno area ricerca	affiliate	Persona che partecipa come relatore ad un convegno dell'area ricerca	GESTIONE CONTRATTI (ADELINE)	VERO
FACADD016	Relatore convegno area didattica	affiliate	Persona che partecipa come relatore ad un convegno dell'area della didattica	GESTIONE CONTRATTI (ADELINE)	VERO
PTAADD007	collaboratore della formazione TA	member;staff	Collaboratore che svolge attività di formazione per il personale tecnico amministrativo su incarico della direzione risorse umane	GESTIONE CONTRATTI (ADELINE)	VERO

ID del ruolo	Descrizione del ruolo	Affiliazione IDEM	Significato del ruolo	Fonte del ruolo	Gestito in ADA
PTAADD008	Collaboratore della formazione (linguistica)	member,staff	Collaboratore esterno che svolge attività di formazione relativamente all'area linguistica su incarico del CIAL rivolta a studenti, TA ed esterni	GESTIONE CONTRATTI (ADELINE)	VERO
FACADD017	Ricercatore a tempo determinato	member,staff	Ricercatore a contratto equiparato ad un ricercatore.	SIRIUM	VERO
OTHEXT005	Personale sanitario esterno	member	Persone esterne che svolgono attività in ambito sanitario (medici, infermieri, tecnici radiologi, etc..) nei centri o nei laboratori dell'Ateneo.	SIRIUM	VERO
FACADD018	Docente in entrata		Docente a cui verrà affidato un incarico di insegnamento di vario tipo non ancora ufficialmente confermato. Viene utilizzato in fase di copertura delle attività didattiche previste dalla nuova offerta formativa. L'assegnazione all'attività specifica avverrà attraverso gli appositi applicativi (UGOV-PD, UP, ESSE3).	SEGRETERIE DI FACOLTÀ	VERO
FACADD019	Professore Emerito	member	Titolo attribuito su proposta di un'apposita commissione ad un Professore cessato con almeno 20 anni di anzianità come Ordinario. Nominato tramite DPR.	ORGANI COLLEGIALI	VERO

Tabella 1: Elenco dei ruoli degli utenti gestiti con affiliazione IDEM

Visione di insieme del processo di accreditamento degli utenti

In UNITN le funzionalità relative al provisioning/deprovisioning degli utenti è implementata in ADA (Anagrafica di Ateneo). Il sistema è composto da un insieme di processi organizzativi, modelli logici, procedure automatizzate, interfacce verso utenti e verso altri sistemi informatici. Il tutto si prende carico di acquisire le informazioni dove disponibili, aggregarle, integrarle con eventuali dati mancanti, normalizzarle secondo un modello logico e di codifica comune ed infine di presentarle in modo omogeneo alle altre applicazioni di Ateneo. Alcune di queste applicazioni sono i sistemi di directory e autenticazione OpenLdap e Active Directory.
L'architettura complessiva del sistema è rappresentata sinteticamente nel diagramma seguente.

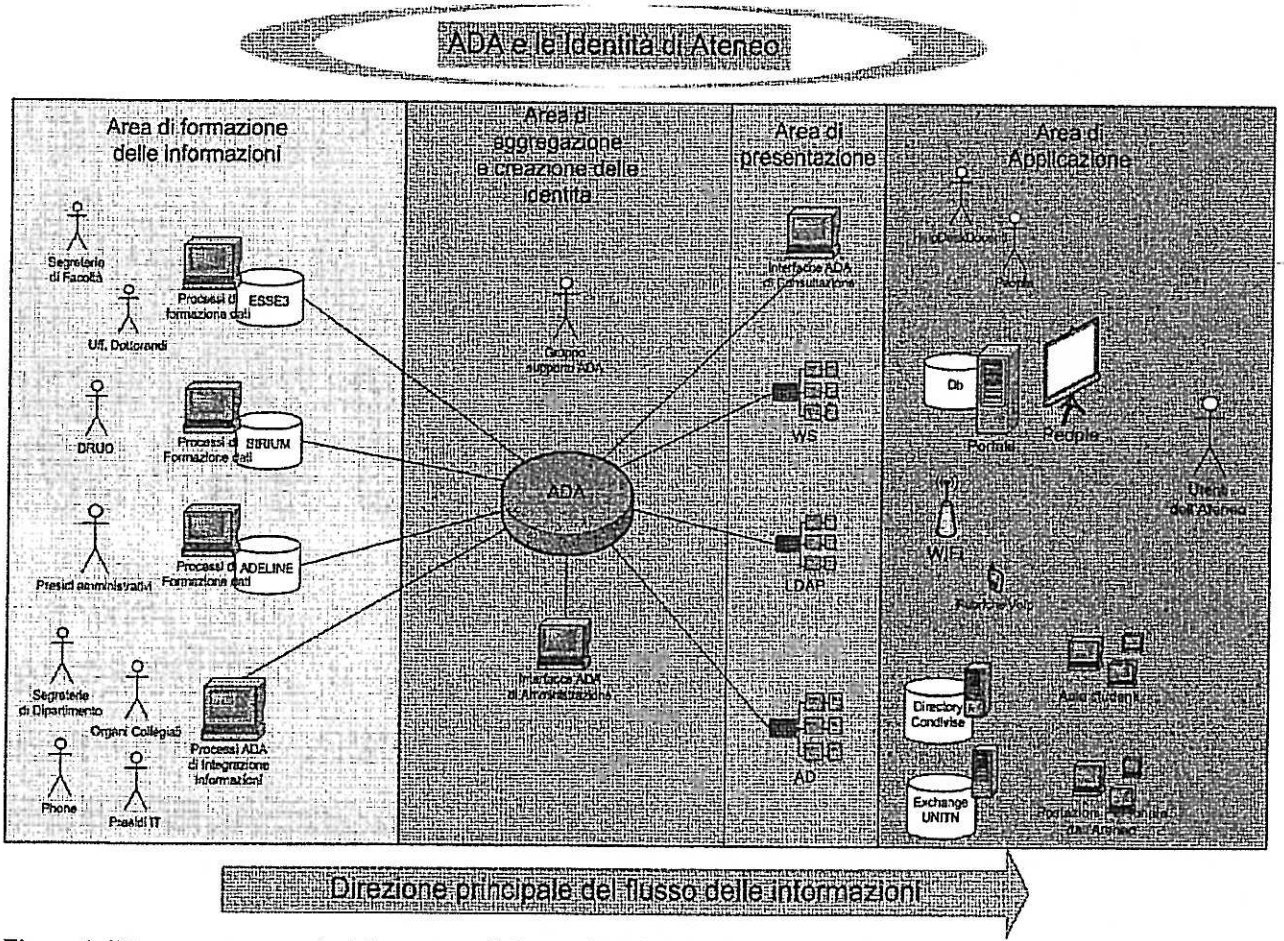

Figura 1: Diagramma generale del processo di formazione delle identità di ateneo

Nella figura sono evidenziate le 4 aree principali coinvolte:
1. Area di formazione delle informazioni: rappresenta i sistemi o le funzioni dei sistemi, in cui le informazioni nascono per i fini applicativi dei sistemi stessi o per i fini specifici di ADA.
2. Area di aggregazione e creazione delle identità: rappresenta il core di ADA, le informazioni vengono aggregate, trasformate e memorizzate per adeguandole al modello logico di ADA.
3. Area di presentazione: raggruppa le interfacce di ADA che rendono disponibili le informazioni sulle identità delle persone.

4. Area di applicazione: elenca alcuni dei servizi di UNITN che utilizzano direttamente o indirettamente le informazioni sulle identità prodotte da ADA.

Processo di accreditamento sintetico

Il diagramma in ***Figura 2: Processo di accreditamento sintetico*** descrive le fasi principali e gli attori coinvolti nel processo di rilascio delle credenziali in UNITN (Account di Ateneo).
Gli aspetti fondamentali del diagramma sono rappresentati dalle seguenti attività:

1) **A2 – autorizzazione e formalizzazione del rapporto con UNITN**: il rilascio di un Account di Ateneo prevede la presenza di un rapporto formalizzato con UNITN e di un autorizzazione, che possono essere ottenuti in due modi differenti:
   a) **Implicito**: derivato dall'approvazione di un particolare processo di business che prevede la creazione di un identità di ateneo e l'assegnazione di un account, es: un contratto, un iscrizione ad un corso di studio, una procedura di selezione, etc. .
   b) **Esplicito**: da parte di un responsabile di 1°livello (Dirigente, Preside, Direttore, etc...) o di un suo delegato). In questo caso è prevista la compilazione di un apposito modulo sostitutivo che svolge ambedue le funzioni (Allegato 1: modulo di autorizzazione inserimento nuova persona e nuovo ruolo in ADA).
2) **A3 – ricerca preventiva dell'identità in ADA**: è fondamentale che ogni richiesta di inserimento di una nuova identità venga preceduta da una fase di ricerca: se l'identità è già presente, va semplicemente aggiunto un ruolo, se non è già presente va creata.
   Questa impostazione è rispettata sia dalle procedure di integrazione dei dati dei sistemi informativi di ateneo, sia dalle interfacce utente che prevedono un inserimento diretto delle identità
3) **A8 – Verifica dell'identità di una persona**: prima di consegnare un nuovo Account di Ateneo, o prima di rilasciare una nuova password, deve sempre essere verificata l'identità di una persona. In caso di non conoscenza diretta, va richiesto un documento di identità.
4) **A18 – Disattivazione di un Account di Ateneo**: quando il periodo di validità di tutti i ruoli associati all'identità della persona è terminato, viene disattivato anche l'account associato alla persona.

Tipologie di processi di accreditamento

Le tipologie dei processi di accreditamento degli utenti in UNITN dipendono principalmente dalle modalità di formazione delle informazioni relative alla loro identità ed in secondo luogo dal ruolo in Ateneo.
Sono gestiti i seguenti tipi di processo:

1. Accreditamento con acquisizione identità da un Sistema di Business (non studenti)
2. Accreditamento con acquisizione identità da un Sistema di Business (studenti)
3. Accreditamento con acquisizione identità direttamente in ADA (non studenti)

La differenziazione tra studenti e non studenti dipende anche dalla diversa gestione delle loro credenziali, che ad esempio, nel caso degli studenti non scadono mai, mentre per gli account dei non studenti, scadono ogni 6 mesi.
Un caso particolare sono i Dottorandi, seguono sia il processo di accreditamento da studente che da non studente, trovandosi alla fine con due set di credenziali.

Sviluppi previsti a breve

Entro breve la differenziazione tra i processi studenti e processi non studenti verrà rivista, con l'obiettivo di uniformare il più possibile i due processi, evitando tra l'altro, di rilasciare 2 account ai Dottorandi.

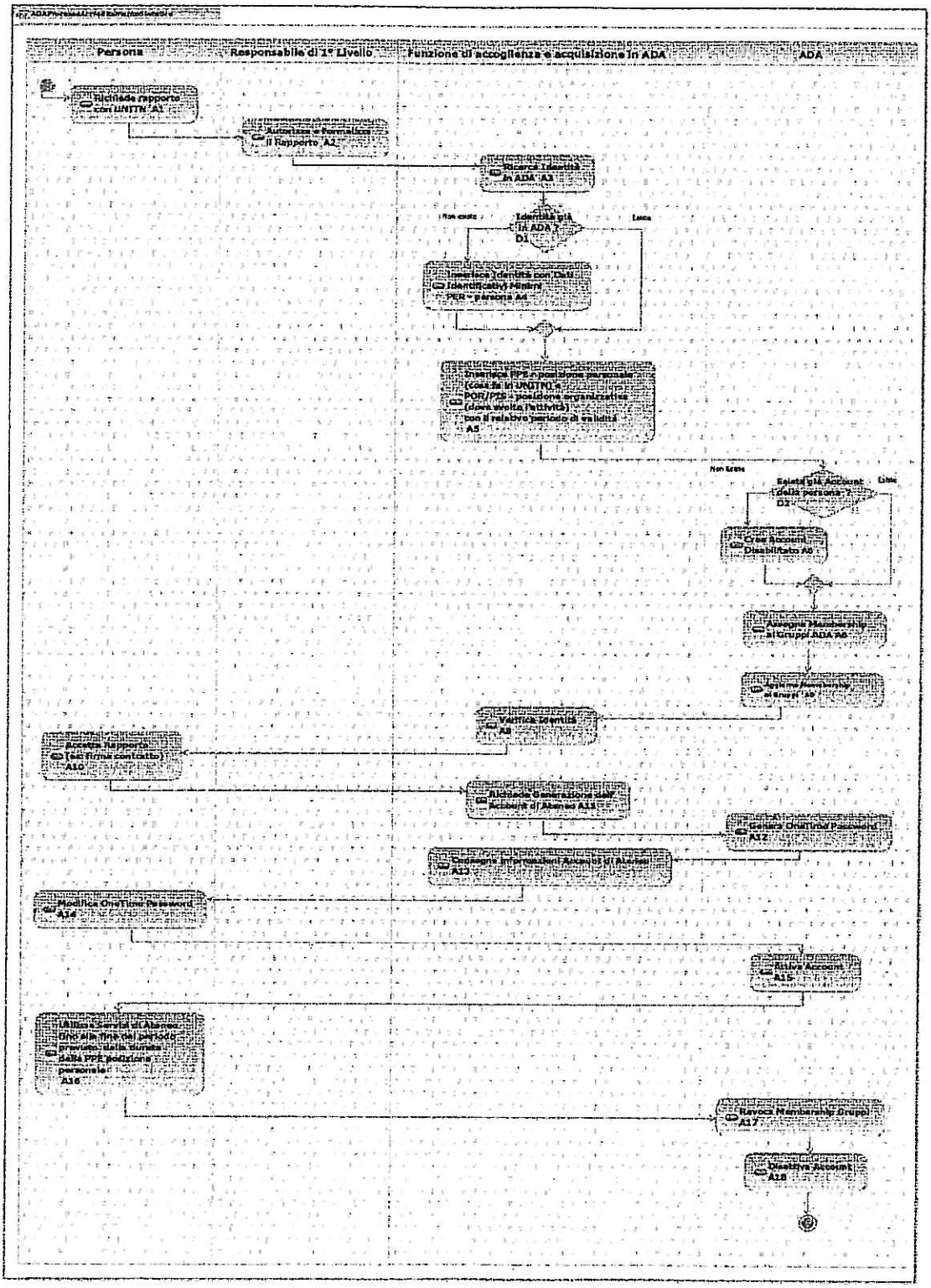

Figura 2: Processo di accreditamento sintetico

Modalità di utilizzo del Account di Ateneo per l'accesso ai servizi

Nello schema di ***Figura 3: Modello di riferimento per l'accesso ai servizi tramite account di ateneo*** viene illustrato il modello di riferimento della modalità di utilizzo degli account di ateneo per l'accesso ai servizi di UNITN.

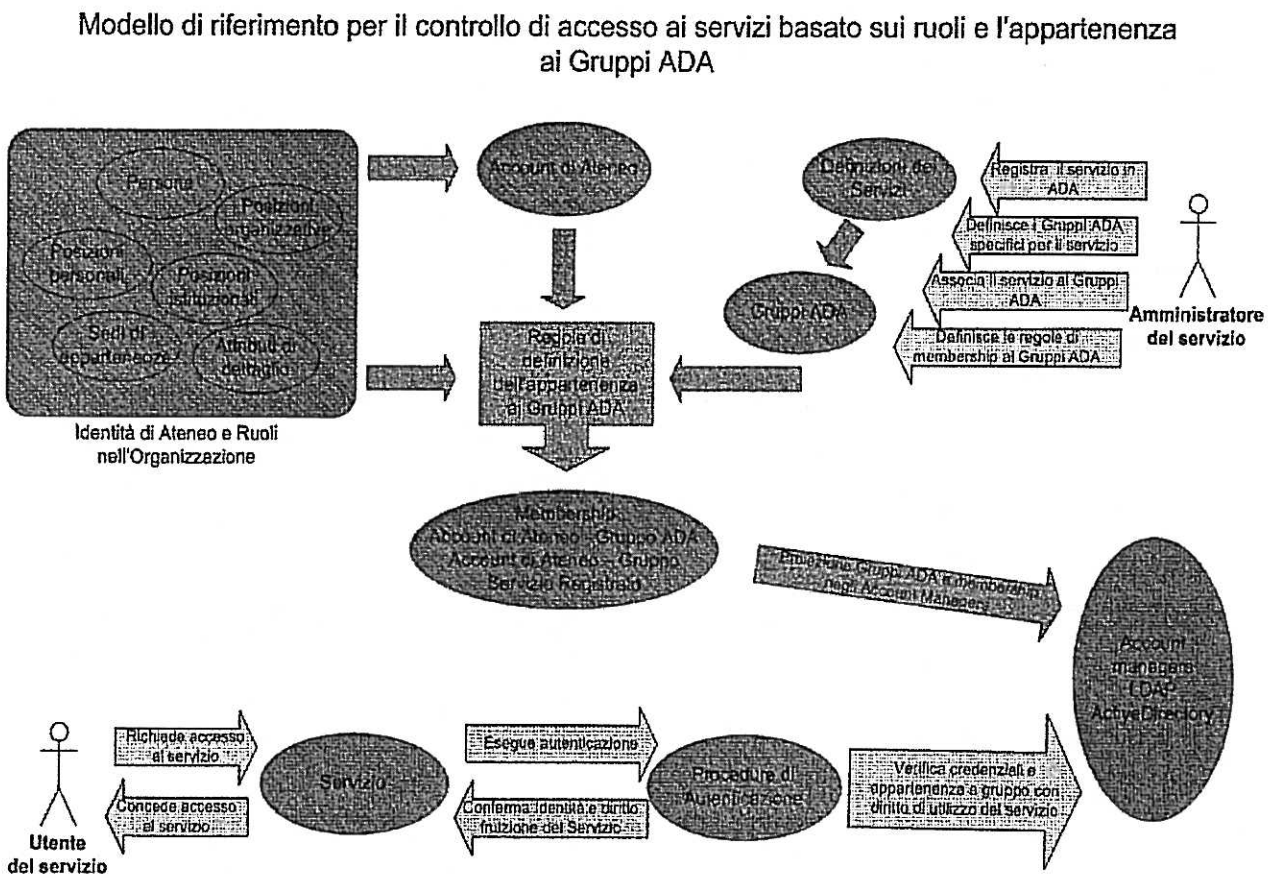

Figura 3: Modello di riferimento per l'accesso ai servizi tramite account di ateneo

In riferimento alla federazione IDEM, la "Procedura di autenticazione" viene svolta utilizzando l'infrastruttura Shibboleth ed i relativi accordi sullo scambio di attributi tra IDP e SP.

Il processo di accreditamento per le varie categorie di utenti

La descrizione dei processi di accreditamento viene riepilogata in 4 tipologie, che corrispondono ai 4 casi presenti in Ateneo:

- Accreditamento con acquisizione identità da un Sistema di Business (non studenti),
- Accreditamento con acquisizione identità da un Sistema di Business (studenti),
- Accreditamento con acquisizione identità da un Sistema di Business (dottorandi),
- Accreditamento con inserimento diretto in ADA.

I 4 tipi di accreditamento sono descritti nei paragrafi successivi.

Accreditamento con acquisizione identità da un Sistema di Business (non studenti)

Il processo

Il diagramma di ***Figura 4: Accreditamento da sistema di Business (non studente)*** rappresenta le principali attività ed i principali attori coinvolti nella gestione delle identità, dei ruoli e degli account di ateneo delle persone le cui informazioni vengono ottenute da uno dei sistemi di business di UNITN.

Il processo è una specializzazione del processo di accreditamento sintetico descritto nel paragrafo Processo di accreditamento sintetico.

I ruoli a cui viene applicato questo processo sono quelli che in ***Tabella 1: Elenco dei ruoli degli utenti gestiti con affiliazione IDEM*** provengono dalle seguenti fonti:

- SIRIUM
- GESTIONE CONTRATTI (ADELINE)
- ESSE3 (Docenti)

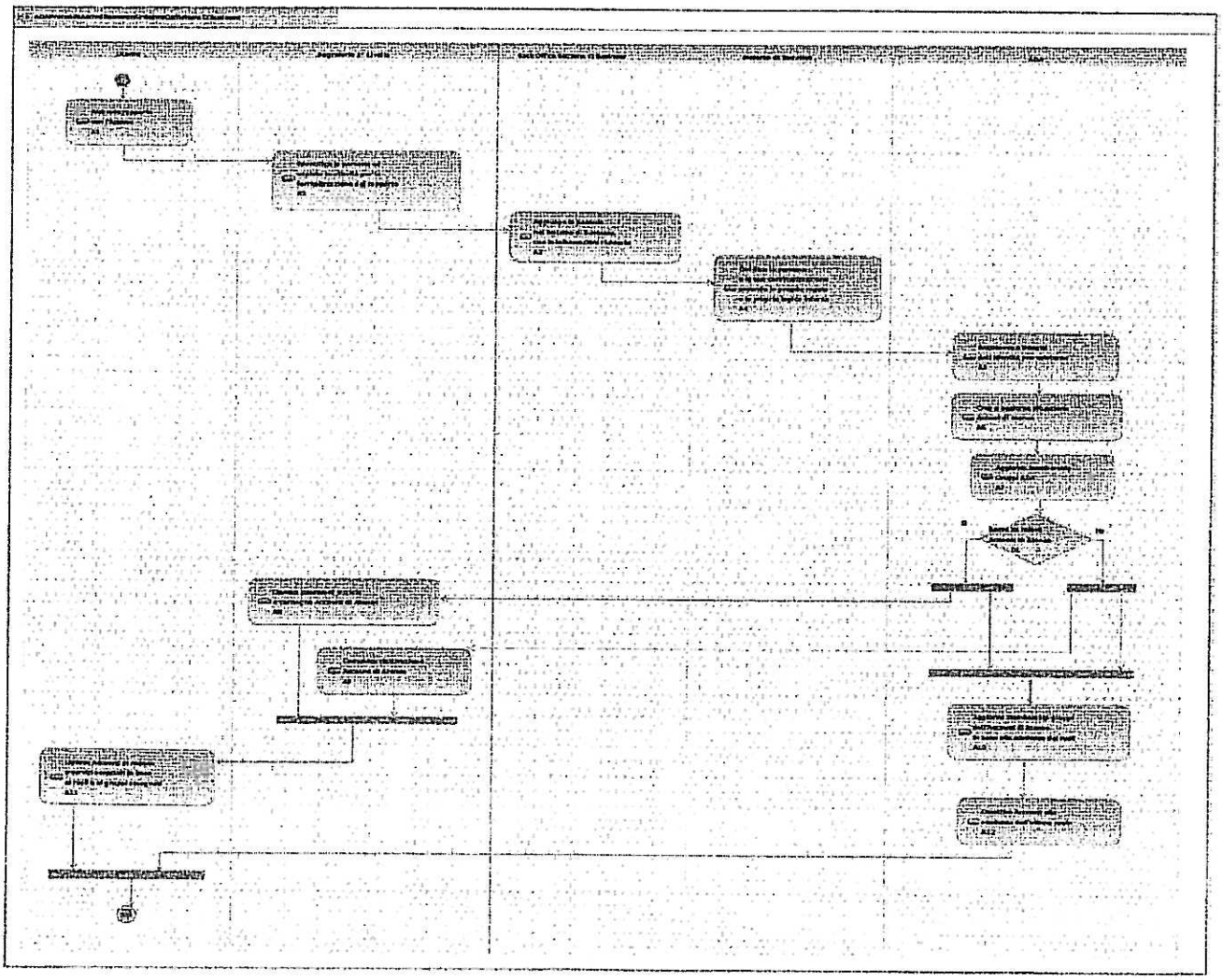

Figura 4: Accreditamento da sistema di Business (non studente)

Modalità di riconoscimento della persona

In questo tipo di accreditamento, l'identità digitale viene derivata dai pre-esisteni processi di business che definiscono formalmente la creazione del rapporto tra persona e Ateneo (Attività A2 del diagramma).
L'identificazione della persona è garantita, ad esempio, dalle normali procedure concorsuali che portano alla formazione di un ruolo da docente, tecnico amministrativo, dottorando, assegnista di ricerca, etc....
Queste procedure prevedono già le attività A2 e A8 del processo sintetico di ***Figura 2: Processo di accreditamento sintetico***:

- l'autorizzazione alla creazione del ruolo (implicitamente concessa dall'avvio delle procedure concorsuali)
- la verifica dell'identità della persona (presentazione dei documenti al concorso)
- formalizzazione del rapporto (firma sul contratto).

Gli uffici preposti a queste attività sono:

- Ufficio personale docente e ricercatore
- Ufficio amministrazione PTA
- Ufficio accoglienza personale e servizi complementari
- Ufficio dottorati
- Presidi amministrativi
- Segreterie di Facoltà e Dipartimento

Caratteristiche dell'identità digitale

L'identità di una persona viene identificata sulla base di questi attributi (*dati identificativi minimi*):

- Nome
- Cognome
- Data di nascita
- Luogo di nascita
- Nazione di nascita
- Sesso

L'insieme di questi dati concorre ad identificare univocamente ogni persona censita in UNITN.
Ad ogni singola combinazione degli attributi precedentemente indicati (una persona) viene assegnato un codice (ID_ADA) alfanumerico che le rimarrà attribuito per sempre.
PPE-posizioni personali
Ad ogni persone vengono assegnati uno o più RUP-ruolo persona che, assieme al periodo di validità formano le PPE-posizioni personali.
In sintesi, le PPE-posizioni personali indicano che cosa una persona fa in UNITN e per quanto tempo.
POR-posizioni organizzative
Ad ogni PPE-posizione personale, vengono assegnati uno o più RUO-ruoli organizzativa ed una o più STO-struttura organizzativa, che assieme ad un periodo di validità, formano la POR-posizioni organizzative.
Alle POS-posizioni organizzative vengono associate anche le SED-sedi che indicano il luogo fisico prevalente in cui viene svolta l'attivita.
In sintesi, le POS-posizioni organizzative indicano dove una persona svolge la propria attività e con quale ruolo organizzativo (responsabile o afferente).

Ad ogni persona sono associati un Account di Ateno, un eventuale indirizzo e-mail ed un eventuale numero di telefono.
Tuttavia, nessuna di queste informazioni è da considerarsi pubblica, possono essere utilizzate solo per i fini istituzionali dell'Ateneo.
Indirizzo e-mail e numero di telefono sono consultabili solo attraverso il People di Ateneo.

Gestione del ciclo di vita

Tutte le informazioni relative all'esistenza e alla durata delle posizioni delle persone sono ottenute dai **Sistemi** di Business che ne definiscono le caratteristiche formali, compresa la durata.
I trasferimenti e le cessazioni vengono acquisiti in ADA automaticamente dai sistemi preposti alla loro gestione.
Quando tutti i ruoli associati ad una persona sono terminati, il relativo account di ateneo viene disabilitato.

Formato e regole delle credenziali

Le credenziali elettroniche che formano l'account di ateneo sono composte di username e password.
Ogni persona in questa categoria possiede un unico account di ateneo (fanno eccezione i Dottorandi, come descritto più avanti)
L'account di ateneo è normalmente nella forma "nome.cognome@unitn.it" (NB: non è l'indirizzo di e-mail, che può essere differente).
La password associata all'account di ateneo ha le seguenti caratteristiche:

- deve avere lunghezza minima di 8 caratteri,
- deve contenere almeno un carattere non alfabetico,
- deve essere diversa dalla vecchia password,
- scade ogni 6 mesi.

Eventuale presenza di credenziali multiple per la stessa persona

Di norma viene rilasciato un unico account di ateneo ad ogni persona. L'unica eccezione sono gli studenti-docenti (i dottorandi) che, per il momento, necessitano di un doppio account per accedere alle aree di ESSE3 studenti e docenti.
A breve la situazione verrà sanata utilizzando Shibboleth anche per l'accesso ad ESSE3.

Modalità di consegna delle credenziali

La consegna delle credenziali avviene contestualmente ad una verifica dell'identità della persona tramite documento di riconoscimento.
Per mezzo di un apposito modulo, viene consegnata una password random con obbligo di modifica immediato.
Gli uffici che possono rilasciare le nuove credenziali per i ruoli in oggetto sono:

- Ufficio accoglienza personale e servizi complementari
- Ufficio dottorati
- Segreterie di Facoltà e Dipartimento
- Segreterie di Direzione

Modalità di recupero delle credenziali smarrite

Il recupero delle credenziali smarrite avviene presentandosi ai Presidi IT (presidi dei servizi informatici presenti nelle varie sedi dell'Ateneo).
Solo i Presidi IT possono re-inizializzare una password già rilasciata.
Anche in questo caso, viene consegnata, per mezzo di un apposito modulo, una password random con obbligo di modifica immediato.

Modalità di gestione smarrimento smartcard/token

Al momento non vengono rilasciati smarcard/token.

Durata dell'accreditamento

La durata dell'accreditamento può essere a termine o a tempo indeterminato, è direttamente collegata al tipo e alla durata del rapporto tra la persona e UNITN, è definita dal periodo di validità della PPE-posizione personale assegnata che lo descrive.

Disabilitazione utente

La disabilitazione di un account di ateneo avviene automaticamente sulla base di due parametri:

- la data di fine del rapporto tra persona e UNITN (PPE-posizione personale),
- l'eventuale periodo di estensione previsto per il RUP-ruolo persona associato alla PPE-posizione personale.

Il periodo di estensione viene utilizzato permettere l'espletamento delle procedure di uscita dall'Ateneo.

Cancellazione definitiva utente

Normalmente la cancellazione definitiva di un account di ateneo non è prevista, l'account viene disabilitato dopo la fine del rapporto tra persona ed ateneo, ma può essere riattivato all'instaurazione di un nuovo rapporto.

Rischi specifici associati alla categoria di utenti

I rischi associati a questa categoria sono principalmente:

1. l'impossibilità di rilasciare un account di ateneo per problemi di formalizzazione del rapporto con l'Ateneo,
2. l'impossibilità di accedere ai servizi a causa di problemi sull'infrastruttura di autenticazione,
3. il furto di identità.

Per quanto riguarda il punto 1, è stata prevista la possibilità di inserire direttamente in ADA ruoli generici e temporanei (es: Ospite), che pur garantendo tutti i requisiti di identificazione e formalizzazione, prevedono delle procedure più snelle e veloci (è sufficiente la verifica dei documenti di riconoscimento e l'autorizzazione di un responsabile di primo livello, vedi modulo Allegato 1).
Per quanto riguarda il punto 2, sono state prese misure sistemistiche per garantire un high availability adeguata.
Per quanto riguarda il punto 3, sono state prese misure informatiche (comunicazioni criptate per il rilascio delle credenziali, complessità minima e scadenza frequente della password, log), procedurali (definizione di un processo preciso con requisiti minimi e formazione delle persone

addette al rilascio delle password) e strutturali (utilizzo di un'unica credenziale per tutti i servizi: non serve più scrivere la password da qualche parte in quanto viene usata molto frequentemente, la password assume un valore tale, anche per la persona a cui viene assegnata, da garantirne un'accurata gestione personale).

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

Al momento non sono implementate credenziali forti in UNITN.

Accreditamento con acquisizione identità da un Sistema di Business (studenti)

Il processo

Il diagramma di ***Figura 5: Accreditamento da sistema di Business (studente)*** rappresenta le principali attività ed i principali attori coinvolti nella gestione delle identità, dei ruoli e degli studenti, le cui informazioni vengono ottenute da ESSE3.
I ruoli a cui viene applicato questo processo sono quelli che in ***Tabella 1: Elenco dei ruoli degli utenti gestiti con affiliazione IDEM*** provengono dalle seguenti fonti:

- ESSE3 (ruoli degli studenti)

Le attività del diagramma dalla A1 alla A7 riguardano l'account assegnato agli studenti in fase di pre-registrazione, questi account non vengono utilizzati per l'accesso alla federazione IDEM.
Le attività dalla A8 in poi sono riferiti all'account studenti in UNITN, che viene utilizzato per l'accesso alla federazione IDEM.
Il processo, dall'attività A8 in poi, è una specializzazione del processo di accreditamento sintetico descritto nel paragrafo Processo di accreditamento sintetico.

Modalità di riconoscimento della persona

In questo tipo di accreditamento, l'identità digitale viene derivata dai processi di immatricolazione degli studenti, che definiscono formalmente la creazione del rapporto tra studente e Ateneo (Attività A8 e A9 del diagramma in ***Figura 5: Accreditamento da sistema di Business (studente)***).
L'identificazione della persona è verificata dai Presidi didattici delle varie sedi dell'Ateneo al momento stesso dell'iscrizione.
Il processo di iscrizione quindi, prevede già le attività A2 e A8 del processo sintetico di ***Figura 2: Processo di accreditamento sintetico***:

- l'autorizzazione alla creazione del ruolo (implicitamente concessa ai Presidi Didattici in quanto responsabili dell'iscrizione degli studenti)
- la verifica dell'identità della persona (presentazione dei documenti di identità per l'iscrizione)
- formalizzazione del rapporto (firma sul modulo di iscrizione).

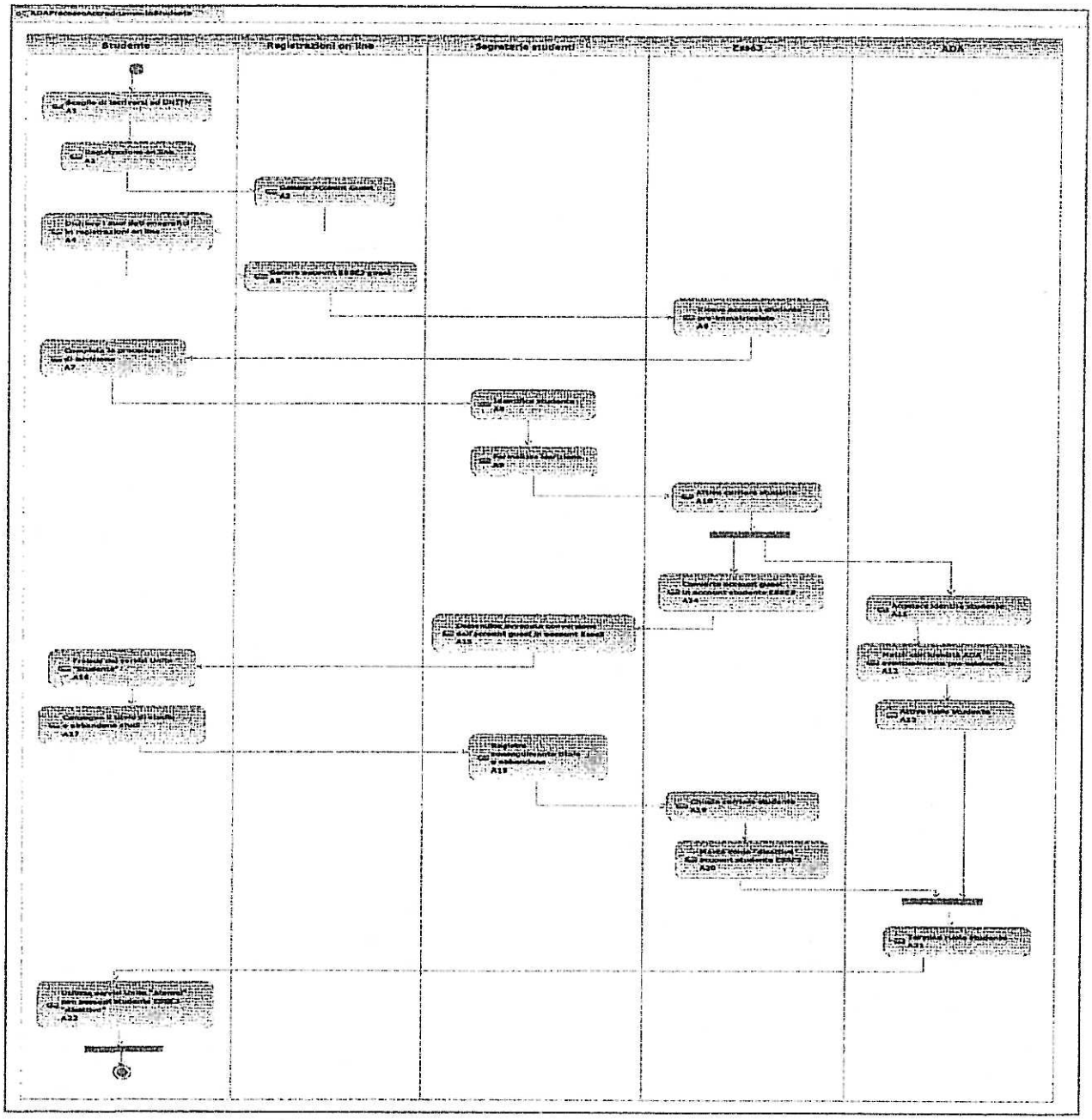

Figura 5: Accreditamento da sistema di Business (studente)

Caratteristiche dell'identità digitale

L'identità di una persona viene identificata sulla base di questi attributi (*dati identificativi minimi*):

- Nome
- Cognome
- Data di nascita
- Luogo di nascita
- Nazione di nascita
- Sesso

L'insieme di questi dati concorre ad identificare univocamente ogni persona censita in UNITN.
Ad ogni singola combinazione degli attributi precedentemente indicati (una persona) viene assegnato un codice (ID_ADA) alfanumerico che le rimarrà attribuito per sempre.

PPE-posizioni personali

Ad ogni persone vengono assegnati uno o più RUP-ruolo persona che, assieme al periodo di validità formano le PPE-posizioni personali.
In sintesi, le PPE-posizioni personali indicano che cosa una persona fa in UNITN e per quanto tempo.

POR-posizioni organizzative

Ad ogni PPE-posizione personale, vengono assegnati uno o più RUO-ruoli organizzativa ed una o più STO-struttura organizzativa, che assieme ad un periodo di validità, formano la POR-posizioni organizzative. Nel caso specifico degli studenti, le STO-strutture organizzative sono i corsi di studio attivi in Ateneo ed il RUO-ruolo organizzativo è "Iscritto a".
Alle POS-posizioni organizzative vengono associate anche le SED-sedi che indicano il luogo fisico prevalente in cui viene svolta l'attivita.
Ad ogni studente è associato un account studente ed un indirizzo e-mail.
Tuttavia, nessuna di queste informazioni è da considerarsi pubblica, possono essere utilizzate solo per i fini istituzionali dell'Ateneo, gli studenti non vengono presentati neanche nel People di Ateneo.

Gestione del ciclo di vita

Tutte le informazioni relative all'esistenza e alla durata delle posizioni degli studenti sono ottenute da ESSE3, che ne definisce le caratteristiche formali, compresa la durata.
I trasferimenti e le cessazioni vengono acquisiti in ADA automaticamente sulla base degli aggiornamenti della carriera dello studente.
Quando lo studente completa o abbandona il corso di studio a cui è iscritto, il suo account studente viene disabilitato.

Formato e regole delle credenziali

[Dove si descrive la tipologia delle credenziali utilizzate nell'organizzazione credentials (e.g., Kerberos, userID/password, PKI, ...) il loro formato, la loro durata, ecc
Se viene usato più di un tipo di credenziali elettroniche come si può determinare chi ha ricevuto quali? Che politiche ci sono per ili rilascio e la gestione di credenziali di tipologie diverse alla stessa persona?
Le credenziali elettroniche che formano l'account studente sono composte di username e password.

Ogni persona in questa categoria possiede un unico account studente (fanno eccezione i Dottorandi, come descritto più avanti)
L'account studente è normalmente nella forma "nome.cognome@studenti.unitn.it" (NB: non è l'indirizzo di e-mail, che può essere differente).
La password associata all'account studente ha le seguenti caratteristiche:

- deve avere lunghezza di 8 caratteri,
- deve contenere almeno un carattere non alfabetico,
- deve essere diversa dalla vecchia password,
- non prevede scadenza.

Eventuale presenza di credenziali multiple per la stessa persona

Viene rilasciato un unico account studente ad ogni persona. L'unica eccezione sono gli studenti-docenti (i dottorandi) che, per il momento, necessitano di un doppio account per accedere alle due aree di ESSE3 studenti e docenti.
A breve la situazione verrà sanata utilizzando Shibboleth anche per l'accesso ad ESSE3.

Modalità di consegna delle credenziali

La consegna delle credenziali avviene contestualmente all'iscrizione ed alla relativa verifica dell'identità della persona.
Per mezzo di un apposito modulo, viene consegnata una password random con obbligo di modifica immediato.
Gli uffici che possono rilasciare le nuove credenziali per i ruoli in oggetto sono:

- Presidi didattici delle facoltà dell'ateneo.

Modalità di recupero delle credenziali smarrite

Il recupero delle credenziali smarrite avviene presentandosi ai presidi didattici delle facoltà.
Anche in questo caso, viene consegnata, per mezzo di un apposito modulo, una password random con obbligo di modifica immediato.

Modalità di gestione smarrimento smartcard/token

Al momento non vengono rilasciati smarcard/token.

Durata dell'accreditamento

La durata dell'accreditamento corrisponde alla durata della carriera da studente della persona.
Termina al conseguimento del titolo o all'abbandono.

Disabilitazione utente

La disabilitazione di un account studente avviene al verificarsi di una o più delle seguenti condizioni:

- conseguimento titolo,
- abbandono,
- irregolarità nel pagamento delle tasse di iscrizione.

Cancellazione definitiva utente

La cancellazione definitiva di un account studente non è prevista, l'account viene disabilitato, ma lo studente può continuare ad utilizzarlo per accedere ai servizi offerti agli alumni.

Rischi specifici associati alla categoria di utenti

I rischi associati a questa categoria sono principalmente:

1. l'impossibilità di accedere ai servizi a causa di problemi sull'infrastruttura di autenticazione,
2. il furto di identità.

Per quanto riguarda il punto 1, sono state prese misure sistemistiche per garantire un high availability adeguata.
Per quanto riguarda il punto 2, sono state prese alcune misure informatiche (comunicazioni criptate per il rilascio delle credenziali, complessità minima), procedurali (definizione di un processo preciso con requisiti minimi e formazione delle persone addette al rilascio delle password) e strutturali (utilizzo di un'unica credenziale per tutti i servizi: non serve più scrivere la password da qualche parte in quanto viene usata molto frequentemente, la password assume un valore tale, anche per la persona a cui viene assegnata, da garantirne un'accurata gestione personale).

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

Al momento non sono implementate credenziali forti in UNITN.

Accreditamento con acquisizione identità da un Sistema di Business (dottorandi)

Il processo

Il diagramma di ***Figura 6: Accreditamento da sistema di business (dottorando)*** rappresenta le principali attività ed i principali attori coinvolti nella gestione delle identità, dei ruoli dei dottorandi, le cui informazioni vengono ottenute da ESSE3.
I ruoli a cui viene applicato questo processo sono quelli che in ***Tabella 1: Elenco dei ruoli degli utenti gestiti con affiliazione IDEM*** provengono dalle seguenti fonti:

- ESSE3 (dottorandi)

Il processo è un mix dei due casi precedenti, in quanto ai dottorandi vengono consegnate due credenziali:

- account studente (accesso area studente di ESSE3)
- account di ateneo (accesso area docente di ESSE3)

Le motivazioni di queste doppie credenziali risiedono nella dualità dell'attività di un dottorando, che spesso svolge sia attività tipiche di uno studente, sia attività di docenza, ma soprattutto in un vincolo tecnico di ESSE3 che prevede due account differenti per accedere a due aree differenti di ESSE3.
Le attività del diagramma dalla A1 alla A4 riguardano la parte di selezione dei dottorandi, possono prevedere il rilascio di account temporanei, ma questi account non vengono utilizzati per l'accesso alla federazione IDEM.
Le attività dalla A5 in poi sono riferiti alla formazione degli account studente e account di ateneo, che possono venire indifferentemente utilizzati per l'accesso alla federazione IDEM.
Il processo, dall'attività A5 in poi, è una specializzazione del processo di accreditamento sintetico descritto nel paragrafo Processo di accreditamento sintetico.

Modalità di riconoscimento della persona

In questo tipo di accreditamento, l'identità digitale viene derivata dai processi di selezione e immatricolazione dei dottorandi, che definiscono formalmente la creazione del rapporto tra studente e Ateneo (Attività A5 e A6 del diagramma in ***Figura 6: Accreditamento da sistema di business (dottorando)***).
L'identificazione della persona è verificata dall'Ufficio dottorati (o dalle segreterie delle Scuole di dottorato).
Il processo di accreditamento dei dottorandi quindi, prevede già le attività A2 e A8 del processo sintetico di ***Figura 2: Processo di accreditamento sintetico:***

- l'autorizzazione alla creazione del ruolo (implicitamente concessa all'Ufficio dottorati in quanto responsabili della selezione e registrazione dei dottorandi)
- la verifica dell'identità della persona (presentazione dei documenti di identità per la registrazione)
- formalizzazione del rapporto (firma sul contratto di dottorato).

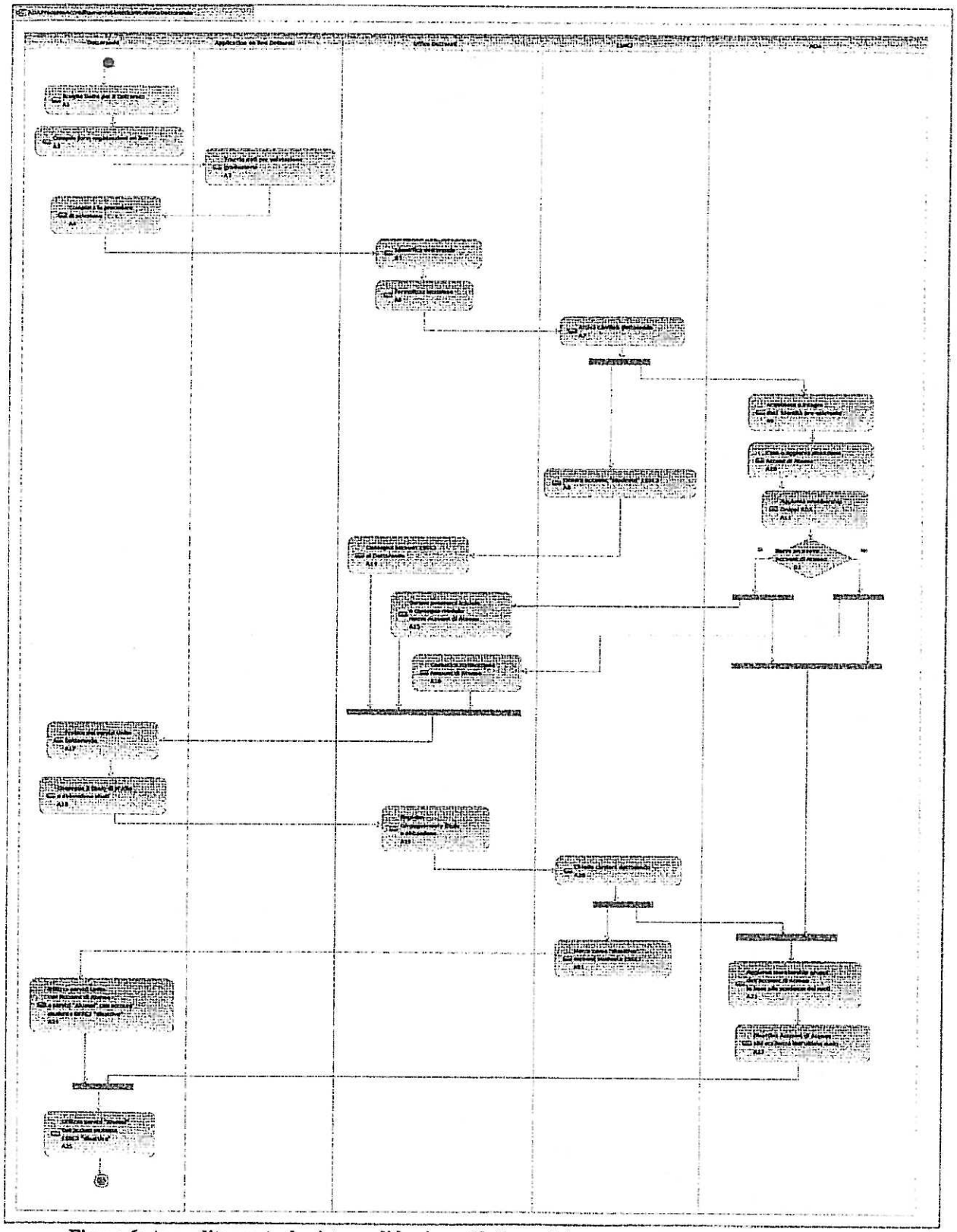

Figura 6: Accreditamento da sistema di business (dottorando)

Caratteristiche dell'identità digitale

L'identità di una persona viene identificata sulla base di questi attributi (*dati identificativi minimi*):

- Nome
- Cognome
- Data di nascita
- Luogo di nascita
- Nazione di nascita
- Sesso

L'insieme di questi dati concorre ad identificare univocamente ogni persona censita in UNITN.
Ad ogni singola combinazione degli attributi precedentemente indicati (una persona) viene assegnato un codice (ID_ADA) alfanumerico che le rimarrà attribuito per sempre.

PPE-posizioni personali

Ad ogni persone vengono assegnati uno o più RUP-ruolo persona che, assieme al periodo di validità formano le PPE-posizioni personali.
In sintesi, le PPE-posizioni personali indicano che cosa una persona fa in UNITN e per quanto tempo.

POR-posizioni organizzative

Ad ogni PPE-posizione personale, vengono assegnati uno o più RUO-ruoli organizzativa ed una o più STO-struttura organizzativa, che assieme ad un periodo di validità, formano la POR-posizioni organizzative. Nel caso specifico degli studenti, le STO-strutture organizzative sono i corsi di dottorato attivi in Ateneo ed il RUO-ruolo organizzativo è "Iscritto a".
Alle POS-posizioni organizzative vengono associate anche le SED-sedi che indicano il luogo fisico prevalente in cui viene svolta l'attivita.
Ad ogni dottorando sono associati, un account studente, un account di ateneo ed un indirizzo e-mail.
Tuttavia, nessuna di queste informazioni è da considerarsi pubblica, possono essere utilizzate solo per i fini istituzionali dell'Ateneo, i dottorandi vengono comunque presentati neanche nel People di Ateneo.

Gestione del ciclo di vita

Tutte le informazioni relative all'esistenza e alla durata delle posizioni dei dottorandi sono ottenute da ESSE3, che ne definisce le caratteristiche formali, compresa la durata.
I trasferimenti e le cessazioni vengono acquisiti in ADA automaticamente sulla base degli aggiornamenti della carriera del dottorando.
Quando il dottorando completa o abbandona il corso di studio a cui è iscritto, il suo account studente ed il suo account di ateneo vengono disabilitati. L'account studente potrà comunque essere utilizzato per accedere ad alcuni servizi rivolti agli alumni.

Formato e regole delle credenziali

Le credenziali elettroniche che formano l'account studente e l'account di ateneo sono composte di username e password.
Ogni persona in questa categoria possiede due account: un account di ateneo ed un account studente.
L'account di ateneo è normalmente nella forma "nome.cognome@unitn.it" (NB: non è l'indirizzo di e-mail, che può essere differente).

La password associata all'account di ateneo ha le seguenti caratteristiche:

- deve avere lunghezza minima di 8 caratteri,
- deve contenere almeno un carattere non alfabetico,
- deve essere diversa dalla vecchia password,
- scade ogni 6 mesi.

L'account studente è normalmente nella forma "nome.cognome@studenti.unitn.it" (NB: non è l'indirizzo di e-mail, che può essere differente).
La password associata all'account studente ha le seguenti caratteristiche:

- deve avere lunghezza di 8 caratteri,
- deve contenere almeno un carattere non alfabetico,
- deve essere diversa dalla vecchia password,
- non prevede scadenza.

Eventuale presenza di credenziali multiple per la stessa persona

Ad ogni dottorando vengono rilasciati due account:

- l'account studente per l'accesso all'area studenti ESSE3 ed ai servizi rivolti agli studenti (es: aule didattiche)
- l'account di ateno per l'accesso all'area docenti di ESSE3 ed ai vari servizi rivolti ai docenti ed al personale che svolge attività di ricerca.

A breve la situazione verrà sanata utilizzando Shibboleth anche per l'accesso ad ESSE3.

Modalità di consegna delle credenziali

La consegna delle credenziali avviene contestualmente all'iscrizione ed alla relativa verifica dell'identità della persona.
Per mezzo di due appositi moduli, vengono consegnate due password random con obbligo di modifica immediato.
Gli uffici che possono rilasciare le nuove credenziali per i ruoli in oggetto sono:

- Ufficio dottorati

Modalità di recupero delle credenziali smarrite

Il recupero delle credenziali smarrite avviene in modo differenziati per i due account:

- account studente: presentandosi ai presidi didattici delle facoltà,
- account di ateno: presentandosi al presidio IT della propria sede di riferimento.

In ogni caso, viene consegnata, per mezzo di un apposito modulo, una password random con obbligo di modifica immediato.

Modalità di gestione smarrimento smartcard/token

Al momento non vengono rilasciati smarcard/token.

Durata dell'accreditamento

La durata dell'accreditamento corrisponde alla durata del ruolo da dottorando. Termina al conseguimento del titolo o all'abbandono.
Può comunque essere esteso, con un ruolo differente, nel caso il dottorando abbia altri incarichi, di didattica o di ricerca, rientrando in uno degli altri tipi di accreditamento descritti in questo documento.

Disabilitazione utente

La disabilitazione di ambedue gli account studente e di ateneo avviene al verificarsi di una o più delle seguenti condizioni:

- conseguimento titolo,
- abbandono

Cancellazione definitiva utente

La cancellazione definitiva di un account studente non è prevista, l'account viene disabilitato, ma lo studente può continuare ad utilizzarlo per accedere ai servizi offerti agli alumni.
Normalmente la cancellazione definitiva di un account di ateneo non è prevista, l'account viene disabilitato dopo la fine del rapporto tra persona ed ateneo, ma può essere riattivato all'instaurazione di un nuovo rapporto.

Rischi specifici associati alla categoria di utenti

I rischi associati a questa categoria sono principalmente:

1. l'impossibilità di accedere ai servizi a causa di problemi sull'infrastruttura di autenticazione,
2. il furto di identità.

Per quanto riguarda il punto 1, sono state prese misure sistemistiche per garantire un high availability adeguata.
Per quanto riguarda il punto 2, sono state prese alcune misure informatiche (comunicazioni criptate per il rilascio delle credenziali, complessità minima), procedurali (definizione di un processo preciso con requisiti minimi e formazione delle persone addette al rilascio delle password) e strutturali (utilizzo di un'unica credenziale per tutti i servizi: non serve più scrivere la password da qualche parte in quanto viene usata molto frequentemente, la password assume un valore tale, anche per la persona a cui viene assegnata, da garantirne un'accurata gestione personale).

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

Al momento non sono implementate credenziali forti in UNITN.

Accreditamento con inserimento diretto in ADA

Il processo

Il diagramma di ***Figura 7: Accreditamento diretto in ADA*** rappresenta le principali attività ed i principali attori coinvolti nella gestione delle identità, dei ruoli e degli account di ateneo delle persone le cui informazioni vengono inserite direttamente in ADA in quanto non presenti in alcun sistemi di business di UNITN.
Il processo è una specializzazione del processo di accreditamento sintetico descritto nel paragrafo Processo di accreditamento sintetico.
I ruoli a cui viene applicato questo processo sono quelli che in ***Tabella 1: Elenco dei ruoli degli utenti gestiti con affiliazione IDEM*** provengono dalle seguenti fonti:

- SEGRETERIE DI FACOLTA
- SEGRETERIE DI DIPARTIMENTO
- SEGRETERIE DI 1° LIVELLO
- ORGANI COLLEGIALI

Modalità di riconoscimento della persona

In questo tipo di accreditamento, l'identità digitale viene inserita direttamente in ADA. Il processo di accreditamento è stato quindi creato appositamente sulla base delle esigenze del sistema di identity management di UNITN.
Questo processo prevede l'espletamento delle attività attività A2 e A8 del processo sintetico di ***Figura 2: Processo di accreditamento sintetico***, di conseguenza nel diagramma di ***Figura 7: Accreditamento diretto in ADA*** sono previste le seguenti attività:

- A8: autorizzazione alla creazione del ruolo da parte di un responsabile di primo livello (Preside, Direttore di dipartimento, Dirigente, etc...) o di un suo delegato,
- A11: verifica identità della persona,
- A13: formalizzazione del rapporto (firma sul modulo di richiesta ruolo in ateneo).

Gli uffici preposti a queste attività sono tutte le segreterie di 1°livello dell'ateneo, in paricolare:

- Segreterie di facoltà,
- Segreterie di dipartimento,
- Segreterie di direzione,
- Segreterie dei centri interdipartimentali
- Ufficio organi collegiali

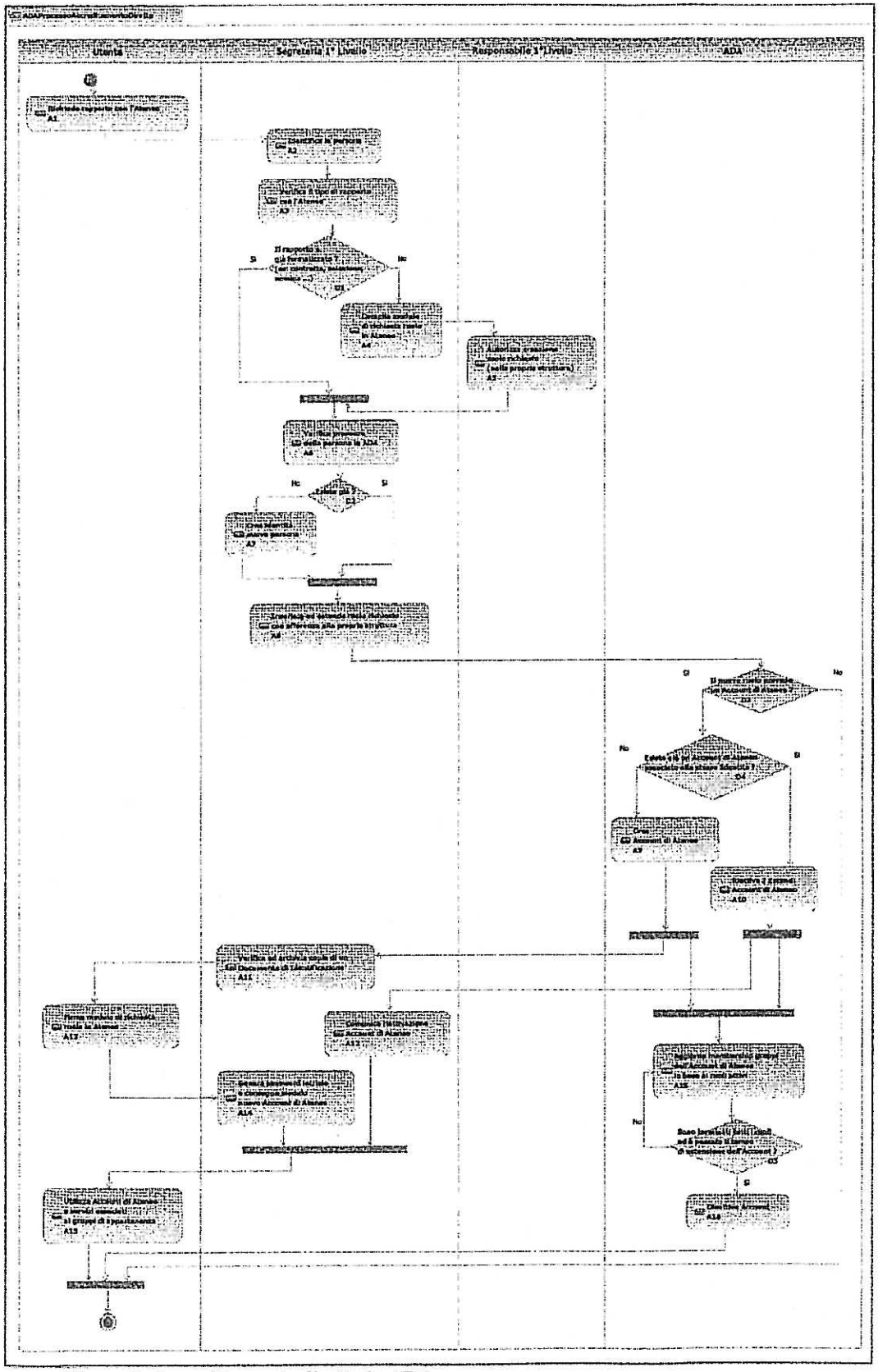

Figura 7: Accreditamento diretto in ADA

Caratteristiche dell'identità digitale

L'identità di una persona viene identificata sulla base di questi attributi (*dati identificativi minimi*):

- Nome
- Cognome
- Data di nascita
- Luogo di nascita
- Nazione di nascita
- Sesso

L'insieme di questi dati concorre ad identificare univocamente ogni persona censita in UNITN.
Ad ogni singola combinazione degli attributi precedentemente indicati (una persona) viene assegnato un codice (ID_ADA) alfanumerico che le rimarrà attribuito per sempre.

PPE-posizioni personali

Ad ogni persone vengono assegnati uno o più RUP-ruolo persona che, assieme al periodo di validità formano le PPE-posizioni personali.
In sintesi, le PPE-posizioni personali indicano che cosa una persona fa in UNITN e per quanto tempo.

POR-posizioni organizzative

Ad ogni PPE-posizione personale, vengono assegnati uno o più RUO-ruoli organizzativa ed una o più STO-struttura organizzativa, che assieme ad un periodo di validità, formano la POR-posizioni organizzative.
Alle POS-posizioni organizzative vengono associate anche le SED-sedi che indicano il luogo fisico prevalente in cui viene svolta l'attivita.
In sintesi, le POS-posizioni organizzative indicano dove una persona svolge la propria attività e con quale ruolo organizzativo (responsabile o afferente).
Ad ogni persona sono associati un Account di Ateno, un eventuale indirizzo e-mail ed un eventuale numero di telefono.
Tuttavia, nessuna di queste informazioni è da considerarsi pubblica, possono essere utilizzate solo per i fini istituzionali dell'Ateneo.
Indirizzo e-mail e numero di telefono sono consultabili solo attraverso il People di Ateneo.

Gestione del ciclo di vita

Tutti i ruoli inseriti in ADA prevedono un periodo di validità, le segreterie di primo livello, ed i relativi responsabili di primo livello, sono responsabili della corretta gestione del tipo e della durata dei ruoli inseriti.

Formato e regole delle credenziali

Le credenziali elettroniche che formano l'account di ateneo sono composte di username e password.
Ogni persona in questa categoria possiede un unico account di ateneo (fanno eccezione i Dottorandi, come descritto più avanti)
L'account di ateneo è normalmente nella forma "nome.cognome@unitn.it" (NB: non è l'indirizzo di e-mail, che può essere differente).
La password associata all'account di ateneo ha le seguenti caratteristiche:

- deve avere lunghezza minima di 8 caratteri,
- deve contenere almeno un carattere non alfabetico,
- deve essere diversa dalla vecchia password,
- scade ogni 6 mesi.

Eventuale presenza di credenziali multiple per la stessa persona

Viene rilasciato un unico account di ateneo ad ogni persona.

Modalità di consegna delle credenziali

La consegna delle credenziali avviene contestualmente ad una verifica dell'identità della persona tramite documento di riconoscimento.
Per mezzo di un apposito modulo, viene consegnata una password random con obbligo di modifica immediato.
Gli uffici che possono rilasciare le nuove credenziali per i ruoli in oggetto sono:

- Segreterie di facoltà,
- Segreterie di dipartimento,
- Segreterie di direzione,
- Segreterie dei centri interdipartimentali
- Ufficio organi collegiali

Modalità di recupero delle credenziali smarrite

Il recupero delle credenziali smarrite avviene presentandosi ai Presidi IT (presidi dei servizi informatici presenti nelle varie sedi dell'Ateneo).
Solo i Presidi IT possono re-inizializzare una password già rilasciata.
Anche in questo caso, viene consegnata, per mezzo di un apposito modulo, una password random con obbligo di modifica immediato.

Modalità di gestione smarrimento smartcard/token

Al momento non vengono rilasciati smarcard/token.

Durata dell'accreditamento

La durata dell'accreditamento è direttamente collegata al tipo e alla durata del rapporto tra la persona e UNITN, è definita dal periodo di validità della PPE-posizione personale assegnata che lo descrive.

Disabilitazione utente

La disabilitazione di un account di ateneo avviene automaticamente sulla base di due parametri:

- la data di fine del rapporto tra persona e UNITN (PPE-posizione personale),
- l'eventuale periodo di estensione previsto per il RUP-ruolo persona associato alla PPE-posizione personale.

Il periodo di estensione viene utilizzato permettere l'espletamento delle procedure di uscita dall'Ateneo.

Cancellazione definitiva utente

Normalmente la cancellazione definitiva di un account di ateneo non è prevista, l'account viene disabilitato dopo la fine del rapporto tra persona ed ateneo, ma può essere riattivato all'instaurazione di un nuovo rapporto.

Rischi specifici associati alla categoria di utenti

I rischi associati a questa categoria sono principalmente:

1. l'impossibilità di rilasciare un account di ateneo per problemi di formalizzazione del rapporto con l'Ateneo,
2. l'impossibilità di accedere ai servizi a causa di problemi sull'infrastruttura di autenticazione,
3. il furto di identità.

Per quanto riguarda il punto 1, è stata prevista la possibilità di inserire direttamente in ADA ruoli generici e temporanei (es: Ospite), che pur garantendo tutti i requisiti di identificazione e formalizzazione, prevedono delle procedure più snelle e veloci (è sufficiente la verifica dei documenti di riconoscimento e l'autorizzazione di un responsabile di primo livello, vedi modulo Allegato 1).
Per quanto riguarda il punto 2, sono state prese misure sistemistiche per garantire un high availability adeguata.
Per quanto riguarda il punto 3, sono state prese misure informatiche (comunicazioni criptate per il rilascio delle credenziali, complessità minima e scadenza frequente della password, log), procedurali (definizione di un processo preciso con requisiti minimi e formazione delle persone addette al rilascio delle password) e strutturali (utilizzo di un'unica credenziale per tutti i servizi: non serve più scrivere la password da qualche parte in quanto viene usata molto frequentemente, la password assume un valore tale, anche per la persona a cui viene assegnata, da garantirne un'accurata gestione personale).

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

Al momento non sono implementate credenziali forti in UNITN.

Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione delle identità ADA è la base per l'autenticazione ed il controllo accesso a gran parte i servizi informatici di Ateneo:

- rete wireless,
- risorse bibliotecarie,
- ESSE3,
- U-Gov,
- Portale di Ateneo,
- e-mail,
- aule studenti
- dominio Active Directory
- etc...

L'autenticazione avviene prevalentemente basandosi sui repository degli account alimentati e sincronizzati da ADA: OpenLdap e ActiveDirectory.
Lo username dell'account di ateneo (nella forma nome.cognome@untin.it) e dell'account studente (nella forma nome.cognome@studenti.untin.it) sono sempre univoci in un determinato istante di tempo.
Possono comunque essere modificati in qualsiasi momento e riassegnati a persone differenti.
Non possono quindi essere utilizzati per identificare in modo preciso e permanente una persona.
Per questi scopi sono disponibili degli ID alfanumerici progressivi assegnati direttamente da ADA alle persone ed agli account.
Il sistema di SSO interno è lo stesso utilizzato per l'accesso alla Federazione IDEM: Shibboleth, la durate delle sessioni è fissata in 30 min.

Partecipazione ad altre federazioni

Al momento non sono previste partecipazioni ad altre federazioni che coinvolgono account e ruoli coinvolti in IDEM.

Allegati

Allegato 1: modulo di autorizzazione inserimento nuova persona e nuovo ruolo in ADA

UNIVERSITÀ DEGLI STUDI DI TRENTO

Direzione Sistemi Informativi Servizi e Tecnologie Informatiche

RICHIESTA REGISTRAZIONE NELL'ANAGRAFICA DI ATENEO (ADA)

Ruoli richiedibili[1]:

- ☐ FACADD007-Titolare di borsa in ambito ricerca
- ☐ FACADD012-Visiting research professor
- ☐ FACADD008-Stagista della ricerca
- ☐ STUPGR004-Dottorando ospite
- ☐ PTAADD003-Stagista area TA
- ☐ PTAADD004-Altro personale TA
- ☐ OTHEXT003-Ospite
- ☐ _____

Periodo di validità del ruolo: dal* _____ al* _____

Con il presente modulo una persona, che per ruolo ricoperto in Ateneo ne ha diritto, (es. un docente responsabile di un progetto di ricerca) (di seguito richiedente) richiede l'inserimento di una persona (di seguito persona da inserire) nell'Anagrafica di Ateneo con uno dei ruoli sopra elencati (es. "OSPITE") associandola ad una struttura della quale è responsabile (es. progetto di ricerca). Con la sottoscrizione del presente modulo il richiedente si assume la responsabilità della correttezza dei dati forniti e dell'utilizzo dei servizi che derivano come conseguenza dell'inserimento di una persona nell'Anagrafica di Ateneo.

SCHEDA RICHIEDENTE: *(*) dati obbligatori*

COGNOME* _____ **NOME*** _____

SCHEDA PERSONA DA INSERIRE: *(*) dati obbligatori*

COGNOME* _____ **NOME*** _____
SESSO*: ☐ MASCHILE ☐ FEMMINILE
CODICE FISCALE: _____
NATO/A IL* ____ /____ /_____ **LUOGO DI NASCITA*** _____
PROVINCIA _____ **NAZIONE DI NASCITA*** _____

STRUTTURA nella quale si richiede l'inserimento _____
SEDE DI LAVORO*: città: _____ **via:** _____ **n°:** _____

ALLEGA: Fotocopia di un documento di identità

Data _____

Firma del richiedente
_____

Firma della persona da inserire
_____

Firma del responsabile di 1° livello **(preside, direttore di dipartimento, dirigente)**
(per approvazione in quanto responsabile dei servizi)
_____

Ai sensi del D.Lgs. 196/2003, si informa che i dati da Lei forniti verranno trattati esclusivamente per i fini istituzionali dell'Università degli Studi di Trento e in relazione ai conseguenti obblighi ad essi collegati, nel rispetto della normativa vigente.

[1] Alcuni ruoli sono attivabili solo in alcune tipologie di strutture organizzative (Facoltà, Dipartimento,Direzione, Centro, etc...).

Mod. reg_ADA v. 1.3.2