UNIVERSITÀ DEGLI STUDI
ROMA TRE

Area Telecomunicazioni

Documento descrittivo del processo di accreditamento degli utenti

Revisioni

Data	Versione	Descrizione modifica	Autore
03/04/2009	1.0	Bozza	Vincenzo Praturlon

Via Ostiense, 159
I-00154 Roma
Tel. +39.6.57332473
Fax +39.6.57332809
e-mail pitocchi@uniroma3.it

Abbreviazioni

ATC: Area Telecomunicazioni

ASI: Area Sistemi

AP: Area Personale

AS: Area Studenti

DPS: Divisione Politiche per gli Studenti

AD: Active Directory

CSA: Carriere e Stipendi Ateneo

ESSE3: Servizi e Segreteria Studenti

Gestore dell’accreditamento

La struttura di Ateneo responsabile del processo di accreditamento degli utenti è l'Area Sistemi Informativi (ASI).
L'assegnazione, il mantenimento e la cancellazione delle identità digitali vengono effettuate in sincronia (manuale o automatica) con la creazione di posizioni amministrative o utenze presso le altre strutture, in particolare in coordinamento con l'Area Personale (AP) e l'Area Studenti (AS)

Utenti gestiti

Di seguito sono elencati i profili identificati nell'Ateneo, con relativa categorizzazione e archivio sorgente (vedi sotto).

Tabella 1

Profilo	Categoria	Archivio sorgente
Personale docente (ordinari, associati, ricercatori)	Teacher	CSA
Collaboratori alla didattica	Teacher	CSA
Collaboratori alla ricerca	Teacher	CSA
Assegnisti di ricerca	Teacher	CSA
Assistente	Teacher	CSA
Cultore della materia	Teacher	CSA
Dirigente	Staff	CSA
Dirigente a contratto	Staff	CSA
Supervisori Scuole di Specializzazione	Staff	CSA
Personale tecnico/amministrativo/bibliotecari a tempo indeterminato/determinato	Staff	CSA
Dottorandi	Staff	CSA
Studenti iscritti ad un qualunque corso di studi	Student	ESSE3
Studenti iscritti a Master	Student	ESSE3
Studenti iscritti a Scuole di specializzazione	Student	ESSE3
Studenti laureati o diplomati	Alumn	ESSE3
Docenti a contratto	Teacher	AD
Collaboratori tecnico/amministrativi	Staff	AD
Collaboratori membri di commissioni	Staff	AD
Collaboratori coordinato continuativo	Staff	AD
Visitatori	Affiliate	AD
Operatori di Aziende	Affiliate	AD
Fornitore	Affiliate	AD
Paganti servizi bibliotecari	Affiliate	AD
Convegnisti	Affiliate	AD
Partecipanti a progetti di ricerca	Affiliate	AD
Volontario servizio civile nazionale	Affiliate	AD
Utenze associati a servizi	Service	AD
Dipendente pubblico di altre amministrazioni statali	Affiliate	AD
Dipendenti privati	Affiliate	AD
Professionisti	Affiliate	AD

Mappatura degli utenti sulle affiliazioni IDEM

Per ogni utente accreditato può essere popolato l'attributo eduPersonAffiliation con valori che ne caratterizzino il profilo organizzativo. Di seguito è riportata la corrispondenza tra le categorie sopra riportate e i valori dell' attributo.

Tabella 2

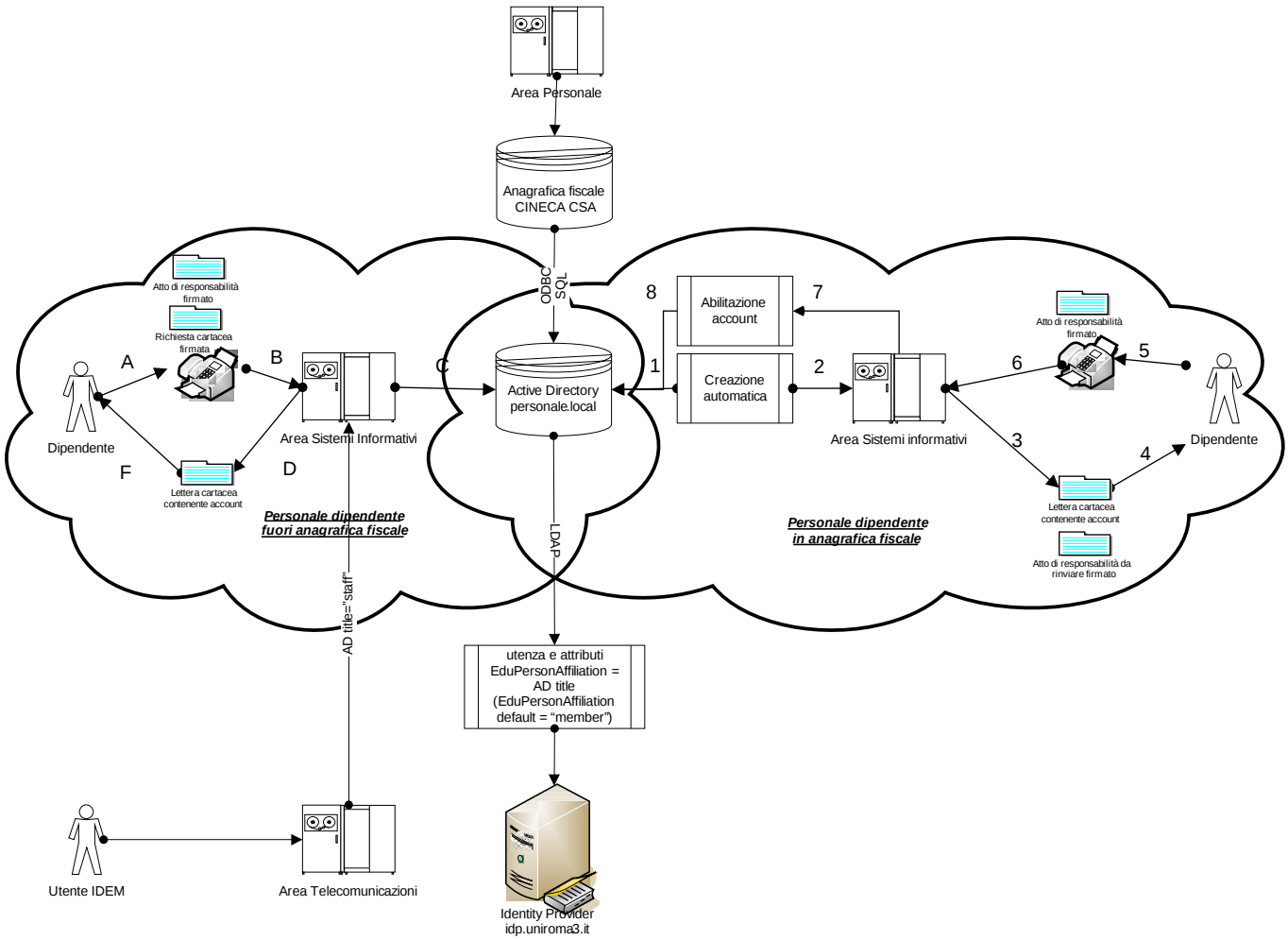
Categoria	Valori eduPerson Affiliation				
	member	staff	student	alumn	affiliate
Teacher	✓	✓			
Staff	✓	✓			
Student *	✓		✓		
Alumn *				✓	
Affiliate					✓
Service					✓

* N.B. categorie per le quali NON vengono rilasciate identità digitali federate (IDEM)

Visione di insieme del processo di accreditamento degli utenti

Il rilascio di identità digitali accreditate presso l'Ateneo è subordinata ad una serie di procedure amministrative, che convergono nella registrazione dell'utente nelle AD di dominio.
Nella AD vengono rappresentate le caratteristiche dell'utente, o via specifici attributi, o con l'afferenza a gruppi o unità organizzative. Queste caratteristiche possono essere associate direttamente, o tramite replica o elaborazione di archivi collegati (vedi Fig. 1).
Le AD sono quindi attualmente il repository autoritativo per le identità digitali accreditate presso l'Ateneo (utenze e attributi relativi).
L'Idp IDEM accede via LDAP a queste informazioni, le elabora, e le mappa agli attributi IDEM.

Figura 1



Il processo di accreditamento

Agli utenti vengono rilasciate credenziali presso l'Ateneo con due procedure distinte, a seconda che l'utente abbia già istaurato, o meno, dei rapporti formali con l'Amministrazione (assunzione, iscrizione, firma contratti e simili).

Nel primo caso la struttura responsabile del processo di accreditamento (ASI) delega la struttura responsabile della gestione del personale (AP) o degli studenti (AS) alla identificazione ed alla caratterizzazione dell'utente. In questo caso l'archivio sorgente, cioè l'archivio in cui vengono inizialmente riportati i dati utente (e che normalmente rimane autoritativo per la gestione dell'utente) è il CSA (per il personale) o l'ESSE3 (per gli studenti). Successivamente l'ASI provvede all'allineamento delle AD con gli archivi sorgenti.

Nel secondo caso l'ASI procede direttamente alla identificazione ed alla caratterizzazione dell'utente, tramite autocertificazioni integrate da controlli incrociati e verifiche a posteriori.
In questo caso l'archivio sorgente è l'AD di dominio personale.local (per il personale) o studenti.local (per gli studenti).

La profilatura dell'utente consente di rappresentare questa differenza, che tipicamente comporta la limitazione delle autorizzazioni (relative al servizio richiesto), fino alla eventuale formalizzazione del rapporto.

Poichè questa discriminazione viene fatta tecnicamente utilizzando delle interrogazioni agli archivi sorgenti, si possono creare delle situazioni in cui il rapporto formale è già stato instaurato (per esempio come da decorrenza di un contratto), ma i relativi riferimenti non sono ancora stati inseriti in negli archivi. In questi casi l'ASI procede di norma come se il rapporto non fosse in essere, fino alla registrazione negli archivi del rapporto.
Nel caso però l'utente abbia instaurato un rapporto formale, registrato in archivio, decaduto negli ultimi 12 mesi, è possibile richiedere che l'utenza venga temporaneamente riabilitata, con pari autorizzazioni, a discrezione dell'ASI.

Figura 2

Use Case
Accreditamento utenti
Università Roma TRE

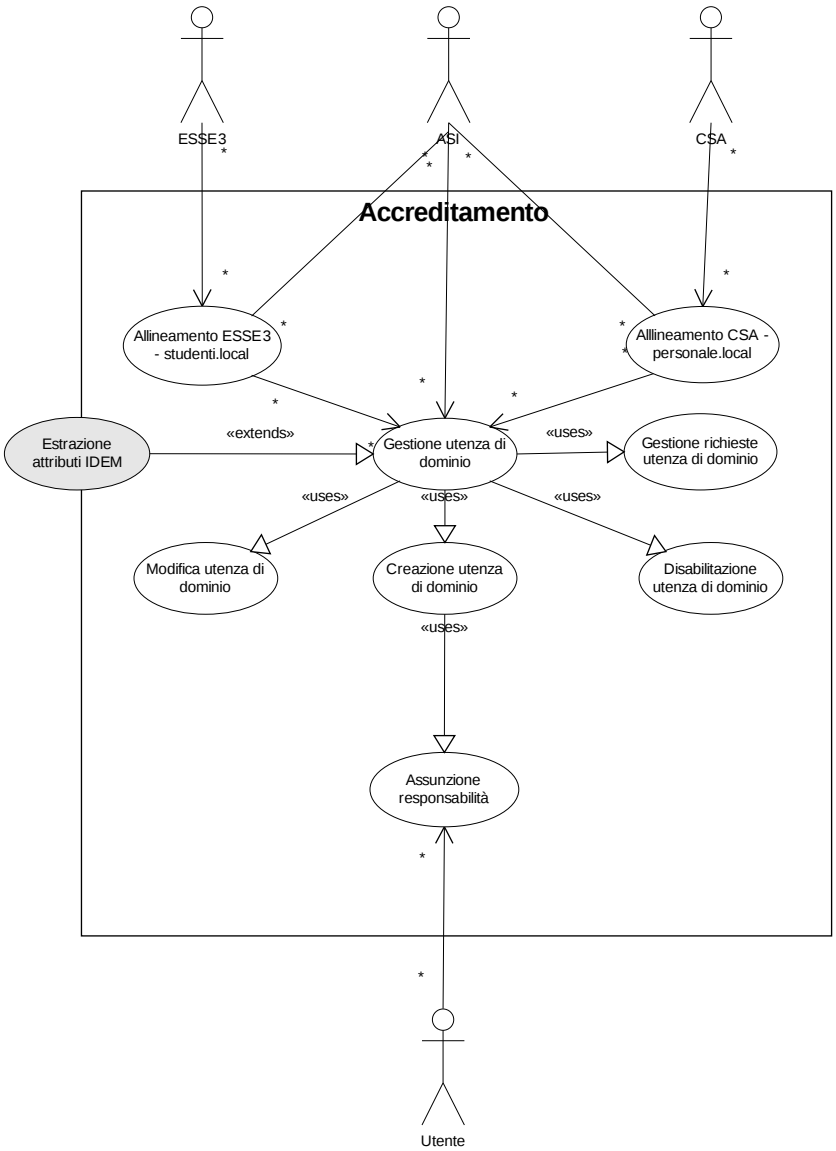
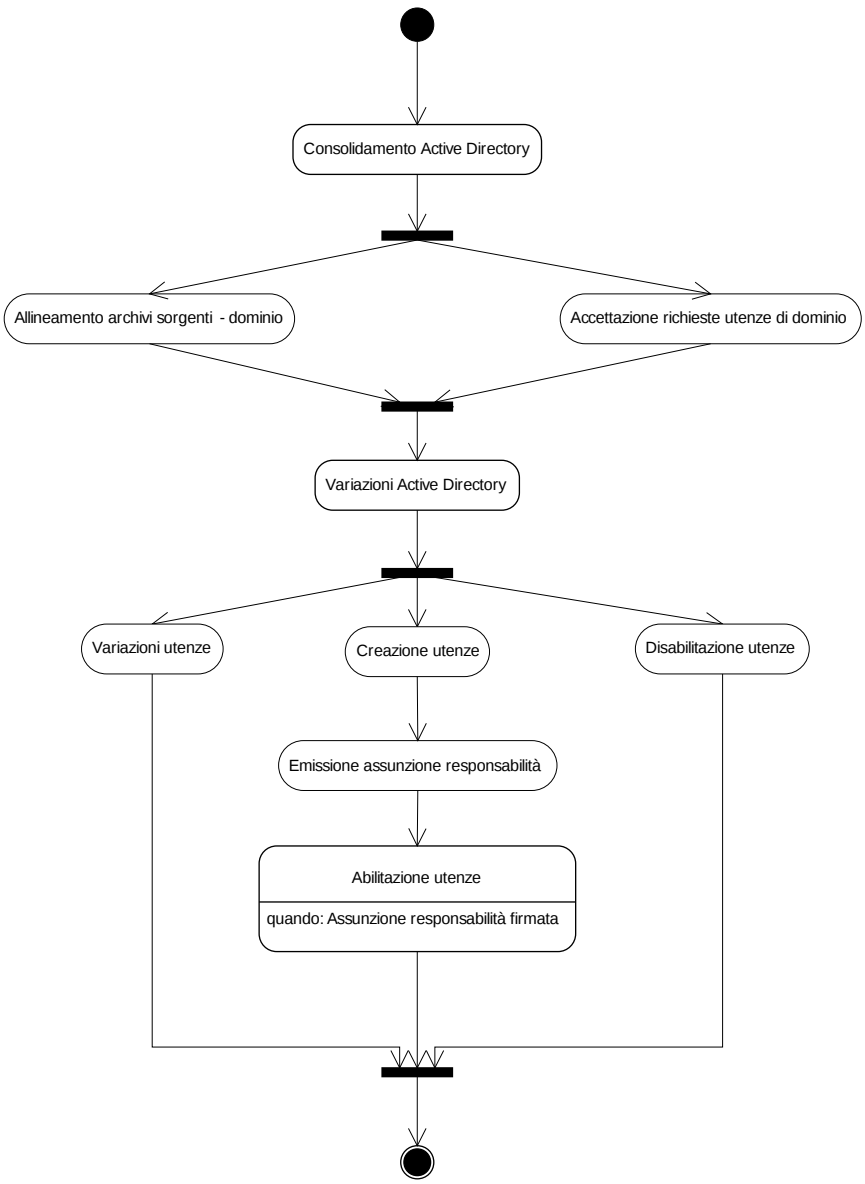


Figura 3

Activity
Accreditamento utenti
Università Roma TRE



Accreditamento utenti con archivio sorgente CSA / ESSE3

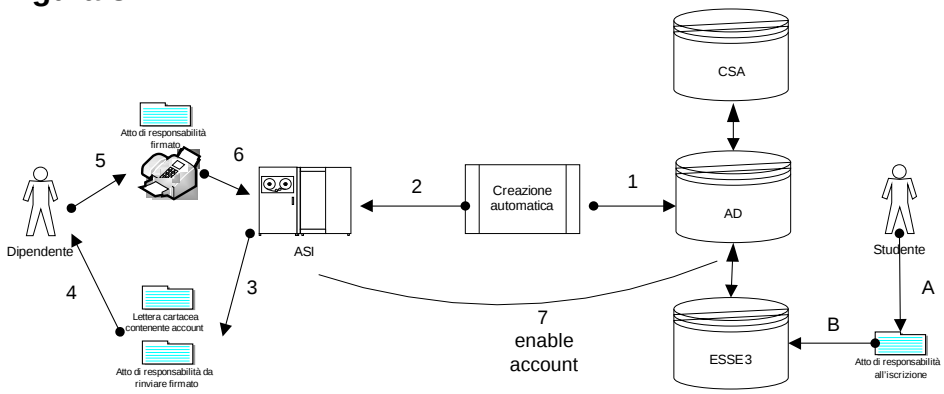
Di seguito viene illustrato il processo di accreditamento per i profili di utenti il cui archivio sorgente (come riportato in tabella 1) è CSA o ESSE3:

- *Personale docente (ordinari, associati, ricercatori)*
- *Collaboratori alla didattica*
- *Collaboratori alla ricerca*
- *Assegnisti di ricerca*
- *Assistente*
- *Cultore della materia*
- *Dirigente*
- *Dirigente a contratto*
- *Supervisori Scuole di Specializzazione*
- *Personale tecnico/amministrativo/bibliotecari a tempo indeterminato/determinato*
- *Dottorandi*
- *Studenti iscritti ad un qualunque corso di studi*
- *Studenti iscritti a Master*
- *Studenti iscritti a Scuole di specializzazione*
- *Studenti laureati o diplomati*

Il processo

Nel caso l'utente abbia un rapporto formale con l'amministrazione, la sua utenza di dominio verrà automaticamente generata sulla base di procedure giornaliere di allineamento con gli archivi sorgenti. L'abilitazione della utenza così generata è subordinata alla firma per accettazione di un atto di responsabilità, e sottoposta a verifiche successive.

Figura 3



Modalità di riconoscimento della persona

La persona viene riconosciuta faccia a faccia da dipendenti dell'Area Personale all'atto della formalizzazione del rapporto con l'ateneo.
In questa occasione vengono validati i dati pre-esistenti (p.e. fascicolo del concorso) con la presentazione di documenti originali (tra cui il documento di riconoscimento).
Contestualmente l'utente è tenuto a sottoscrivere una scheda informativa che viene inserita negli archivi di ateneo.

Rischi specifici associati alla categoria di utenti

Essendo il processo vincolato piuttosto rigidamente alle varie procedure amministrative interne, con i relativi tempi burocratici, è possibile che le utenze rilasciata non siano costantemente allineate con lo stato del rapporto formale con l'Ateneo.
In alcuni casi non è possibile (per esempio nel caso di un trasferimento), o è troppo complesso (per esempio nel caso di rapporti di durata molto limitata) definire a priori una scadenza realistica del rapporto, e l'utenza potrebbe rimanere erroneamente attiva per qualche tempo.

Accreditamento utenti con archivio sorgente AD

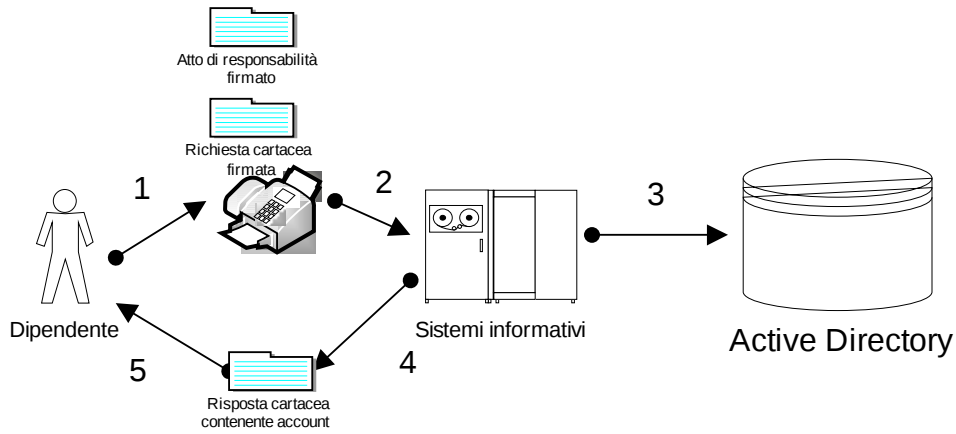
Di seguito viene illustrato il processo di accreditamento per i profili di utente il cui archivio sorgente (come riportato in tabella 1) è costituito dalle AD di dominio:

- *Docenti a contratto*
- *Collaboratori tecnico/amministrativi*
- *Collaboratori membri di commissioni*
- *Collaboratori coordinato continuativo*
- *Visitatori*
- *Operatori di Aziende*
- *Fornitore*
- *Paganti servizi bibliotecari*
- *Convegnisti*
- *Partecipanti a progetti di ricerca*
- *Volontario servizio civile nazionale*
- *Utenze associati a servizi*
- *Dipendente pubblico di altre amministrazioni statali*
- *Dipendenti privati*
- *Professionisti*

Il processo

Nel caso l'utente, all'atto di utilizzare un servizio di Ateneo, non risulti accreditato, può fare direttamente richiesta di rilascio delle credenziali di domino. La richiesta è subordinata alla firma per accettazione di un atto di responsabilità, e sottoposta a verifiche successive.

Figura 4



Modalità di riconoscimento della persona

Il richiedente non viene identificato di persona. La domanda deve essere però contro-firmata da un responsabile di struttura. L'ASI può a discrezione verificare direttamente, o tramite la struttura di afferenza, l'effettiva rispondenza degli estremi comunicati.

Rischi specifici associati alla categoria di utenti

Essendo il processo iniziato da una autocertificazione da parte del richiedente, esiste la possibilità di rilasciare credenziali a fronte di richieste contraffatte, o non veritiere.
Per mitigare il rischio complessivo, è prassi contattare la struttura del responsabile che contro-firma la richiesta, nel caso di anomalie o inconsistenze nella compilazione, richieste multiple, dubbia eligibilità del richiedente e simili.
Il numero contenuto di utenze di questo tipo permette comunque, di norma, di identificare in modo affidabile il richiedente. Inoltre spesso la richiesta è "attesa" (per esempio a seguito di concorsi l'ASI viene preventivamente avvisata dell'imminente arrivo di un lotto di richieste) ed eventuali richieste anomale verrebbero facilmente individuate.

Gestione delle utenze

Di seguito vengono illustrate le modalità di gestione ed il ciclo di vita delle utenze rilasciate.

Formato e regole delle credenziali

Il generale le credenziali vengono rilasciate all'utente in forma di nome utente e password.

Il nome utente è formato partendo dal nome e cognome nella forma ***n[o]cognome***
(la [o] rappresenta il secondo carattere del nome in caso di omonimia)

La complessità della password richiesta è di almeno 8 caratteri con almeno due delle tre condizioni vere:

- almeno un carattere speciale
- almeno un carattere numerico
- almeno un carattere maiuscolo

Le credenziali del tipo nome utente e password possono essere rilasciate senza scadenza, nel caso di rapporti di durata indeterminata.

Per alcune strutture (Amministrazione) l'Area Telecomunicazioni rilascia una SmartCard (Carta Multiservizi) con certificato digitale, abilitato per l'autenticazione, emesso dalla CA di Postecom.
La SmartCard certifica una utenza del tipo nome@personale.local.
Poichè i controller di dominio riconoscono Postecom come root CA attendibile, è possibile autenticarsi sulle postazioni in dominio via SmartLogon.
Il certificato emesso ha la durata di due anni.

Eventuale presenza di credenziali multiple per la stessa persona

Di norma le utenze di dominio sono univoche. Sporadicamente alcune persone vengono associate ad utenze multiple, per mantenere allineate le credenziali di specifici applicativi legacy (in via di dismissione), non integrabili con l'autenticazione di dominio.

Modalità di consegna delle credenziali

La comunicazione delle credenziali avviene in forma cartacea e tramite posta interna. In caso di particolare urgenza (cambio password) la password può essere comunicata tramite SMS, esclusivamente sul cellulare di servizio.

Modalità di recupero delle credenziali smarrite

Le password sono criptate e non possono in alcun caso essere recuperate, ma solo rigenerate.

Modalità di gestione smarrimento smartcard

In caso di smarrimento l'utente è tenuto a bloccare tempestivamente la carta utilizzando le procedure definite da Poste Italiane ed informare l'Area Telecomunicazioni.

Durata dell’accreditamento

La scadenza inizialmente rilasciata (salvo che per rapporti di durata indefinita) è pari a quella del rapporto (contratto o simili) dichiarato dal richiedente, e viene periodicamente allineata con il più recente dei rapporti in essere.

Disabilitazione utente

Le utenze vengono disabilitate 10 giorni dopo la cessazione del rapporto.
Si prevede in futuro di lasciare le utenze abilitate a vita, con privilegi minimi (per esempio con status affiliate o alumn), perchè l'Ateneo di fatto mantiene attivi alcuni servizi, come la posta elettronica, per molto tempo.

Cancellazione definitiva utente

Le utenze non vengono di norma cancellate.

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

Attualmente l'utente può utilizzare lo smartlogon via smartcard solo su postazioni in dominio.
Nel csao il certificato sia scaduto l'utente può comunque utilizzare nome utente e password.
Gli applicativi di Ateneo accettano solo nome utente e password.