# Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione Università degli Studi di Verona



*Le informazioni fornite in questo documento sono accurate alla data del 01/06/2012*

Revisioni....2
Nota introduttiva....2
Abbreviazioni....3
Gestore dell'accreditamento....4
Utenti gestiti....5
Profilo Identificativo....6
Profilo Identificativo per le CID Personale....6
Profilo Identificativo per le CID Studenti....7
Mappatura degli utenti sulle affiliazioni IDEM....8
Visione di insieme del processo di accreditamento degli utenti....8
Cicli di vita....9
Relazioni....10
Appartenenza, afferenza, incarichi....10
Il processo di accreditamento per il Personale Interno ed Esterno....11
Il processo....11
Modalità di riconoscimento della persona....11
Caratteristiche dell'identità digitale....11
Gestione del ciclo di vita....11
Formato e regole delle credenziali....11
Eventuale presenza di credenziali multiple per la stessa persona....12
Modalità di consegna delle credenziali....12
Modalità di recupero delle credenziali smarrite....12
Modalità di gestione smarrimento smartcard/token....12
Durata dell'accreditamento....12
Disabilitazione utente....12
Cancellazione definitiva utente....12
Rischi specifici associati alla categoria di utenti....12
Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)....12
Il processo di accreditamento per gli Studenti Iscritti....12
Creazione....12
Modifica....12
Profilo di Base....12
Profilo Applicativo....13
Variazione di stato....13
Cancellazione....13
Studenti Post-Lauream e Specializzandi....13
Creazione....13
Modifica....13
Profilo di Base....13
Profilo Applicativo....13
Variazione di stato....14
Cancellazione....14
Studenti Alumni....14
Creazione....14
Modifica....14
Profilo di Base....14
Profilo Applicativo....14
Variazione di stato....14
Cancellazione....14
Studenti in Limbo....14
Creazione....15
Modifica....15

Profilo di Base....15
Profilo Applicativo....15
Variazione di stato....15
Cancellazione....15
Personale Accademico, Dottorando, Dirigente e Tecnico-Amministrativo....15
Creazione....15
Modifica....16
Profilo di Base....16
Profilo Applicativo....16
Variazione di stato....16
Cancellazione....16
Sotto-Processi condivisi....16
Provisioning del Profilo di Base del Personale Interno....16
Gestione della password (dimenticata e di prima assegnazione)....17
Gestione della userID (dimenticata e di prima assegnazione)....18
Gestione della password (dimenticata e di prima assegnazione) in modalità self-service....19
Gestione della userID dimenticata in modalità self-service (TODO)....19
Modifica del Profilo Applicativo....20
Gestione automatica dello stato....21
Blocco Amministrativo....22
Il sistema di autenticazione e autorizzazione interno....22
Profilo Applicativo....22
Profili di base....24
Partecipazione ad altre federazioni....27

## Revisioni

| Data | Versione | Descrizione modifica | Autore |
|---|---|---|---|
| 03/04/2009 | 0.1 | Bozza | Roberto Gaffuri |
| 29/05/2009 | 0.2 | Bozza | MLM |
| 31/072009 | 0.3 | Rilasciato | MLM |
| 02/12/09 | 0.4 | Corretta la nota introduttiva sulla pubblicità del documento | RC |
| 01/06/12 | 0.5 | Lettura e correzione data | Anna Bianchi |

## 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

| Abbreviazione | Descrizione |
|---|---|
| Amministrazione (UniVR) | Università degli Studi di Verona |
| Gestione Identità di Ateneo (GIA) | Sistema informativo gestionale delle operazioni di accreditamento informatico |
| Risorsa Autorevole | Sistema informativo fonte dei dati per le operazioni di accreditamento informatico |
| Risorsa Provisonata | Sistema informativo destinatario delle operazioni di accreditamento informatico |
| Responsabile dell'Anagrafica | Responsabile ai sensi del Dlgs 196/2003 dell'identificazione e dell'autorizzazione all'accesso allo spazio informatico dell'Ateneo |
| Gestore di Identità | Responsabile interno a GIA ai sensi del Dlgs 196/2003 della gestione delle identità informatiche con privilegi definiti dal ruolo organizzativo |
| Classe di Identità (CID) | Identificativo di insieme di utenti che accedono nell'organizzazione UniVR da una stesso struttura organizzativa e sono poi gestiti attraverso un medesimo insieme di attività e flussi informativi |
| Sottoclasse di Identità (SID) | Identificativo di insieme di utenti appartenenti alla stessa CID e caratterizzati dallo stesso tipo di rapporto con Univr e quindi dallo stesso insieme di privilegi nello spazio informatico |
| Identità Virtuale (VID) | Associazione interna a GIA tra un utente e l'insieme di dati e credenziali disponibili presso le Risorse Autorevoli e le Risorse Provisionate |
| | |

## Gestore dell'accreditamento

L'Amministrazione provvede all'accreditamento informatico attraverso il sistema di Identity Management denominato GIA che permette la gestione automatica del ciclo di vita (creazione, modifica, disabilitazione) delle identità e delle credenziali elettroniche degli utenti.
Il processo di accreditamento degli utenti si basa sulla integrazione tra Risorse Autorevoli e Risorse Provisionate e su deleghe amministrative garantite dal sistema GIA.
Gli Utenti (persone) appartenenti ad una stessa Classe d'Identità, accedono all'organizzazione UniVR con accreditamento gestito da medesime strutture organizzative e medesimo insieme di attività e flussi informativi.
Gli Utenti (persone) appartenenti ad una stessa Sottoclasse d'Identità appartengono alla stessa Classe di Identità e sono caratterizzati dallo stesso tipo di rapporto con UniVR e quindi dallo stesso insieme di privilegi nello spazio informatico.
I processi di accreditamento sono distinti sulla base delle Classi di Identità mentre i contenuti dell'accreditamento sono gestiti sulla base delle Sottoclassi di Identità.
I Ruoli nella gestione delle identità e le responsabilità ai sensi del Dlgs 196/2003 sono definiti sulla base del posizione organizzativa e delle attribuzioni formali conseguenti sia di carattere collettivo che individuale.
Di seguito sono riportate in forma tabellare le informazioni relative ai Ruoli Amministrativi UniVR–GIA delle entità coinvolte nel processo di accreditamento e di gestione delle credenziali e alle relative responsabilità.

| Ruoli Amministrativi UniVR-GIA | |
|---|---|
| Responsabilità | Descrizione |
| Tecnico di Facoltà | Questo ruolo individua le responsabilità di verifica dell'identità ed attivazione del password reset per tutte le identità associabili alle Strutture Decentrate (in Fase 1 sono esclusi i Centri). |
| Tecnico SIA | Questo ruolo individua le responsabilità di verifica dell'identità ed attivazione del password reset per tutte le identità associabili alle Amministrazioni Centrali (in Fase 1 sono esclusi gli Organi e le Biblioteche). |
| Responsabile CDR | I responsabili dei CDR sono coinvolti in alcuni processi come quello relativo alla richiesta di accesso per un ospite o l'estensione dei privilegi di accesso. |
| Gestore GIA | Questo ruolo consente l'amministrazione di tutte le funzionalità del sistema GIA, ovvero corrisponde ad una sorta di super-utente. |
| Direzione GIA | A questo ruolo è associato un sottoinsieme delle capacità amministrative del GIA, soprattutto riferite alla gestione dei report e statistiche. |
| Responsabile Gestione Privilegi | Questo ruolo individua genericamente l'autorità nel fornire o revocare l'assegnazione di privilegi di accesso ad un particolare utente e dipende dal tipo di privilegio considerato.<br>Ad esempio nel caso del privilegio di accesso all'applicativo CIA (Contabilità Integrata di Ateneo), tale autorità sarà assegnata nell'ambito della Direzione Finanza e Contabilità. Nel GIA il ruolo in oggetto viene specializzato nelle seguenti responsabilità "Gestore Servizi FCO", "Gestore Servizi Protocollo" e "Gestore Servizi SIA". |
| Responsabile Anagrafica Personale | Responsabile Gestione Anagrafica Personale (definisce il ruolo amministrativo della figura professionale che assume la responsabilità della gestione dei dati anagrafici del Personale sia in fase di creazione che di modifica (ad esempio delle date di inizio/fine rapporto). |
| Responsabile Anagrafica Esterni | Responsabile Gestione Anagrafica Esterni (definisce il ruolo amministrativo della figura professionale che assume la responsabilità della gestione dei dati anagrafici degli Esterni sia in fase di creazione che di modifica (ad esempio delle date di inizio/fine rapporto). |
| Responsabile Anagrafica Studenti | Responsabile Gestione Anagrafica Studenti (definisce il ruolo amministrativo della figura professionale che assume la responsabilità della gestione dei dati anagrafici degli Studenti sia in fase di creazione che di modifica (ad esempio delle date di inizio/fine rapporto). |

Di seguito sono riportate in forma tabellare le informazioni relative ai Ruoli Utente UniVR–GIA gestiti nel processo di accreditamento.

| Ruoli Utente UniVR-GIA | | |
|---|---|---|
| Classe di Identità | Ruolo UniVR | Sorgente autoritativa |
| Studenti | Iscritti | Per questa classe le Risorse Autorevoli sono ESSE3 del Cineca (studenti Iscritti, In limbo, Alumni) e fino al 2011 è la vista GAS (Gestione Anagrafica Studenti) sul gestionale di backoffice SEGRE di UniVR (studenti Specializzandi e Post-Lauream) |

| Ruoli Utente UniVR-GIA | | |
|---|---|---|
| | Specializzandi | |
| | Post-Laurearn | |
| | Alumni | |
| | In limbo | |
| Personale | Accademici (Strutturati / Non Strutturati) | Per questa classe la Risorsa Autorevole è la vista GAP (Gestione Anagrafica Personale) sul gestionale di backoffice dbERW che gestisce i contenuti del Web Integrato di Ateneo nonché tutte le informazioni sull'offerta formativa e l'organizzazione |
| | Dottorandi | |
| | Tecnico-Amministrativi (Strutturati / Non Strutturati) | |
| Esterni | Consulenti&Fornitori | Per questa classe la Risorsa Autorevole è la vista GAE (Gestione Anagrafica Esterni) sul gestionale di backoffice dbERW che gestisce i contenuti del Web Integrato di Ateneo che gestisce tutte le informazioni sull'offerta formativa e l'organizzazione |
| | Ospedalieri | |
| | 150h | |
| Frequentatori | Ospiti | Per queste classe la Risorsa Autorevole è il sistema GIA stesso attraverso funzionalità delegate a Docenti, Responsabili di Anagrafica e Operatori di Biblioteca |
| | Congressisti | |
| | Studenti ospiti | |
| | Studenti frequentatori | |
| | Frequentatori biblioteca | |

## Utenti gestiti

Di seguito sono riportate in forma tabellare tutte le Classi e Sottoclassi di Identità UniVR gestite dai Responsabili di Anagrafica e gli ammnistratori GIA attraverso i gestionale delle Risorse Autorevoli e GIA.
Per ciascuna classe o sottoclasse distinta è indicato in colonna "Federazione IDEM" lo stato federativo previsto.

| Ruoli Utente UniVR-GIA | | |
|---|---|---|
| Classe d'Identità Utente (CID) | Sottoclasse di Identità (SID) | Federazione IDEM |
| Personale (CID-UTE-PER-GEN) | SID-UTE-PER-TAS (TA Strutturato) | Sì |
| | SID-UTE-PER-TAN (TA Non Strutturato) | Sì |
| | SID-UTE-PER-ACS (Accademico Strutturato) | Sì |
| | SID-UTE-PER-ACN (Accademico Non Strutturato) | Sì |
| | SID-UTE-PER-DIS (Dirigente Strutturato) | Sì |
| | SID-UTE-PER-DIN (Dirigente Non Strutturato) | Sì |
| | SID-UTE-PER-DOT (Dottorandi) | Sì |
| | SID-UTE-PER-GRA (In Grazia) | Sì |
| | SID-UTE-PER-GEN (da usare quando non si desidera precisare il SID) | Non pertinente |
| Studenti (CID-UTE-STU-GEN) | SID-UTE-STU-SPE (Studenti/Specializzandi) | Sì |
| | SID-UTE-STU-POS (Studenti/Post-Lauream) | Sì |
| | SID-UTE-STU-ISC (Studenti/Iscritti) | Sì |
| | SID-UTE-STU-ALU (Studenti/Alumni) | Sì |

| Ruoli Utente UniVR-GIA | | |
|---|---|---|
| | SID-UTE-STU-LMB (Studenti/In Limbo) | Sì |
| | SID-UTE-STU-GEN<br>(da usare quando non si desidera precisare il SID) | Non pertinente |
| Esterni/Ospedalieri Non Universitari<br>(CID-UTE-EST-HOS) | SID-UTE-EST-GEN<br>(da usare quando non si desidera precisare il CID) | NO |
| Esterni/Consulenti-Fornitori<br>(CID-UTE-EST-CON) | SID-UTE-EST-GEN<br>(da usare quando non si desidera precisare il CID) | NO |
| Esterni/150h<br>(CID-UTE-EST-150) | SID-UTE-EST-GEN<br>(da usare quando non si desidera precisare il CID) | NO |
| Frequentatori/Ospiti<br>(CID-UTE-FRE-OSP) | SID-UTE-FRE-GEN<br>(da usare quando non si desidera precisare il CID) | NO |
| Frequentatori/Biblioteca<br>(CID-UTE-FRE-BIB) | SID-UTE-FRE-GEN<br>(da usare quando non si desidera precisare il SID) | NO |
| Frequentatori/Congressisti<br>(CID-UTE-FRE-CNG) | SID-UTE-FRE-GEN<br>(da usare quando non si desidera precisare il CID) | NO |
| Frequentatori/Studenti ospiti<br>(CID-UTE-FRE-STO) | SID-UTE-FRE-GEN<br>(da usare quando non si desidera precisare il CID) | NO |
| Frequentatori/Studenti frequentatori<br>(CID-UTE-FRE-STF) | SID-UTE-FRE-GEN<br>(da usare quando non si desidera precisare il CID) | NO |

## Profilo Identificativo

Il Profilo Identificativo è costituito da un insieme di attributi d'identità che caratterizzano l'utente al punto di vista anagrafico ed organizzativo. Come descritto nei successivi capitoli, queste informazioni vengono rilevate dal GIA in modo automatico dalle varie sorgenti autoritative associate alle top-level CID. In altre parole il sistema GIA controlla costantemente le risorse (database) alle quali si appoggiano i vari sistemi di gestione anagrafica ed intercetta tutti gli eventi corrispondenti alla creazione o modifica delle identità presenti in questi contenitori.
In seguito alla rilevazione di un evento di creazione presso una anagrafica, il GIA provvede a leggerne i dati corrispondenti e a creare una VID i cui attributi d'identità di base sono valorizzati con i dati anagrafico-organizzativo ricevuti dall'anagrafica e presentati nell'interfaccia web esposta agli amministratori del GIA. Non tutti i dati provenienti dall'anagrafica vengono effettivamente utilizzati per comporre il Profilo Identificativo, in quanto i meta-dati di controllo non vengono presi in considerazione.
Nei paragrafi che seguono vengono descritti gli attributi del Profilo Identificativo per ciascuna delle classi d'identità.
NOTA
Essendo il contenuto del Profilo Identificativo controllato (remotamente) tramite le applicazioni di anagrafica previste per le varie CID Top-Level, ne consegue che il Profilo Identificativo può solo essere solo consultato e non modificato a livello di interfacce di amministrazione in GIA.

## *Profilo Identificativo per le CID Personale*

La sorgente autoritativa per gli utenti appartenenti alla CID Personale è costituita dal sistema GAP e gli attributi, provenienti da essa, che comporranno il Profilo Identificativo di questa classe d'identità, è riportato in tabella 1 (la lista è la stessa per tutte le SID).
Nel contesto del GIA il termine **"rapporto"** individua una relazione fra un soggetto ed UniVR nella quale il soggetto presta un servizio descritto da una qualifica presso una determinata struttura organizzativa in un determinato periodo di tempo. Internamente al GIA le caratteristiche del rapporto sono caratterizzate dalle seguenti corrispondenze:

- la qualifica corrisponde alla coppia di attributi CID, SID: a livello di GAP/GAE il Responsabile dei dati anagrafici specificherà una qualifica che poi verrà internamente mappata in una coppia CID, SID
- la struttura organizzativa verrà selezionata a livello di interfaccia GAP/GAE attraverso i nomi estesi delle varie strutture organizzative, mentre internamente verranno utilizzati i codici delle strutture organizzative descritti in allegato
- il periodo di tempo è caratterizzato da una data di inizio o di eventuale rinnovo ed una data di fine rapporto. Durante la creazione di un nuovo rapporto o del suo rinnovo, il Responsabile dei dati anagrafici dovrà specificare la data di inizio o di rinnovo del rapporto. Il sistema GIA, se la qualifica individua un rapporto di lavoro a tempo determinato, calcolerà in modo automatico la data di fine rapporto sommando alla data iniziale un valore di durata massima pre-definita per ogni tipologia di CID/SID.

| Nome attributo | Obbligatorio | Descrizione |
|---|---|---|
| Nome | SI' | Nome dell'utente |
| Cognome | SI' | Cognome dell'utente |

| Nome attributo | Obbligatorio | Descrizione |
|---|---|---|
| Sesso | SI' | M/F |
| AccountId | SI' | Attributo generato automaticamente dal GIA in accordo alle account policy e propagato alle risorse per la definizione degli account. |
| Password | SI' | Password, inizialmente definita dal GIA in accordo alle policy di gestione, e successivamente aggiornata dall'utente. |
| e-mail | SI' | L'indirizzo di email è generato automaticamente dal GIA |
| dataNascita | NO | Data di nascita dell'utente |
| codiceFiscale | SI' | Codice fiscale dell'utente. |
| Numero di Telefono | NO | Numero di telefono fisso dell'utente |
| Numero di Cellulare | NO | Numero di telefono mobile dell'utente |
| Numero di FAX | NO | Numero di FAX di riferimento per l'utente |
| Note | NO | Eventuali note |
| Numero di matricola | NO | Il numero di matricola è generato automaticamente dal GIA solamente per gli utenti che hanno stabilito con UniVR un rapporto subordinato (il tipo di rapporto di lavoro è implicito nella definizione delle qualifiche associate all'utente). |
| Rapporti | SI' | Lista dei rapporti (la definizione di rapporto è riportata nel seguito) che caratterizza il particolare utente di classe Personale. |

*Tabella 1: Profilo Identificativo Personale*

L'interfaccia grafica che consente la visualizzazione del profilo identificativo provvederà ad elencare tutti i rapporti dello specifico utente Personale e per ciascuno di essi visualizzerà la coppia CID/SID, la struttura organizzativa e la data di fine rapporto calcolata (solo per i rapporti a tempo determinato).
I rapporti visualizzati sono quelli attivi al momento della visualizzazione i quali possono essere in stato attivo o non attivo. I primi sono quelli la cui data di scadenza è successiva a quella attuale, mentre i secondi quelli la cui data di scadenza precede quella attuale.
I rapporti possono anche essere rimossi, ma solo tramite i sistemi GAP/GAE e in tale situazione il GIA rimuove all'utente i privilegi di visibilità o di accesso derivanti dal rapporto stesso.

## Profilo Identificativo per le CID Studenti

La sorgente autoritativa per gli utenti appartenenti alla CID Studenti è costituita dalla risorsa DB-Studenti e gli attributi, provenienti da essa, che comporranno il Profilo Identificativo di questa classe d'identità é riportato in tabella 2 (la lista è la stessa per tutte le eventuali sottoclassi).

| Nome attributo | Obbligatorio | Descrizione |
|---|---|---|
| Nome | SI' | Nome dell'utente |
| Cognome | SI' | Cognome dell'utente |
| AccountId | SI' | Attributo generato automaticamente da ESSE3 in accordo alle account policy per gli Studenti (algoritmo prefissato) e propagato alla risorsa LDAP-Studenti per la definizione dell'account. |
| Password | SI' | Password, inizialmente definita da ESSE3 in accordo alle policy di gestione, e successivamente aggiornata dall'utente studente. |
| Numero di matricola | SI' | Il numero di matricola dello studente. |
| Codice Fiscale | SI' | Codice Fiscale |
| Lista rapporti | SI' | Questa è una descrizione della storia della carriera dello studente. Il formato è stato definito in modo da uniformare il trattamento dello studente da parte di GIA in modo analogo con quanto effettuato per le altre classi di identitità trattate da GIA |
| Codice di Facoltà | SI' | Codice di Facoltà |
| Codice di Corso | SI' | Codice di Corso |
| Anno accademico | SI' | Anno accademico |

| Nome attributo | Obbligatorio | Descrizione |
|---|---|---|
| Anno di iscrizione | SI' | Anno di iscrizione |
| Codice di stato | SI' | Stato dello studente |

*Tabella 2: Profilo Identificativo Studenti*

## Mappatura degli utenti sulle affiliazioni IDEM

Di seguito sono indicate in forma tabellare le Affiliazioni IDEM previste per le CID e SID UniVR.

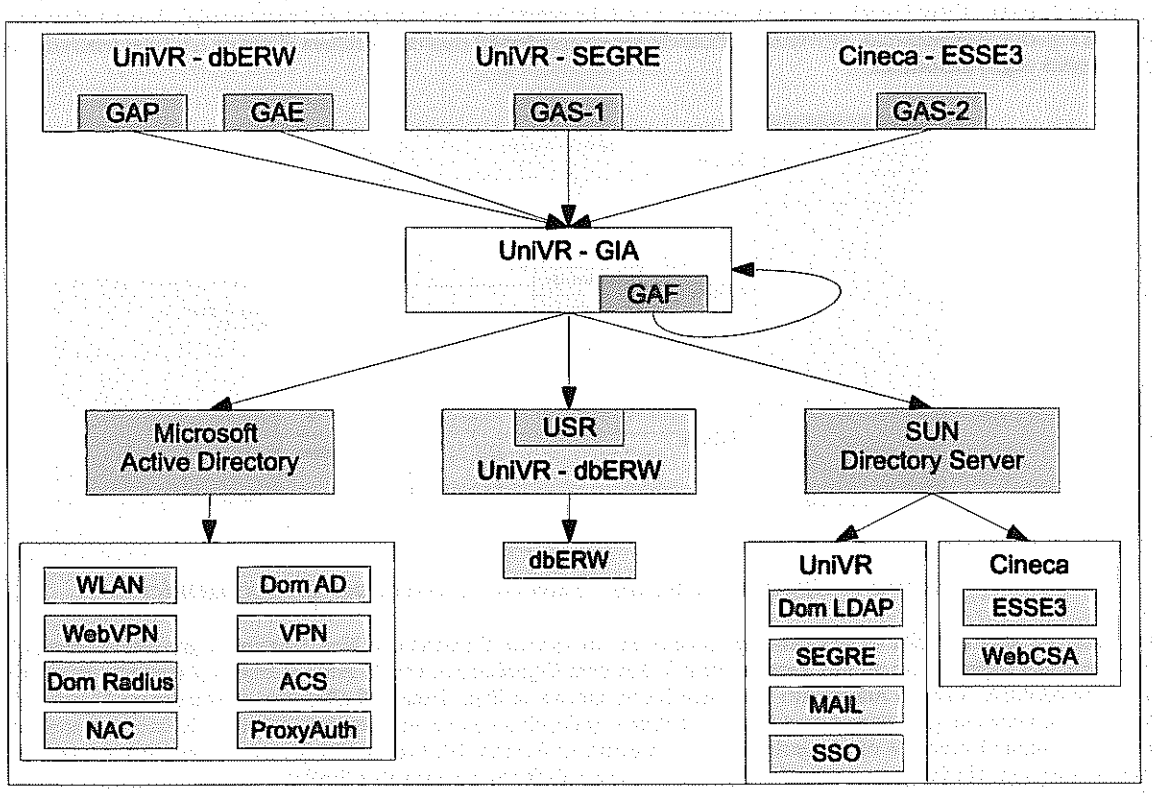
| Ruoli Utente UniVR-GIA | | |
|---|---|---|
| Classe d'Identità Utente (CID) | Sottoclasse di Identità (SID) | Affiliazione IDEM |
| Personale (CID-UTE-PER-GEN) | SID-UTE-PER-TAS (TA Strutturato) | Staff |
| | SID-UTE-PER-TAN (TA Non Strutturato) | Staff |
| | SID-UTE-PER-ACS (Accademico Strutturato) | Staff |
| | SID-UTE-PER-ACN (Accademico Non Strutturato) | Staff |
| | SID-UTE-PER-DIS (Dirigente Strutturato) | Staff |
| | SID-UTE-PER-DIN (Dirigente Non Strutturato) | Staff |
| | SID-UTE-PER-DOT (Dottorandi) | Staff |
| | SID-UTE-PER-GRA (In Grazia) | Staff |
| Studenti (CID-UTE-STU-GEN) | SID-UTE-STU-SPE (Studenti/Specializzandi) | Student |
| | SID-UTE-STU-POS (Studenti/Post-Lauream) | Student |
| | SID-UTE-STU-ISC (Studenti/Iscritti) | Student |
| | SID-UTE-STU-ALU (Studenti/Alumni) | Student |
| | SID-UTE-STU-LMB (Studenti/In Limbo) | Student |

## Visione di insieme del processo di accreditamento degli utenti

Di seguito sono rappresentati in forma grafica i processi di accreditamento per le CID di UniVR, i flussi informatici conseguenti e i punti di accesso allo spazio informatico da parte degli utenti.
Le componenti logiche sono le seguenti:

1. Applicativi di gestione anagrafica (in grigio-blu)
   a) UniVR – dbERW, gestionale del Web Integrato di Ateneo
   b) UniVR – SEGRE, gestionale della carriera studenti Specializzandi e Post-Lauream
   c) Cineca – ESSE3, gestionale della carriera degli studenti Iscritti a Lauree e Lauree Specialistiche
2. Applicativo di Gestione delle Identità di Ateneo UniVR-GIA (in giallo chiaro)
3. Moduli applicativi di gestione anagrafica (in blu)
   a) GAP - Personale Interno
   b) GAE - Personale Esterno
   c) GAS-1 - Studenti Specializzandi e Post Lauream
   d) GAS-2 - Studenti Iscritti
   e) GAF – Utenti Frequentatori
4. Risorse Provisionate (in arancio)
   a) Microsoft – Active Directory, Domini di Ateneo
   b) SUN -Directory Server, Infrastruttura Ldap di Ateneo
   c) UniVR – dbERW – USR, credenziali utenti backoffice del Web Integrato di Ateneo
5. Sistemi informativi accreditati (in verde chiaro)
   a) Dom AD, Foresta Active Directory di Ateneo
   b) Dom LDAP, Domini di autenticazione LDAP di Ateneo (Laboratori Informatici di Ateneo, Strutture decentrate accreditate)
   c) SEGRE, gestionale della carriera studenti Specializzandi e Post-Lauream

d) ESSE3, gestionale della carriera degli studenti Iscritti a Lauree e Lauree Specialistiche
e) MAIL, Servizio di Posta elettronica di Ateneo
f) WLAN, Rete Wireless di Ateneo
g) WebVPN e VPN, Accesso sicuro da remoto a rete UniVR
h) Dom Radius, Domini di Autenticazione RADIUS
i) ACS, Domini di Autenticaziuone CISCO ACS
j) ProxyAuth, Browsing autenticato
k) SSO, Servizio di autenticazione in SingleSignOn e Federata




## Cicli di vita

Di seguito vengono riportati i cicli di vita per le le Classi di Identità gestite da UniVR-GIA. Il ciclo di vita di una identità di tipo "utente" riguarda tutte le attività associate alla gestione delle identità informatiche (account) e che vengono eseguite quando una persona "entra" nell'organizzazione UniVR (creazione), quando le sue informazioni d'identità vengono aggiornate (modifica), quando la persona "esce" dall'organizzazione (cancellazione) ovvero interrompe i rapporti con essa.
In generale queste attività non sono tutte di tipo "informatico" e quindi la gestione del ciclo di vita viene descritta attraverso un processo o un insieme di processi, ovvero da attività e flussi informativi rispettivamente eseguite e scambiati fra attori di tipo diverso.
Nell'ambito dell'organizzazione UniVR e del gestionale GIA per ogni CID è individuato un ciclo di vita delle identità appartenenti che è composto dalle fasi di creazione, modifica e cancellazione, ciascuna delle quali è descritta da un processo:

1. il processo di creazione di una identità che rappresenta gli attori, i flussi e le attività che permettono di associare ad una Identità le credenziali informatiche e i privilegi necessari per svolgere le mansioni previste dal ruolo assunto dall'Utente quando essa entra nell'organizzazione UniVR; questa associazione viene stabilita inserendo alcune informazioni anagrafiche nel sistema GAP o GAE ed associando alla Virtual Identity un Profilo di Base che effettua il provisioning automatico degli account.
2. il processo di modifica di una identità di classe CID che rappresenta gli attori, i flussi e le attività che permettono di effettuare delle modifiche agli attributi della specifica Identità nelle evoluzioni di ruolo e privilegi dell'Utente nell'ambito di UniVR; queste modifiche possono essere relative al profilo di base (ad esempio l'unità organizzativa di appartenenza), al profilo applicativo (ad esempio i privilegi di accesso) oppure allo stato dell'identità, in particolare per quanto riguarda l'abilitazione o disabilitazione
3. il processo di cancellazione di una identità di classe CID che rappresenta gli attori, i flussi e le attività che permettono di interrompere il rapporto o i rapporti stabiliti fra lo specifico Utente e l'organizzazione UniVR

I paragrafi che seguono descrivono in dettaglio le relazioni tra strutture, responsabili e utenti e i processi implementati per la gestione delle Identità appartenenti alle CID.

## *Relazioni*

Questo paragrafo descrive alcune caratteristiche associabili ad alcune delle qualifiche individuate nella fase di assessment come le relazioni fra qualifiche e strutture organizzative oppure i rapporti di lavoro o retribuzione.

### Appartenenza, afferenza, incarichi

Le relazioni di appartenenza e afferenza caratterizzano alcune classi d'Identità e Strutture Organizzative, ovvero i Docenti / Ricercatori e Facoltà / Dipartimenti, e possono essere definite in generale come relazioni di "membership". Il class diagram UML riportato in Figura 1: Appartenenza, afferenza ed incarichi per gli accademici riporta la struttura di queste relazioni relativamente alla classe d'Identità degli Accademici:

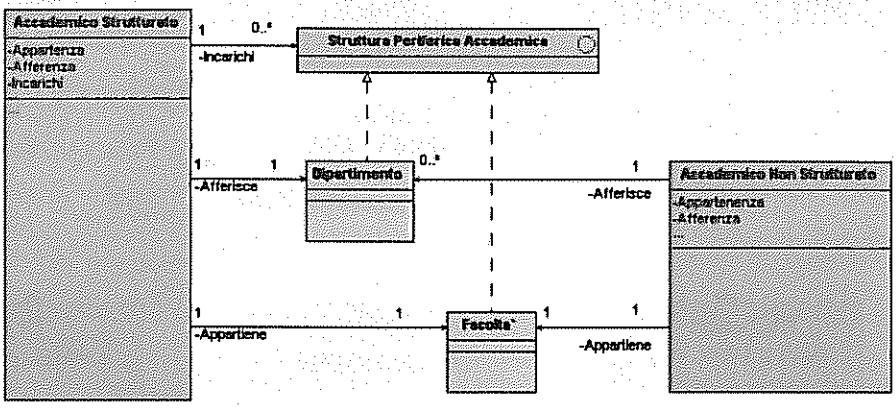



*Figura 1: Appartenenza, afferenza ed incarichi per gli accademici*

La relazione più forte è quella di appartenenza, ovvero un Accademico Strutturato o Non Strutturato (docente/ricercatore) deve almeno avere una appartenenza ad una Facoltà che è la Struttura Organizzativa con la quale si stipula il contratto in seguito alla vincita di un concorso. Tutti gli Accademici Strutturati hanno almeno un Dipartimento di afferenza, mentre per gli Accademici Non Strutturati (ad esempio un professore a contratto) l'afferenza è opzionale anche se estremamente comune e la facoltà di appartenenza è sempre la Struttura Decentrata con la quale si stipula in contratto formale. Gli Accademici Strutturati sono inoltre opzionalmente caratterizzati da incarichi di ricerca presso Dipartimenti o incarichi di docenza presso altre facoltà.
Simili relazioni possono essere individuate anche per la Qualifica di TA senza distinzione fra il contratto di tipo Strutturato e Non Strutturato e queste figure professionali sono presenti sia nelle Direzioni Centrali che nelle Strutture Decentrate.
Per i TA in carico presso le Direzioni Centrali, le relazioni sono quelle descritte in Figura 2: Appartenenza, afferenza ed incarichi per i TA: i TA appartengono ad una delle Direzioni Centrali le quali sono suddivise in Aree e queste sono ulteriormente suddivise in Unità Operative. Oltre all'appartenenza, il TA afferisce ad un'Area, ma ha incarichi (opzionali) presso uno delle Unità Operative che la compongono.

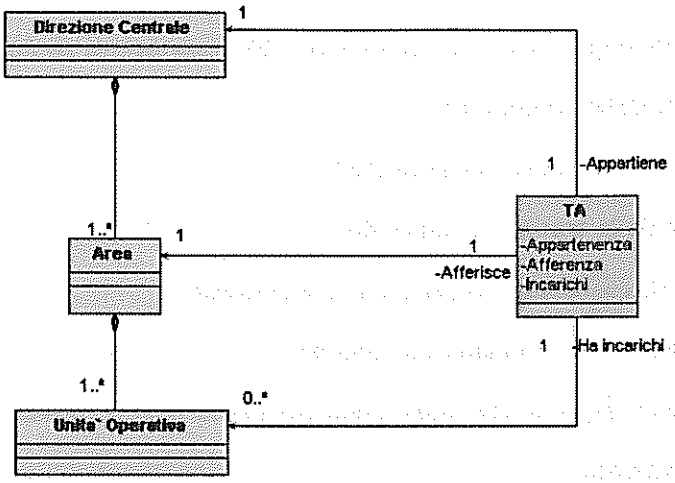



*Figura 2: Appartenenza, afferenza ed incarichi per i TA*

I TA in carico presso le Strutture Decentrate hanno, con esse, delle relazioni simili a quelle degli Accademici.

## *Il processo di accreditamento per il Personale Interno ed Esterno*

*[Dove si descrive in dettaglio il processo di accreditamento per una certa categoria. Questo capitolo è iterato per tutte le categorie significative. Il processo è ben descritto dai seguenti paragrafi...]*

### Il processo

*[Dove si rappresenta il processo in modo sintetico con gli attori coinvolti- Ideale usare un Activity Diagram UML]*

### Modalità di riconoscimento della persona

*[Dove si dice come avviene il riconoscimento della persona, cioè il processo amministrativo per attribuire una identità digitale che fa sì che per quella certa persona venga creato un record nel database delle identità digitali. Identificare gli uffici preposti (ad es. Segreteria studenti, Risorse Umane, Desk delle biblioteche, ecc...).*
*]*

### Caratteristiche dell'identità digitale

*[Dove si dice quali caratteristiche (attributi) vengono associate all'identità digitale che viene creata (ad es. nome, cognome, codice fiscale, matricola, emial, telefono, unità organizzativa di afferenza, ecc...]*

*[Quali delle caratteristiche/attributi possono essere considerati pubblici e vengono forniti a chiunque ne faccia richiesta?]*

### Gestione del ciclo di vita

*[Dove si dice come viene mantenuta aggiornata la situazione della persona nel database delle identità digitali in concomitanza di cambiamenti (es: cambio struttura, cambio corso, cambio ruolo, uscita, ...]*

### 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?*

### Eventuale presenza di credenziali multiple per la stessa persona

*[Dove si descrive se e perché vengono rilasciate credenziali diverse della stessa tipologia per la stessa persona]*

### Modalità di consegna delle credenziali

*[Dove si descrive come avviene la consegna delle credenziali]*

### Modalità di recupero delle credenziali smarrite

*[Dove si descrive come avviene la riconsegna della password se dimenticata]*

### Modalità di gestione smarrimento smartcard/token

*[Dove si descrive come avviene la gestione dell'eventuale smarrimento di una smartcard se utilizzata]*

### Durata dell'accreditamento

*[Dove si descrive la durata dell'accreditamento per la categoria in esame]*

### Disabilitazione utente

*[Dove si descrivono le modalità di disabilitazione - sincrone o asincrone con la scadenza dei contratti – degli utenti e dove si descrivono gli effetti delle disabilitazioni]*

### Cancellazione definitiva utente

*[Quando e come avviene la cancellazione definitiva di un utente]*

### Rischi specifici associati alla categoria di utenti

*[Dove si descrivono i rischi e i problemi associati a questa categoria e le misure in fase di attuazione per superare le criticità]*

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

*[Dove si descrive come interoperano eventuali credenziali forti e deboli associate alla persona]*

## *Il processo di accreditamento per gli Studenti Iscritti*

Questo paragrafo riporta la descrizione dei processi e dei workflow previsti per la gestione di una identità di sottoclasse Studenti Iscritti.

### Creazione

Le attività e i flussi informativi eseguiti dagli attori partecipanti al processo sono i seguenti[1]:

1. La gestione di tutti gli studenti iscritti a UniVR è di competenza della Direzione Studenti - Area Segreteria Studenti.
2. Tutte le informazioni relative allo stato dei vari studenti vengono gestite attraverso ESSE3. Un flusso informativo permette l'allineamento delle informazioni tra ESSE3 e GIA.
3. Tale flusso è automatizzato e gestisce l'intero ciclo di vita dello studente: creazione, modifica, aggiornamento, disabilitazione, abilitazione e cancellazione.

### Modifica

La modifica della identità dell'utente può essere relativa agli attributi che definiscono il suo profilo anagrafico, all'insieme di privilegi che definiscono l'estensione di profilo applicativo oppure allo stato dell'identità (abilitato o disabilitato). I paragrafi che seguono ne illustrano i dettagli.

### Profilo di Base

Come descritto in precedenza, il profilo di base viene selezionato in base alla CID e SID di appartenenza ed assegnato in modo automatico alla virtual identity nella fase di creazione. Le informazioni che fanno parte di questo profilo sono sotto il controllo del

---

1 I numeri associati a ciascun capoverso costituiscono solo un indicatore di sequenza nella descrizione del processo.

sistema di gestione anagrafica studenti ESSE3 (GS3), ovvero il sistema GIA intercetta il flusso informativo da esso generato e genera i corrispondenti flussi di provisioning verso le risorse.
La modifica delle informazioni del profilo in oggetto per gli Studenti Iscritti prevede le seguenti attività e flussi:

1. Il processo è avviato da Responsabili del procedimento della Segreteria Studenti
2. Il Responsabile del procedimento effettua le modifiche del profilo anagrafico e conferma la variazione (le invia al GS3). Possibili attributi che possono essere modificati sono: variazioni di stato carriera o variazioni anagrafiche.
3. Il sistema GS3 riceve i dati modificati e li memorizza nel proprio database.
4. Il sistema GIA intercetta la variazione ai dati del profilo anagrafico o di carriera e calcola le eventuali variazioni da applicare al profilo anagrafico di base ed al profilo applicativo di base.
5. Il GIA propaga quindi le variazioni dell'identità alle risorse coinvolte nel profilo. Questo significa che le variazioni del profilo applicativo di base potrebbero determinare l'aggiunta o la rimozione di account associati all'utente.

### Profilo Applicativo

Il processo di modifica del Profilo Applicativo, essendo in comune ad altri processi, è descritto in paragrafo successivo.

### Variazione di stato

Il processo di variazione dello stato di una identità, essendo in comune ad altri processi, è descritto in paragrafo successivo.

### Cancellazione

Come da requisiti, le identità degli utenti non possono mai essere cancellate dal sistema GIA e quindi il corrispondente processo non è definito.
Si noti comunque che, essendo lo stato delle identità controllato automaticamente dal GIA, quando un utente termina i servizi relativi ai vari rapporti stabiliti con UniVR, la corrispondente identità viene automaticamente[2] disabilitata.

## *Il processo di accreditamento per gli Studenti Post-Lauream e Specializzandi*

Questo paragrafo riporta la descrizione dei processi e dei workflow previsti per la gestione di una identità delle sottoclassi Studenti Post-Lauream e Specializzandi.

### Creazione

Le attività e i flussi informativi eseguiti dagli attori partecipanti al processo sono i seguenti[3]:

4. La gestione di tutti gli studenti iscritti a UniVR è di competenza della Direzione Studenti - Area Post-Lauream.
5. Tutte le informazioni relative allo stato dei vari studenti vengono gestite attraverso DB-Studenti (fino a migrazione al sistema GS3). Un flusso informativo permette l'allineamento delle informazioni tra DB-Studenti e GIA.
6. Tale flusso è automatizzato e gestisce l'intero ciclo di vita dello studente: creazione, modifica, aggiornamento, disabilitazione, abilitazione e cancellazione.

### Modifica

La modifica della identità dell'utente può essere relativa agli attributi che definiscono il suo profilo anagrafico, all'insieme di privilegi che definiscono l'estensione di profilo applicativo oppure allo stato dell'identità (abilitato o disabilitato). I paragrafi che seguono ne illustrano i dettagli.

### Profilo di Base

Come descritto in precedenza, il profilo di base viene selezionato in base alla CID e SID di appartenenza ed assegnato in modo automatico alla virtual identity nella fase di creazione. Le informazioni che fanno parte di questo profilo sono sotto il controllo del sistema di gestione anagrafica studenti DB-Studenti (GAS), ovvero il sistema GIA intercetta il flusso informativo da esso generato e genera i corrispondenti flussi di provisioning verso le risorse.
La modifica delle informazioni del profilo in oggetto per gli Studenti Iscritti prevede le seguenti attività e flussi:

1. Il processo è avviato da Responsabili del procedimento del Post-Lauream
2. Il Responsabile del procedimento effettua le modifiche del profilo anagrafico e conferma la variazione (le invia al GAS). Possibili attributi che possono essere modificati sono: variazioni di stato carriera o variazioni anagrafiche.
3. Il sistema GAS riceve i dati modificati e li memorizza nel proprio database.
4. Il sistema GIA intercetta la variazione ai dati del profilo anagrafico o di carriera e calcola le eventuali variazioni da applicare al profilo anagrafico di base ed al profilo applicativo di base.
5. Il GIA propaga quindi le variazioni dell'identità alle risorse coinvolte nel profilo. Questo significa che le variazioni del profilo applicativo di base potrebbero determinare l'aggiunta o la rimozione di account associati all'utente.

### Profilo Applicativo

Il processo di modifica del Profilo Applicativo, essendo in comune ad altri processi, è descritto in paragrafo successivo.

---

2 Si suppone ovviamente che, almeno per le CID di tipo Personale ed Esterni, i gestori delle anagrafiche GAP/GAE aggiornino correttamente le date di fine servizio per i vari rapporti.

3 I numeri associati a ciascun capoverso costituiscono solo un indicatore di sequenza nella descrizione del processo.

### Variazione di stato

Il processo di variazione dello stato di una identità, essendo in comune ad altri processi, è descritto in paragrafo successivo.

### Cancellazione

Come da requisiti, le identità degli utenti non possono mai essere cancellate dal sistema GIA e quindi il corrispondente processo non è definito.
Si noti comunque che, essendo lo stato delle identità controllato automaticamente dal GIA, quando un utente termina i servizi relativi ai vari rapporti stabiliti con UniVR, la corrispondente identità viene automaticamente[4] disabilitata.

## *Studenti Alumni*

Questo paragrafo riporta la descrizione dei processi e dei workflow previsti per la gestione di una identità di sottoclasse Studenti Alumni.

### Creazione

Una VID della sottoclasse Alumni viene generata per modifica di VID preesistente a seguito di variazione di stato da studente regolarmente iscritto a studente laureato.

### Modifica

La modifica della identità dell'utente può essere relativa agli attributi che definiscono il suo profilo anagrafico, all'insieme di privilegi che definiscono l'estensione di profilo applicativo oppure allo stato dell'identità (abilitato o disabilitato). I paragrafi che seguono ne illustrano i dettagli.

### Profilo di Base

Come descritto in precedenza, il profilo di base viene selezionato in base alla CID e SID di appartenenza ed assegnato in modo automatico alla virtual identity nella fase di creazione. Le informazioni che fanno parte di questo profilo sono sotto il controllo del sistema di gestione anagrafica studenti ESSE3 (GS3), ovvero il sistema GIA intercetta il flusso informativo da esso generato e genera i corrispondenti flussi di provisioning verso le risorse.
La modifica delle informazioni del profilo in oggetto per gli Studenti Iscritti prevede le seguenti attività e flussi:

6. Il processo è avviato da Responsabili del procedimento della Segreteria Studenti
7. Il Responsabile del procedimento effettua le modifiche del profilo anagrafico e conferma la variazione (le invia al GS3). Possibili attributi che possono essere modificati sono: variazioni di stato carriera o variazioni anagrafiche.
8. Il sistema GS3 riceve i dati modificati e li memorizza nel proprio database.
9. Il sistema GIA intercetta la variazione ai dati del profilo anagrafico o di carriera e calcola le eventuali variazioni da applicare al profilo anagrafico di base ed al profilo applicativo di base.
10. Il sistema GIA propaga quindi le variazioni dell'identità alle risorse coinvolte nel profilo. Questo significa che le variazioni del profilo applicativo di base potrebbero determinare l'aggiunta o la rimozione di account associati all'utente.

### Profilo Applicativo

Il processo di modifica del Profilo Applicativo, essendo in comune ad altri processi, è descritto nel paragrafo .

### Variazione di stato

Il processo di variazione dello stato di una identità, essendo in comune ad altri processi, è descritto nel paragrafo .

### Cancellazione

Come da requisiti [2], le identità degli utenti non possono mai essere cancellate dal sistema GIA e quindi il corrispondente processo non è definito.
Si noti comunque che, essendo lo stato delle identità controllato automaticamente dal GIA, quando un utente termina i servizi relativi ai vari rapporti stabiliti con UniVR, la corrispondente identità viene automaticamente[5] disabilitata.

## *Il processo di accreditamento per gli Studenti in Limbo*

Questo paragrafo riporta la descrizione dei processi e dei workflow previsti per la gestione di una identità di classe Studenti in Limbo.

---

4 Si suppone ovviamente che, almeno per le CID di tipo Personale ed Esterni, i gestori delle anagrafiche GAP/GAE aggiornino correttamente le date di fine servizio per i vari rapporti.

5 Si suppone ovviamente che, almeno per le CID di tipo Personale ed Esterni, i gestori delle anagrafiche GAP/GAE aggiornino correttamente le date di fine servizio per i vari rapporti.

### Creazione

Una VID della sottoclasse Limbo viene generata per modifica di VID preesistente a seguito di variazione di stato da studente disabilitato a studente in limbo.

### Modifica

La modifica della identità dell'utente può essere relativa agli attributi che definiscono il suo profilo anagrafico, all'insieme di privilegi che definiscono l'estensione di profilo applicativo oppure allo stato dell'identità (abilitato o disabilitato). I paragrafi che seguono ne illustrano i dettagli.

### Profilo di Base

Come descritto in precedenza, il profilo di base viene selezionato in base alla CID e SID di appartenenza ed assegnato in modo automatico alla virtual identity nella fase di creazione. Le informazioni che fanno parte di questo profilo sono sotto il controllo del sistema di gestione anagrafica studenti ESSE3 (GS3), ovvero il sistema GIA intercetta il flusso informativo da esso generato e genera i corrispondenti flussi di provisioning verso le risorse.
La modifica delle informazioni del profilo in oggetto per gli Studenti Iscritti prevede le seguenti attività e flussi:

11. Il processo è avviato da Responsabili del procedimento della Segreteria Studenti
12. Il Responsabile del procedimento effettua un Password Reset sull'anagrafica dello studente.
13. Il sistema GS3 riceve i dati modificati e li memorizza nel proprio database.
14. Il sistema GIA intercetta la variazione ai dati del profilo anagrafico o di carriera e calcola le eventuali variazioni da applicare al profilo anagrafico di base ed al profilo applicativo di base.
15. Il sistema GIA propaga quindi le variazioni dell'identità alle risorse coinvolte nel profilo. Questo significa che le variazioni del profilo applicativo di base potrebbero determinare l'aggiunta o la rimozione di account associati all'utente.

### Profilo Applicativo

Il processo di modifica del Profilo Applicativo, essendo in comune ad altri processi, è descritto nel paragrafo .

### Variazione di stato

Il processo di variazione dello stato di una identità, essendo in comune ad altri processi, è descritto nel paragrafo .

### Cancellazione

Come da requisiti [2], le identità degli utenti non possono mai essere cancellate dal sistema GIA e quindi il corrispondente processo non è definito.
Si noti comunque che, essendo lo stato delle identità controllato automaticamente dal GIA, quando un utente termina i servizi relativi ai vari rapporti stabiliti con UniVR, la corrispondente identità viene automaticamente[6] disabilitata.

## *Il processo di accreditamento per il Personale Accademico, Dottorando, Dirigente e Tecnico-Amministrativo*

Questo paragrafo riporta la descrizione dei processi e dei workflow previsti per la gestione di una identità delle sottoclassi del Personale Accademico, Dottorando, Dirigente e Tecnico-Amministrativo, Strutturato e Non strutturato.

### Creazione

Le attività e i flussi informativi eseguiti dagli attori partecipanti al processo sono i seguenti[7]:

1. Il processo viene avviato quando, nell'ambito di una generica struttura organizzativa di Amministrazione Centrale (SAC) o di Struttura Decentrata (SDE) nasce l'esigenza accreditare all'accesso alle risorse IT di UniVR Utenti delle sottoclassi considerate
2. Il processo è svolto direttamente dal Responsabile CDR (ADM-RSP-CDR) ai sesnsi del Dlgs 196/2003 oppure il Gestore GIA (ADM-GES-GIA) a seguito di assegnazione di incarico o ruolo all'utente da parte di UniVR, oppure da personale delegato al ruolo di Responsabile della Gestione Anagrafica del Personale (ADM-RSP-GAP) in servizio presso la segreteria della generica struttura organizzativa (GEN-SAC-SEG oppure GEN-SDE-SEG).
3. Quando il Responsabile GAP riceve la richiesta, verifica se essa si riferisce al profilo anagrafico di un Utente già presente in GAP. In caso positivo verifica ed eventualmente aggiorna i dati del profilo, viceversa crea un nuovo profilo anagrafico in accordo alla definizione del profilo utente definito in precedenza. Il Responsabile GAP conferma la variazione o l'inserimento del profilo e si pone in attesa della mail di conferma della creazione dell'account generata dal Sistema GIA.
4. Quando il Sistema GAP riceve il profilo anagrafico, esso viene memorizzato nel proprio database interno.
5. Il Sistema GIA intercetta il nuovo profilo anagrafico inserito nel database ed avvia il sotto-processo di Provisioning del Profilo di Base per il Personale. I dettagli di questo sotto-processo sono riportati in paragrafo successivoErrore: sorgente del riferimento non trovata.

---

6 Si suppone ovviamente che, almeno per le CID di tipo Personale ed Esterni, i gestori delle anagrafiche GAP/GAE aggiornino correttamente le date di fine servizio per i vari rapporti.

7 I numeri associati a ciascun capoverso costituiscono solo un indicatore di sequenza nella descrizione del processo.

6. Il sotto-processo di provisioning invia una mail al Responsabile GAP con i dati della VID appena creata, tra i quali l'accountId. Il Responsabile GAP invia al richiedente una notifica di conferma dell'operazione e quindi comunica direttamente all'utente interessato l'accountId, necessario per il completamento dell'assegnazione della prima password.
7. Il Tecnico di Facoltà o SIA di gestirà questa classe di utenti indipendentemente dalla loro struttura di destinazione.
8. Dopo aver ricevuto la conferma della richiesta, il ruolo richiedente può eventualmente avviare la procedura di modifica della Estensione di Profilo Applicativo, ad esempio per estendere l'insieme dei privilegi di accesso (vedi paragrafo ).
9. Quando l'Utenteprende servizio presso la struttura SAC o SDE, esso deve prima presentarsi presso il Tecnico di Facoltà o SIA per l'assegnazione della prima password. La procedura di gestione della password è sempre la stessa ed i dettagli sono riportati nel paragrafo .

### Modifica

La modifica della identità dell'utente può essere relativa agli attributi che definiscono il suo profilo anagrafico, all'insieme di privilegi che definiscono l'estensione di profilo applicativo oppure allo stato dell'identità (abilitato o disabilitato). I paragrafi che seguono ne illustrano i dettagli.

### Profilo di Base

Come descritto in precedenza, il profilo di base viene selezionato in base alla CID e SID di appartenenza ed assegnato in modo automatico alla virtual identity nella fase di creazione. Le informazioni che fanno parte di questo profilo sono sotto il controllo del sistema di gestione anagrafica personale (GAP), ovvero il sistema GIA intercetta il flusso informativo da esso generato e genera i corrispondenti flussi di provisioning verso le risorse.
La modifica delle informazioni del profilo in oggetto per il TA Strutturato prevede le seguenti attività e flussi:

1. Il processo è avviato dal Responsabile CDR o il Responsabile GAP attraverso il sistema di gestione anagrafica corrispondente.
2. Il Responsabile CDR/GAP effettua le modifiche del profilo anagrafico e conferma la variazione (le invia al GAP). Possibili attributi che possono essere modificati sono: aggiunta o rimozione di un rapporto, variazione di un rapporto (es. struttura organizzativa, qualifica o data di inizio e fine) o variazioni anagrafiche.
3. Il sistema GAP riceve i dati modificati e li memorizza nel proprio database.
4. Il sistema GIA intercetta la variazione ai dati del profilo anagrafico/organizzativo e calcola le eventuali variazioni da applicare al profilo anagrafico di base ed al profilo applicativo di base.
5. Il GIA propaga quindi le variazioni dell'identità alle risorse coinvolte nel profilo. Questo significa che le variazioni del profilo applicativo di base potrebbero determinare l'aggiunta o la rimozione di account associati all'utente.
6. Infine il sistema GIA invia, come conferma, una notifica via mail al Responsabile GAP che ha effettuato la variazione determinando la terminazione del processo.

### Profilo Applicativo

Il processo di modifica del Profilo Applicativo, essendo in comune ad altri processi, è descritto nel paragrafo .

### Variazione di stato

Il processo di variazione dello stato di una identità, essendo in comune ad altri processi, è descritto nel paragrafo .

### Cancellazione

Come da requisiti [2], le identità degli utenti non possono mai essere cancellate dal sistema GIA e quindi il corrispondente processo non è definito.
Si noti comunque che, essendo lo stato delle identità controllato automaticamente dal GIA, quando un utente termina i servizi relativi ai vari rapporti stabiliti con UniVR, la corrispondente identità viene automaticamente[8] disabilitata.

## *Sotto-Processi condivisi di gestione dell'accreditamento*

Questo paragrafo riunisce alcuni sotto-processi e workflow utilizzati da molti dei processi di Gestione delle Identità.

### Provisioning del Profilo di Base del Personale Interno

Questo sotto-processo, essendo eseguito completamente dal sistema GIA, è in realtà un workflow eseguito nel contesto del prodotto GIA. Le attività eseguite da tale workflow sono di seguito riportate:

1. Dopo aver intercettato il flusso di inserimento dell'utente nel database del sistema GAP, il GIA legge le informazioni anagrafiche dell'utente quali nome, cognome, strutture organizzative presso le quali l'utente svolge dei servizi e la coppia [CID, SID]. Con queste informazioni il GIA provvede a creare la Identità Virtuale nel contenitore delle VID di pertinenza, identificato sulla base della CID e/o della struttura di appartenenza. La VID viene inizialmente creata con una password casuale al fine di impedire all'utente di accedere al sistema prima di aver completato la richiesta iniziale della password di accesso.
2. In funzione dei parametri CID e SID, viene individuato l'IM-Role che definisce il Profilo di Base per la specifica classe d'identità alla quale l'utente appartiene

8 Si suppone ovviamente che, almeno per le CID di tipo Personale ed Esterni, i gestori delle anagrafiche GAP/GAE aggiornino correttamente le date di fine servizio per i vari rapporti.

3. Sempre in funzione dei parametri CID e SID, ma anche sulla base di altre informazioni quali le strutture organizzative di servizio, viene quindi elaborato il profilo applicativo di base che prevede le eventuali restrizioni di autorizzazione nei servizi di directory sulla base delle strutture di appartenenza
4. Dopo aver elaborato i profili con gli opportuni valori degli attributi d'identità, il sistema GIA avvia in parallelo le attività di user provisioning vere e proprie, ovvero provvede alla creazione degli account (identità informatiche) presso le risorse previste dal profilo di base che per le identità di classe Personale sono costituite da:
   4.1. Servizi di directory AD ed LDAP del Personale con l'accesso di base ai servizi di rete
   4.2. Servizi di posta elettronica
   4.3. Account per l'accesso all'applicazione in dbERW
   4.4. Se il tipo di contratto stabilito fra l'utente ed UniVR è di tipo subordinato, allora viene creato un account anche presso l'applicazione di Gestione delle Presenze al fine di consentire il tracciamento delle presenze tramite badge
5. Al termine il workflow genera automaticamente due notifiche in forma di email:
   5.1. Una indirizzata ai responsabili Anagrafica Personale (ADM-RSP-GAP) e contenente un messaggio di conferma dell'avvenuto inserimento, ma soprattutto l'accountId da comunicare all'utente creato
   5.2. Una indirizzata al Tecnico SIA (ADM-TEC-SIA) o Tecnico di Facoltà (ADM-TEC-FAC) per segnalare l'arrivo del nuovo utente e consentire l'avvio della procedura di assegnazione della password. Se un utente ha stabilito rapporti con più di una Facoltà o Dipartimento, il Tecnico di Facoltà considerato è quello associato alla "Facoltà Primaria" (quella identificata come tale in dbERW).
   Ovviamente nel corso del processo di provisioning automatico la password casuale, inizialmente definita per la VID, viene propagata a tutte e risorse previste dal profilo di base e quindi l'utente è in possesso dell'accountId, ma non potrà mai accedere ai servizi di rete o applicativi prima di aver completato la fase di gestione della password.

## Gestione della password (dimenticata e di prima assegnazione)

Il termine "gestione della password" indica le procedure da attuare sia nella fase di prima assegnazione della password ad un nuovo utente, sia nella fase in cui un utente ha dimenticato la password associata al proprio accountId (userid/login) ed ha quindi la necessità di ripristinare l'accesso al sistema GIA ed ai servizi e applicazioni. In realtà i due scenari "assegnazione prima password" e "password dimenticata" individuano la stessa situazione e pertanto le corrispondenti gestioni vengono consolidate in un unico sotto-processo.
Di seguito sono riportate le attività ed i flussi informativi eseguite e scambiati rispettivamente fra gli attori del sotto-processo che sono rappresentati da un generico utente (CID-UTE-PER-GEN), il sistema GIA (SIS-GIA) ed il Tecnico di Facoltà (ADM-TEC-FAC) oppure il Tecnico SIA (ADM-TEC-SIA):

1. Il sotto-processo viene avviato dall'utente in corrispondenza di due situazioni (eventi):
   1.1. L'utente ha preso servizio ed ha ricevuto (oggetto BPMN "AND gateway" - vedi allegato) l'accountId, ovvero la stringa che rappresenta l'identificatore per la login ai sistemi
   1.2. L'utente ha dimenticato la password e deve ripristinare l'accesso ai sistemi

   In entrambi i casi l'utente è in possesso dell'accountId, ma non conosce la password per completare la procedura di autenticazione.
2. Tramite un qualsiasi web browser, l'utente accede al sistema GIA la cui pagina iniziale consente di accedere, ovviamente in modalità anonima, ai due servizi "Richiesta password di primo accesso" e "Password dimenticata". I due servizi sono sostanzialmente identici e si differenziano internamente solo per flussi informativi diversi. L'utente, in funzione del contesto nel quale si trova, seleziona uno dei due servizi di Gestione Password.
3. In seguito alla richiesta dell'utente, il sistema GIA avvia un workflow di gestione che presenta all'utente un modulo di richiesta informazioni tra le quali, l'accountId necessario per identificarlo. Per i dettagli delle informazioni raccolte fare riferimento allo use case corrispondente.
4. L'utente compila il modulo di richiesta e conferma l'inserimento al GIA che accetta la richiesta dell'utente.
5. Il GIA effettua un controllo sull'accountId che deve corrispondere ad un utente esistente nel sistema. Questo controllo permette anche di limitare le eventuali "richieste spam" in quanto nel caso di utente inesistente il processo termina immediatamente dopo aver visualizzato a video un messaggio di errore.
6. Se la richiesta dell'utente è relativa alla password dimenticata, il sistema GIA invia una notifica al Tecnico SIA o di Facoltà per segnalare che un utente si presenterà per le operazioni di identificazione.
7. Proseguendo nel workflow, il sistema GIA genera internamente una password iniziale "IPWD" ed un identificatore sequenziale ("Forgotten Password ID" - FPID) che identifica la richiesta inoltrata dall'utente. Queste due informazioni sono visualizzate all'utente il quale viene quindi invitato dal sistema a confermare il proseguimento della richiesta di gestione password. L'utente deve prendere nota sia della IPWD che del FPID perché verranno in seguito utilizzate dalla procedura.
8. Il sistema GIA visualizza quindi un modulo riassuntivo di tutti i parametri della richiesta, con la sola esclusione della password. Il workflow si sospende in attesa di un evento di approvazione che dovrà essere invocato da parte del Tecnico SIA o di Facoltà.
9. L'utente deve stampare il modulo riassuntivo e presentarsi fisicamente al Tecnico SIA o di Facoltà per effettuare le operazioni di identificazione. In alternativa alla presenza fisica è possibile prevedere un invio del modulo di richiesta via FAX congiuntamente ad una fotocopia di un documento di riconoscimento.
10. Quando l'utente di presenta presso il Tecnico SIA o di Facoltà, quest'ultimo verifica la presenza della mail di notifica ricevuta in un apposito account funzionale e la corrispondenza dell'identificatore di richiesta FPID e procede con la verifica del documento d'identità.
11. In caso di anomalia il processo termina immediatamente e richiede una gestione manuale. Lo stesso comportamento viene assunto se il Tecnico decide di non approvare la richiesta.

12. Se a valle delle verifiche il Tecnico SIA o di Facoltà decide di approvare la richiesta, il Tecnico si collega al sistema GIA, individua la richiesta di approvazione attraverso l'identificatore FPID, effettua l'operazione di approvazione e conferma l'operazione all'utente.
13. L'evento di approvazione viene ricevuto dal sistema GIA il quale riprende l'esecuzione del workflow di controllo della procedura effettuando una forma speciale di password reset dell'accountId che prevede la generazione di password casuale per gli account associati alla VID, ma l'assegnazione della password IPWD all'account del GIA. In questo modo l'utente non puó accedere alle risorse, ma può accedere al GIA per avviare la procedura di aggiornamento della password.
14. L'utente, dopo aver ricevuto la conferma dal Tecnico SIA o di Facoltà deve accedere al sistema GIA tramite un qualsiasi web browser ed utilizzare, come credenziali, la coppia [accountId, IPWD]
15. A questo punto il GIA autentica l'utente e, poiché l'accountId è in stato di reset, forza l'utente ad aggiornare la propria password.
16. Il processo si conclude definitivamente in uno stato in cui l'utente è stato identificato, come richiesto dalla normativa, ed è in possesso di credenziali che nemmeno nelle fasi transitorie della procedura sono a conoscenza degli amministratori.

## Gestione della userID (dimenticata e di prima assegnazione)

1. Ll termine "gestione della password" indica le procedure da attuare sia nella fase di prima assegnazione della password ad un nuovo utente, sia nella fase in cui un utente ha dimenticato la password associata al proprio accountId (userid/login) ed ha quindi la necessità di ripristinare l'accesso al sistema GIA ed ai servizi e applicazioni. In realtà i due scenari "assegnazione prima password" e "password dimenticata" individuano la stessa situazione e pertanto le corrispondenti gestioni vengono consolidate in un unico sotto-processo.
2. Di seguito sono riportate le attività ed i flussi informativi eseguite e scambiati rispettivamente fra gli attori del sotto-processo che sono rappresentati da un generico utente (CID-UTE-PER-GEN), il sistema GIA (SIS-GIA) ed il Tecnico di Facoltà (ADM-TEC-FAC) oppure il Tecnico SIA (ADM-TEC-SIA):
3. Il sotto-processo viene avviato dall'utente in corrispondenza di due situazioni (eventi):
   3.1. L'utente ha preso servizio ed ha ricevuto (oggetto BPMN "AND gateway" - vedi allegato) l'accountId, ovvero la stringa che rappresenta l'identificatore per la login ai sistemi
   3.2. L'utente ha dimenticato la password e deve ripristinare l'accesso ai sistemi
4. In entrambi i casi l'utente è in possesso dell'accountId, ma non conosce la password per completare la procedura di autenticazione.
5. Tramite un qualsiasi web browser, l'utente accede al sistema GIA la cui pagina iniziale consente di accedere, ovviamente in modalità anonima, ai due servizi "Richiesta password di primo accesso" e "Password dimenticata". I due servizi sono sostanzialmente identici e si differenziano internamente solo per flussi informativi diversi. L'utente, in funzione del contesto nel quale si trova, seleziona uno dei due servizi di Gestione Password.
6. In seguito alla richiesta dell'utente, il sistema GIA avvia un workflow di gestione che presenta all'utente un modulo di richiesta informazioni tra le quali, l'accountId necessario per identificarlo. Per i dettagli delle informazioni raccolte fare riferimento allo use case corrispondente.
7. L'utente compila il modulo di richiesta e conferma l'inserimento al GIA che accetta la richiesta dell'utente.
8. Il GIA effettua un controllo sull'accountId che deve corrispondere ad un utente esistente nel sistema. Questo controllo permette anche di limitare le eventuali "richieste spam" in quanto nel caso di utente inesistente il processo termina immediatamente dopo aver visualizzato a video un messaggio di errore.
9. Se la richiesta dell'utente è relativa alla password dimenticata, il sistema GIA invia una notifica al Tecnico SIA o di Facoltà per segnalare che un utente si presenterà per le operazioni di identificazione.
10. Proseguendo nel workflow, il sistema GIA genera internamente una password iniziale "IPWD" ed un identificatore sequenziale ("Forgotten Password ID" - FPID) che identifica la richiesta inoltrata dall'utente. Queste due informazioni sono visualizzate all'utente il quale viene quindi invitato dal sistema a confermare il proseguimento della richiesta di gestione password. L'utente deve prendere nota sia della IPWD che del FPID perché verranno in seguito utilizzate dalla procedura.
11. Il sistema GIA visualizza quindi un modulo riassuntivo di tutti i parametri della richiesta, con la sola esclusione della password. Il workflow si sospende in attesa di un evento di approvazione che dovrà essere invocato da parte del Tecnico SIA o di Facoltà.
12. L'utente deve stampare il modulo riassuntivo e presentarsi fisicamente al Tecnico SIA o di Facoltà per effettuare le operazioni di identificazione. In alternativa alla presenza fisica è possibile prevedere un invio del modulo di richiesta via FAX congiuntamente ad una fotocopia di un documento di riconoscimento.
13. Quando l'utente di presenta presso il Tecnico SIA o di Facoltà, quest'ultimo verifica la presenza della mail di notifica ricevuta in un apposito account funzionale e la corrispondenza dell'identificatore di richiesta FPID e procede con la verifica del documento d'identità.
14. In caso di anomalia il processo termina immediatamente e richiede una gestione manuale. Lo stesso comportamento viene assunto se il Tecnico decide di non approvare la richiesta.
15. Se a valle delle verifiche il Tecnico SIA o di Facoltà decide di approvare la richiesta, il Tecnico si collega al sistema GIA, individua la richiesta di approvazione attraverso l'identificatore FPID, effettua l'operazione di approvazione e conferma l'operazione all'utente.
16. L'evento di approvazione viene ricevuto dal sistema GIA il quale riprende l'esecuzione del workflow di controllo della procedura effettuando una forma speciale di password reset dell'accountId che prevede la generazione di password casuale per gli account associati alla VID, ma l'assegnazione della password IPWD all'account del GIA. In questo modo l'utente non puó accedere alle risorse, ma può accedere al GIA per avviare la procedura di aggiornamento della password.
17. L'utente, dopo aver ricevuto la conferma dal Tecnico SIA o di Facoltà deve accedere al sistema GIA tramite un qualsiasi web browser ed utilizzare, come credenziali, la coppia [accountId, IPWD]

18. A questo punto il GIA autentica l'utente e, poiché l'accountId è in stato di reset, forza l'utente ad aggiornare la propria password.
19. Il processo si conclude definitivamente in uno stato in cui l'utente è stato identificato, come richiesto dalla normativa, ed è in possesso di credenziali che nemmeno nelle fasi transitorie della procedura sono a conoscenza degli amministratori.

## Gestione della password (dimenticata e di prima assegnazione) in modalità self-service

1. Il termine "gestione della password" indica le procedure da attuare sia nella fase di prima assegnazione della password ad un nuovo utente, sia nella fase in cui un utente ha dimenticato la password associata al proprio accountId (userid/login) ed ha quindi la necessità di ripristinare l'accesso al sistema GIA ed ai servizi e applicazioni. In realtà i due scenari "assegnazione prima password" e "password dimenticata" individuano la stessa situazione e pertanto le corrispondenti gestioni vengono consolidate in un unico sotto-processo.
2. Di seguito sono riportate le attività ed i flussi informativi eseguite e scambiati rispettivamente fra gli attori del sotto-processo che sono rappresentati da un generico utente (CID-UTE-PER-GEN), il sistema GIA (SIS-GIA) ed il Tecnico di Facoltà (ADM-TEC-FAC) oppure il Tecnico SIA (ADM-TEC-SIA):
3. Il sotto-processo viene avviato dall'utente in corrispondenza di due situazioni (eventi):
   3.1. L'utente ha preso servizio ed ha ricevuto (oggetto BPMN "AND gateway" - vedi allegato) l'accountId, ovvero la stringa che rappresenta l'identificatore per la login ai sistemi
   3.2. L'utente ha dimenticato la password e deve ripristinare l'accesso ai sistemi
4. In entrambi i casi l'utente è in possesso dell'accountId, ma non conosce la password per completare la procedura di autenticazione.
5. Tramite un qualsiasi web browser, l'utente accede al sistema GIA la cui pagina iniziale consente di accedere, ovviamente in modalità anonima, ai due servizi "Richiesta password di primo accesso" e "Password dimenticata". I due servizi sono sostanzialmente identici e si differenziano internamente solo per flussi informativi diversi. L'utente, in funzione del contesto nel quale si trova, seleziona uno dei due servizi di Gestione Password.
6. In seguito alla richiesta dell'utente, il sistema GIA avvia un workflow di gestione che presenta all'utente un modulo di richiesta informazioni tra le quali, l'accountId necessario per identificarlo. Per i dettagli delle informazioni raccolte fare riferimento allo use case corrispondente.
7. L'utente compila il modulo di richiesta e conferma l'inserimento al GIA che accetta la richiesta dell'utente.
8. Il GIA effettua un controllo sull'accountId che deve corrispondere ad un utente esistente nel sistema. Questo controllo permette anche di limitare le eventuali "richieste spam" in quanto nel caso di utente inesistente il processo termina immediatamente dopo aver visualizzato a video un messaggio di errore.
9. Se la richiesta dell'utente è relativa alla password dimenticata, il sistema GIA invia una notifica al Tecnico SIA o di Facoltà per segnalare che un utente si presenterà per le operazioni di identificazione.
10. Proseguendo nel workflow, il sistema GIA genera internamente una password iniziale "IPWD" ed un identificatore sequenziale ("Forgotten Password ID" - FPID) che identifica la richiesta inoltrata dall'utente. Queste due informazioni sono visualizzate all'utente il quale viene quindi invitato dal sistema a confermare il proseguimento della richiesta di gestione password. L'utente deve prendere nota sia della IPWD che del FPID perché verranno in seguito utilizzate dalla procedura.
11. Il sistema GIA visualizza quindi un modulo riassuntivo di tutti i parametri della richiesta, con la sola esclusione della password. Il workflow si sospende in attesa di un evento di approvazione che dovrà essere invocato da parte del Tecnico SIA o di Facoltà.
12. L'utente deve stampare il modulo riassuntivo e presentarsi fisicamente al Tecnico SIA o di Facoltà per effettuare le operazioni di identificazione. In alternativa alla presenza fisica è possibile prevedere un invio del modulo di richiesta via FAX congiuntamente ad una fotocopia di un documento di riconoscimento.
13. Quando l'utente di presenta presso il Tecnico SIA o di Facoltà, quest'ultimo verifica la presenza della mail di notifica ricevuta in un apposito account funzionale e la corrispondenza dell'identificatore di richiesta FPID e procede con la verifica del documento d'identità.
14. In caso di anomalia il processo termina immediatamente e richiede una gestione manuale. Lo stesso comportamento viene assunto se il Tecnico decide di non approvare la richiesta.
15. Se a valle delle verifiche il Tecnico SIA o di Facoltà decide di approvare la richiesta, il Tecnico si collega al sistema GIA, individua la richiesta di approvazione attraverso l'identificatore FPID, effettua l'operazione di approvazione e conferma l'operazione all'utente.
16. L'evento di approvazione viene ricevuto dal sistema GIA il quale riprende l'esecuzione del workflow di controllo della procedura effettuando una forma speciale di password reset dell'accountId che prevede la generazione di password casuale per gli account associati alla VID, ma l'assegnazione della password IPWD all'account del GIA. In questo modo l'utente non puó accedere alle risorse, ma può accedere al GIA per avviare la procedura di aggiornamento della password.
17. L'utente, dopo aver ricevuto la conferma dal Tecnico SIA o di Facoltà deve accedere al sistema GIA tramite un qualsiasi web browser ed utilizzare, come credenziali, la coppia [accountId, IPWD]
18. A questo punto il GIA autentica l'utente e, poiché l'accountId è in stato di reset, forza l'utente ad aggiornare la propria password.
19. Il processo si conclude definitivamente in uno stato in cui l'utente è stato identificato, come richiesto dalla normativa, ed è in possesso di credenziali che nemmeno nelle fasi transitorie della procedura sono a conoscenza degli amministratori.

## Gestione della userID dimenticata in modalità self-service (TODO)

1. Il termine "gestione della password" indica le procedure da attuare sia nella fase di prima assegnazione della password ad un nuovo utente, sia nella fase in cui un utente ha dimenticato la password associata al proprio accountId (userid/login) ed

ha quindi la necessità di ripristinare l'accesso al sistema GIA ed ai servizi e applicazioni. In realtà i due scenari "assegnazione prima password" e "password dimenticata" individuano la stessa situazione e pertanto le corrispondenti gestioni vengono consolidate in un unico sotto-processo.

2. Di seguito sono riportate le attività ed i flussi informativi eseguite e scambiati rispettivamente fra gli attori del sotto-processo che sono rappresentati da un generico utente (CID-UTE-PER-GEN), il sistema GIA (SIS-GIA) ed il Tecnico di Facoltà (ADM-TEC-FAC) oppure il Tecnico SIA (ADM-TEC-SIA):
3. Il sotto-processo viene avviato dall'utente in corrispondenza di due situazioni (eventi):
   3.1. L'utente ha preso servizio ed ha ricevuto (oggetto BPMN "AND gateway" - vedi allegato) l'accountId, ovvero la stringa che rappresenta l'identificatore per la login ai sistemi
   3.2. L'utente ha dimenticato la password e deve ripristinare l'accesso ai sistemi
4. In entrambi i casi l'utente è in possesso dell'accountId, ma non conosce la password per completare la procedura di autenticazione.
5. Tramite un qualsiasi web browser, l'utente accede al sistema GIA la cui pagina iniziale consente di accedere, ovviamente in modalità anonima, ai due servizi "Richiesta password di primo accesso" e "Password dimenticata". I due servizi sono sostanzialmente identici e si differenziano internamente solo per flussi informativi diversi. L'utente, in funzione del contesto nel quale si trova, seleziona uno dei due servizi di Gestione Password.
6. In seguito alla richiesta dell'utente, il sistema GIA avvia un workflow di gestione che presenta all'utente un modulo di richiesta informazioni tra le quali, l'accountId necessario per identificarlo. Per i dettagli delle informazioni raccolte fare riferimento allo use case corrispondente.
7. L'utente compila il modulo di richiesta e conferma l'inserimento al GIA che accetta la richiesta dell'utente.
8. Il GIA effettua un controllo sull'accountId che deve corrispondere ad un utente esistente nel sistema. Questo controllo permette anche di limitare le eventuali "richieste spam" in quanto nel caso di utente inesistente il processo termina immediatamente dopo aver visualizzato a video un messaggio di errore.
9. Se la richiesta dell'utente è relativa alla password dimenticata, il sistema GIA invia una notifica al Tecnico SIA o di Facoltà per segnalare che un utente si presenterà per le operazioni di identificazione.
10. Proseguendo nel workflow, il sistema GIA genera internamente una password iniziale "IPWD" ed un identificatore sequenziale ("Forgotten Password ID" - FPID) che identifica la richiesta inoltrata dall'utente. Queste due informazioni sono visualizzate all'utente il quale viene quindi invitato dal sistema a confermare il proseguimento della richiesta di gestione password. L'utente deve prendere nota sia della IPWD che del FPID perché verranno in seguito utilizzate dalla procedura.
11. Il sistema GIA visualizza quindi un modulo riassuntivo di tutti i parametri della richiesta, con la sola esclusione della password. Il workflow si sospende in attesa di un evento di approvazione che dovrà essere invocato da parte del Tecnico SIA o di Facoltà.
12. L'utente deve stampare il modulo riassuntivo e presentarsi fisicamente al Tecnico SIA o di Facoltà per effettuare le operazioni di identificazione. In alternativa alla presenza fisica è possibile prevedere un invio del modulo di richiesta via FAX congiuntamente ad una fotocopia di un documento di riconoscimento.
13. Quando l'utente di presenta presso il Tecnico SIA o di Facoltà, quest'ultimo verifica la presenza della mail di notifica ricevuta in un apposito account funzionale e la corrispondenza dell'identificatore di richiesta FPID e procede con la verifica del documento d'identità.
14. In caso di anomalia il processo termina immediatamente e richiede una gestione manuale. Lo stesso comportamento viene assunto se il Tecnico decide di non approvare la richiesta.
15. Se a valle delle verifiche il Tecnico SIA o di Facoltà decide di approvare la richiesta, il Tecnico si collega al sistema GIA, individua la richiesta di approvazione attraverso l'identificatore FPID, effettua l'operazione di approvazione e conferma l'operazione all'utente.
16. L'evento di approvazione viene ricevuto dal sistema GIA il quale riprende l'esecuzione del workflow di controllo della procedura effettuando una forma speciale di password reset dell'accountId che prevede la generazione di password casuale per gli account associati alla VID, ma l'assegnazione della password IPWD all'account del GIA. In questo modo l'utente non puó accedere alle risorse, ma può accedere al GIA per avviare la procedura di aggiornamento della password.
17. L'utente, dopo aver ricevuto la conferma dal Tecnico SIA o di Facoltà deve accedere al sistema GIA tramite un qualsiasi web browser ed utilizzare, come credenziali, la coppia [accountId, IPWD]
18. A questo punto il GIA autentica l'utente e, poiché l'accountId è in stato di reset, forza l'utente ad aggiornare la propria password.
19. Il processo si conclude definitivamente in uno stato in cui l'utente è stato identificato, come richiesto dalla normativa, ed è in possesso di credenziali che nemmeno nelle fasi transitorie della procedura sono a conoscenza degli amministratori.

## Modifica del Profilo Applicativo

Se la componente di base del Profilo Applicativo è gestita in modo automatico nell'ambito del Profilo di Base, la componente di Estensione del Profilo Applicativo può essere oggetto di modifica e in modalità manuale attraverso un processo che coinvolge una funzione **richiedente** ed una di **approvatore**.
Il generale, un richiedente inoltra tramite il GIA una richiesta di modifica delle Estensione di Profilo Applicativo associata ad un **utente target**.
La richiesta arriva ad un approvatore il quale può confermare o rifiutare la variazione dei privilegi di accesso.
Le attività e i flussi informativi sono di seguito riportati:

1. Il processo di modifica della Estensione del Profilo Applicativo può essere avviato dalle persone che assumono i ruoli di Responsabile CDR (ADM-RSP-CDR) oppure dal Gestore GIA (ADM-GES-GIA) i quali, come prima attività, devono collegarsi al sistema GIA.
   Nell'ambito specifico di questo processo, sono questi ruoli che assumono la funzione di richiedente della modifica.

2. Poiché la richiesta fa riferimento ad un utente target, la prima attività svolta dal richiedente è quella di individuare nella vista centralizzata la Identità Virtuale che corrisponde all'utente target il cui Profilo Applicativo deve essere modificato. La ricerca può essere effettuata navigando manualmente fra le viste organizzativa e funzionale, oppure con il motore di ricerca integrato nel GIA. Se la VID dell'utente target non è presente nel sistema, il processo termina immediatamente.
3. Dopo aver individuato la VID interessata, il richiedente seleziona la form che corrisponde all'Estensione del Profilo Applicativo e nella quale sono visualizzati tutti i privilegi di accesso alle applicazioni e servizi che sono assegnati o che possono essere assegnati all'utente target.
4. Il richiedente deve modificare come desiderato l'insieme dei privilegi di accesso attraverso delle operazioni di selezione o de-selezione: queste operazioni equivalgono ad una variazione degli attributi d'identità dell'utente target. La modifica deve quindi essere confermata dal richiedente e tale operazione provoca internamente al GIA l'avvio del workflow di aggiornamento dell'identità dell'utente target (Update Task)
5. Il sistema GIA analizza il nuovo assetto della Estensione del Profilo Applicativo. Poiché ogni privilegio è definito attraverso un IM-Role, tale analisi si traduce nelle operazioni di provisioning o de-provisioning di alcuni ruoli e queste operazioni possono essere eventualmente vincolate dalla decisione di un approvatore (ruolo amministrativo ADM-RSP-PRV). Per ogni privilegio la cui variazione richiede una approvazione ad un decisore, il GIA invia una mail per richiedere l'intervento di quest'ultimo: gli approvatori possono essere diversi per ciascuno tipo di privilegio.
6. Dopo aver inviato le notifiche agli approvatori, il GIA sospende l'esecuzione del workflow in attesa delle risposte di questi ultimi.
7. Ogni approvatore di privilegio coinvolto nel processo e genericamente indicato con il codice ADM-RSP-PRV, dopo aver ricevuto la mail di notifica, si collega al GIA, individua la richiesta di approvazione pendente e procede con l'operazione di approvazione o rifiuto. In quest'ultimo caso, attraverso una breve causale, specifica anche le motivazioni del rifiuto.
8. Quando il GIA riceve l'esito dell'approvatore (approvazione o rifiuto), riprende l'esecuzione del workflow di controllo e se la richiesta di variazione è stata approvata, provvede a propagare nelle risorse interessate le modifiche relative ai privilegi di accesso. Queste ultime si possono concretizzare nella fornitura o rimozione di un account oppure nella variazione di membership ad un gruppo AD/LDAP.
9. In ogni caso viene inviato al richiedente una mail che descrive l'esito della richiesta e il processo di modifica termina.

## Gestione automatica dello stato

Nella Fase 1 di progetto, le variazioni di stato di una identità sono rappresentate dallo stato di abilitazione o disabilitazione. Quando una identità è nello stato di disabilitazione, tutte le identità elettroniche associate all'utente sono disabilitate e l'utente non può accedere ad alcun servizio o applicazione.
Lo stato non può essere modificato direttamente dai responsabili dei dati anagrafici, ma viene piuttosto gestito in modo automatico dal GIA analizzando le date di fine rapporto (una o più) associate a ciascuna identità.
Questo tipo di gestione si applica solamente al Personale (interno) ed al (personale) Esterno. Lo stato degli Ospiti viene gestito in modo automatico, ma con una modalità diversa, mentre lo stato degli studenti è delegato alla corrispondente applicazione di gestione utilizzata dalla segreteria studenti.
Per gestire le situazioni particolari, viene comunque definito un meccanismo di disabilitazione manuale chiamato "Blocco Amministrativo", ma tale capacità è disponibile solo per il ruolo amministrativo del Gestore GIA.
Il workflow relativo al Blocco Amministrativo è descritto nel paragrafo , mentre la modifica automatica dello stato è descritta dal workflow riportato di seguito:

1. Il workflow di gestione automatica dello stato viene attivato dal GIA in modo completamente autonomo e periodicamente nel tempo, tipicamente nel corso della notte.
2. Il workflow scandisce tutte le VID presenti nel GIA ed appartenenti alle CID del Personale (interno) o del (personale) Esterno ed applica il workflow di "Gestione Stato VID" descritto successivamente.
3. Se tale workflow individua la condizione di preavviso di scadenza account, il GIA invia una mail di notifica all'utente (CID-UTE-GEN-GEN) con un testo opportunamente personalizzato in funzione della tipologia di CID (Personale o Esterni) alla quale l'utente appartiene.
4. Quando l'utente riceve la notifica che avverte dell'avvicinamento della scadenza dell'account, l'utente ha la facoltà di richiedere al gestore anagrafica di riferimento (GAP o GAE a seconda della CID dell'utente) una estensione della durata dell'accesso. Tale richiesta può essere inoltrata direttamente o via mail al responsabile GAP/GAE il quale, se ritenuto opportuno, provvederà ad aggiornare opportunamente la data di fine rapporto associata all'utente.

Per quanto riguarda il workflow "Gestione Stato VID" le attività e i flussi informativi sono di seguito riportati:

1. Il workflow viene invocato dal processo di gestione automatica dello stato dell'identità.
2. Il workflow legge le informazioni d'identità associate alla VID considerata e calcola la data di potenziale disabilitazione che corrisponde alla data di fine rapporto più lontana da quella corrente.
3. Se la VID sotto analisi è disabilitata, non è stata superata la data di potenziale disabilitazione e non sussiste il blocco amministrativo, allora la VID viene (ri)abilitata. Questa condizione si verifica, ad esempio, quando il Gestore GIA sblocca una identità che in precedenza era in stato di Blocco Amministrativo.
4. Se la VID è abilitata ed è stata superata la data di potenziale disabilitazione, allora la VID viene automaticamente disabilitata. Questa è la condizione che si verifica normalmente alla scadenza naturale di un account.
5. Il successivo controllo permette di intercettare la condizione di preavviso di scadenza verificando il periodo di preavviso che intercorre fra la data di potenziale disabilitazione e la data corrente. Se sussiste la condizione di preavviso, il GIA invia automaticamente all'utente interessato una notifica via mail che avverte l'avvicinarsi della data di scadenza dell'account.

Si noti che con questo tipo di gestione dello stato dell'identità, quest'ultima viene disabilitata, ma anche ri-abilitata automaticamente sotto in controllo delle date di fine rapporto che caratterizzano un utente. Infatti, se una identità viene disabilitata in seguito alla

scadenza di tutti i rapporti ed uno di questi viene rinnovato dal Gestore dati anagrafici modificando opportunamente la data di inizio del nuovo rapporto, l'identità verrà automaticamente ri-abilitata fino alla nuova scadenza.
Quindi lo stato di una identità viene determinato solo sulla base del rapporto di durata maggiore ed è globale, ovvero solo quando l'ultimo rapporto scade viene disabilitata la VID e tutti gli account associati. Questo comportamento è in pieno accordo con il modello di Gestione delle Identità in base al quale i privilegi di accesso alle applicazioni/servizi non sono concessi in funzione dei rapporti, ma del profilo applicativo.
Il sistema GIA, comunque, non analizza solo la data di fine rapporto più lontana, ma prende in considerazione tutte le date di fine rapporto con lo scopo di calcolare correttamente l'ambito operativo di ciascuna identità. Per le risorse di tipo gerarchico (Active Directory ed LDAP) infatti, la struttura organizzativa di appartenenza associata al rapporto permette di limitare l'ambito di visibilità di una identità. Ad esempio se una identità ha un rapporto con la Facoltà di Economia, nell'ambito di Active Directory o del directory LDAP verrà limitata la visibilità al solo sotto-ramo corrispondente.
Pertanto, quando un rapporto scade, oppure viene rimosso dal Gestore Anagrafica (GAP/GAE), vengono opportunamente aggiornate le appartenenze ai gruppi AD/LDAP che determinano le visibilità (chiamate anche "scope").

### Blocco Amministrativo

La funzione di Blocco Amministrativo consente ad un amministratore del GIA di disabilitare immediatamente una identità indipendentemente dallo stato controllato indirettamente attraverso le date di fine servizio associate ai rapporti "Utente-UniVR". In figura Errore: sorgente del riferimento non trovata è descritto il corrispondente processo.
Il Blocco Amministrativo è caratterizzato da una priorità maggiore del controllo automatico di disabilitazione, ma quando il blocco viene rimosso, lo stato effettivo dell'identità viene determinato solo in base al controllo automatico.
Le attività ed i flussi sono di seguito riportati:

1. Il processo può essere avviato solo da un sottoinsieme di ruoli amministrativi, ovvero dal Gestore GIA, il Tecnico SIA ed il Tecnico di Facoltà i quali, come prima operazione, devono collegarsi al sistema GIA.
2. Poiché la funzione di Blocco Amministrativo si riferisce alla identità di uno specifico utente, l'amministratore deve selezionare la corrisponde VID per mezzo dei meccanismi resi disponibili dal GIA (navigazione o ricerca). Se la VID non esiste il processo termina immediatamente, altrimenti l'amministratore seleziona da interfaccia grafica la funzione nativa di disabilitazione dell'utente messa a disposizione dal prodotto GIA.
3. Il GIA visualizza quindi la form web associata alla funzione di disabilitazione dell'utente, la quale presenta il flag (check-mark) corrispondente al Blocco Amministrativo.
4. L'amministratore ha quindi la possibilità di impostare o resettare tale flag, il cui valore si riflette in una variabile interna associata alla VID dell'utente selezionato
5. *Quando l'amministratore conferma l'operazione, il GIA procede con il workflow aggiornando immediatamente lo stato della VID. Se quest'ultima deve essere posta in stato di Blocco Amministrativo, essa viene immediatamente disabilitata. Se invece il Blocco Amministrativo viene rimosso, lo stato della VID dipende dall'esito del controllo automatico basato sulle date di fine servizio.*

## Il sistema di autenticazione e autorizzazione interno

### Profilo Applicativo

Il Profilo Applicativo individua l'insieme di applicazioni e servizi che un utente è autorizzato ad utilizzate e dove il permesso di accesso è rappresentato dalla fornitura di un account presso una applicazione/servizio (risorsa) oppure dall'assegnazione di uno specifico privilegio puntuale quale l'inserimento in gruppi di un directory server: questo permesso è definito "E-Role".
Pertanto il termine Profilo Applicativo può essere definito formalmente come un insieme di E-Role ciascuno dei quali fornisce o revoca l'accesso ad una applicazione o servizio.

NOTA
Il concetto di E-Role individua una autorizzazione di alto livello, ovvero con un basso livello di granulosità e come tale non entra nel merito della possibile abilitazione o disabilitazione delle funzionalità di ogni singola applicazione la cui gestione viene lasciata a livello locale dell'applicazione stessa.
L'insieme ufficiale di applicazioni che verranno gestite dal sistema GIA nella Fase 1 di progetto é riportato nell'allegato Errore: sorgente del riferimento non trovata, mentre la tabella 3 descrive i Ruoli Elementari che saranno resi disponibili per la composizione del Profilo Applicativo di Base e della Estensione di Profilo.
Gli elementi riportati in tabella sono i seguenti:

- **nome** del ruolo elementare che sarà reso disponibile a livello di interfaccia grafica per indicare l'applicazione/servizio concessa all'utente
- **codice** da usare nelle codifiche interne
- **rule** che può essere associata ad alcuni attributi del ruolo. Le rule riportate sono quelle "visibili" al momento dell'analisi, ma potrebbe essere necessario definirne delle altre, ovvero tutte le eventuali specializzazioni verranno gestite attraverso la definizione di regole e non con l'introduzione di ruoli più specializzati[9].

9 Ad esempio, per le risorse LDAP e in relazione alla applicazione della mail, l'indirizzo di posta elettronica da associare ad un utente di classe Personale è funzione del SID (Strutturato/Non Strutturato) ed eventualmente della

- la **descrizione** del ruolo

Si assume inoltre che l'assegnazione ad un utente di un E-Role che effettua l'inserimento dell'utente in un gruppo definito in un directory (AD/LDAP) venga effettuata dopo aver assegnato allo stesso utente l'E-Role che fornisce a quest'ultimo l'account sul directory. Ad esempio, per fornire ad un utente Personale l'E-Role `EROLE-TITULUS` , all'utente deve essere prima assegnato l'E-Role `EROLE-RETEPER`.

Gli E-Role riportati in tabella possono essere combinati fra loro per definire la componente di base del Profilo Applicativo oppure per definire l'Estensione di Profilo.

| Nome | Codice | Rule | Descrizione |
|---|---|---|---|
| Servizi Rete Personale | `EROLE-RETEPER` | Inserimento in gruppi AD per restringere lo scope di accesso alla rete. | Fornisce l'accesso alla rete interna di UniVR creando un account nel ramo AD dedicato al Personale Interno. Questo ruolo viene usato anche per erogare l'accesso di rete agli Ospiti per il quale, attraverso la rule, vengono ridotti i privilegi. |
| Servizi Rete Studenti | `EROLE-RETESTU` | Inserimento in gruppi AD per restringere lo scope di accesso alla rete. | Fornisce l'accesso alla rete AD di UniVR dedicata agli Studenti creando un account nel ramo AD corrispondente. |
| Email Personale | `EROLE-MAILPER` | Inserimento in gruppi LDAP per restringere lo scope di accesso alla rete. Gestione del dominio della mail in funzione della CIS/SID e della struttura di appartenenza. | Fornisce al Personale sia l'accesso alla mail che un account Samba in quanto entrambi si appoggiano al ramo Personale del directory realizzato con SJS Directory Server |
| Email Studenti | `EROLE-MAILSTU` | Inserimento in gruppi LDAP per restringere lo scope di accesso. | Fornisce allo Studente sia l'accesso alla mail che un account Samba in quanto entrambi si appoggiano al ramo Studenti del directory realizzato con SJS Directory Server |
| Applicazione dbERW | `EROLE-APDBERW` | | Fornisce un account per l'applicazione dbERW. Questo è previsto solo per gli utenti di tipo Personale. |
| Applicazione CIA | `EROLE-APPLCIA` | | Fornisce un account per l'applicazione CIA. Questo è previsto solo per un sottoinsieme degli utenti di classe Personale. |
| Applicazione Titulus | `EROLE-TITULUS` | Inserimento in gruppi AD per restringere lo scope di utilizzo all'applicazione. | Fornisce un account per l'applicazione Titulus. Questo è previsto solo per un sottoinsieme degli utenti di classe Personale. |
| Accesso Wireless Personale | `EROLE-AWLSPER` | Inserimento in gruppi AD per restringere lo scope di accesso alla rete. | Fornisce il privilegio di accesso (inserimento in gruppi AD) alla rete Wireless basata sulla infrastruttura AD per il Personale. |
| Applicazione Gestione Presenze | `EROLE-GESPRES` | | Provvede a creare un account presso l'applicazione Aliseo e che consente il tracciamento delle presenze. Questo account è previsto per tutti gli utenti di tipo Subordinato. |
| Accesso Web VPN | `EROLE-AWEBVPN` | Inserimento in gruppi AD per restringere lo scope di accesso alla rete. | Fornisce l'accesso al servizio VPN via Web che si realizza attraverso l'inserimento in gruppi AD del Personale. |
| Accesso Client VPN | `EROLE-ACLTVPN` | Inserimento in gruppi AD per restringere lo scope di accesso alla rete. | Fornisce l'accesso al servizio VPN realizzato con Fat Client. Si realizza attraverso l'inserimento in gruppi AD del Personale. |
| Accesso Wireless Studenti | `EROLE-AWLSSTU` | Inserimento in gruppi AD per restringere lo scope di accesso alla rete. | Fornisce il privilegio di accesso (inserimento in gruppi AD) alla rete Wireless basata sulla infrastruttura AD per gli Studenti. |
| Accesso al servizio Help Desk | `EROLE-HELPDSK` | Inserimento in gruppi AD per restringere lo scope di accesso ai servizi. | Fornisce l'accesso ai servizi di base di Help-Desk attraverso l'inserimento in gruppi AD del Personale. |

struttura organizzativa di appartenenza.

*Tabella 3: Ruoli Elementari*

### Profili di base

Il Profilo di Base è composto dal Profilo Identificativo e dalla componente di base del Profilo Applicativo ed è caratterizzato dal fatto che il provisioning dei resource account che ne fanno parte segue un processo automatico, ovvero appena l'utente viene creato o modificato tramite il sistema della sorgente autoritativa, le modifiche si propagano automaticamente, grazie al GIA, alle risorse.
Il Profilo Identificativo non è implementato attraverso IM-Role, ma semplici attributi che fanno parte della Virtual Identity e che dipendono, come illustrato in precedenza, dalla CID.
Al fine di inserire nel flusso di provisioning automatico anche la creazione di alcuni account e la fornitura di alcune autorizzazioni, viene inserita nel Profilo di Base anche una componente degli E-Role che compongono il Profilo Applicativo: questo insieme di E-Role definisce il Profilo Applicativo di Base. Diversamente dal Profilo Identificativo, tale componente è resa funzione non solo dalla CID, ma anche dall'SID in quanto la sola CID esprime un livello di granulosità troppo basso.
Dal punto di vista dell'implementazione, anche il Profilo Applicativo di Base viene modellato attraverso un IM-Role e quindi viene implicitamente definita una gerarchia di ruoli a 2 livelli

- il livello inferiore definito dagli E-Role che rappresentano privilegi di accesso
- il livello superiore definito da un IM-Role che incapsula i ruoli elementari

La tabella 4 riassume, per ciascuna CID e SID considerate nella Fase 1 di progetto, i Profili Applicativi di Base e la loro composizione in termini di E-Role.

| CID/SID | Codice Profilo Applicativo di Base | E-Role componenti | Descrizione |
|---|---|---|---|
| SID-UTE-PER-TAS | PROBAS-UTE-PER-TAS | EROLE-RETEPER<br>EROLE-MAILPER<br>EROLE-APDBERW<br>EROLE-AWLSPER<br>EROLE-GESPRES<br>EROLE-AWEBVPN<br>EROLE-HELPDSK | Profilo Applicativo di Base per i TA Strutturati |
| SID-UTE-PER-TAN | PROBAS-UTE-PER-TAN | EROLE-RETEPER<br>EROLE-APDBERW<br>EROLE-HELPDSK | Profilo Applicativo di Base per i TA Non Strutturati |
| SID-UTE-PER-ACS | PROBAS-UTE-PER-ACS | EROLE-RETEPER<br>EROLE-MAILPER<br>EROLE-APDBERW<br>EROLE-AWLSPER<br>EROLE-AWEBVPN<br>EROLE-HELPDSK | Profilo Applicativo di Base per gli Accademici Strutturati |
| SID-UTE-PER-ACN | PROBAS-UTE-PER-ACN | EROLE-RETEPER<br>EROLE-APDBERW<br>EROLE-HELPDSK | Profilo Applicativo di Base per gli Accademici Non Strutturati |
| SID-UTE-PER-DIS | PROBAS-UTE-PER-DIS | EROLE-RETEPER<br>EROLE-MAILPER<br>EROLE-APDBERW<br>EROLE-AWLSPER<br>EROLE-GESPRES<br>EROLE-AWEBVPN<br>EROLE-HELPDSK | Profilo Applicativo di Base per i Dirigenti Strutturati |
| SID-UTE-PER-DIN | PROBAS-UTE-PER-DIN | EROLE-RETEPER<br>EROLE-APDBERW<br>EROLE-HELPDSK | Profilo Applicativo di Base per i Dirigenti Non Strutturati |

| CID/SID | Codice Profilo Applicativo di Base | E-Role componenti | Descrizione |
|---|---|---|---|
| SID-UTE-PER-DOT | PROBAS-UTE-PER-DOT | EROLE-RETEPER<br>EROLE-APDBERW<br>EROLE-HELPDSK | Profilo Applicativo di Base per i Dottorandi |
| SID-UTE-STU-SPE | PROBAS-UTE-STU-SPE | EROLE-RETEPER<br>EROLE-HELPDSK | Profilo Applicativo di Base per gli Studenti Specializzandi |
| SID-UTE-STU-POS | PROBAS-UTE-STU-POS | EROLE-RETEPER<br>EROLE-HELPDSK | Profilo Applicativo di Base per gli Studenti Post-Lauream |
| SID-UTE-STU-ISC | PROBAS-UTE-STU-ISC | EROLE-RETESTU<br>EROLE-MAILSTU<br>EROLE-AWLSSTU | Profilo Applicativo di Base per gli Studenti Iscritti |
| CID-UTE-EST-HOS | PROBAS-UTE-EST-HOS | | Profilo Applicativo di Base per gli Esterni Ospedalieri. Per default ad essi non viene assegnata alcuna autorizzazione di base. |
| CID-UTE-EST-CON | PROBAS-UTE-EST-CON | | Profilo Applicativo di Base per gli Esterni Consulenti. Per default ad essi non viene assegnata alcuna autorizzazione di base. |
| CID-UTE-EST-150 | PROBAS-UTE-EST-150 | | Profilo Applicativo di Base per gli Esterni – Studenti 150h. Per default ad essi non viene assegnata alcuna autorizzazione di base. |
| CID-UTE-FRE-OSP | PROBAS-UTE-FRE-OSP | EROLE-RETEPER | Per i Frequentatori-Ospiti, il ruolo assegna tramite rule dei privilegi di accesso minimi. |

*Tabella 4: Composizione dei Profili Applicativi di Base*

Si noti che per quanto riguarda gli Studenti, il flusso di sincronizzazione richiede sostanzialmente che a valle dell'inserimento di una identità nel DB-Studenti venga creato e mantenuto sincronizzato un acccount nel ramo studenti della risorsa LDAP e AD. Tale account, a parte il provisioning degli attributi necessari per la gestione della mail e dell'accesso wireless, deve essere considerato come un account di riferimento rispetto al quale altre applicazioni di gestione andranno ad aggiungere le proprie definizioni.Modifica del Profilo Applicativo

Diversamente dal Profilo Applicativo di Base che è determinato a priori, il Profilo Applicativo può essere modificato in modo manuale attraverso un processo di modifica delle autorizzazioni.

Tale processo prevede due fasi: una figura di amministratore GIA inoltra la richiesta di modifica, un altra figura amministrativa GIA eventualmente approva la richiesta ed applica in modo manuale la modifica delle autorizzazioni di accesso richieste.

L'oggetto della modifica del Profilo Applicativo è costituito dalla componente di quest'ultimo chiamata **Estensione di Profilo Applicativo** e che è costituita dall'insieme, o una parte di esso, di E-Role non assegnati dal flusso di provisioning automatico. La dimensione di questo insieme è variabile e dipendente, analogamente alla componente dinamica del Profilo Applicativo, sia dal CID che dall'SID. Inoltre per modellare l'Estensione, non viene utilizzato alcun IM-Role di aggregazione in quanto le autorizzazioni devono poter essere gestite in modo puntuale.

L'amministratore che desidera inoltrare una richiesta di modifica della estensione di profilo, dovrà prima di tutto selezionare l'identità nella vista centralizzata e quindi visualizzare il profilo applicativo della stessa. L'interfaccia grafica presenterà quindi un elenco variabile, ma predefinito, di E-Role che l'amministratore potrà selezionare o deselezionare[10], specificando eventuali parametri:

- l'operazione di selezione indica una richiesta di assegnazione di autorizzazione all'accesso
- l'operazione di deselezione indica una richiesta di revoca dell'accesso

Inoltre la richiesta di assegnazione o revoca per ciascuna autorizzazione potrà, in funzione del tipo della medesima, essere soggetta ad approvazione. L'azione effettiva di assegnazione o revoca delle autorizzazioni sarà solitamente manuale, ma potrebbe anche essere resa automatica (si tratta di assegnare un IM-Role ad un utente).

La tabella 5 riporta, per ciascun CID/SID, l'elenco dei possibili E-Role che possono far parte della Estensione di Profilo Applicativo e chi, in termini di ruolo amministrativo, può inoltrare la richiesta di estensione e la eventuale approvazione (gli acronimi sono definiti nel capitolo Errore: sorgente del riferimento non trovata).

10 In realtà l'interfaccia visualizza due liste: la lista degli E-Role disponibili e la lista degli E-Role assegnati. L'amministratore richiedente avrà la facoltà di modificare il contenuto della lista dei ruoli assegnati.

| CID o SID | E-Role | Richiedente | Approvazione | Descrizione |
|---|---|---|---|---|
| SID-UTE-PER-TAS | EROLE-APPLCIA | ADM-RSP-CDR | ADM-SER-FCO | Estensione per i TA Strutturati |
| | EROLE-TITULUS | ADM-RSP-CDR | ADM-SER-PRO | |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| SID-UTE-PER-TAN | EROLE-MAILPER | ADM-RSP-CDR | NO | Estensione per i TA Non Strutturati |
| | EROLE-APPLCIA | ADM-RSP-CDR | ADM-SER-FCO | |
| | EROLE-TITULUS | ADM-RSP-CDR | ADM-SER-PRO | |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSPER | ADM-RSP-CDR | NO | |
| | EROLE-GESPRES | ADM-RSP-CDR | NO | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | NO | |
| SID-UTE-PER-ACS | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | Estensione per gli Accademici Strutturati |
| SID-UTE-PER-ACN | EROLE-MAILPER | ADM-RSP-CDR | NO | Estensione per gli Accademici Non Strutturati |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSPER | ADM-RSP-CDR | NO | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | NO | |
| SID-UTE-PER-DIS | EROLE-APPLCIA | ADM-RSP-CDR | ADM-SER-FCO | Estensione per i Dirigenti Strutturati |
| | EROLE-TITULUS | ADM-RSP-CDR | ADM-SER-PRO | |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| SID-UTE-PER-DIN | EROLE-MAILPER | ADM-RSP-CDR | NO | Estensione per i Dirigenti Non Strutturati |
| | EROLE-APPLCIA | ADM-RSP-CDR | ADM-SER-FCO | |
| | EROLE-TITULUS | ADM-RSP-CDR | ADM-SER-PRO | |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSPER | ADM-RSP-CDR | NO | |
| | EROLE-GESPRES | ADM-RSP-CDR | NO | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | NO | |
| SID-UTE-PER-DOT | EROLE-MAILPER | ADM-RSP-CDR | NO | Estensione per i Dottorandi |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSSTU | ADM-RSP-CDR | NO | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | NO | |
| SID-UTE-STU-SPE | EROLE-MAILPER | ADM-RSP-CDR | NO | Estensione per gli Studenti Specializzandi |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSSTU | ADM-RSP-CDR | NO | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | NO | |
| SID-UTE-STU-POS | EROLE-MAILPER | ADM-RSP-CDR | NO | Estensione per gli Studenti Post-Lauream |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSSTU | ADM-RSP-CDR | NO | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | NO | |
| SID-UTE-STU-ISC | | ADM-RSP-CDR | | Nessuna estensione per gli Studenti Iscritti |

| CID o SID | E-Role | Richiedente | Approvazione | Descrizione |
|---|---|---|---|---|
| CID-UTE-EST-HOS | EROLE-RETEPER | ADM-RSP-CDR | ADM-SER-SIA | Estensione per gli Esterni Ospedalieri. |
| | EROLE-MAILPER | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-APDBERW | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSPER | ADM-RSP-CDR | ADM-SER-SIA | |
| CID-UTE-EST-CON | EROLE-RETEPER | ADM-RSP-CDR | ADM-SER-SIA | Estensione per gli Esterni Consulenti. |
| | EROLE-MAILPER | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-APDBERW | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWEBVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-ACLTVPN | ADM-RSP-CDR | ADM-SER-SIA | |
| | EROLE-AWLSPER | ADM-RSP-CDR | ADM-SER-SIA | |
| CID-UTE-EST-150 | EROLE-RETEPER | ADM-RSP-CDR | ADM-SER-SIA | Estensione per gli Esterni Studenti 150h. |
| CID-UTE-FRE-OSP | | ADM-RSP-CDR | NO | Per i Frequentatori-Ospiti non è prevista alcuna estensione. |

*Tabella 5: Composizione delle Estensioni di Profilo Applicativo*

*[Per quali applicazioni interne all'organizzazione viene utilizzato questo sistema di gestione delle identità?]*

*[Gli identificatori principali di ogni persona, come "net ID," eduPersonPrincipalName, o eduPersonTargetedID, sono univoci una volta assegnati? Possono venire riutilizzati? In quali casi?]*

*[Se nell'organizzazione è fornito il "single sign-on" (SSO) o la possibilità di avere un sistema unico di autenticazione per più applicazioni e l'organizzazione vuole utilizzare questo sistema per autenticare l'accesso ai servizi della Federazione, si descrivano gli aspetti chiave della sicurezza di questo sistema includendo la descrizione dei timeout imposti dal sistema e della terminazione delle sessioni.]*

## Partecipazione ad altre federazioni

*[L'organizzazione partecipa ad altre Federazioni di Autenticazione e Autorizzazione? Se sì, quali? Descrivere gli elementi che possono essere di interesse per gli altri partecipanti ed eventuali problematiche.]*