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 05/06/2012

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
02/12/2009	0.4	Corretta la nota introduttiva sulla pubblicità del documento	RC
01/06/2012	0.7	Correzione	
05/06/2012	0.8	Revisione	AB

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	Definizione
Amministrazione (UniVR)	Università degli Studi di Verona
Centro di Responsabilità (CDR)	Struttura organizzativa di UniVR avente Responsabilità ai fini del Dlgs 196/2003 e dei processi di accreditamento informatico
Responsabile dell'Anagrafica (RSA)	Responsabile ai sensi del Dlgs 196/2003 dell'identificazione e dell'autorizzazione all'accesso allo spazio informatico dell'Ateneo
Identity Management (IdM)	Sistema e procedure per la gestione delle credenziali elettroniche degli utenti
Access Management (AM)	Sistema e procedure per la gestione dell'autenticazione e autorizzazione nell'accesso a servizi informatici
Gestione Identità di Ateneo (GIA)	Sistema informativo gestionale delle operazioni di accreditamento informatico
Risorsa Autorevole (RA)	Sistema informativo fonte dei dati per le operazioni di accreditamento informatico
Risorsa Provisionata (RP)	Sistema informativo destinatario delle operazioni di accreditamento informatico
Gestore di Identità (GSI)	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
Single Sign On (SSO)	Processo di AM univoco per insieme di risorse informatiche diverse
Realm (RLM)	Dominio di autenticazione
Entity (EID)	Entità coinvolta nelle procedure di AM e SSO
Circle Of Trust (COT)	Insieme di EID mutuamente accreditate per procedure di AM e SSO
Identity Provider (IDP)	Fornitore di servizi di accreditamento nelle procedure di AM e SSO
Service Provider (SP)	Fornitore di servizi informatici soggetti ad accreditamento attraverso procedure di AM e SSO

Gestore dell'accreditamento

L'Amministrazione provvede all'accreditamento informatico attraverso il sistema di Identity Management denominato GIA il quale 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) sono classificati sulla base dell'appartenenza a Classi e Sottoclassi di Identità:

- gli appartenenti ad una stessa Classe d'Identità, accedono all'organizzazione UniVR con accreditamento gestito da strutture organizzative omogenee e omogenei insiemi di attività e flussi informativi;
- gli 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 quindi 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. 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-Lauream	
	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 amministratori 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
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
	SID-UTE-STU-LMB (Studenti/In Limbo)	Sì
Esterni/Ospedalieri Non Universitari (CID-UTE-EST-HOS)	SID-UTE-EST-GEN	NO

Ruoli Utente UniVR-GIA		
Esterni/Consulenti-Fornitori (CID-UTE-EST-CON)	SID-UTE-EST-GEN	NO
Esterni/150h (CID-UTE-EST-150)	SID-UTE-EST-GEN	NO
Frequentatori/Ospiti (CID-UTE-FRE-OSP)	SID-UTE-FRE-GEN	NO
Frequentatori/Biblioteca (CID-UTE-FRE-BIB)	SID-UTE-FRE-GEN	NO
Frequentatori/Congressisti (CID-UTE-FRE-CNG)	SID-UTE-FRE-GEN	NO
Frequentatori/Studenti ospiti (CID-UTE-FRE-STO)	SID-UTE-FRE-GEN	NO
Frequentatori/Studenti frequentatori (CID-UTE-FRE-STF)	SID-UTE-FRE-GEN	NO

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

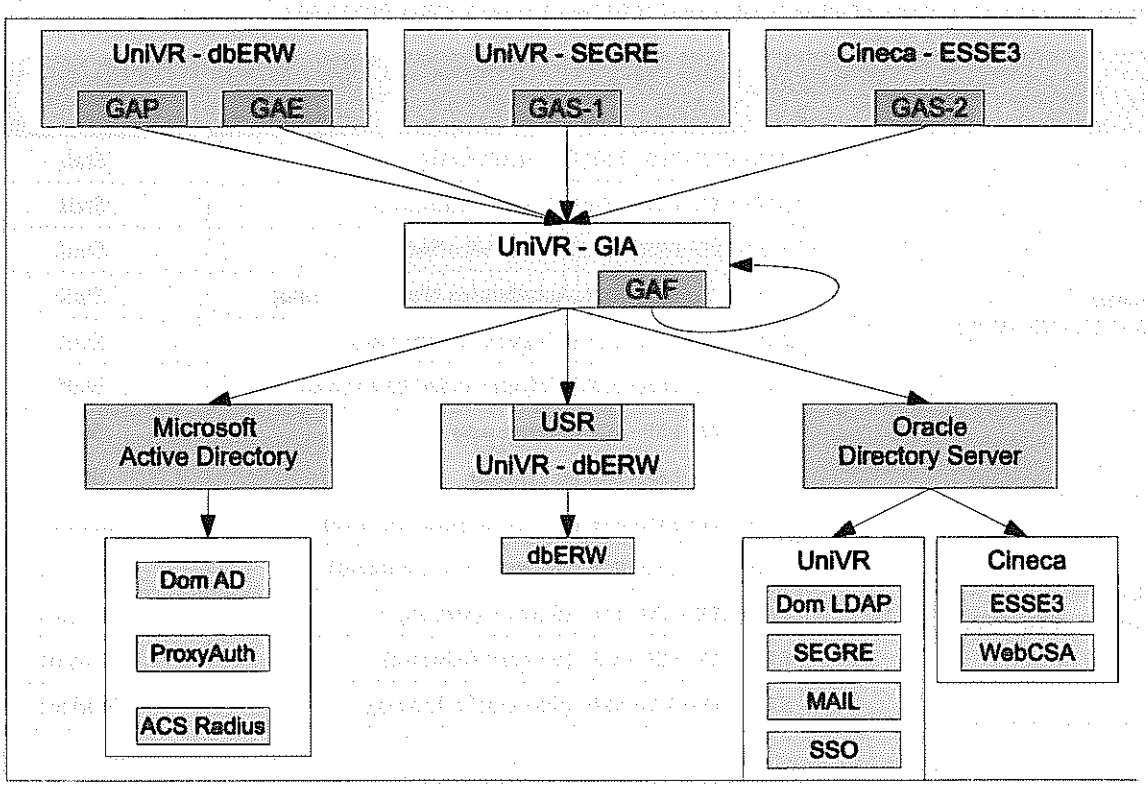
Visione di insieme del processo di accreditamento degli utenti

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) **Oracle 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 Autenticazione CISCO ACS
   j) **ProxyAuth**, Browsing autenticato
   k) **SSO**, Servizio di autenticazione in SingleSignOn e Federata



Cicli di vita delle Identità Informatiche

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 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 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.

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. Queste informazioni vengono rilevate dal GIA in modo automatico dalle varie sorgenti autoritative associate alle CID attraverso il controllo costante delle risorse informatiche alle quali si appoggiano i vari sistemi di gestione dell'anagrafica e l'intercettazione di 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 Risorsa Autorevole, il sistema 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 sistema GIA.
Nei paragrafi che seguono vengono descritti gli attributi del Profilo Identificativo per ciascuna delle classi d'identità.
Essendo il contenuto del Profilo Identificativo controllato (remotamente) tramite le applicazioni di anagrafica previste per le varie CID, 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 Risorsa Autorevole per gli utenti appartenenti alla CID Personale è costituita dal sistema di Gestione dell'Anagrafica del Personale (GAP) e gli attributi, provenienti da essa, che comporranno il Profilo Identificativo di questa classe d'identità, sono riportati 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
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

Nome attributo	Obbligatorio	Descrizione
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 provvede ad elencare tutti i rapporti dello specifico utente Personale e per ciascuno di essi visualizza la coppia CID/SID, la struttura organizzativa e la data di fine rapporto calcolata. I rapporti possono essere in stato attivo o non attivo ma vengono visualizzati solo quelli attivi al momento della interrogazione. 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 con una operazione di disabilitazione dell'account.

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 identità trattate da GIA
Codice di Facoltà	SI'	Codice di Facoltà
Codice di Corso	SI'	Codice di Corso
Anno accademico	SI'	Anno accademico
Anno di iscrizione	SI'	Anno di iscrizione
Codice di stato	SI'	Stato dello studente

Tabella 2: Profilo Identificativo Studenti

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.

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.
La tabella 3 descrive i Ruoli Elementari che sono disponibili per la composizione del Profilo Applicativo di Base e della Estensione di Profilo.
Gli elementi riportati in tabella sono i seguenti:

- **Nome** – Ruolo elementare indicativo di applicazione o servizio concessa all'utente
- **E-Role** - codice del ruolo elementare
- **Regola** – descrizione operazioni legate all'assegnazione del ruolo
- **Descrizione** – Descrizione del ruolo

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	E-Role	Regola	Descrizione
Servizi Rete Personale	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	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	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	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	APDBERW		Fornisce un account per l'applicazione dbERW. Questo è previsto solo per gli utenti di tipo Personale.
Applicazione CIA	APPLCIA		Fornisce un account per l'applicazione CIA. Questo è previsto solo per un sottoinsieme degli utenti di classe Personale.
Applicazione Titulus	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	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	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	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	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	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	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.

Tabella 3: Ruoli Elementari

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:

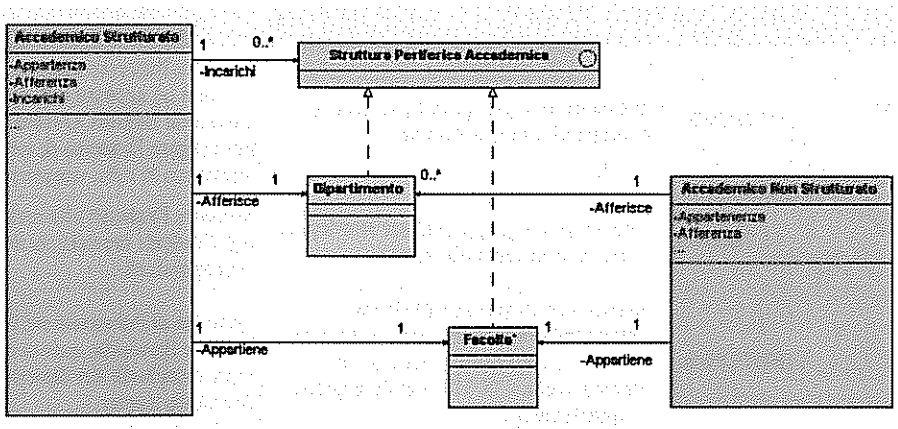


Figura 1: Appartenenza, afferenza ed incarichi per gli accademici

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.

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

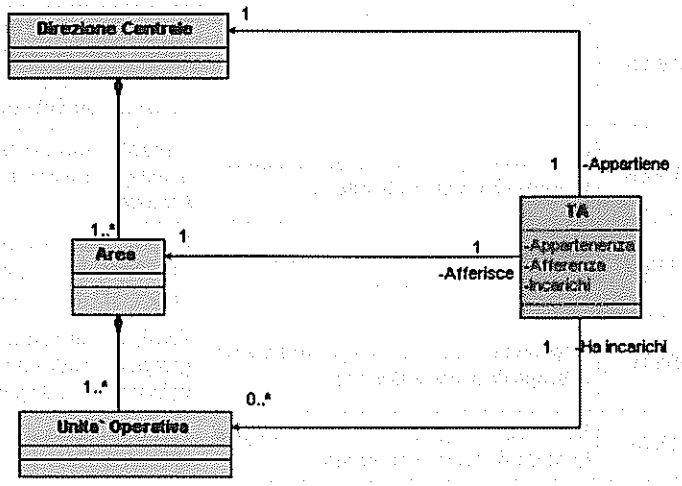


Figura 2: Appartenenza, afferenza ed incarichi per i TA

Il processo di accreditamento per gli Studenti Iscritti

Questo paragrafo riporta la descrizione dei processi e dei flussi 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. 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 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.

Formato e regole delle credenziali

Il formato e le regole delle credenziali, 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

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 disabilitata.

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

Questo paragrafo riporta la descrizione dei processi e dei flussi 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:

1. La gestione di tutti gli studenti iscritti a UniVR è di competenza della Direzione Studenti - Area Post-Lauream.
2. Tutte le informazioni relative allo stato dei vari studenti vengono gestite attraverso DB-Studenti. Un flusso informativo permette l'allineamento delle informazioni tra DB-Studenti 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 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.

Formato e regole delle credenziali

Il formato e le regole delle credenziali, 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 disabilitata.

Il processo di accreditamento per gli Studenti Alumni

Questo paragrafo riporta la descrizione dei processi e dei flussi 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:

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 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 in paragrafo successivo.

Formato e regole delle credenziali

Il formato e le regole delle credenziali, 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

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 disabilitata.

Il processo di accreditamento per gli Studenti in Limbo

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

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 VID 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:

1. Il processo è avviato da Responsabili del procedimento della Segreteria Studenti
2. Il Responsabile del procedimento effettua un Password Reset sull'anagrafica dello studente.
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 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 in paragrafo successivo.

Formato e regole delle credenziali

Il formato e le regole delle credenziali, 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

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 disabilitata.

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

Questo paragrafo riporta la descrizione dei processi e dei flussi 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:

1. Il processo viene avviato quando, nell'ambito di una generica struttura organizzativa di Amministrazione Centrale o di Struttura Decentrata nasce l'esigenza accreditare all'accesso alle risorse informatiche di UniVR Utenti delle sottoclassi considerate.
2. Il processo è svolto direttamente dal Responsabile CDR (ADM-RSP-CDR) ai sensi 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.
3. Il Responsabile GAP provvede all'identificazione dell'Utente e all'accertamento dei requisiti necessari per l'accreditamento e, di fronte ad esito positivo, crea o aggiorna il profilo anagrafico in accordo.
4. Il Sistema GAP riceve le variazioni del profilo anagrafico.
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 successivo.
6. Il sotto-processo di provisioning invia una mail al Responsabile GAP con i dati della VID appena creata, tra i quali l'accountId viene comunicato direttamente all'Utente in accreditamento.
7. 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.
8. Quando l'Utente prende 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 in paragrafo successivo.

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 VID 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.
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 in paragrafo successivo.

Formato e regole delle credenziali

Il formato e le regole delle credenziali, 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

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 disabilitata.

Sotto-Processi condivisi di gestione dell'accreditamento

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

Provisioning del Profilo di Base

Questo sotto-processo è in realtà un flusso eseguito nel contesto del sistema GIA.
Le attività eseguite da tale flusso sono di seguito riportate:

1. Dopo aver intercettato l'inserimento dell'utente nelle Risorse Autoritative, 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 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 procedura di inizializzazione della password di accesso.
2. In funzione dei parametri CID e SID, viene individuato un RUOLO che definisce il Profilo di Base per la specifica classe d'identità alla quale l'utente appartiene
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 secondo i criteri generali descritti nella sezione successiva.
5. Al termine il workflow genera automaticamente notifiche in forma di email ai referenti della procedura:
   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.

Formato e regole delle credenziali

Il sistema GIA allo stato attuale prevede la realizzazione del cosiddetto singolo login via UserID/Password, ovvero l'utilizzo di credenziali uniche per l'accesso a tutte le Risorse Provisionate, sia direttamente attraverso account di risorse, sia indirettamente attraverso l'uso di servizi di autenticazione, autorizzazione e controllo all'accesso che si basino su servizi di directory come Microsoft Active Directory o Oracle Directory Server.
Le politiche relative agli accountID sono differenziate a seconda della Risorse Autorevole che ne effettua il provisioning:

- **Personale Interno ed Esterno** - accountID di 8 caratteri costituito dei primi 6 caratteri del Codice Fiscale concatenati con 2 cifre numeriche casuali
- **Studenti Iscritti** - accountID di 8 caratteri costituito dalle lettere ID concatenate con 6 cifre numeriche progressive
- **Studenti post-laurearn** - accountID di 8 caratteri costituito dalle lettere VR concatenate con 6 cifre numeriche progressive
- **Frequentatori** – accountID costituito da parte letterale specifica a secondo della sottoclasse (es. OSP per gli ospiti, acronimo congresso per congressisti, ecc.) e parte numerica progressiva

I criteri di robustezza della password previsti nel sistema GIA sono:

- **Lunghezza minima**: 8
- **Lunghezza massima**: 32
- **Minimo numerici**: 1
- **Minimo maiuscoli**: 1
- **Minimo minuscoli**: 1
- **Minimo speciali**: 1

E' prevista l'introduzione della scadenza della password a 3/6 mesi per il Personale Interno.
Non sono attualmente in uso smartcard o token.

Gestione della password di primo accesso o dimenticata via supporto tecnico o self-service

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.
Sono previste modalità alternative: la prima prevede l'intervento del supporto tecnico nelle procedure di identificazione e approvazione; la seconda è compiuta in modalità autonoma ed è disponibile agli utenti che abbiano preventivamente registrato in GIA un indirizzo email privato e sicuro.
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 nel caso abbia dimenticato la password e sia in possesso dell'accountID, ovvero la stringa che rappresenta l'identificatore per la login ai sistemi

2. Tramite un qualsiasi web browser, l'utente accede al sistema GIA la cui pagina iniziale consente di accedere, ovviamente in modalità anonima, ai servizi "Richiesta password di primo accesso", "Password dimenticata" e "Password dimenticata via email", servizi che sono sostanzialmente identici e si differenziano per modalità di accertamento dell'identità del richiedente
3. In seguito alla richiesta dell'utente, il sistema GIA avvia un flusso di gestione che tramite form web richiede ed verifica l'accountId necessario per identificarlo, l'eventuale email privata e sicura e le eventuali informazioni di contatto per gestire problemi nella procedura
4. Nel caso sia stata selezionata la procedura "Password dimenticata via email" viene attivato un task aggiuntivo che:
   - richiede un indirizzo "Email address privato e sicuro" e ne verifica l'esistenza e unicità come attributo nell'insieme di utenti accreditati (una casella a disposizione di più utenti non è privata né sicura)
   - verifica che l'utente non abbia associato alcun Admin Role interno a GIA (i ruoli amministrativi hanno bisogno di procedure di verifica rafforzate)
5. Proseguendo nel flusso, 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.
6. Il sistema GIA visualizza quindi un modulo riassuntivo di tutti i parametri della richiesta, con la sola esclusione della password, genera un task di cambio password che viene sospeso in attesa di approvazione.
7. L'evento di approvazione che sblocca il flusso e permette il reset della password comporta un riconoscimento diretto o indiretto dell'utente:
   7.1. nel caso sia stata attivata la procedura "Richiesta password di primo accesso" o "Password dimenticata" l'utente dovrà ricorrere ad un riconoscimento diretto, ovvero 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 inviare il modulo di richiesta controfirmato via FAX congiuntamente ad una fotocopia di un documento di riconoscimento.
   7.2. nel caso sia stata attivata la procedura "Password dimenticata via email" l'utente dovrà ricorrere ad un riconoscimento indiretto, ovvero dovrà accedere alla casella postale indicata da se stesso nel sistema GIA come privata e sicura per poter sbloccare la procedura
8. L'approvazione viene effettuata:
   8.1. nel caso di riconoscimento diretto dal Tecnico SIA o di Facoltà, che una volta accertata l'identità del richiedente si collega al sistema GIA, individua la richiesta di approvazione attraverso l'identificatore FPID e la approva.
   8.2. nel caso di riconoscimento indiretto, l'Utente riceverà una mail dal sistema GIA nella casella privata e sicura contenente un URL con i parametri ID e CHIAVE, validi per 24 ore, per approvare autonomamente la richiesta entro 1 giorno
9. L'evento di approvazione viene ricevuto dal sistema GIA il quale riprende l'esecuzione del flusso di controllo della procedura effettuando una forma speciale di password reset dell'accountId
10. 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 via supporto o self-service

Il termine "gestione della userID" indica le procedure da attuare nella fase in cui un utente ha dimenticato la userID associata al proprio accountIded ha quindi la necessità di ripristinare l'accesso al sistema GIA, ai servizi e applicazioni.
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):

11. l'utente si presenta dal Tecnico di Facoltà per l'identificazione personale e la comunicazione diretta dell'accountID dimenticato.
12. l'utente delega a termini di legge persona di fiducia per la procedura di cui al punto precedente
13. in caso abbia preventivamente inserito l'indirizzo email privato e sicuro tra gli attributi del sistema GIA, l'utente può ricorrere alla procedura "AccountId dimenticato via email" che lo comunica via posta elettronica

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. Il richiedente dovrà cercare ed aprire in modifica la Identità Virtuale che corrisponde all'utente target il cui Profilo Applicativo deve essere modificato e 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 che se confermata provoca internamente a GIA l'avvio del flusso di aggiornamento dell'identità dell'utente target (Update Task)

3. Il sistema GIA analizza il nuovo assetto della Estensione del Profilo Applicativo e poiché ogni privilegio è definito attraverso un Ruolo Utente, 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.
4. Dopo aver inviato le notifiche agli approvatori, il GIA sospende l'esecuzione del workflow in attesa delle risposte di questi ultimi che provvedono utilizzando i privilegi amministrativi di cui sono in possesso
5. 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.
6. Sia in caso di approvazione che di rifiuto viene inviato al richiedente una mail che descrive l'esito della richiesta e il processo di modifica termina.

Gestione automatica dello stato

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.
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 descritto in paragrafo successivo.
La modifica automatica dello stato è descritta di seguito:

1. Il flusso di gestione automatica dello stato viene attivato dal GIA in modo completamente autonomo e periodicamente nel tempo, tipicamente nel corso della notte.
2. Il flusso è scandito sulla base di date di controllo, scadenza e termine, calcolate dinamicamente ad ogni variazione di stato dell'utenza e associate alle VID presenti nel GIA e applica il flusso di "Gestione Stato VID" descritto successivamente.
3. Se tale flusso 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 flusso "Gestione Stato VID" le attività e i flussi informativi sono di seguito riportati:

1. Il flusso viene invocato dal processo di gestione automatica dello stato dell'identità.
2. Il flusso 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. Se la VID presenta privilegi o profili in scadenza, a seguito ad esempio di scadenza incarico presso UNIVR, viene ricalcolato il Profilo Applicativo e successivamente aggiornate le Risorse Provisionate e la data di verifica successiva.
6. 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 controllo, scadenza e termine, che caratterizzano una VID sulla base delle date di inizio/fine rapporto con UniVR dell'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 e eseguire i necessari controlli e aggiornamenti di privilegi. 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 dal profilo identificativo e applicativo dell'Utente.
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 che assumono il ruolo di **richiedente**.
2. Il richiedente dovrà cercare la Identità Virtuale e attivare o disattivare la funzione di disabilitazione dell'utente messa a disposizione da GIA controllata da un flag di stato.
3. 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 del profilo identificativo e del profilo applicativo.

Il sistema di autenticazione e autorizzazione interno

Il sistema di autorizzazione e autorizzazione interno allo spazio informatico dell'Ateneo gestito dal sistema GIA si basa su due componenti:

1. flussi di accreditamento e profilatura generali basati sulle Classi e Sottoclassi di Identità degli Utenti gestiti dal sistema GIA direttamente o indirettamente, ad esempio via self-provisioning applicativo
2. flussi di autorizzazione e profilatura specifiche gestiti dai Gestori Applicativi sulla base di politiche interne alle applicazioni

Questi flussi di accreditamento e profilatura si traducono nella configurazione del cosiddetto Profilo Applicativo dell'Utente descritto nei paragrafi precedenti che è costituito dalla componente di Base obbligatoria e dalla componente Estesa facoltativa.

Profilo Applicativo di Base

Il Profilo di Base di un utente è composto dal Profilo Identificativo e dalla componente di base del Profilo Applicativo ed è caratterizzato dal fatto che il provisioning degli account nelle risorse che ne fanno parte segue un processo automatico, ovvero appena l'utente viene creato o modificato tramite la risorsa autoritativa, le modifiche si propagano automaticamente da GIA alle risorse.
Il Profilo Identificativo, descritto nei paragrafi precedenti, non è implementato attraverso Ruolo Utente, ma esclusivamente attraverso 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 aspetti di profilatura di livello generale viene inserita nel Profilo di Base anche un insieme di E-Role che vanno a costituire il Profilo Applicativo di Base che, diversamente dal Profilo Identificativo, è funzione non solo dalla CID ma anche dalla SID.
Dal punto di vista dell'implementazione, anche il Profilo Applicativo di Base viene modellato attraverso un Ruolo Utente 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 Ruolo Utente che incapsula i ruoli elementari

La tabella 4 riassume, per ciascuna CID e SID accreditate alla Federazione IDEM, i Profili Applicativi di Base e la loro composizione in termini di E-Role.

CID/SID	Estensione Codice Profilo Applicativo di Base (PROBAS-UTE-....)	E-Role componenti	Descrizione
SID-UTE-PER-TAS	PER-TAS	RETEPER	Profilo Applicativo di Base per i TA Strutturati
		MAILPER	
		APDBERW	
		AWLSPER	
		GESPRES	
		AWEBVPN	
		HELPDSK	
SID-UTE-PER-TAN	PER-TAN	RETEPER	Profilo Applicativo di Base per i TA Non Strutturati
		APDBERW	
		HELPDSK	
SID-UTE-PER-ACS	PER-ACS	RETEPER	Profilo Applicativo di Base per gli Accademici

CID/SID	Estensione Codice Profilo Applicativo di Base (PROBAS-UTE-...)	E-Role componenti	Descrizione
		MAILPER	Strutturati
		APDBERW	
		AWLSPER	
		AWEBVPN	
		HELPDSK	
SID-UTE-PER-ACN	PER-ACN	RETEPER	Profilo Applicativo di Base per gli Accademici Non Strutturati
		APDBERW	
		HELPDSK	
SID-UTE-PER-DIS	PER-DIS	RETEPER	Profilo Applicativo di Base per i Dirigenti Strutturati
		MAILPER	
		APDBERW	
		AWLSPER	
		GESPRES	
		AWEBVPN	
		HELPDSK	
SID-UTE-PER-DIN	PER-DIN	RETEPER	Profilo Applicativo di Base per i Dirigenti Non Strutturati
		APDBERW	
		HELPDSK	
SID-UTE-PER-DOT	PER-DOT	RETEPER	Profilo Applicativo di Base per i Dottorandi
		APDBERW	
		HELPDSK	
SID-UTE-STU-SPE	STU-SPE	RETEPER	Profilo Applicativo di Base per gli Studenti Specializzandi
		HELPDSK	
SID-UTE-STU-POS	STU-POS	RETEPER	Profilo Applicativo di Base per gli Studenti Post-Lauream
		HELPDSK	
SID-UTE-STU-ISC	STU-ISC	RETESTU	Profilo Applicativo di Base per gli Studenti Iscritti
		MAILSTU	
		AWLSSTU	

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 account 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.

Profilo Applicativo Esteso

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:

1. una figura di amministratore GIA inoltra la richiesta di modifica,
2. 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.

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 .

CID o SID	E-Role	Richiedente	Approvazione	Descrizione
SID-UTE-PER-TAS	APPLCIA	ADM-RSP-CDR	ADM-SER-FCO	Estensione per i TA Strutturati
	TITULUS	ADM-RSP-CDR	ADM-SER-PRO	
	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	
SID-UTE-PER-TAN	APPLCIA	ADM-RSP-CDR	ADM-SER-FCO	Estensione per i TA Non Strutturati
	TITULUS	ADM-RSP-CDR	ADM-SER-PRO	
	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	
SID-UTE-PER-ACS	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	Estensione per gli Accademici Strutturati
SID-UTE-PER-ACN	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	Estensione per gli Accademici Non Strutturati
SID-UTE-PER-DIS	APPLCIA	ADM-RSP-CDR	ADM-SER-FCO	Estensione per i Dirigenti Strutturati
	TITULUS	ADM-RSP-CDR	ADM-SER-PRO	
	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	
SID-UTE-PER-DIN	APPLCIA	ADM-RSP-CDR	ADM-SER-FCO	Estensione per i Dirigenti Non Strutturati
	TITULUS	ADM-RSP-CDR	ADM-SER-PRO	
	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	
SID-UTE-PER-DOT	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	Estensione per i Dottorandi
SID-UTE-STU-SPE	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	Estensione per gli Studenti Specializzandi
SID-UTE-STU-POS	ACLTVPN	ADM-RSP-CDR	ADM-SER-SIA	Estensione per gli Studenti Post-Lauream
SID-UTE-STU-ISC				Nessuna estensione per gli Studenti Iscritti

Tabella 5: Composizione delle Estensioni di Profilo Applicativo

I servizi di base dei processi di autenticazione e controllo all'accesso si basano su applicazioni che gestiscono il catalogo e i profili degli utenti nonché lo spazio autoritativo:

1. Microsoft Active Directory - su cui si appoggiano i servizi di autorizzazione all'accesso di dominio, wireless e vpn (via Radius)
2. Oracle Directory Server - su cui si appoggiano i servizi di accesso ai Laboratori informatici, alla posta elettronica, titulus
3. Oracle OpenSSO – su cui si appoggiano i servizi di Single Sign On interni e federati.

Di seguito è riportato schematicamente il disegno della foresta Microsoft Active Directory con le relazioni di trust.

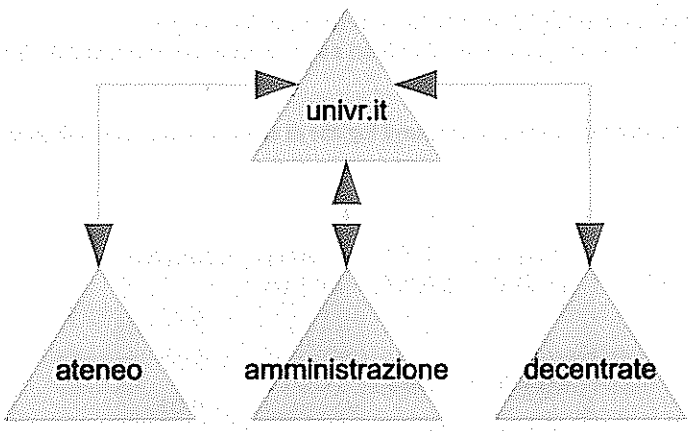


Illustrazione 1: Schema Foresta Active Directory

A commento della Illustrazione 1:

1. la radice UNIVR.IT gestisce i servizi primari di Dominio quali DNS e servizi ad autorizzazione di classe Enterprise Admin
2. il ramo ATENEO.UNIVR.IT contiene gli account utente e i gruppi utente globali utente gestiti direttamente dal sistema GIA
3. il ramo AMMINISTRAZIONE.UNIVR.IT gestisce i computer, i devices e le relative policy, pertinenti alle strutture dell'amministrazione centrale
4. il ramo DECENTRATE.UNIVR.IT gestisce i computer, i devices e le relative policy, pertinenti alle strutture Decentrate (Facoltà, Dipartimenti, Centri, ecc.)

La struttura del dominio ATENEO.UNIVR.IT della foresta Active Directory è identica a quella della radice UNIVR.IT di Oracle Directory Server come descritto nello schema seguente.

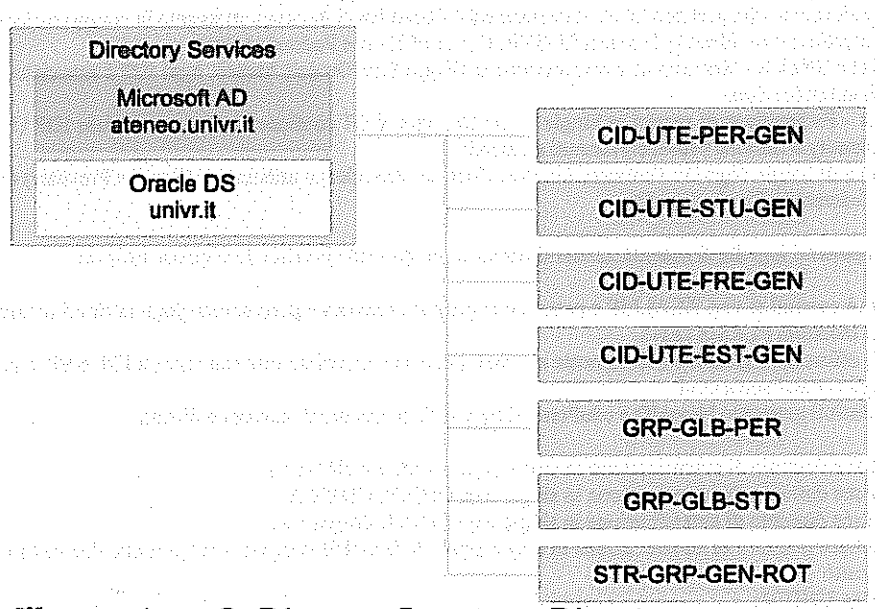


Illustrazione 2: Disegno Struttura Directory

A commento della Illustrazione 2 si descrivono i sottorami generali relativi alla CID e ai gruppi di privilegio globali degli utenti :

- CID-UTE-PER-GEN - ramo delle voci relative agli account del Personale
- CID-UTE-STU-GEN - ramo delle voci relative agli account degli Studenti
- CID-UTE-FRE-GEN - ramo delle voci relative agli account dei Frequentatori
- CID-UTE-EST-GEN – ramo delle voci relative agli account dei Collaboratori Esterni
- GRP-GLB-PER – ramo dei gruppi globali dedicati a servizi specifici di Ateneo

- GRP-GLB-STD – rami dei gruppi globali dedicati a servizi generali di Ateneo
- STR-GRP-GEN-ROT – ramo dei gruppi globali dedicati a servizi generali e specifici delle Strutture

Nella Illustrazione 3 seguente vengono descritte le componenti logiche di alto livello dei servizi di Autenticazione e Single Sign On Federati.

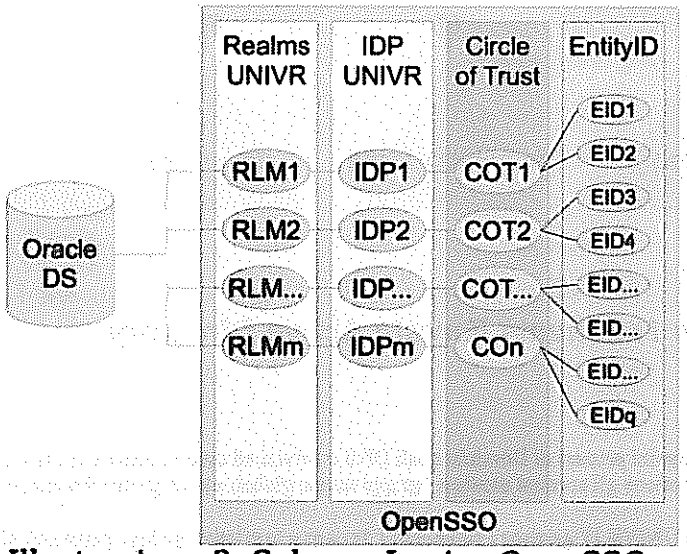


Illustrazione 3: Schema Logico OpenSSO

A commento vengono descritte le singole componenti e le relazioni definite tra esse:

1. **Oracle Directory Server (DS)** – è il datastore ldap degli account e dei gruppi utente, viene gestito da GIA e interrogato da OpenSSO con filtri specifichi per ciascun dominio di autenticazione (REALMS)
2. **OpenSSO** – applicazione che gestisce l'Autenticazione ed il Controllo di Accesso attraverso la configurazione e la gestione di dominii di autenticazione, Identity Provider UNIVR, Circle of Trust e Federated Entity
3. **Identity Provider UNIVR** – Servizio di autenticazione in Single Sign On dell'Ateneo, ogni IDP è associato univocamente a un dominio di autenticazione
4. **Circle Of Trust** – Federazione di servizi in Single Signo On, ogni COT contiene almeno un servizio IDP UNIVR e uno o più EntityID (Identity o Service Provider) ritenuti affidabili
5. **EntityID** – Entità di Single Sign On Federato, fornitori (Identity Provider) o utilizzatori (Service Provider) di servizi di autenticazione federata in Single Sign On

L'Ateneo per le varie componenti logiche di autenticazione federata sopra descritte gestisce le seguenti istanze:

1. **Datastore:**
   1.1. il datastore è comuni ai vari REALMS e permette la gestione univoca e permanente degli attributi utente all'accesso federato in modalità PERSISTENT
   1.2. il NameID offuscato è generato casualmente al primo accesso e associato univocamente a IDP e SP in modo da essere riusato negli accessi successivi
   1.3. IDP e SP distinti generano NameID e eduPersonTargetedID permanenti, univoci e distinti
2. **Realms:**
   2.1. /ate – gestisce dominio di autenticazione in single sign on interno all'Ateneo
   2.2. /cin – gestisce dominio di autenticazione in single sign UNIVR-CINECA
   2.3. /ggl – gestisce dominio di autenticazione in single sign UNIVR-Guglielmo
   2.4. /idem - gestisce dominio di autenticazione in single sign UNIVR-IDEM oggetto del presente documento di accreditamento
3. **Identity Provider UNIVR:**
   3.1. IdP-UniVR-Ateneo - gestisce l'autenticazione in single sign on interno all'Ateneo
   3.2. IdP-UniVR-Ateneo-Cineca – gestisce l'autenticazione UNIVR nella Federazione UNIVR-CINECA
   3.3. IdP-UniVR-Ateneo-Guglielmo – gestisce l'autenticazione UNIVR nella Federazione UNIVR-Guglielmo
   3.4. IdP-UniVR-Ateneo-Idem - gestisce l'autenticazione UNIVR nella Federazione IDEM
4. **Circle Of Trust UNIVR:**
   4.1. COT-UniVR-Ateneo – Gestisce l'accreditamento di IDP e SP interni all'Ateneo
   4.2. COT-Univr-Ateneo-Cineca – Gestisce l'accreditamento UNIVR di IDP e SP interni alla Federazione UNIVR-CINECA
   4.3. COT-Univr-Ateneo-Guglielmo – Gestisce l'accreditamento UNIVR di IDP e SP interni alla Federazione Guglielmo

4.4. COT-UniVR-Ateneo-Idem – Gestisce l'accreditamento UNIVR di IDP e SP interni alla Federazione IDEM

5. **Entità Federate**:
   l'elenco delle Entità Federate accreditate può essere gestito manualmente o con procedure automatiche in relazione alle regole di della federazione.

I **principii** ispiranti la configurazione del Single Sign On sopra descritti sono i seguenti:

- **Separazione delle responsabilità** – ogni Federazione risponde a Enti e Normative propri che non devono essere né direttamente né indirettamente propagate ad altre Federazioni;
- **Separazione dei domini di autenticazione** – ogni Federazione deve avere specifico insieme di utenti UNIVR autorizzati all'accesso;
- **Separazione dei servizi di autenticazione** – ogni Federazione deve avere specifico IDP UNIVR a gestire l'accesso per garantire le politiche di sicurezza concordate;
- **Separazione degli attributi di autenticazione** – ogni Federazione deve avere specifico sottoinsieme di attributi utente che deve essere concordato, per estensione e modalità di gestione, in modo tale da garantire la riservatezza dell'utente.

Sulla base delle scelte operate e descritte in questo paragrafo si può ritenere che le singole Federazioni siano ragionevolmente isolate da UNIVR in modo tale da poterne garantire funzionalità e rispetto delle norme interne.