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

Le informazioni fornite in questo documento sono accurate alla data del 24/10/2012

Revisioni

Data	Versione	Descrizione modifica	Autore
24/10/2012	1.0		M. Ferrante, T.Podestà

1) Abbreviazioni

UniGePASS : sistema gestione indentità di Ateneo
CSITA : Centro Servizi Informatici e Telematici di Ateneo

2) Gestore dell'accreditamento

Sono responsabili del processo di accreditamento degli utenti le seguenti strutture:

Dipartimento Studenti e Dipartimento formazione post-lauream	Studenti
Dipartimento Gestione risorse umane	Personale
Dipartimenti, scuole e centri	Utenti temporanei Altri utenti

CSITA è responsabile del processo di accreditamento per gli aspetti tecnico-informatici e del servizio di supporto/assistenza.

3) Utenti gestiti

Al fine del presente documento, per "utenti" si intendono persone umane. Le eventuali credenziali utilizzate da utenze di servizi (es. protocolli di comunicazione tra sistemi, caselle di posta utilizzate da uffici, stampanti che comunicano con il produttore attraverso proxy HTTP, ecc...) non sono considerate nel presente documento e non vengono propagate al di là dei sistemi coinvolti nelle operazioni che ne fanno uso.

Gli utenti sono associati a zero o più "classi di utenza", largamente basate sulla semantica dell'attributo eduPersonAffiliation dello schema eduPerson.
Utenti senza affiliazione (non propagati al di fuori di UniGe):

- preimmatricolati
- rappresentati delle istituzioni negli Organi Accademici
- personale deceduto

Gli utenti abilitati ad accedere ai servizi generici, in particolare WiFi, HTTP proxy e PC delle aule informatiche, hanno classe **member**.

Personale

Il personale è identificato dal rapporto giuridico e, sostanzialmente, dal fatto di essere pagato dall'Ateneo. Il sistema autoritativo per il personale è SIPERT. Il personale è classificato in tre classi non disgiunte:

- ricercatori e docenti
- personale tecnico-amministrativo, socio-sanitario e area biblioteche
- collaboratori.

Ogni utente del personale, cioè registrato come attivo in SIPERT, ha affiliazione **employee**. Rientrano esclusivamente in questa classe (per gli aspetti del personale):

- dottorandi
- assegnisti di ricerca

- collaboratori a progetto

Il personale inquadrato secondo CCNL del comparto Università o assimilabile, sia accademico, sia TAB, ha affiliazione **staff**. A titolo di esempio:

- personale tecnico/amministrativo a tempo indeterminato o determinato
- lavoratori interinali
- ricercatori, associati e ordinari.

Il personale accademico, ricercatori, associati, ordinari e docenti a contratto (cioè tutti coloro che possono avere incarichi didattici) hanno affiliazione **faculty**.

Studenti

Gli studenti sono identificati quali titolari di una carriera accademica. Il sistema autoritativo per gli studenti è Segreterie. Si noti che per alcuni utenti è possibile essere contemporaneamente affiliati alle classi del personale e degli studenti.
Gli studenti regolarmente iscritti e in regola con le tasse secondo il regolamento didattico (in tempo per laurearsi con mora, 36 mesi dopo l'ultimo pagamento) sono affiliati come classe **student**. Comprendono:

- studenti e laureandi dei corsi di studi (laurea o specialistica)
- dottorandi
- studenti delle scuole di specializzazione
- studenti dei master universitari di I e II livello

Gli utenti che hanno completato un corso di studi che fornisce un titolo legale (laurea, laurea specialistica o dottorato) sono classificati nella classe **alumn**.

Utente temporanei

Sono classificati nella classe **guest** gli utenti che hanno la necessità di accedere alla rete via WiFi e HTTP proxy per un periodo di tempo limitato. La registrazione e il ciclo di vita dell'utente sono gestiti direttamente delle strutture che chiedono l'abilitazione all'attivazione di tale tipologia di identità digitali.
Comprendono:

- partecipanti a convegni e conferenze
- visitatori occasionali.

Altri utenti

Alcuni utenti che non sono gestiti da alcun sistema autoritativo, ma che sono sotto la diretta responsabilità di un altro utente che ne garantisce la corretta registrazione e la gestione del ciclo di vita.

Il personale accademico pensionato, a meno di altre affiliazioni, può mantenere la propria utenza, su richiesta del responsabile dell'ultima struttura di afferenza, registrata nella classe **retiree**.

Su richiesta del responsabile di una struttura, possono essere registrati degli utenti nella classe **affiliate**, nel caso abbiamo bisogno di un set minimo di servizi. A titolo di esempio:

- *visiting professor*
- consulenti
- personale di ditte esterne
- personale dell'Ospedale San Martino o dell'Ospedale Giannina Gaslini.

Di seguito viene riportate in tabella l'affiliazione adottata per i principali gruppi di utenti appartenenti alle categorie sopra individuate (**Personale, Studenti, Utenti temporanei, Altri utenti**).

categoria	utenti	staff	faculty	employee	member	student	affiliate	alumn	retiree	guest	nessuna affiliazione
Personale	docente	X	X	X	X						
	ricercatore	X	X	X	X						
	collaboratore a progetto			X	X						
	assegnisti di ricerca			X	X						
	personale TA[1]	X		X	X						
	collaboratori linguistici	X	X	X	X						
	collaboratori a contratto	X		X	X						
	lavoratore interinale	X		X	X						
Studenti	studente				X	X					
	studente erasmus				X	X					
	studente master				X	X					
	specializzando				X	X					
	dottorando			X	X	X					
	laureato							X			
Utenti temporanei	partecipante a convegni e conferenze									X	
Altri utenti	docente a contratto	X	X	X	X						
	cultore della materia				X						
	fornitore[2 3]				X		X				
	libero professionista [2 4]				X		X				
	dipendente azienda sanitaria[2]				X		X				
	dipendente altro ente di ricerca[2]				X		X				
	pensionato[5]								X		
Senza affiliazione	studente preiscritto										X
	rappresentante ente esterno										X

[1] compreso personale Area biblioteche e Area socio-sanitaria
[2] l'affiliazione attribuita all'utente può essere, in alternativa, **affiliate** oppure **member** in base ad attività svolta/servizi dei quali necessita l'utente
[3] dipendente o titolare di ditta fornitrice
[4] contratto personale con partita IVA
[5] l'eventuale ulteriore affiliazione, oltre **retiree,** può essere attribuita su richiesta di responsabile di struttura

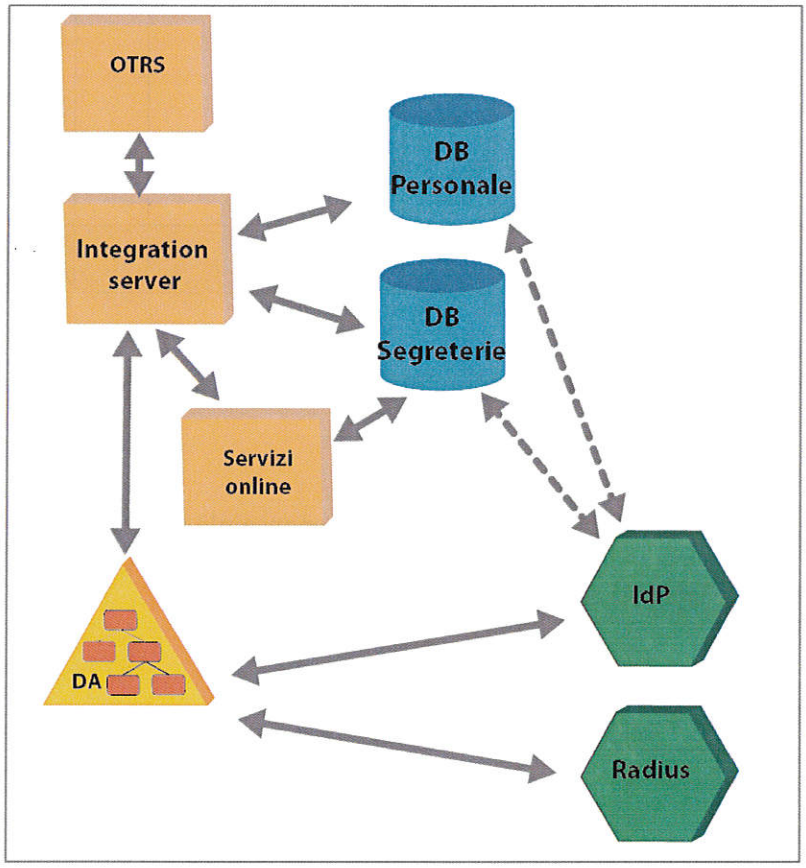
4) Mappatura degli utenti sulle affiliazioni IDEM

categoria	utenti	staff	member	student	affiliate	alum	esclusi
Personale	docente	X	X				
	ricercatore	X	X				
	collaboratore a progetto	X	X				
	assegnisti di ricerca	X	X				
	personale TA	X	X				
	collaboratori linguistici	X	X				
	collaboratori a contratto	X	X				
	lavoratore interinale	X	X				
Studenti	studente		X	X			
	studente erasmus		X	X			

	studente master specializzando dottorando laureato	 X	X X X	X X X		 X	
Utenti temporanei							X
Altri utenti	docente a contratto cultore della materia fornitore[1] libero professionista[1] dipendente azienda sanitaria[1] dipendente altro ente di ricerca[1] pensionato	X	X X X X X X		 X X X X X		
Senza affiliazione	studente preiscritto rappresentante istituzionale						X X

[1] l'affiliazione attribuita all'utente può essere, in alternativa, **affiliate** oppure **member** in base ad attività svolta/servizi dei quali necessita l'utente

5) Visione di insieme del processo di accreditamento degli utenti



UniGePASS è il sistema di autenticazione e gestione identità digitali per tutte le categorie riportate al punto 3.*Utenti gestiti*.
La stessa directory LDAP è utilizzata per tutte le tipologie di utenti.

Fonti autoritative dei dati in essa contenuti sono:

- per la categoria **Studenti** il DB Segreterie gestito tramite l'applicativo client/server Segreterie (sviluppato internamente) e aggiornato anche via portale Servizi Online
- per la categoria **Personale** il DB Personale gestito tramite l'applicativo client/server SIPERT .

Per le categorie **Utenti temporanei** e **Altri utenti** è utilizzato il portale OTRS (Open-source Ticket Request System).

La gestione del ciclo di vita delle identità digitali, per le categorie **Personale** e **Altri utenti** è in fase di revisione, in concomitanza con la migrazione da SIPERT a CSA.

Per tutte le categorie di utenti le credenziali sono del tipo nome utente e password.
Non vengono rilasciate credenziali forti che interagiscano con esse.

Le identità digitali degli utenti cessati delle categorie **Personale** e **Studenti** non vengono cancellate dai DB Segreterie e Personale, ma solo dalla directory LDAP.

6) Il processo di accreditamento per la categoria Studenti

Il processo

Lo **studente** di corso di laurea, laurea magistrale e a ciclo unico al momento della preimmatricolazione on line, se non ne è già in possesso, riceve un nome utente (S seguito dal numero di matricola) e le istruzioni per impostare una password. Durante lo stesso processo vengono acquisiti l'accettazione della policy di Ateneo relativa all'uso delle credenziali UniGePASS e dei servizi di rete e il consenso al trattamento dei dati personali. Alla conferma della domanda presso il Salone dell'immatricolazione, i dati dello studente vengono inseriti nel DB Segreterie e viene aggiornata l'affiliazione a **student, member**.
Struttura organizzativa di riferimento: Dipartimento Studenti

Lo **studente Erasmus** riceve credenziali e badge presso il Servizio Mobilità Internazionale e Accoglienza Studenti Stranieri. Contestualmente l'ufficio preposto acquisisce l'accettazione della policy di Ateneo relativa all'uso delle credenziali UniGePASS e dei servizi di rete.
La creazione delle credenziali è contestuale all'inserimento dei dati dello studente nel DB Segreterie.
Struttura organizzativa di riferimento: Dipartimento Studenti

Lo **studente di Master, scuola di Specializzazione, Dottorato**, se non ne è già in possesso, riceve credenziali e badge presso il Servizio Alta Formazione. Contestualmente l'ufficio preposto acquisisce l'accettazione della policy di Ateneo relativa all'uso delle credenziali UniGePASS e dei servizi di rete.
La creazione delle credenziali è contestuale all'inserimento dei dati dello studente nel DB Segreterie.
Struttura organizzativa di riferimento: Dipartimento formazione post-lauream

Modalità di riconoscimento della persona

Lo **studente** al momento della consegna dei documenti necessari per l'iscrizione è identificato tramite accertamento di documento d'identità, di cui vengono registrati gli estremi.

Caratteristiche dell'identità digitale

Gli attributi associati alla categoria comprendono:
- Nome
- Cognome
- Indirizzo email
- Matricola
- Indirizzi e-mail alternativi (alias)
- Corso di studi

- Telefono cellulare (eventuale)
- Indirizzo email esterno (eventuale)

Nessun attributo è considerato pubblico.

Gestione del ciclo di vita

Le modifiche alla carriera degli **Studenti** sono gestite tramite il sistema client/server Segreterie.
Gli eventi propagati dal DB autoritativo alla directory LDAP comprendono:

evento	misure adottate	tempo/periodicità di propagazione dal DB autoritativo
Trasferimento ad altro ateneo	Le credenziali dello studente trasferito vengono bloccate	entro 24 ore
Rinuncia	Le credenziali dello studente trasferito vengono bloccate.	entro 24 ore
Laurea	Lo studente è spostato nella categoria alumn. Le credenziali rimangono attive per 3 anni dopo la laurea. Dopo tale periodo le credenziali vengono cancellate. Lo studente che necessita di accedere ai servizi di Segreteria online successivamente può riattivarle utilizzando la procedura di recupero password. Il laureato che si iscrive a un altro corso di studio mantiene anche l'affiliazione alumn.	entro 24 ore
Cambio corso di studio		entro 24 ore
Tasse non in regola	Le credenziali dello studente non in regola con il pagamento delle tasse vengono bloccate al 31/3 dell'anno successivo (es. per le tasse dell'a.a. 2011/12 al 31/3 2013)	mensile

I dati che lo studente può modificare direttamente online comprendono: password, indirizzo email esterno e numero telefono cellulare.

Formato e regole delle credenziali

Per tutte le categorie di utenti le credenziali sono del tipo nome utente e password.
La password deve essere lunga almeno 8 caratteri e contenere un carattere tra . ; $! @ - > <

Eventuale presenza di credenziali multiple per la stessa persona

Non è previsto il rilascio di credenziali personali multiple all'utente per la stessa categoria.
Agli utenti che rientrano contemporaneamente nella categoria Studenti e nelle categorie Personale o Altri utenti possono essere attribuite credenziali distinte.

Modalità di consegna delle credenziali

Durante il processo di preimmatricolazione online lo studente riceve il nome utente, mentre la password viene impostata dallo studente stesso.
Negli altri casi lo studente riceve il nome utente corrispondente alla matricola online e la password presso l'ufficio preposto.

Modalità di recupero delle credenziali smarrite

Lo studente che ha inserito numero di telefono cellulare o un indirizzo di posta elettronica esterno può reimpostare la password tramite procedura self-service online raggiungibile dalla pagina di autenticazione.
Alternativamente lo studente può:

- recarsi direttamente presso la Segreteria Studenti o presso lo Sportello dello Studente di dipartimento/scuola
- inviare via fax al Service Desk numero di telefono cellulare e copia documento di identità.

Modalità di gestione smarrimento smartcard/token

Al momento non vengono rilasciati smartcard/token agli utenti in questa categoria.

Durata dell'accreditamento

Le credenziali rimangono attive per 3 anni dopo la laurea. Tuttavia lo studente mantiene il diritto di accesso ai servizi di Segreteria online e può riattivare le credenziali utilizzando la procedura di recupero password.
Lo studente perde il diritto di accesso ai servizi di Segreteria online con la formalizzazione di trasferimento o rinuncia.

Disabilitazione utente

A seguito di trasferimento o rinuncia le credenziali vengono bloccate entro 24 ore dalla registrazione dell'evento nel DB autoritativo.
Le credenziali utente possono essere bloccate anche in caso di violazione delle policy di Ateneo, con particolare riferimento al *Regolamento dell'Università degli Studi di Genova per la realizzazione e gestione della rete dati.*
Alla riabilitazione l'utente deve impostare una nuova password.

Cancellazione definitiva utente

I dati nel DB autoritativo non vengono cancellati. Entry e credenziali UniGePASS rimangono in directory LDAP per 6 mesi oltre la data di disabilitazione.

Rischi specifici associati alla categoria di utenti

Difficoltà di gestione dell'affiliazione nel periodo che intercorre fra il conseguimento della laurea e l'iscrizione a corso di laurea magistrale o altro corso post-laurea.
Sottovalutazione dell'importanza di proteggere le proprie credenziali.
Non è al momento operativa la gestione automatica della scadenza della password.
Manca una policy formalizzata relativa a cancellazione dalla directory al termine del rapporto di lavoro/ studio.

Interoperabilità tra credenziali deboli ed eventuali credenziali forti

Al momento non vengono rilasciate credenziali forti agli utenti in questa categoria.

7) Il processo di accreditamento per la categoria di utenti Personale

La gestione del ciclo di vita è in fase di revisione, in concomitanza con la migrazione da SIPERT a CSA.

Il processo

Il riconoscimento *de visu* dell'utente e l'acquisizione dei dati personali rientrano nelle competenze del Servizio personale docente e del Servizio personale tecnico amministrativo del Dipartimento Gestione risorse umane.

La creazione delle credenziali NON è contestuale all'inserimento dei dati nel DB Personale.
L'utente che al momento della stipula del contratto non è già in possesso di credenziali UniGePASS può chiederne l'attribuzione compilando l'apposito modulo, che comprende l'accettazione della policy di Ateneo relativa all'uso delle credenziali e dei servizi di rete e l'informativa sul trattamento dei dati personali. Il modulo deve pervenire al Service Desk presso C.S.I.T.A. che, utilizzando l'interfaccia web del portale OTRS provvede anche ad effettuare le verifiche necessarie a garantire unicità dell'entry, e invia le credenziali in busta chiusa all'utente presso la sede di servizio o della struttura di afferenza. Durante lo stesso processo può essere attivata la casella email su server di Ateneo.
Se l'utente era già in possesso di credenziali il processo di *conciliazione* rispetto al DB autoritativo affettua i necessari aggiornamenti dell'affiliazione e degli altri attributi, compresa eventuale data di scadenza.

Modalità di riconoscimento della persona

L'utente al momento della consegna dei documenti necessari per l'attivazione del contratto di lavoro è identificato tramite accertamento di documento d'identità, di cui vengono registrati gli estremi.

Caratteristiche dell'identità digitale

Gli attributi associati alla categoria comprendono:
- Nome
- Cognome
- Indirizzo email
- Matricola
- Indirizzi e-mail alternativi (alias)
- Telefono
- Struttura di appartenenza
- Scadenza del contratto (per rapporti di lavoro a tempo determinato)
- Telefono cellulare (eventuale)
- Indirizzo email esterno (eventuale)
- Indirizzo home page personale (eventuale)

I dati
- Nome
- Cognome
- Indirizzo email
- Telefono
- Struttura di appartenenza
- Indirizzo home page personale (eventuale)

del personale con affiliazione **staff** sono pubblicati sul sito web di ateneo.

Gestione del ciclo di vita

Le modifiche alla carriera del **Personale** sono gestite tramite i sistemi client/server SIPERT e Segreterie.
Gli eventi propagati dal DB autoritativo alla directory LDAP comprendono:

evento	misure adottate	tempo/periodicità di propagazione dal DB autoritativo
cessazione-Trasferimento	L'affiliazione dell'utente è aggiornata in **affiliate**, viene impostato l'attributo scadenza e inviato un avviso all'utente dell'imminente blocco delle credenziali. L'utente è invitato a impostare via interfaccia web l'inoltro della posta elettronica a un indirizzo esterno.	mensile
cessazione-Dimissioni	Le credenziali vengono bloccate.	mensile
cessazione-Pensionamento	L'affiliazione dell'utente è aggiornata in **retiree**, viene impostato l'attributo scadenza e inviato un avviso all'utente dell'imminente blocco delle credenziali. L'utente è invitato a impostare via interfaccia web l'inoltro della posta elettronica a un indirizzo esterno. Il personale docente può chiedere, via interfaccia web, il mantenimento delle credenziali e della casella di posta elettronica fino a 2 anni oltre la data di pensionamento.	mensile
cessazione-Decesso	Le credenziali dell'utente vengono bloccate.	mensile
Variazione struttura di afferenza		mensile

Gli attributi che l'utente può modificare direttamente online comprendono: password e home page personale.

Formato e regole delle credenziali

Per tutte le categorie di utenti le credenziali sono del tipo nome utente e password.
La password deve essere lunga almeno 8 caratteri e contenere un carattere tra . ; $! @ - > <

Eventuale presenza di credenziali multiple per la stessa persona

Non è previsto il rilascio di credenziali personali multiple all'utente per la stessa categoria.
Agli utenti che rientrano contemporaneamente nella categoria Studenti e nelle categorie Personale o Altri utenti possono essere attribuite credenziali distinte.
L'utente che passa alla categoria Altri utenti mantiene le stesse credenziali e gli attributi vengono aggiornati per rispecchiare il nuovo rapporto con l'Ateneo.

Modalità di consegna delle credenziali

L'utente riceve le credenziali in busta chiusa via posta interna o a mano.

Modalità di recupero delle credenziali smarrite

L'utente del quale risulta registrato numero di telefono cellulare o indirizzo di posta elettronica esterno può recuperare la password tramite procedura self-service online raggiungibile dalla pagina di autenticazione.
Alternativamente deve recarsi direttamente presso il Service Desk C.S.I.T.A. o inviare richiesta allegando copia di un documento d'identità per ricevere la nuova password in busta chiusa.

Modalità di gestione smarrimento smartcard/token

Non vengono rilasciate smartcard agli utenti in questa categoria.

Durata dell'accreditamento

Per l'utente con contratto a tempo determinato la scadenza è impostata in fase di accreditamento, mentre per il personale a tempo indeterminato la scadenza è impostata alla registrazione della cessazione del rapporto di lavoro. La durata dell'accreditamento nella categoria Personale dipende dalla chiusura del rapporto di lavoro e dall'inquadramento: blocco alla scadenza in caso di dimissioni e decesso, blocco dal mese successivo in caso di trasferimento, pensionamento, scadenza contratto.
Il personale docente può :
- chiedere il prolungamento dell'accreditamento fino a 2 anni con affiliazione **retiree** dopo il pensionamento, -
- concordare la durata del prolungamento con affiliazione **affiliate** in base all'attività didattica residua in caso di trasferimento.

Disabilitazione utente

L'utente con contratto a tempo determinato riceve via posta elettronica due preavvisi, rispettivamente 6 mesi prima e un mese prima della scadenza.
L'utente con contratto a tempo indeterminato riceve un avviso dell'imminente blocco delle credenziali dopo la registrazione della cessazione per pensionamento o trasferimento.
Alla data di scadenza l'affiliazione è aggiornata ad **affiliate** o **retiree.**
Le credenziali vengono disabilitate con procedura automatica a partire dal mese successivo la scadenza. Prima di effettuare la disabilitazione la procedura interroga il DB Personale per accertare la formalizzazione di un ulteriore contratto fra l'Ateneo e l'utente.
La disabilitazione delle credenziali del personale docente può essere posticipata su richiesta dell'utente :

- fino a 2 anni dopo il pensionamento
- in base all'attività didattica residua in caso di trasferimento.

Le credenziali utente possono essere bloccate anche in caso di violazione delle policy di Ateneo, con particolare riferimento al *Regolamento dell'Università degli Studi di Genova per la realizzazione e gestione della rete dati.*
Alla riabilitazione l'utente deve impostare una nuova password.

Cancellazione definitiva utente

I dati nel DB autoritativo non vengono cancellati. Entry e credenziali UniGePASS rimangono in directory LDAP per 6 mesi oltre la data di disabilitazione.

Rischi specifici associati alla categoria di utenti

Sottovalutazione dell'importanza di proteggere le proprie credenziali.
Non è al momento operativa la gestione automatica della scadenza della password.
Manca una policy formalizzata relativa a cancellazione dalla directory al termine del rapporto di lavoro/ studio.
Rischio di richieste di attivazione credenziali falsificate.
Comunicazione di credenziali personali ai collaboratori quando l'applicazione non gestisce il meccanismo di delega.

Interoperabilità tra credenziali deboli ed eventuali credenziali forti

L'unico caso di utilizzo di credenziali deboli e forti riguarda il personale docente che utilizza il servizio per la registrazione elettronica degli esami. L'accesso al servizio avviene tramite credenziali UniGePASS, mentre la firma dei verbali avviene con certificato digitale.

8) Il processo di accreditamento per la categoria di Utenti temporanei

Il processo

Il responsabile di struttura (Dipartimento, Scuola, Centro) può chiedere l'attivazione del servizio di accreditamento di utenti temporanei.
Il riconoscimento dell'utente e l'acquisizione dei dati personali viene effettuato dalle unità di personale per le quali viene formalizzata la richiesta di autorizzazione. La durata dell'accreditamento deve essere impostata all'atto della creazione delle credenziali, non può superare i sei mesi e non è prorogabile.
Il personale autorizzato all'uso della procedura di accreditamento utilizza un'interfaccia web configurata su portale OTRS per inserire inserire i dati, attivare le credenziali e, eventualmente, modificare la data di scadenza.
Alla consegna delle credenziali l'utente deve sottoscrivere l'accettazione della policy di Ateneo relativa all'uso delle credenziali e dei servizi di rete e l'informativa sul trattamento dei dati personali.
A seguito dell'adesione a EduRoam l'esigenza di attribuire credenziali personali temporanee per l'accesso alla rete Wifi e HTTP proxy si è significativamente ridotta.

Modalità di riconoscimento della persona

L'utente è identificato tramite accertamento di documento d'identità, di cui vengono registrati e conservati gli estremi presso la struttura responsabile.

Caratteristiche dell'identità digitale

Gli attributi associati alla categoria comprendono:
- Nome
- Cognome
- Indirizzo email
- scadenza
- Telefono cellulare (eventuale)
- Indirizzo email esterno (eventuale)

Nessun attributo è considerato pubblico.

Gestione del ciclo di vita

L'utente non può modificare direttamente nessun dato.
Alla data di scadenza le credenziali vengono bloccate tramite procedura automatica.

Formato e regole delle credenziali

Per tutte le categorie di utenti le credenziali sono del tipo nome utente e password.

La password deve essere lunga almeno 8 caratteri e contenere un carattere tra . ; $! @ - > <

Eventuale presenza di credenziali per la stessa persona

Non è previsto il rilascio di credenziali personali multiple all'utente che appartiene a questa categoria.

Modalità di consegna delle credenziali

Alla consegna delle credenziali l'utente deve sottoscrivere l'accettazione della policy di Ateneo relativa all'uso delle credenziali e dei servizi di rete e l'informativa sul trattamento dei dati personali.
Le credenziali vengono consegnate a mano direttamente all'utente che al primo accesso deve reimpostare la password.

Modalità di recupero delle credenziali smarrite

L'utente che ha fornito un numero di telefono cellulare o un indirizzo di posta elettronica esterno può reimpostare la password tramite procedura self-service online raggiungibile dalla pagina di autenticazione.
In alternativa l'utente deve rivolgersi al personale autorizzato della struttura.

Modalità di gestione smarrimento smartcard/token

Non vengono rilasciati smartcard/token agli utenti in questa categoria.

Durata dell'accreditamento

La durata dell'accreditamento corrisponde alla durata impostata all'attivazione.

Disabilitazione utente

Alla scadenza mediante procedura automatica giornaliera.

Cancellazione definitiva utente

Entry e credenziali UniGePASS rimangono in directory LDAP per 6 mesi oltre la data di disabilitazione.

Rischi specifici associati alla categoria di utenti

Al momento non esiste un repository centralizzato per la registrazione e conservazione degli estremi del documento di identità dell'utente.

Interoperabilità tra credenziali deboli ed eventuali credenziali forti

Non vengono rilasciate credenziali forti agli Utenti temporanei.

9) Il processo di accreditamento per la categoria di Altri utenti

La gestione del ciclo di vita è in fase di revisione, in concomitanza con la migrazione da SIPERT a CSA.

Il processo

La richiesta di nuovo accreditamento o di prolungamento dell'accreditamento corrente deve essere presentata dal responsabile di struttura (Dipartimento, Scuola, Centro) tramite apposito modulo.
Il modulo comprende una sezione sottoscritta dal responsabile di struttura coi dati personali dell'utente necessari per l'attivazione delle credenziali, previa verifica di precedenti attribuzioni di credenziali allo stesso utente, e gli estremi del rapporto/attività necessari per stabilire la durata dell'accreditamento e l'affiliazione e una sezione che deve essere sottoscritta dall'utente, per l'accettazione della policy di Ateneo relativa all'uso delle credenziali e dei servizi di rete e l'informativa sul trattamento dei dati personali.
Il modulo deve pervenire al Service Desk presso C.S.I.T.A. che, utilizzando l'interfaccia web del portale OTRS provvede anche ad effettuare le verifiche necessarie a garantire unicità dell'entry, e invia le credenziali in busta chiusa all'utente all'indirizzo di Ateneo specificato nella richiesta.
Durante lo stesso processo può essere attivata la casella email su server di Ateneo.
Se l'utente è già in possesso di credenziali UniGePASS nella categoria **Personale** o **Altri utenti** il Service Desk effettua i necessari aggiornamenti dell'affiliazione e degli altri attributi, compresa data di scadenza dell'accreditamento.

Modalità di riconoscimento della persona

L'utente è identificato tramite accertamento di documento d'identità, di cui vengono registrati e conservati gli estremi presso la struttura richiedente.

Caratteristiche dell'identità digitale

Gli attributi associati alla categoria comprendono:
- Nome
- Cognome
- Indirizzo email
- Indirizzi e-mail alternativi (alias)
- Telefono
- Struttura di afferenza
- Scadenza dell'accreditamento
- Telefono cellulare (eventuale)
- Indirizzo email esterno (eventuale)

Nessun attributo è considerato pubblico.

Gestione del ciclo di vita

Gli attributi che l'utente può modificare direttamente online comprendono: password e indirizzo email.
Altre eventuali modifiche degli attributi, compresa variazione della data di scadenza, vengono effettuate dal Service Desk presso C.S.I.T.A. su segnalazione della struttura di afferenza dell'utente.

Formato e regole delle credenziali

Per tutte le categorie di utenti le credenziali sono del tipo nome utente e password.
La password deve essere lunga almeno 8 caratteri e contenere un carattere tra . ; $! @ - > <

Eventuale presenza di credenziali multiple per la stessa persona

Non è previsto il rilascio di credenziali personali multiple all'utente per la stessa categoria.
Agli utenti che rientrano contemporaneamente nella categoria Studenti e nelle categorie Personale o Altri utenti possono essere attribuite credenziali distinte.
L'utente che passa alla categoria Personale mantiene le stesse credenziali e gli attributi vengono armonizzati in un'unica entry nella directory LDAP attraverso una procedura automatica di *conciliazione*.

Modalità di consegna delle credenziali

L'utente riceve le credenziali in busta chiusa.

Modalità di recupero delle credenziali smarrite

L'utente che ha fornito numero di telefono cellulare o indirizzo di posta elettronica esterno può recuperare la password tramite procedura self-service online raggiungibile dalla pagina di autenticazione.
Alternativamente deve recarsi direttamente presso il Service Desk C.S.I.T.A. o inviare richiesta allegando copia di un documento d'identità per ricevere la nuova password in busta chiusa.

Modalità di gestione smarrimento smartcard/token

Non vengono rilasciate smartcard agli utenti in questa categoria.

Durata dell'accreditamento

La durata dell'accreditamento per la categoria **Altri utenti** dipende dalla data di scadenza del rapporto fra utente e struttura richiedente.

Disabilitazione utente

L'utente riceve via posta elettronica due preavvisi, rispettivamente 6 mesi prima e un mese prima della scadenza. La comunicazione viene inviata per conoscenza anche al responsabile della struttura che ha chiesto l'accreditamento.
Alla data di scadenza l'affiliazione è aggiornata ad **affiliate**.
Le credenziali vengono disabilitate con procedura automatica a partire dal mese successivo la scadenza. Prima di effettuare la disabilitazione la procedura interroga il DB Personale per accertare l'eventuale formalizzazione di un ulteriore contratto fra l'Ateneo e l'utente.

Le credenziali utente possono essere bloccate anche in caso di violazione delle policy di Ateneo, con particolare riferimento al *Regolamento dell'Università degli Studi di Genova per la realizzazione e gestione della rete dati.*
Alla riabilitazione l'utente deve impostare una nuova password.

Cancellazione definitiva utente

Entry e credenziali UniGePASS rimangono in directory LDAP per 6 mesi oltre la data di disabilitazione.

Rischi specifici associati alla categoria di utenti

Non è al momento operativa la gestione automatica della scadenza della password.
Sottovalutazione dell'importanza di proteggere le proprie credenziali.
Manca una policy formalizzata per l'accreditamento dell'utente.
Comunicazione di credenziali personali ai collaboratori quando l'applicazione non gestisce il meccanismo di delega.
Al momento non esiste un repository centralizzato per la registrazione e conservazione degli estremi del documento di identità dell'utente.

Interoperabilità tra credenziali deboli ed eventuali credenziali forti

Nessuna

10) Il sistema di autenticazione e autorizzazione interno

Servizi

I servizi che permettono l'accesso con il nome utente e la password UniGePASS comprendono:

- Servizio di posta elettronica di Ateneo, compresi Webmail, sistema antispam, servizio di liste.
- Servizio di posta elettronica per gli studenti
- Siti di e-learning AulaWeb
- Rete GENUAwifi
- Alcuni portali e siti di facoltà e dipartimenti
- Accesso ai computer in aree e laboratori studenti

L'elenco completo, a disposizione degli utenti, è raggiungibile dalla pagina di autenticazione. L'indirizzo attuale è https://unigepass.unige.it/servizi.

Identificatori principali

Gli identificatori principali di ogni persona sono univoci una volta assegnati e non possono essere riutilizzati.
L'attributo eduPersonTargetedID è generato per via algoritmica e presentato di default secondo la sintassi richiesta da Internet2.

Single SignOn

L'Ateneo utilizza simpleSAMLphp per il servizio UniGePASS SSO , che consente l'accesso a:

- Servizi online
- Fase di calcolo per il pagamento online (tasse studenti)
- Liste di posta (Sympa)
- Webmail studenti.

Lo stesso IdP è stato configurato per la partecipazione a IDEM.

La sessione autenticata ha durata di default (8 ore).
La procedura di uscita (Single Logout), attivata dall'utente e inoltrata da un SP partecipante alla sessione verso l'IdP, viene gestita secondo le specifiche tecniche SAML Core.

11) Supporto all'utenza

Il supporto all'utenza viene erogato principalmente dal settore Service Desk di C.S.I.T.A., che si serve di OTRS (Open-source Ticket Request System) per la creazione e gestione di ticket, generati a partire da messaggi di posta elettroniche, richieste inserite via interfaccia web e richieste telefoniche.
Gli studenti hanno a disposizione un numero verde.
Il servizio è operativo nei giorni feriali dal lunedì al venerdì.
Le informazioni dettagliate sono raggiungibili dalla pagina di autenticazione.

12) Partecipazione ad altre federazioni

L'Università degli Studi di Genova aderisce alla federazione **Eduroam.**