Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione Università degli Studi di Napoli Federico II

Revisioni

Data	Versione	Descrizione modifica	Autore
30/05/2010	1	Impostazione documento	Pollio
03/06/2010	2	Scrittura paragrafi 5 e 6	Bonfiglio/Pollio/Vuolo
04/06/2010	3	Correzioni criteri password	Pollio
09/06/2010	4	Corretto par. 6 – inserito schema di principio par. 4	Pollio
09/07/2010	5	Corretto par. 6 – identificazione studenti	Garofalo/Pollio

Abbreviazioni

Le abbreviazioni utilizzate nel documento sono:

CSA – Procedure informatiche e database autorevole di identità per la categoria Staff
CSI – Centro di Ateneo per i Servizi Informativi
GEDAS – Procedure informatiche e database autorevole di identità per la categoria Student
SIS – Area Sistemi di Elaborazione e Microinformatica del CSI
UNINA – Università degli Studi di Napoli Federico II

Sommario

Le informazioni fornite in questo documento sono accurate alla data del **9/07/2010**

1. Gestore dell'accreditamento

La responsabilità del processo di accreditamento degli utenti che afferiscono ad UNINA è affidata agli Uffici del Personale (Docenti e Ricercatori e Tecnico-Amministrativo) per la categoria Staff, e agli Uffici delle Segreterie Studenti di facoltà per la categoria Student. La gestione delle identità digitali di tutti gli utenti è affidata a SIS; informazioni su SIS sono rinvenibili sul sito web del CSI all'url http://www.csi.unina.it/flex/cm/pages/ServeBLOB.php/L/IT/IDPagina/44

2. Utenti gestiti

Le categorie di utenti gestite da UNINA, e le relative cardinalità, sono le seguenti:

Staff	
Docenti	1.663
Personale tecnico amministrativo a tempo indeterminato	3.809
Ricercatori	1.223

Student	
Dottorandi	786
Iscritti a CdS di I e II livello/Master/Scuole di Specializzazione	96.270
Studenti ERASMUS	248

Alumn *(dal 1/1/2005)*	
Dottorati	115
Laureati di CdS/Master/Scuole di Specializzazione	53.900

Affiliate
Nessuno

B2B/Servizi
Nessuno

3. Mappatura degli utenti sulle affiliazioni IDEM

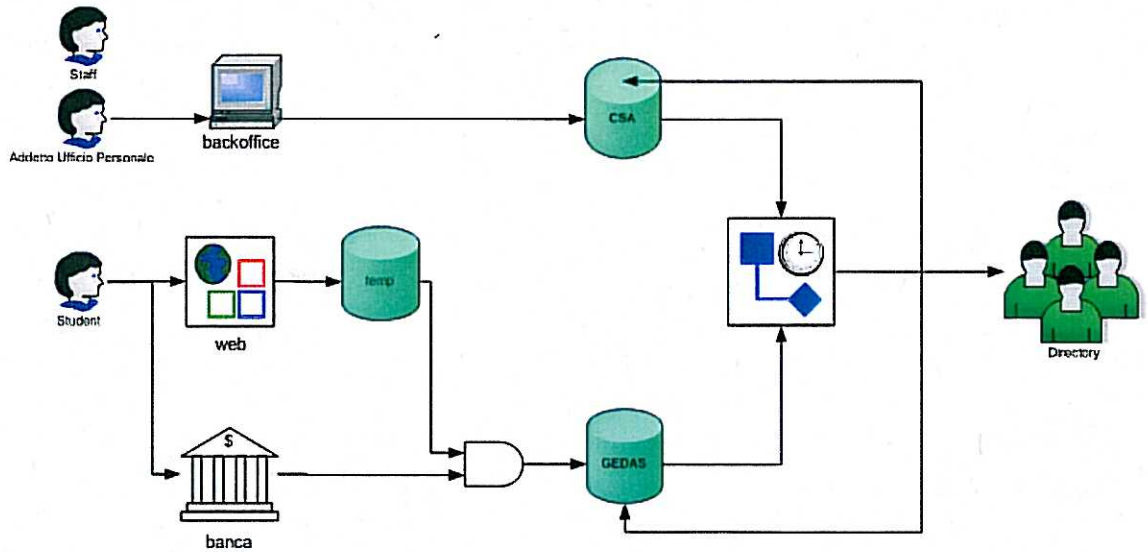
L'associazione in UNINA tra le categorie di utenti (ruoli) e le affiliazioni sono riportate nella seguente tabella:

Ruolo	Affiliazione
Docenti	Staff, Member
Docenti a contratto	Staff, Member
Dottorandi	Student, Member
Dottorati	Alumn, Member
Laureati di corsi di studio/Master/Scuole di Specializzazione	Alumn, Member
Personale tecnico amministrativo a tempo indeterminato	Staff, Member
Ricercatori	Staff, Member
Studenti iscritti a corsi di studio di primo e secondo livello	Student, Member
Studenti iscritti a Master	Student, Member

Studenti iscritti a Scuole di Specializzazione	Student, Member
Studenti ERASMUS	Student, Member

4. Visione di insieme del processo di accreditamento degli utenti

L'accreditamento degli utenti in UNINA si basa su un processo, composto da molteplici componenti, strutturato in fasi e differenziato per categoria di utenza (Staff e Student).
Per la categoria Staff, la prima fase è costituita da una applicazione di backend mediante la quale, gli operatori responsabili del processo nell'ambito degli Uffici del Personale, accreditano l'utente; questa operazione termina con il consolidamento delle informazioni dell'utente nel corrispondente database (CSA).
Per la categoria Student, il primo livello è costituito da un frontend web mediante il quale i soggetti interessati (gli studenti che intendono immatricolarsi presso UNINA) provvedono direttamente a fornire e registrare i loro dati identificativi: con il pagamento delle tasse di immatricolazione, i dati identificativi dello studente sono consolidati automaticamente nel corrispondente database (GEDAS).
La seconda fase del processo di accreditamento degli utenti è uguale per entrambe le categorie di utenti. Questa fase è costituita da procedure informatiche che, in modalità automatica schedulata su base giornaliera, prelevano dai database autorevoli per le rispettive categorie di utenti (CSA, GEDAS) le informazioni utente, generano ed associano ai nuovi utenti un identificativo univoco di identità, propagano gli attributi di identità al directory di UNINA ed aggiornano i database delle rispettive categorie di utenti con l'identificativo univoco di identità.
La terza fase consiste nella comunicazione, ad entrambe le categorie di utenti, del proprio identificativo univoco di identità e del codice di abilitazione personale (PUK per la categoria Staff e PIN per la categoria Student) all'uso dei servizi self service di gestione della propria identità (attivazione identità e scelta password, reset password). Le modalità con le quali avviene questa comunicazione sono differenziate per Staff e Student e sono dettagliate nel seguito di questo documento.
La quarta fase consiste nell'attivazione, da parte degli utenti, dell'identità digitale e nel successivo utilizzo delle credenziali di autenticazione (identificativo univoco di identità e password definita dall'utente) sia nel punto di accesso unico ai servizi costituito dall'Area Riservata presente sul portale UNINA che nei singoli servizi messi a loro disposizione.
Nel seguito si riporta un diagramma che illustra l'architettura di principio del processo di accreditamento sopra descritta.



5. Il processo di accreditamento per la categoria di utenti Staff

Modalità di riconoscimento della persona

Il processo amministrativo che porta all'attribuzione di una identità digitale ad un utente appartenente al ruolo Staff è di responsabilità e competenza degli Uffici del Personale di UNINA, in particolare l'Ufficio Personale Docente e Ricercatori per i Docenti ed i Ricercatori e l'Ufficio Personale Tecnico-Amministrativo per il Personale Tecnico Amministrativo a tempo indeterminato. Il riconoscimento di un nuovo utente avviene attraverso contatto diretto tra gli incaricati del procedimento nell'ambito dei rispettivi uffici e l'utente con la consegna di copie di documenti personali a validità legale (Carta di Identità, Patente, ecc.); è di esclusiva responsabilità dei suddetti incaricati il mantenimento delle informazioni associate all'utente nel corrispondente database CSA, mentre è responsabilità di SIS il mantenimento delle informazioni di identità digitale associate all'utente nel directory di UNINA.

Caratteristiche dell'identità digitale

Ad un utente appartenente al ruolo Staff è associato un identificativo univoco di identità costituito da Nome.Cognome. Le collisioni sono gestite automaticamente dalle procedure informatiche di generazione dell'identificativo attraverso l'aggiunta di un progressivo intero numerico nella parte finale della stringa Cognome. Gli attribuiti associati all'identità digitale di un utente appartenente al ruolo Staff nel momento in cui viene generato l'identificativo sono:
Nome, Cognome, Codice Fiscale, Matricola, Indirizzo email (Nome.Cognome@unina.it), Unità organizzativa di afferenza, PUK (codice personale, memorizzato in formato crittografato nel directory, abilitante all'utilizzo dei servizi self-service), Ruolo.
Gli attributi che possono essere considerati pubblici e forniti a chiunque ne faccia richiesta sono:
Nome, Cognome, Indirizzo email, Unità organizzativa di afferenza, Ruolo

Gestione del ciclo di vita

Le variazioni degli attributi associati ad un utente appartenente al ruolo Staff sono di competenza e responsabilità degli incaricati del procedimento nell'ambito delle unità organizzative degli uffici del personale di UNINA. L'aggiornamento degli attributi associati all'identità digitale dell'utente è effettuato automaticamente da procedure informatiche che, in modalità schedulata, provvedono a rilevare le modifiche degli attributi utente in CSA aggiornando coerentemente il directory di UNINA.

Formato e regole delle credenziali

Le credenziali di autenticazione per gli utenti appartenenti al ruolo Staff sono costituite dalla coppia Nome.Cognome e Password; quest'ultima è scelta direttamente dall'utente all'atto della prima attivazione della sua identità digitale, conformemente alle regole imposte (lunghezza minima otto caratteri). Non è prevista alcuna politica relativamente alla durata della password. Non è previsto l'uso e l'assegnazione di credenziali di tipologia diversa.

Eventuale presenza di credenziali multiple per la stessa persona

Non è prevista l'assegnazione di credenziali multiple per la categoria di utenti appartenenti al ruolo Staff.

Modalità di consegna delle credenziali

Successivamente all'inserimento di un nuovo utente nel database CSA ed a valle del processo automatico di generazione dell'identità digitale, il CSI provvede ad inviare all'utente una comunicazione scritta protocollata in busta chiusa nella quale sono contenute le seguenti informazioni:

- Identificativo Utente nel formato Nome.Cognome
- Indirizzo di posta elettronica nel formato Nome.Cognome@unina.it
- Codice PUK nel formato alfanumerico con lunghezza di 10 caratteri

In questa fase l'identità digitale dell'utente non è attiva; la sua attivazione viene effettuata dall'utente stesso, in modalità self service, mediante l'utilizzo di una applicazione web in https. In particolare l'utente, dopo essersi identificato attraverso la coppia di credenziali Codice Fiscale e PUK, attiva il suo identificativo utente Nome.Cognome e definisce la sua password di accesso. In modo sincrono l'identità digitale dell'utente viene abilitata all'uso dei servizi informatici.

Modalità di recupero delle credenziali smarrite

Nel caso in cui si dimentichi la password di accesso ai servizi, l'utente, in modalità self service mediante l'utilizzo di una applicazione web in https, dopo essersi identificato attraverso la coppia di credenziali Codice Fiscale e PUK, ha la possibilità di resettare la password per definirne una nuova; non è previsto il recupero della password precedente. La variazione ha effetto immediato ai fini dell'autenticazione dell'utente sui servizi informatici.
Nel caso di smarrimento del codice PUK, l'utente è tenuto ad effettuare denuncia dell'evento agli organi di sicurezza (Polizia di Stato, Carabinieri) e ad inviare copia della denuncia al CSI; successivamente il CSI provvede ad inviare all'utente comunicazione scritta protocollata in busta chiusa nella quale è contenuto un nuovo codice PUK.

Modalità di gestione smarrimento smartcard/token

Non applicabile in quanto non sono utilizzati nell'organizzazione dispositivi smartcard/token.

Durata dell'accreditamento

Al momento non è definita alcuna politica che stabilisca la durata dell'accreditamento per la categoria di utenti appartenenti al ruolo Staff. Al termine del rapporto di lavoro dell'utente con l'organizzazione UNINA l'identità nel directory è etichettata opportunamente per tener conto dello stato dell'utente.

Disabilitazione utente

Al termine del rapporto di lavoro dell'utente con l'organizzazione UNINA (cessazione), mediante procedure eseguite in modalità automatica, si disabilita l'identità digitale dell'utente all'accesso all'Area Riservata di UNINA.

Cancellazione definitiva utente

Al momento non è definita alcuna politica che stabilisca le modalità di cancellazione definitiva di un utente appartenente al ruolo Staff.

Rischi specifici associati alla categoria di utenti

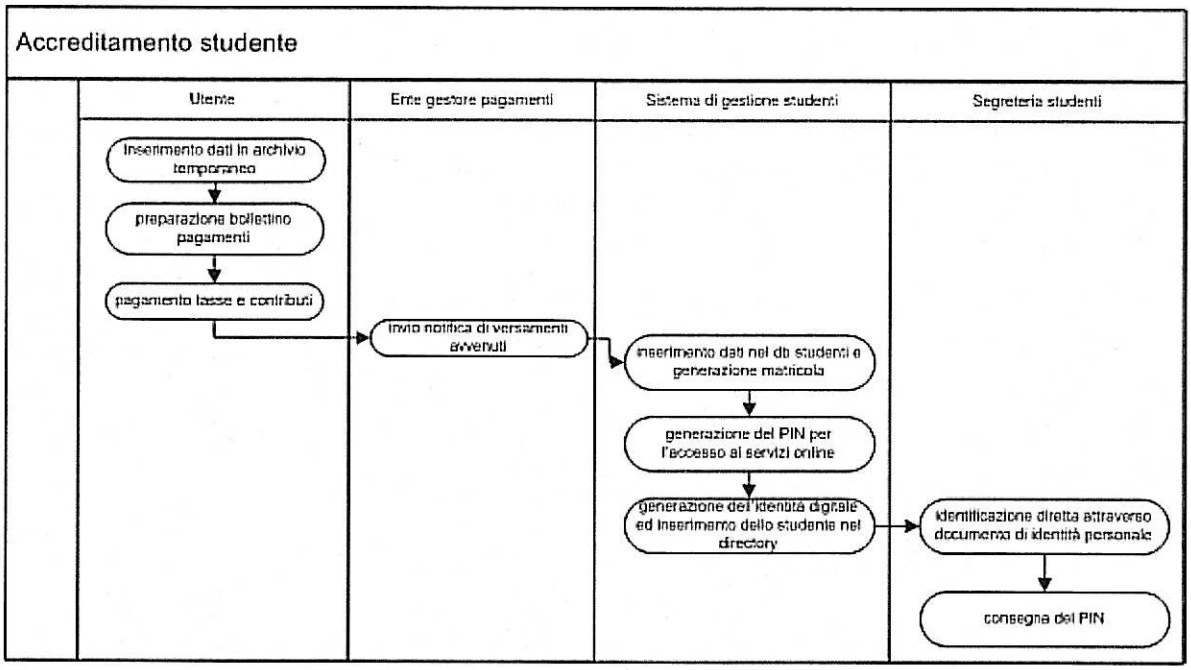
Per la categoria di utenti appartenenti al ruolo Staff si evidenzia la mancanza di policy riguardanti durata della password, durata dell'accreditamento e criteri per la cancellazione degli utenti dal directory al termine del rapporto di lavoro. La definizione delle policy è all'attenzione degli Organi di Governo di UNINA.

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

Non applicabile in quanto non sono utilizzate smartcard.

6. Il processo di accreditamento per la categoria di utenti Student/Alumn

Il processo



Modalità di riconoscimento della persona

Il processo che porta all'attribuzione di una identità digitale ad un soggetto appartenente alla categoria Student si svolge in parte online ed in parte a seguito di identificazione diretta *de visu*, attraverso l'acquisizione dei dati di un documento di identità personale, da parte degli incaricati delle Segreterie Studenti. In particolare uno studente che intenda immatricolarsi presso UNINA, attraverso un servizio web, si registra fornendo tutte le informazioni atte ad identificarlo, compreso gli estremi di un documento di riconoscimento; nella registrazione, lo studente fornisce un indirizzo di posta elettronica sul quale vuole ricevere comunicazioni e sceglie una password di accesso al servizio. In questa fase le informazioni dello studente non sono consolidate nel database autorevole di identità della categoria Student (GEDAS) né nel directory di UNINA. Al momento del pagamento delle tasse universitarie, le informazioni dello studente sono automaticamente consolidate in GEDAS. Procedure informatiche eseguite in modalità schedulata su base giornaliera, prelevano da GEDAS le informazioni dei nuovi utenti, generano ed associano ai nuovi utenti un identificativo univoco di identità, propagano gli attributi di identità al directory di UNINA ed aggiornano il database GEDAS con l'identificativo univoco di identità. Il riconoscimento dello

studente avviene al momento della consegna, da parte degli incaricati delle Segreterie Studenti, dei documenti che lo accreditano come tale presso UNINA (libretto universitario, lettera contenente il codice PIN in busta chiusa sigillata), previa verifica dell'identità attraverso un documento di identità personale.

Caratteristiche dell'identità digitale

Ad un utente appartenente al ruolo Student è associato un identificativo univoco di identità costituito da *prima_lettera_del_Nome*.Cognome: a tale identificativo è associato un indirizzo di posta elettronica nel dominio @studenti.unina.it. Le eventuali collisioni sull'identificativo sono gestite automaticamente dalle procedure informatiche di generazione dell'identificativo attraverso l'aggiunta progressiva di una ulteriore lettera del Nome; nel caso con la stringa Nome completo si verifichi ancora collisione, si utilizza un progressivo intero numerico nella parte finale della stringa Cognome. Gli attribuiti associati all'identità digitale di un utente appartenente al ruolo Student nel momento in cui viene generato l'identificativo sono:
Nome, Cognome, Codice Fiscale, Matricola, Indirizzo email (*prima lettera del Nome*.Cognome@studenti.unina.it), Facoltà, Corso di Laurea, PIN (codice personale, memorizzato in formato crittografato nel directory, abilitante all'utilizzo dei servizi self-service).
Gli attributi che possono essere considerati pubblici e forniti a chiunque ne faccia richiesta sono:
Nome, Cognome, Indirizzo email, Facoltà, Corso di Laurea.

Gestione del ciclo di vita

Le variazioni degli attributi associati ad un utente appartenente al ruolo Student sono di competenza e responsabilità degli incaricati del procedimento nell'ambito delle unità organizzative degli uffici delle Segreterie Studenti di UNINA. L'aggiornamento degli attributi associati all'identità digitale dell'utente è effettuato automaticamente da procedure informatiche che, in modalità schedulata, provvedono a rilevare le modifiche degli attributi utente in GEDAS aggiornando coerentemente il directory di UNINA. Al momento del conseguimento del titolo di studio, un utente appartenente al ruolo Student passa in maniera automatica al ruolo Alumn e le sue credenziali sono attive per i quattro anni solari successivi alla data di laurea.

Formato e regole delle credenziali

Le credenziali di autenticazione per gli utenti appartenenti al ruolo Student sono costituite dalla coppia *prima_lettera_del_Nome*.Cognome e Password; quest'ultima è scelta direttamente dall'utente all'atto della prima attivazione della sua identità digitale, conformemente alle regole imposte (lunghezza minima otto caratteri, presenza almeno di un carattere maiuscolo). Non è prevista alcuna politica relativamente alla durata della password. Non è previsto l'uso e l'assegnazione di credenziali di tipologia diversa.

Eventuale presenza di credenziali multiple per la stessa persona

Agli utenti appartenenti al ruolo Student sono associate credenziali diverse della stessa tipologia al fine di mantenere comunque valide nel tempo le modalità di identificazione che di volta in volta sono state attivate. In particolare gli studenti possono utilizzare in modo equivalente ed in alternativa le seguenti coppie di credenziali:

- login: *prima_lettera_del_Nome.Cognome* oppure *Codice Fiscale* oppure *Matricola* del CdS
- password: *quella scelta in fase di attivazione dell'identità* oppure *codice PIN*

Modalità di consegna delle credenziali

Per gli utenti appartenenti al ruolo Student è prevista la consegna, da parte delle Segreterie Studenti di Facoltà, del codice PIN personale. Questa operazione viene effettuata al momento del rilascio del libretto universitario, da parte degli operatori delle Segreterie incaricati del procedimento, attraverso la consegna allo studente in busta chiusa del codice PIN, previa verifica dell'identità attraverso un documento di identità personale.
In questa fase l'identità digitale dell'utente non è attiva; la sua attivazione viene effettuata dall'utente stesso, in modalità self service, mediante l'utilizzo di una applicazione web in https. In particolare l'utente, dopo essersi identificato attraverso la coppia di credenziali Codice Fiscale e PIN, attiva il suo identificativo utente *prima_lettera_del_Nome.Cognome* e definisce la sua password di accesso.

Modalità di recupero delle credenziali smarrite

Per gli utenti appartenenti al ruolo Student è prevista la possibilità di recuperare il proprio codice PIN nel caso di dimenticanza e/o smarrimento. In modalità self service, lo studente si identifica attraverso la coppia di credenziali Codice Fiscale e identificativo univoco di identità (*prima_lettera_del_Nome.Cognome*) e chiede di voler recuperare il codice PIN. Il sistema, dopo aver verificato le credenziali di autenticazione provvede ad inviare all'indirizzo di posta elettronica istituzionale dello studente (*prima_lettera_del_Nome.Cognome@studenti.unina.it*) il codice PIN.
Nel caso in cui lo studente dimentichi la password di accesso ai servizi, l'utente, in modalità self service mediante l'utilizzo di una applicazione web in https, dopo essersi identificato attraverso la coppia di credenziali Codice Fiscale e PIN, ha la possibilità di resettare la password per definirne una nuova; non è previsto il recupero della password precedente. La variazione ha effetto immediato ai fini dell'autenticazione dell'utente sui servizi informatici.

Modalità di gestione smarrimento smartcard/token

Non applicabile in quanto non sono utilizzati nell'organizzazione dispositivi smartcard/token.

Durata dell'accreditamento

La durata dell'accreditamento per gli utenti della categoria Student/Alumn è pari a quattro anni solari dopo il conseguimento del titolo di studio: al termine di questo periodo l'identità è etichettata opportunamente nel directory di UNINA. Analogo trattamento è effettuato per gli studenti rinunciatari, decaduti o trasferiti.

Disabilitazione utente

Non prevista.

Cancellazione definitiva utente

Al momento non è definita alcuna politica che stabilisca le modalità di cancellazione definitiva dal directory di un utente appartenente al ruolo Student/Alumn.

Rischi specifici associati alla categoria di utenti

Per la categoria di utenti appartenenti al ruolo Student/Alumn si evidenzia la mancanza di policy riguardanti i criteri per la cancellazione degli utenti dal directory. La definizione delle policy è all'attenzione degli Organi di Governo di UNINA.

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

Non applicabile in quanto non sono utilizzate smartcard.

7. Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione delle identità descritto in questo documento è utilizzato per tutte le applicazioni di UNINA ad uso degli utenti del ruolo Staff e Student.
Gli identificatori principali *net ID*, *eduPersonPrincipalName* e *eduPersonTargetedID* una volta assegnati sono univoci e non possono essere riassegnati o riutilizzati.
UNINA utilizza un sistema sviluppato in house che realizza una soluzione di autenticazione unica per alcune applicazioni (Area Riservata); essendo questo sistema fortemente personalizzato per le specifiche esigenze interne all'organizzazione, non si prevede di utilizzare la soluzione per autenticare l'accesso ai servizi della Federazione.

8. Partecipazione ad altre federazioni

UNINA non partecipa ad altre Federazioni di Autenticazione e Autorizzazione.