Documento descrittivo del processo di accreditamento degli utenti dell'Università Ca' Foscari di Venezia

Le informazioni fornite in questo documento sono accurate alla data del 15/07/2010

Revisioni

Data	Versione	Descrizione modifica	Autore
03/05/2010	0.1	Rilascio prima bozza ufficiale per verifiche interne	Alberto Piotto
04/05/2010	0.2	Controllo ortografia, aggiustamenti sui servizi coinvolti e sulla categoria ospiti	Alberto Piotto, Stefano Claut, Roberto Marin
15/07/2010	0.3	Versione definitiva	Alberto Piotto

Abbreviazioni

Personale t/a: Personale tecnico amministrativo
CSA: Applicativo del CINECA per la gestione delle carriere e stipendi del personale
ESSE3: Applicativo Kion/Cineca per la gestione delle carriere degli studenti
CSITA: Centro Servizi Informatici e Telecomunicazioni di Ateneo di Ca' Foscari
AD: Microsoft Active Directory
DOGRU: Divisione Organizzazione e Gestione delle Risorse Umane
IDP: IDentity Provider

Gestore dell'accreditamento

- Per gli studenti è responsabile la segreteria studenti, settore immatricolazioni e accoglienza.
- Per il personale tecnico/amministrativo assunto è responsabile la Divisione Organizzazione e Gestione delle Risorse Umane
- Per il personale Docente, ricercatori, assistenti, lettori di scambio è responsabile la Sezione Personale Docente.
- Per le altre categorie, affiliati, obiettori di coscienza, collaboratori a vario titolo è responsabile il CSITA.
- Per gli ospiti delle biblioteche sono responsabili le segreterie delle varie biblioteche.
- Per gli ospiti di eventi è responsabile l'organizzatore dell'evento.

Utenti gestiti

Gli utenti sono suddivisi in base alla modalità di accreditamento descritta in seguito

Personale strutturato

Personale tecnico amministrativo a tempo determinato e indeterminato, circa 550, inclusi nell'IDP.
Personale docente, circa 400, inclusi nell'IDP.
Ricercatori, circa 150, inclusi nell'IDP.

Personale non strutturato e collaboratori

Docenti a contratto, circa 700, inclusi nell'IDP.
Collaboratori a contratto, circa 300, inclusi nell'IDP.
Assegnisti, circa 100, inclusi nell'IDP.
Collaboratori personali di membri dello staff, circa 100 non inclusi nell'IDP.
Collaboratori per assistenza (persone di ditte esterne che necessitano dell'accesso per prestare assistenza tecnica), circa 10 non inclusi nell'IDP (salvo per necessità particolari).

Studenti

Studenti attualmente iscritti a corsi di laurea, dottorati, master, scuole di specializzazione e corsi singoli, circa 25.000, inclusi nell'IDP.
Studenti che hanno conseguito il titolo, circa 70.000, inclusi nell'IDP.
Studenti non più attivi che non hanno conseguito il titolo, circa 60.000, inclusi nell'IDP.

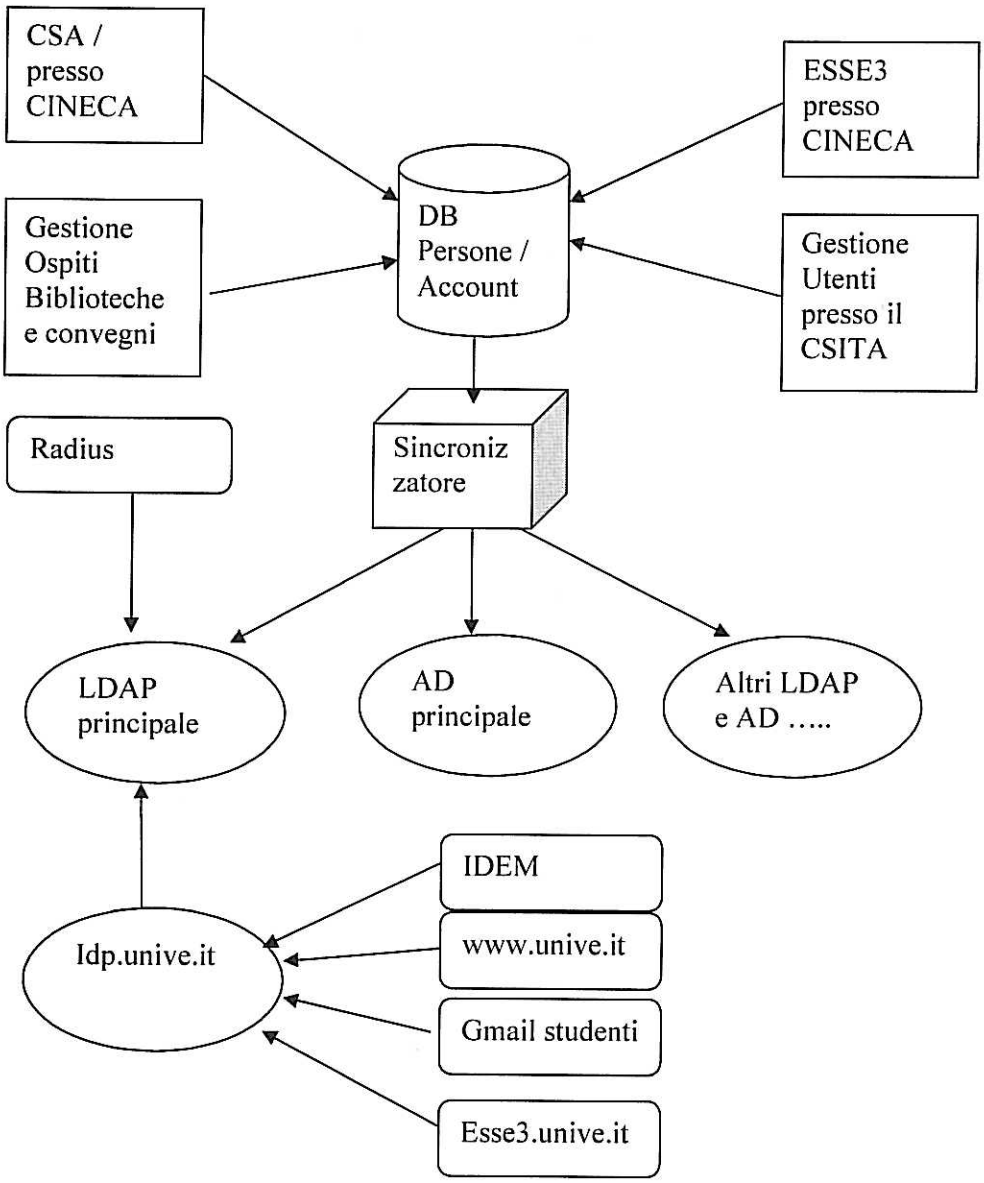
Ospiti

Ospiti delle biblioteche, circa 2000 non inclusi nell'IDP
Ospiti di eventi (convegni conferenze), circa 200, non inclusi nell'IDP

Mappatura degli utenti sulle affiliazioni IDEM

Personale Strutturato (Personale Docente, Persoanle TA), assegnisti, ricercatori	staff, member
Studenti attivi	student, member
Ex studenti	alum
Personale non strutturato (collaboratori a contratto, professori a contratto)	staff, member
Personale non strutturato (servizio civile, borsisti, collaboratori esterni)	member

Visione di insieme del processo di accreditamento degli utenti



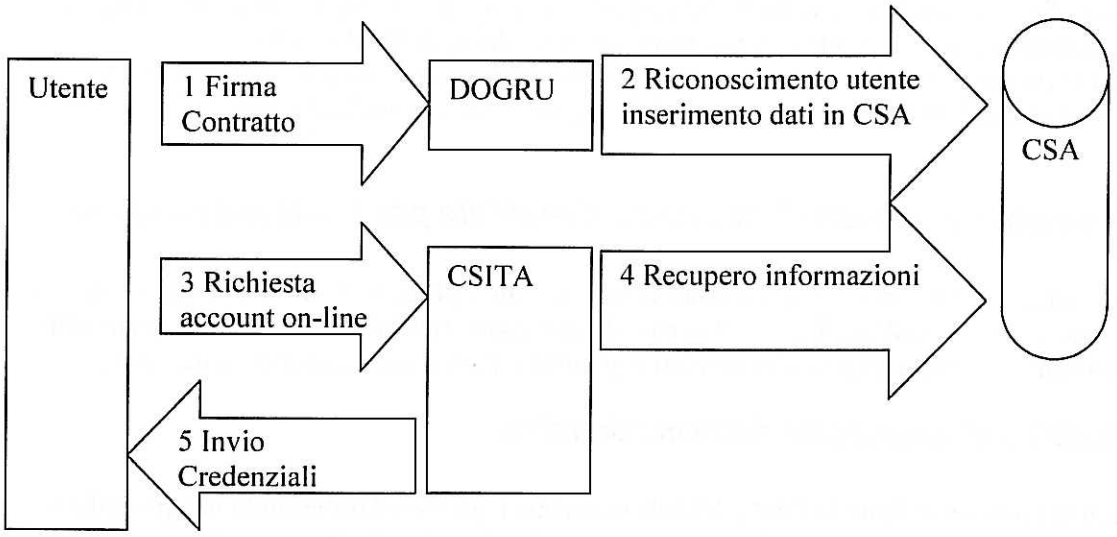
Tutte le informazioni relative alle persone, agli account a loro abbinati, ai ruoli, alle categorie ecc. sono contenute in un database dedicato. In base alla categoria dell'utente i dati provengono da applicativi diversi: il personale docente e t/a strutturato viene importato dall'applicazione CSA, gli studenti vengono importati da ESSE3, gli ospiti temporanei da una procedura utilizzata dalle biblioteche e dai responsabili di convegni ed eventi. Infine per tutte le categorie non importabili direttamente da altri database (collaboratori a vario titolo, volontari servizio civile, fornitori esterni ecc..) si ricorre ad una procedura per l'accreditamento in uso al CSITA.

A partire da questo database in base allo stato delle persone (attive, cessate ecc..) una serie di script automatici vanno ad alimentare e aggiornare un LDAP principale utilizzato per i servizi più

importanti (IDP, VPN, posta elettronica ecc) e altri server LDAP e AD secondari utilizzati soprattutto per l'accesso fisico a computer in aule studio, biblioteche, uffici ecc..
L'LDAP principale viene utilizzato dall'IDP che fornisce il servizio di SSO al portale www.unive.it, al servizio esse3.unive.it e alla federazione IDEM

Il processo di accreditamento per la categoria Personale strutturato

Il processo



Modalità di riconoscimento della persona

Il riconoscimento viene effettuato, mediante un documento di riconosciment, degli operatori della DOGRU, Sezione personale TA e sezione Personale Docente al momento della firma del contratto di assunzione. Successivamente l'operatore carica i dati anagrafici nell'applicazione CSA.

Caratteristiche dell'identità digitale

Al momento della registrazione vengono salvati i dati anagrafici generali (data e luogo di nascita, indirizzi di residenza e domicilio, codice fiscale e numero di telefono) . La persona viene abbinata all'unità organizzativa di afferenza.
Vengono resi pubblici solo il nome, cognome e l'unità organizzativa di afferenza, oltre a recapiti (telefono e e-mail) forniti dall'Università. I recapiti personali (email e telefono personali) non vengono pubblicati salvo non espressamente richiesto dall'utente.

Gestione del ciclo di vita

Il database delle persone viene sincronizzato giornalmente con la procedura CSA quindi le variazioni di carriera o di ruolo della persona si riflettono direttamente anche nelle sue credenziali.

Formato e regole delle credenziali

Le credenziali dell'utente sono costituite da un username alfanumerico (per il personale non è ammesso username solo numerico) di almeno 2 caratteri a libera scelta dell'utente. Il sistema di default propone nome.cognome e fornisce una password alfanumerica di almeno 8 caratteri che contiene obbligatoriamente lettere minuscole, maiuscole e numeri. Se una persona appartiene a più categorie contemporaneamente deve richiedere l'accreditamento per ogni categoria.
Lo username ha validità di un anno dopo il quale per effettuale il rinnovo l'utente deve esprimere l'intenzione di usarlo ancora. Al termine del rapporto di lavoro con l'ente la categoria della persona cambia automaticamente in ospite e lo username rimane valido per un altro anno.
L'utente non può cambiare username, mentre la password può essere modificata a piacere, il sistema verifica che la nuova password soddisfi le regole di sicurezza citate sopra.

Eventuale presenza di credenziali multiple per la stessa persona

Per questa categoria possono essere rilasciate credenziali multiple solo per l'utilizzo del servizio di posta elettronica, ovvero oltre all'account personale si possono richiedere altri account (marchiati come secondari) che non vengono riconosciuti dagli altri servizi e non sono inclusi nell'IDP.

Modalità di consegna delle credenziali

L'utente, una volta accreditato in CSA, richiede username e password utilizzando una procedura on-line. Questa procedura riconosce la persona tramite il codice fiscale, il nome e il ruolo. Una volta selezionato o confermato lo username e la modalità di consegna della password la procedura salva la richiesta in database.
Successivamente un operatore del CSITA verifica la validità delle informazioni la password (con una procedura che genera password casuali) e prepara la lettera di accredito che può essere consegnata in uno dei seguenti modi (a scelta dall'utente):

- Invio delle credenziali tramite SMS
- Invio ad un indirizzo di posta elettronica preesistente
- Invio a mezzo posta ordinaria
- Ritiro a mano presso gli uffici del CSITA

Alla consegna della lettera viene raccomandato all'utente di cambiare la password prima possibile, anche se questa operazione non è obbligatoria.

Modalità di recupero delle credenziali smarrite

Per questa categoria non è previsto un recupero automatico delle credenziali, l'utente deve recarsi presso gli uffici del CSITA e, previo riconoscimento, gli viene assegnata una nuova password.

Durata dell'accreditamento

L'account è valido per un anno dall'accreditamento trascorso il quale l'utente lo può rinnovare utilizzando una procedura automatica on-line (di fatto si vuole solo sapere che l'utente sta utilizzando effettivamente le credenziali).

Disabilitazione utente

Se l'utente non rinnova annualmente l'account quest'ultimo viene disabilitato. Vengono bloccati tutti i servizi tranne quello di rinnovo account e alcuni servizi essenziali legati al rapporto di lavoro (esempio cedolino paga on-line).
Al termine del rapporto di lavoro automaticamente l'utente passa nella categoria ospiti. Di default (salvo richieste particolari) l'unico servizio che rimane attivo per un ulteriore anno è quello di posta elettronica.

Cancellazione definitiva utente

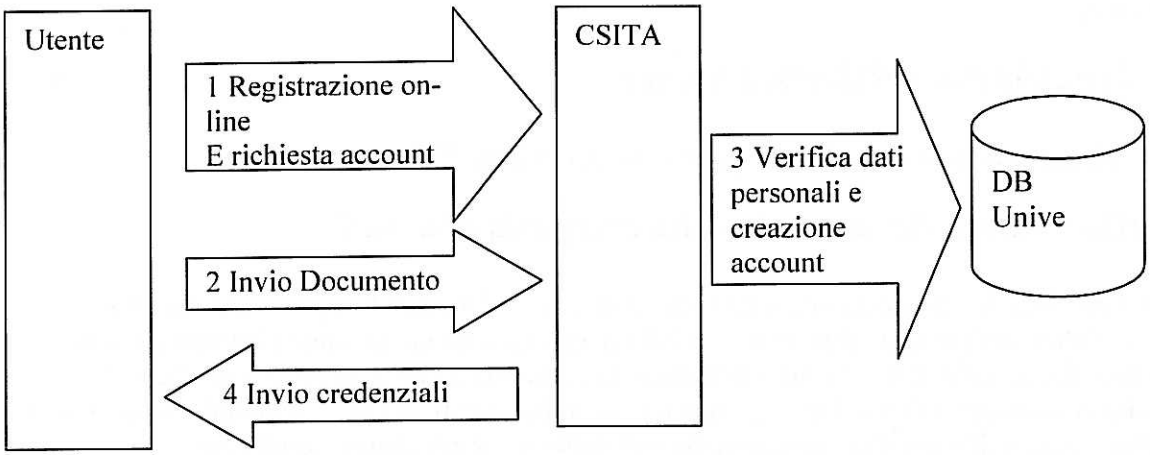
La cancellazione definitiva avviene dopo un anno dal termine del rapporto di lavoro.

Rischi specifici associati alla categoria di utenti

Uno dei grossi rischi di questa categoria è che alcune procedure (cambio password smarrita, rinnovi, abilitazioni) in situazioni particolari di emergenza vengono eseguite via telefono quindi senza una sicura verifica dell'identità dell'utente (ad esempio un docente fuori sede che ha la necessità di accedere all'area riservata urgentemente). Per questi casi si sta pensando ad un sistema di rinnovo e accredito via SMS con un numero di cellulare preregistrato e verificato.
Altro problema potrebbe che una persona a conoscenza dei dati personali di un neoassunto faccia richiesta di accreditamento a nome del neoassunto stesso.
Il rischio però è abbastanza remoto anche perché l'utente "reale" si accorgerebbe dell'accaduto entro breve (la richiesta account è obbligatoria e una volta effettuata blocca le successive).

Il processo di accreditamento per la categoria Personale non strutturato e collaboratori.

Il processo



Modalità di riconoscimento della persona

Il riconoscimento avviene in più fasi; dapprima l'utente fa una richiesta on-line inserendo i dati personali in una procedura web, quindi consegna o manda via fax o email una copia di un documento di identità al CSITA.
Successivamente parte in automatico una mail di segnalazione al responsabile della struttura presso cui l'utente ha dichiarato di essere collaboratore. Se il responsabile conferma la collaborazione e il documento risulta valido l'operatore del CSITA verifica la validità dei dati personali e crea l'account.

Caratteristiche dell'identità digitale

Al momento della registrazione tramite web vengono richiesti i dati anagrafici generali (data luogo di nascita, indirizzo di residenza e domicilio, codice fiscale e numero di telefono) questi dati verranno poi verificati prima della consegna della password.
Vengono resi pubblici solo il nome, cognome e l'unità organizzativa di afferenza, oltre a recapiti (telefono e e-mail) forniti dall'Università. I recapiti personali (email e telefono personali) non vengono pubblicati salvo non espressamente richiesto dall'utente.

Gestione del ciclo di vita

I dati personali vengono aggiornati su richiesta dell'utente, e ripresentati annualmente per la conferma assieme alla richiesta di rinnovo account.

Formato e regole delle credenziali

Le credenziali dell'utente sono costituite da un username alfanumerico (per questa categoria non è ammesso username solo numerico) di almeno 2 caratteri a libera scelta dell'utente. Il sistema di default propone nome.cognome e fornisce una password alfanumerica di almeno 8 caratteri che contiene obbligatoriamente lettere minuscole, maiuscole e numeri. Se una persona appartiene a più categorie contemporaneamente deve richiedere l'accreditamento per ogni categoria.
Lo username è valido per un anno dopo di cui l'utente dovrà fare domanda di rinnovo on-line la quale deve essere confermata dal responsabile della struttura. In questa occasione verrà anche chiesta conferma dei dati anagrafici.
L'utente non può cambiare username, mentre la password può essere modificata a piacere, il sistema verifica che la nuova password soddisfi le regole di sicurezza citate sopra.

Eventuale presenza di credenziali multiple per la stessa persona

Per questa categoria possono essere rilasciate credenziali multiple solo per l'utilizzo del servizio di posta elettronica, ovvero oltre all'account personale si possono richiedere altri account (marchiati come secondari) che non vengono riconosciuti dagli altri servizi e non sono inclusi nell'IDP.

Modalità di consegna delle credenziali

Dopo che l'utente si è registrato, un operatore del CSITA verifica la sua posizione presso la struttura e, ricevuta copia del documento di identità e verifica la validità delle informazioni, genera l'account e la password (con una procedura che genera password casuali). Successivamente prepara la lettera di accredito che può essere consegnata in uno dei seguenti modi (a scelta del richiedente):

- Invio delle credenziali tramite SMS
- Invio ad un indirizzo di posta elettronica preesistente
- Invio a mezzo posta ordinaria
- Ritiro a mano presso gli uffici del CSITA

Alla consegna della lettera viene raccomandato all'utente di cambiare la password prima possibile, anche se questa operazione non è obbligatoria.

Modalità di recupero delle credenziali smarrite

Per questa categoria non è previsto un recupero automatico delle credenziali, l'utente deve recarsi presso gli uffici del CSITA e, previo riconoscimento, gli viene assegnata una nuova password.

Durata dell'accreditamento

L'account è valido per un anno dall'accreditamento; alla scadenza l'utente deve effettuare una richiesta di rinnovo che viene sottoposta a conferma al responsabile della struttura di appartenenza.

Disabilitazione utente

Se l'utente non rinnova annualmente l'account quest'ultimo viene disabilitato. Vengono bloccati tutti i servizi tranne il servizio di rinnovo e alcuni servizi essenziali legati al rapporto di lavoro (esempio cedolino paga on-line).

Cancellazione definitiva utente

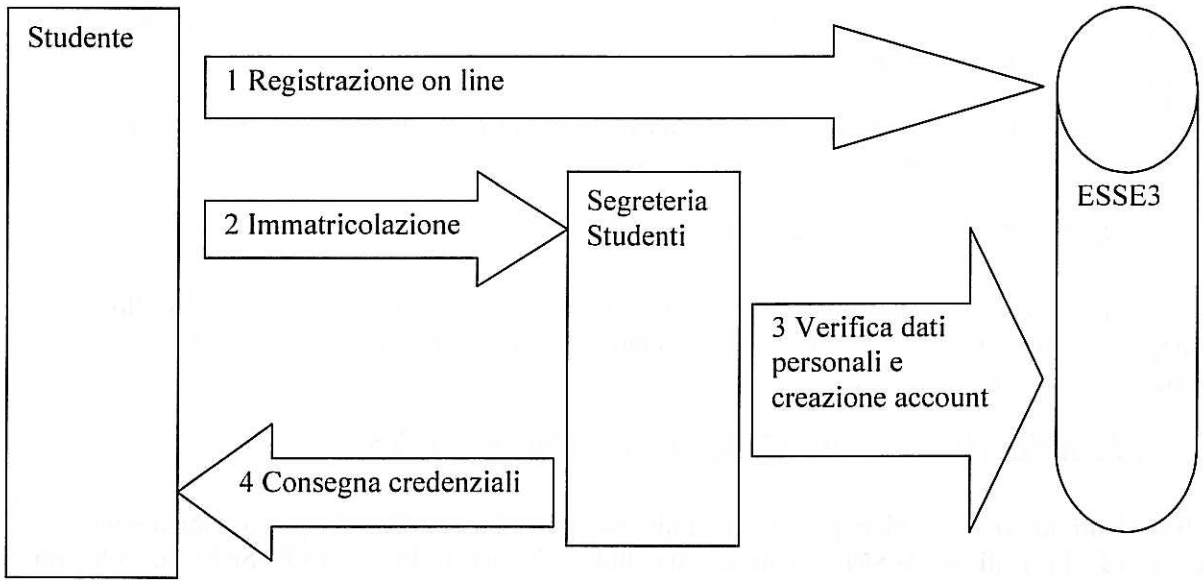
La cancellazione definitiva avviene dopo un anno dalla disabilitazione.

Rischi specifici associati alla categoria di utenti

Oltre ai problemi già discussi per la categoria personale strutturato e legati alla gestione telefonica di richieste quali cambio password, rinnovi ecc.. per questa categoria c'è un problema legato al riconoscimento degli utenti da parte dei responsabili. Può capitare che un responsabile accetti un account di questo tipo senza verificare attentamente la sussistenza di un contratto o di una qualche forma di collaborazione reale, inoltre a volte viene data la conferma anche per semplice conoscenza della persona.
Attualmente gli utenti non sono obbligati a cambiare la password a determinate scadenze. Si sta valutando l'obbligo di un cambio password periodico.

Il processo di accreditamento per la categoria Studenti

Il processo



Modalità di riconoscimento della persona

Il riconoscimento viene effettuato da parte personale delle segreterie studenti al momento dell'immatricolazione tramite richiesta di documento di identità. Contestualmente l'operatore inserisce i dati anagrafici in ESSE3. E' possibile anche che lo studente si sia registrato preventivamente dal sito, in questo caso l'operatore deve solo controllare la validità dei dati inseriti.

Caratteristiche dell'identità digitale

Al momento della registrazione vengono caricati i dati anagrafici generali (data e luogo di nascita, indirizzo di residenza e domicilio, codice fiscale, numero di telefono fisso e cellulare e l'indirizzo email privato). I dati degli studenti non vengono resi pubblici.

Gestione del ciclo di vita

Il database delle persone viene sincronizzato giornalmente con la procedura ESSE3 quindi le variazioni di carriera o di dati anagrafici dello studente si riflettono direttamente anche sulle sue credenziali.

Formato e regole delle credenziali

Le credenziali dell'utente sono costituite da un username numerico che corrisponde al numero di matricola e da una password alfanumerica di almeno 8 caratteri che contiene obbligatoriamente

lettere minuscole, maiuscole, e numeri. L'utente non può cambiare username, mentre la password può essere modificata a piacere, il sistema però verifica che la nuova password soddisfi le regole di sicurezza citate sopra.

Eventuale presenza di credenziali multiple per la stessa persona

Una persona può avere un solo account di tipo studente. In caso lo studente abbia più matricole (fino al 2009 veniva data una matricola per ogni carriera) solo l'ultima è abilitata come username per l'accesso ai servizi.
Se uno studente è anche collaboratore o dipendente presso l'Ateneo dovrà fare due procedura di accredito distinte e avrà credenziali diverse, una per ogni ruolo.

Modalità di consegna delle credenziali

Le credenziali vengono consegnate al momento dell'immatricolazione sotto forma di foglio stampato. Si raccomanda allo studente di cambiare prima possibile la password, anche se questa operazione non è obbligatoria.

Modalità di recupero delle credenziali smarrite

Gli studenti possono cambiare password tramite una procedura on-line che genera una nuova password e la spedisce via SMS al numero di cellulare depositato in segreteria. Se lo studente non ha lasciato il numero di telefono il cambio password può essere effettuato solo recandosi personalmente in segreteria o chiamando il callcenter (in questo caso viene richiesto l'invio di copia del documento di identità).

Durata dell'accreditamento

L'account non ha scadenza. Finché uno studente è attivo è abilitato a tutti i servizi di Ateneo (accesso alle biblioteche, wifi, area riservata, mense ecc..). Quando si laurea o cessa vengono disabilitati tutti i servizi tranne l'accesso all'area riservata per la stampa dei certificati e le procedure amministrative. Questo accesso rimane a vita.

Disabilitazione utente

L'account viene disabilitato solo in caso di fatti gravi come provvedimento cautelativo.

Cancellazione definitiva utente

L'utente non viene mai cancellato, salvo in caso di inserimenti errati.

Rischi specifici associati alla categoria di utenti

Il rischio maggiore legato a questa categoria di utenti è determinato dal fatto che spesso gli studenti sottovalutano l'importanza di proteggere adeguatamente le proprie credenziali, può capitare quindi che queste vengano rivelate ad altre persone per vari motivi. E' in atto da un po' di tempo una campagna di sensibilizzazione sull'argomento.

Attualmente gli utenti non sono obbligati a cambiare la password a determinate scadenze. Si sta valutando l'obbligo di un cambio password periodico.

Il processo di accreditamento per la categoria Ospiti

Questa categoria di utenti non è inclusa nell'IDP e la gestione varia da caso a caso, esponiamo quindi solo le caratteristiche principali per completezza.

Gli utenti possono ottenere un account ospite a vario titolo e questo viene rilasciato solo se la persona non ricade in nessuna delle categorie esposte fino ad ora.
Gli account ospite vengono utilizzati solo per l'accesso alla rete WiFi o ai computer delle biblioteche, inoltre se sono rilasciati in occasione di eventi particolari (conferenze, convegni ecc..) sono validi solo per la durata dell'evento.
Lo username e la password vengono generati in automatico nel formato 150XXX per le biblioteche e guestXXXX per le altre strutture, e non sono modificabili dall'utente.
In caso di account legati a un evento, l'organizzatore è responsabile dell'accreditamento degli utenti che avviene tramite riconoscimento con documento di identità e l'inserimento dei dati in una apposita procedura. I dati raccolti sono quelli richiesti dalla legge per l'accesso alla rete e non vengono pubblicati in nessun modo.
L'utente non può né cambiare né recuperare la password, in caso di necessità questa operazione può essere fatta solo dal responsabile che genera una nuova password.
Alla scadenza l'account viene disabilitato e i dati personali vengono mantenuti per il tempo previsto dalla legge in caso di contestazioni e poi eliminati.
Gli username scaduti vengono riciclati (modificando la password) per i nuovi ospiti, viene però mantenuta traccia dell'intervallo di tempo preciso durante il quale un certo username è stato assegnato ad una certa persona.

Il sistema di autenticazione e autorizzazione interno

Il sistema di autenticazione e autorizzazione viene usato per i seguenti servizi:

- Accesso all'area riservata del portale di Ateneo
- Accesso all'area riservata del sito ESSE3 (in SSO assieme al portale di Ateneo)
- Servizio di posta elettronica del dominio @unive.it
- Accesso ai server web dedicati ai siti personali (virgo.unive.it e venus.unive.it).
- Accesso fisico alle biblioteche
- Accesso alla rete WiFi di Ateneo
- Accesso ai computer pubblici in aule studio e biblioteche.
- Accesso alle colonnine self-service di Ateneo.
- Accesso al servizio VPN di Ateneo
- Accesso a IDEM
- Accesso gmail studenti

L'identificatore dell'utente è rappresentato dal suo username, alcuni identificatori possono venire riutilizzati, ad esempio "rettore" viene assegnato di volta in volta al rettore attuale, però questi account sono abilitati solo al servizio di posta elettronica e non vengono inclusi nell'IDP. Per tutti gli altri servizi l'utente utilizza il suo account personale che non viene riutilizzato.

Per quanto riguarda gli ospiti invece vengono utilizzati degli username presi da un pool e quindi riutilizzati. Questi username però non vengono inclusi nell'IDP,

Partecipazione ad altre federazioni

Attualmente esiste una federazione tra l'Università Ca' Foscari di Venezia e l'Università IUAV di Venezia, la federazione permette agli utenti di una Università di accedere alla rete WIFI dell'altra. Dato che la federazione riguarda solo l'autenticazione dell'utente non vengono scambiati dati personali tra le due Università.

Venezia 15/07/2010

Il Referente Organizzativo
Dott. Alberto Piotto