Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione UNICAM

Revisioni 1
Nota introduttiva 1
Abbreviazioni 1
Gestore dell'accreditamento 3
Utenti gestiti 3
    Personale 3
    Studente 3
Mappatura degli utenti sulle affiliazioni IDEM 4
Visione di insieme del processo di accreditamento degli utenti 4
Il processo di accreditamento per la categoria di utenti Personale 4
    Il processo 4
    Modalità di riconoscimento della persona 4
    Caratteristiche dell'identità digitale 4
    Gestione del ciclo di vita 5
    Formato e regole delle credenziali 5
    Eventuale presenza di credenziali multiple per la stessa persona 5
    Modalità di consegna delle credenziali 5
    Modalità di recupero delle credenziali smarrite 5
    Modalità di gestione smarrimento smartcard/token 5
    Durata dell'accreditamento 5
    Disabilitazione utente 5
    Cancellazione definitiva utente 6
    Rischi specifici associati alla categoria di utenti 6
    Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard) 6
Il processo di accreditamento per la categoria di utenti Studente 7
    Il processo 7
    Modalità di riconoscimento della persona 7
    Caratteristiche dell'identità digitale 7
    Gestione del ciclo di vita 7
    Formato e regole delle credenziali 7
    Eventuale presenza di credenziali multiple per la stessa persona 7
    Modalità di consegna delle credenziali 7
    Modalità di recupero delle credenziali smarrite 8
    Modalità di gestione smarrimento smartcard/token 8
    Durata dell'accreditamento 8
    Disabilitazione utente 8
    Cancellazione definitiva utente 8
    Rischi specifici associati alla categoria di utenti 8
    Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard) 8
Il sistema di autenticazione e autorizzazione interno 9
Partecipazione ad altre federazioni 9

Revisioni

Data	Versione	Descrizione modifica	Autore
01/10/2012	0.1	Stesura iniziale	Fausto Marcantoni
23/10/2012	0.2	Minori revisioni	Fausto Marcantoni
05/11/2012	1.0	Rilasciato	Fausto Marcantoni

Nota introduttiva

Il presente documento contiene le indicazioni tecnico-operative di carattere generale finalizzate all'adesione dell'Università degli studi di Camerino alla Federazione IDEM –coordinata dal Consortium GARR.

Abbreviazioni

AAA Authentication, Authorization, Accounting
AAI Authentication and Authorization Infrastructure
CINFO Centro Servizi Informatici e sistemi informativi
DOPAU Documento sul Processo di Accreditamento degli Utenti
DPS Documento Programmatico sulla Sicurezza
IAM Identity and Access Management
IdP Identity Provider
RADIUS Remote Authentication Dial-In User Service
SP Service Provider
SSO Single Sign On
UNICAM Università degli Studi di Camerino
URL Uniform Resource Locator

Gestore dell'accreditamento

L'accreditamento è gestito dalle seguenti strutture:

- Ufficio del Personale, per il personale docente e tecnico-amministrativo e per tutti gli altri soggetti che stipulano con Unicam un contratto di collaborazione e/o insegnamento, all'atto della firma del contratto.
- Segreterie Studenti, per gli studenti immatricolati a qualsiasi titolo presso Unicam.
- CINFO, per il personale e per tutti gli altri soggetti che hanno titolo all'utilizzo dei servizi internet e posta elettronica erogati da Unicam, a seguito di identificazione personale.

La raccolta dei dati, il filtraggio e l'armonizzazione sono in capo al CINFO.
Eventuali azioni correttive ai processi sopra illustrati vengono effettuate dal CINFO
La gestione dell'accreditamento riguarda esclusivamente il ciclo di vita delle identità digitali mentre la definizione e la formalizzazione del rapporto di lavoro dell'individuo con l'ateneo ne è un prerequisito.

Utenti gestiti

Nella tabelle seguenti sono riportate tutte le categorie d'utenza presenti in ateneo e la loro appartenenza ad una macro categoria meglio descritta nel seguito.

N	Descrizione categoria utenze d'ateneo	Codice macro categoria
1	Personale docente e tecnico-amministrativo	P
2	Studente	S

Tabella di dettaglio delle categorie di utenza classificate in ateneo

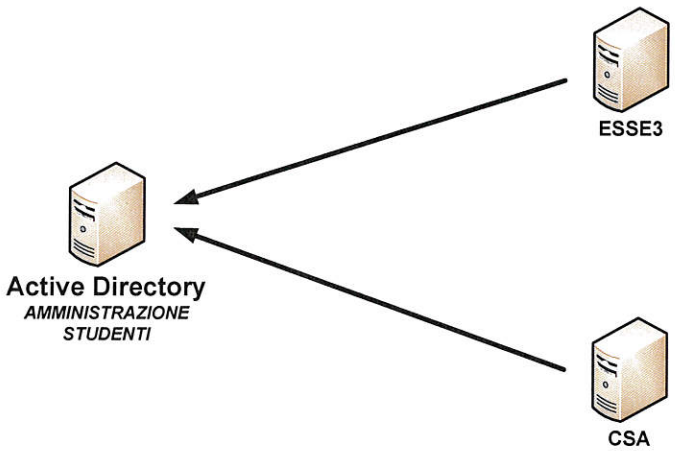
N	Codice	Nome macro categoria	Elenco categorie incluse
1	P	Personale	Personale docente di ruolo, Docente supplente esterno, Docente a contratto, Personale ricercatore di ruolo, Assegnista di ricerca, Personale tecnico ed amm.vo a tempo indet./det., Dottorandi, Dottorandi di Università consorziate
2	S	Studente	Studente, Studente frequentatore, Laureato,Studente Erasmus

Tabella delle macro categorie di utenza classificate in ateneo

Visione di insieme del processo di accreditamento degli utenti

La base dati degli utenti e le informazioni associate alle identità digitali vengono conservate all'interno di un database Oracle e gestite tramite applicativi client e applicativi Web.
Una procedura eseguita ad intervalli regolari effettua gli aggiornamenti sul database LDAP (che alimenta i servizi Shibboleth e RADIUS) sul server Active Directory (che gestisce il dominio UNICAM.IT per i computer desktop) e infine sul server di posta MAIL.UNICAM.IT (per la gestione delle caselle di posta elettronica).

Un'altra procedura sincronizza invece le informazioni di tutti gli studenti presenti nel database Esse3. Il link di cambio password è attivo nella applicazione Web di Esse3 nella sezione "Area riservata".
L'utente utilizza le proprie credenziali per l'accesso alle postazioni delle aule informatiche e delle postazioni pubbliche di Unicam e presso tutti i servizi locali che utilizzano il server LDAP per autenticare i propri utenti.
Il grafico seguente illustra il flusso dei dati ed evidenzia in rosso le connessioni sicure.



Il processo di accreditamento per la categoria di utenti P - Personale

Il processo

Struttura organizzativa di riferimento: Ufficio del Personale.
Responsabile accreditamento: Responsabili dell'Ufficio del Personale.
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali delle categorie trattate in questo capitolo.

Modalità di riconoscimento della persona

Ufficio di riferimento: Ufficio del Personale.
Modalità di riconoscimento della persona: avviene al momento dell'assunzione con la presenza fisica della persona presso l'ufficio preposto che effettua il controllo dei documenti d'identità personale e ne trattiene copia agli atti. Contestualmente viene consegnata alla persona la documentazione relativa al consenso per il trattamento dei dati personali e alle acceptable user policy (AUP) del GARR. Il processo si conclude con l'accettazione delle AUP e con il rilascio del consenso del trattamento dei dati da parte della persona mediante la sottoscrizione autografa di un modulo cartaceo che viene acquisito agli atti. A questo punto l'ufficio preposto esegue l'inserimento del record personale all'interno del database delle identità digitali mediante apposita applicazione web client protetta.

Caratteristiche dell'identità digitale

Elenco degli Attributi associati all'identità digitale: i dati anagrafici, i dati di rubrica (mail, telefono, fax), il codice fiscale, l'identificativo, il numero del badge e i dati dell'inquadramento (area e struttura di appartenenza, afferenza didattica, inquadramento, stato di servizio, ecc.).

Elenco degli Attributi associati all'identità digitale considerati pubblici: Gli unici dati pubblici sono nome e cognome, telefono, fax, mail, area e struttura di appartenenza, afferenza didattica.

Gestione del ciclo di vita

L'aggiornamento del database delle identità digitali è a carico degli uffici preposti. Il ciclo di vita dell'identità digitale avviato con l'accreditamento iniziale prosegue con gli stessi strumenti di gestione e le medesime modalità di accesso all'applicazione web client di attribuzione dell'identità digitale. Quando un utente subisce variazioni, queste vengono sincronizzate con tutti i sistemi.

Formato e regole delle credenziali

Le credenziali fornite sono del tipo: userID/password.
Nel corso degli anni sono stati adottati diversi criteri per l'assegnazione degli UserID e, per questa ragione, si riscontrano le seguenti tipologie di UserID:

- nome.cognome;
- cognome + 1° lettera del nome;
- nome.

La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri.
A tutti i dipendenti viene inoltre rilasciata una tessera con banda magnetica e RFID utilizzata per rilevare le presenze.

Eventuale presenza di credenziali multiple per la stessa persona

Le credenziali multiple servono per servizi diversi e non interagiscono.

Modalità di consegna delle credenziali

Le credenziali sono consegnate dall'Ufficio del Personale.

Modalità di recupero delle credenziali smarrite

Le credenziali smarrite e/o dimenticate possono essere richieste solo all'ufficio preposto per una nuova assegnazione.

Modalità di gestione smarrimento smartcard/token

La tessera magnetica con RFID smarrita e/o deteriorata può essere richiesto all'Ufficio del Personale. In caso di smarrimento è revocato il precedente ed emesso uno nuovo.

Durata dell'accreditamento

Gli utenti di questa categoria sono accreditati per tutto il tempo in cui sussiste il rapporto di lavoro.

Disabilitazione utente

Per le categorie caratterizzate da un rapporto di lavoro a termine la disabilitazione avviene in modo automatico alla data di fine rapporto. Per le altre categorie del personale l'eventuale disabilitazione

viene fatta manualmente dall'ufficio del personale attraverso una specifica procedura applicativa. Dall'avvenuta disabilitazione la persona non potrà più condurre con successo la procedura di autenticazione.

Cancellazione definitiva utente

Per le categorie caratterizzate da un rapporto di lavoro a termine la cancellazione definitiva viene fatta manualmente dall'ufficio del personale. Per le categorie caratterizzate da un rapporto di lavoro a tempo indeterminato (o di ruolo) non è prevista la cancellazione.

Rischi specifici associati alla categoria di utenti

La procedura manuale di disattivazione e cancellazione dell'utente può essere soggetta a dimenticanze ed errori umani. Al fine di mitigare questo rischio è prevista una verifica periodica con il database dei contratti detenuto dall'ufficio del personale.

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

Non è prevista interoperabilità tra credenziali deboli e forti per le categorie di utenti trattata.

Il processo di accreditamento per la categoria di utenti S - Studente

Il processo

Struttura organizzativa di riferimento: Segreteria studenti.
Responsabile accreditamento: Responsabili della Segreteria studenti.
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali delle categorie trattate in questo capitolo.

Modalità di riconoscimento della persona

Ufficio di riferimento: Segreterie studenti.
Modalità di riconoscimento della persona: avviene al momento dell'immatricolazione con la presenza fisica della persona presso la Segreterie studenti che effettua il controllo dei documenti d'identità personale e ne trattiene copia agli atti. Il processo si conclude con il rilascio del consenso del trattamento dei dati da parte della persona mediante la sottoscrizione autografa di un modulo cartaceo che viene acquisito agli atti. A questo punto l'ufficio preposto esegue l'inserimento del record personale all'interno del sistema Esse3 delle identità digitali mediante apposita applicazione web client protetta.

Caratteristiche dell'identità digitale

Elenco degli Attributi associati all'identità digitale: tutti i dati dell'anagrafica, i dati della facoltà, del corso di laurea, dell'indirizzo di studi, dell'anno di corso, dello stato di avanzamento degli studi.
Elenco degli Attributi associati all'identità digitale considerati pubblici: nessuno dato è pubblico.

Gestione del ciclo di vita

L'aggiornamento del database delle identità digitali è a carico dell'ufficio preposto ed il ciclo di vita è pilotato dal sistema di gestione degli studenti Esse3. Gli strumenti di gestione e le modalità di accesso all'applicazione sono i medesimi del processo di attribuzione dell'identità digitale.

Formato e regole delle credenziali

Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici, nella forma nome.cognome. La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri.

Eventuale presenza di credenziali multiple per la stessa persona

Non esistono casi particolari della categoria studenti per i quali è prevista la generazione di due identità digitali. Solo in caso di dipendenti che si iscrivono ad un corso di laurea di UNICAM, vengono analizzate soluzioni particolari.

Modalità di consegna delle credenziali

Le credenziali sono inviate dalla Segreteria studenti, presso l'indirizzo indicato dallo studente al momento dell'immatricolazione tramite busta chiusa.

Modalità di recupero delle credenziali smarrite

In caso di userID smarrito e/o di mancata ricezione della busta chiusa, le credenziali possono essere

- richieste di persona alla Segreteria studenti o allo sportello Unicitt@
- richieste mediante una procedura web che invierà una nuova pwd su un indirizzo email che lo studente ha indicato sotto propria responsabilità con una comunicazione formale.

Modalità di gestione smarrimento smartcard/token

Non sono utilizzati smartcard/token.

Durata dell'accreditamento

Agli utenti di questa categoria l'accreditamento viene revocato solo in caso di cessazione degli studi o di trasferimento a un altro Ateneo.

Disabilitazione

L'identità digitale rimane sempre attiva. Nel caso in cui lo studente si sia laureato, può comunque accedere all'applicativo di gestione della sua carriera.

Cancellazione definitiva utente

Non è prevista la cancellazione definitiva di uno studente.

Rischi specifici associati alla categoria di utenti

Non si evidenziano rischi specifici per la categoria di utenti trattata.

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

Non è prevista interoperabilità tra credenziali deboli e forti per le categorie di utenti trattata.

Il sistema di autenticazione e autorizzazione interno

Elenco delle applicazioni interne all'ateneo che utilizzano il sistema di gestione delle identità:

Applicazioni
Accessi pubblici alla rete dati d'ateneo
Accessi sicuri in VPN da internet alla rete dati d'ateneo
Gestione amministrativa del personale
Protocollo elettronico
Servizi bibliotecari di consultazione e prestito
Servizi di posta elettronica/mailing list del personale e degli studenti
Servizio di accounting stampa
Piattaforma di E-Learning Moodle

Tabella delle applicazioni interne e relativo metodo di autenticazione

Gli identificatori principali di ogni persona, una volta assegnati, sono univoci e secondo le direttive di IDEM non possono essere riutilizzati. La durata delle sessioni di autenticazione rispetta i valori di default di Shibboleth.

Partecipazione ad altre federazioni

Unicam parteciperà nel breve futuro alla Federazione Italiana Eduroam coordinata dal consortium GARR che ha lo scopo di facilitare l'accesso alla rete GARR agli utenti mobili delle organizzazioni partecipanti.