PROT. ARRIVO N. E/11506
DEL - 7 LUG. 2010
CONSORTIUM GARR

Documento descrittivo del processo di accreditamento degli utenti dell'Organizzazione Università Politecnica delle Marche

Le informazioni fornite in questo documento sono accurate alla data del ***15 Giugno 2010***

Indice

Revisioni

Data	Versione	Descrizione modifica	Autore
10/05/2010	0.1	Bozza	Paola Gasparini Giuliano Latini Daniele Ripanti Sandro Tumini
15/06/10	0.2	Rilasciato	Paola Gasparini Giuliano Latini Daniele Ripanti Sandro Tumini

Nota introduttiva

La partecipazione alla Federazione IDEM ("Federazione") abilita l'organizzazione partecipante ("Università Politecnica delle Marche") ad utilizzare la tecnologia di Shibboleth di condivisione degli attributi relativi alle identità per gestire l'accesso alle risorse on-line che possono essere rese disponibili all'interno della comunità IDEM. Un obiettivo della Federazione è quello di sviluppare, nel tempo, degli standard per le organizzazioni al fine di assicurare che le asserzioni sugli attributi che vengono scambiate siano sufficientemente robuste e fidate per gestire l'accesso ad importanti risorse protette. Con la crescita della fiducia interna, la Federazione spera che i Partecipanti alla fine possano fidarsi dei sistemi di identity management e dei sistemi di gestione di accesso alle risorse degli altri partecipanti come si fidano dei propri.

Fondamentalmente ci si aspetta dai Partecipanti che essi forniscano agli altri Partecipanti asserzioni sugli attributi autorevoli e accurate e che ciascuno riceva asserzioni sugli attributi protette e nel rispetto dei vincoli di privacy imposti dalla Federazione o dalla fonte delle informazioni. Per raggiungere tale obiettivo IDEM richiede che ogni Partecipante renda disponibile agli altri Partecipanti certe informazioni di base riguardanti il proprio sistema di identity management, incluse le informazioni relative agli attributi che vengono utilizzati per la Federazione.

I due criteri per garantire che gli Identity Provider forniscano asserzioni di attributi fidate sono: (1) che il sistema di gestione delle identità ricada sotto la supervisione degli organismi che hanno responsabilità direttive e gestionali nell'Organizzazione e che (2) il sistema che emette le credenziali per gli utenti finali (e.g., PKI certificates, userids/passwords, Kerberos principals, etc.) sia dotato di appropriate misure di gestione del rischio (e.g., authentication and authorization standards, security practices, risk assessment, change management controls, audit trails, etc.)

Il Documento DOPAU prodotto dal Partecipante DEVE contenere le informazioni elencate nel presente modello.

In caso di modifica delle procedure o informazioni descritte nel documento, esso DEVE essere prontamente aggiornato e ne deve essere data comunicazione alla Federazione.

Abbreviazioni

A.D.A.	Active Directory di Ateneo
Ce.S.M.I.	Centro Servizi Multimediali e Informatici di Ateneo
C.S.A.	Applicazione per la gestione del personale - "Carriere e Stipendi di Ateneo"
G.I.S.S.	Applicazione per l'amministrazione del database delle Segreterie Studenti – "Gestione Integrata Segreterie Studenti"
N.I.A.	Nucleo Informatico Amministrativo

Gestore dell'accreditamento

I gestori dell'accreditamento degli utenti sono i due centri servizi informatici di Ateneo:

1. Il Nucleo Informatico Amministrativo (N.I.A.)
2. Il Centro Servizi Multimediali e Informatici (Ce.S.M.I.)

Il N.I.A. si occupa:

1. della profilazione degli utenti istituzionali provenienti dall'archivio del personale strutturato e dal database della Segreteria Studenti – di norma mediante procedure di migrazione automatica degli utenti;
2. della disattivazione manuale e mediante batch delle utenze attive al termine del rapporto con l'Università Politecnica delle Marche (es: in seguito al conseguimento della laurea per lo studente, al termine del rapporto di lavoro - pensionamenti/dimissioni/trasferimenti - per il personale).

Il Ce.S.M.I. si occupa:

1. della profilazione degli utenti a contratto che, seguendo la procedura di accreditamento indicata, fanno richiesta di credenziali per l'accesso ai servizi dell'Ateneo;
2. della chiusura della posizione mediante disattivazione manuale delle utenze presenti nel repository.

Responsabili dell'infrastruttura di profilazione degli utenti:

1. Ing. Giovanni Marconi – Direttore - N.I.A.
2. Ing. Raul Castagnani – Direttore – Ce.S.M.I.

Utenti gestiti

Le tipologie di utenti gestiti dall'Ateneo nel processo di accreditamento e rilascio di credenziali sono i seguenti:

1. staff
2. student
3. affiliate

Al momento la cardinalità degli insiemi è la seguente:

|Staff| =

|Student| =

|Affiliate| =

Le tipologie definite comprendono le seguenti categorie di utenti:

STAFF

- Personale docente
- Ricercatori
- Personale Tecnico/Amministrativo
- Assegnisti di ricerca
- Supplenti didattici
- Ricercatori a tempo determinato
- Professori a contratto

STUDENT

- Studenti regolarmente iscritti
- Studenti LLP/Erasmus
- Dottorandi di ricerca

AFFILIATE

- Collaboratori tecnico/amministrativi
- Collaborazioni "coordinate e continuative" / "a progetto"
- Collaboratori membri di commissioni
- Collaboratori alla didattica

- Collaboratori alla ricerca
- Visiting professor
- Visitatori esterni ospiti di strutture di ricerca
- Ospiti

Mappatura degli utenti sulle affiliazioni IDEM

La mappatura degli utenti presenti nel repository A.D.A. è la seguente:

Attributo A.D.A.	**Attributo IDEM /Cardinalità (NUM)**
cn = P[0-9]*	Staff / num: **1829**
cn = X[0-9]*	Affiliate / num: **530**
cn = S[0-9]*	Student / num: **30546**

Ad esempio l'utente

con attributo **cn** in A.D.A. → **P99999**

sarà presentato alla Federazione IDEM come utente con attributo

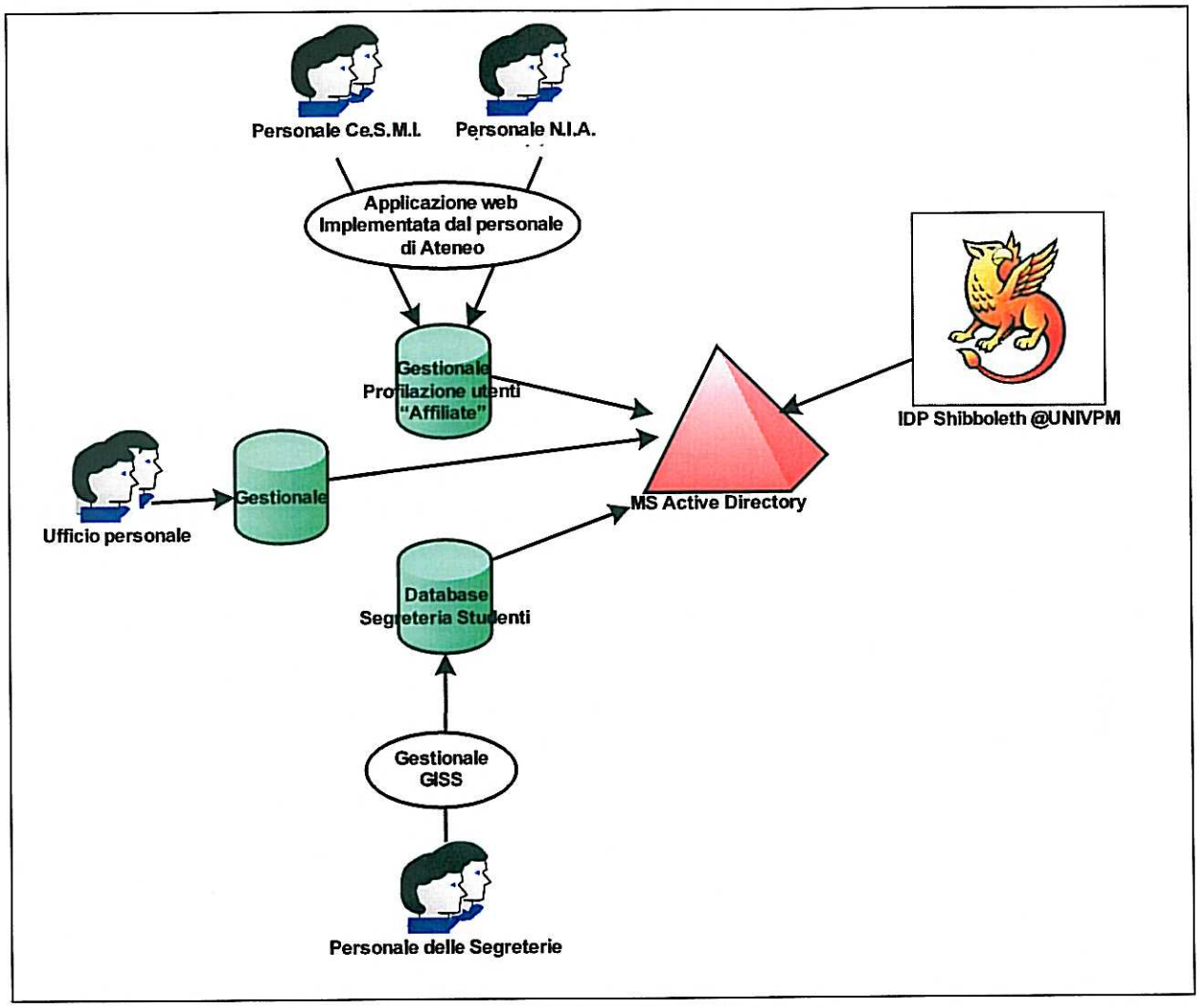
eduPersonScopedAffiliation → staff

Gli attributi rilasciati dall'Ateneo sono:

Attributo A.D.A.	**Attributo IDEM**
Derivato da "cn" -> mappatura statica	eduPersonScopedAffiliation
(sAMAccountName + salt)* * "la generazione del eduPersonTargetedID è calcolata dal"IDP a partire dall'attributo univoco sAMAccountName"	eduPersonTargetedID
mail	eduPersonPrincipalName
mail	mail
displayName	cn
c	PreferredLanguage

Visione di insieme del processo di accreditamento degli utenti

Schema riepilogativo del processo di accreditamento degli utenti



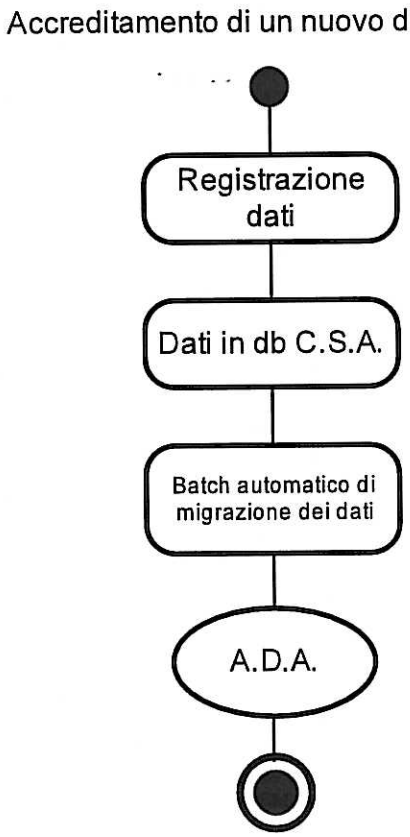
L'utente utilizza le credenziali ottenute per:

- accedere ai calcolatori dei laboratori informatici/strutture di Ateneo mediante logon nei sistemi Microsoft iscritti nell'infrastruttura;
- accedere alla rete Internet in modo autenticato mediante captive-portal;
- accedere alla rete mediante il servizio Wireless;
- consultare la propria mailbox istituzionale (per la sola tipologia di utenti "student");
- autenticarsi in applicazioni web come ad esempio:

- area riservata del portale di Ateneo con funzioni granulari per categoria d'utente;
- proxy autenticato per l'accesso alle risorse elettroniche da reti esterne;
- piattaforma di e-learning basata su Moodle;
- piattaforma CMS per l'editing dei siti web dei Dipartimenti basata su Drupal;
- applicazioni web specifiche per la richiesta di manutenzione/assistenza;
- gestionale per la guidà dello studente;
- richieste di assegnazioni di aule;
- compilazione di moduli on-line (es: questionario dei laureandi, nulla osta, suggerimenti, etc.);
- richieste di servizi multimediali quali videoconferenze, web streaming, etc.

Il processo di accreditamento per la categoria di utenti **staff**

Il processo



Modalità di riconoscimento della persona

Accreditamento mediante verifica del documento d'identità valido presso l'ufficio personale – Sezione personale tecnico/amministrativo e Sezione personale docente.

Caratteristiche dell'identità digitale

Gli attributi associati alla persona in fase di inserimento della scheda sono relativi ai dati anagrafici:

1. Nome
2. Cognome

3. Luogo e data di Nascita
4. Residenza
5. Cittadinanza
6. Recapito telefonico
7. Stato civile
8. Codice fiscale

Sono inoltre associate all'utente informazioni relative a:

1. Struttura di appartenenza interna all'Università Politecnica delle Marche
2. Inquadramento professionale (livello e area)
3. Numero di matricola
4. Indirizzo e-mail
5. Ruolo

Gli attributi che possono essere considerati pubblici sono:

1. Nome
2. Cognome
3. Indirizzo e-mail
4. Struttura di Appartenenza
5. Ruolo

Gestione del ciclo di vita

L'aggiornamento della scheda con gli attributi associati all'utente è compito dell'ufficio personale che interviene sull'anagrafica e sui dati relativi alla posizione all'interno dell'Ateneo in base a cambiamenti di ruolo oppure a modifiche segnalate dal dipendente in merito ai propri dati anagrafici (cambio residenza, recapito telefonico, stato civile). L'aggiornamento delle schede viene effettuato giornalmente mediante batch.

Formato e regole delle credenziali

Le credenziali assegnate sono basate su userID/password. Nell'archivio C.S.A. viene memorizzata soltanto la matricola e la procedura di migrazione della scheda in A.D.A.

procederà con la generazione della password secondo un algoritmo che permette all'utente di ricavare il codice.
La password iniziale poi sarà modificabile dall'utente mediante una funzione disponibile nell'area riservata del portale dell'Ateneo.

Eventuale presenza di credenziali multiple per la stessa persona

L'Ateneo rilascia SMARTCARD con certificati digitali per il personale docente attualmente coinvolto nella procedura di verbalizzazione informatizzata degli esami di profitto.
La SMARTCARD è consegnata dal personale tecnico del N.I.A. e attualmente viene impiegata soltanto nel servizio indicato e comunque mai durante il procedimento di accreditamento già descritto.

Modalità di consegna delle credenziali

L'ufficio personale comunica al dipendente, al momento della registrazione dei dati, la matricola assegnata. La password è poi calcolata mediante un algoritmo descritto all'utente e basato sui propri dati personali.

Modalità di recupero delle credenziali smarrite

I centri servizi possono procedere con il cambio della password mediante richiesta da parte del personale. Il personale verifica mediante riconoscimento della persona la richiesta inoltrata. E' inoltre possibile il recupero mediante procedura guidata nel portale di Ateneo.

Modalità di gestione smarrimento smartcard/token

Il dipendente deve dare comunicazione tempestiva al personale del N.I.A. che procederà con la disattivazione del certificato digitale. Il dipendente deve inoltre denunciare agli organi competenti lo smarrimento del documento elettronico.

Durata dell'accreditamento

Le credenziali rimangono attive per tutta la durata del rapporto di lavoro.

Disabilitazione utente

Attualmente non è prevista la disabilitazione temporanea delle credenziali assegnate al personale dipendente.

Cancellazione definitiva utente

La cancellazione definitiva dell'utente avviene al momento della conclusione del rapporto lavorativo mediante procedura manuale di cancellazione dell'anagrafica e delle credenziali.

Rischi specifici associati alla categoria di utenti

Possibilità di violazione della password.

La procedura di cambio della password prevede il rispetto dell'attuale normativa e pertanto l'utente deve scegliere un codice con complessità validata dal sistema.

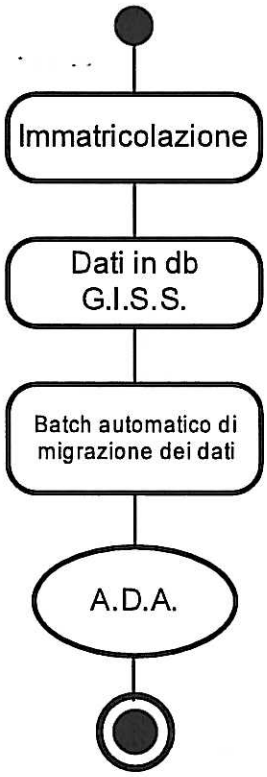
Interoperabilità tra credenziali deboli (username+pwd) ed eventuali credenziali forti (smartcard)

Nessuna.

Il processo di accreditamento per la categoria di utenti **student**

Il processo

Accreditamento di un nuovo studente



Modalità di riconoscimento della persona

Compilazione della modulistica cartacea predisposta per l'immatricolazione e accreditamento dello studente mediante verifica del documento d'identità valido presso la Segreteria Studenti.

Caratteristiche dell'identità digitale

Gli attributi associati alla persona in fase di inserimento della scheda sono relativi ai dati anagrafici:

1. Nome
2. Cognome

3. Luogo e data di Nascita
4. Residenza
5. Cittadinanza
6. Recapito telefonico
7. Stato civile
8. Codice fiscale

Gli attributi che possono essere considerati pubblici sono:

1. Nome
2. Cognome
3. Indirizzo e-mail
4. Ruolo

Gestione del ciclo di vita

Lo studente può aggiornare autonomamente le informazioni relative a:

1. Indirizzo email
2. Residenza
3. Recapito telefonico

attraverso una procedura presente nell'area riservata del portale di Ateneo.

Formato e regole delle credenziali

Le credenziali assegnate sono basate su userID/password. Nell'archivio G.I.S.S. viene memorizzata la matricola e la password.
La password iniziale sarà modificabile dallo studente mediante la funzione "Cambio password" disponibile nell'area riservata del portale dell'Ateneo.

Eventuale presenza di credenziali multiple per la stessa persona

Nessuna.

Modalità di consegna delle credenziali

Inizializzazione della password mediante algoritmo noto e successivo cambio password obbligatorio. Consegna a mano del numero di matricola, codice che rappresenta lo username dell'utente.

Modalità di recupero delle credenziali smarrite

I centri servizi possono procedere con il cambio della password. Il personale verifica mediante riconoscimento della persona e del documento d'identità la richiesta.

Modalità di gestione smarrimento smartcard/token

Il personale dietro richiesta e dopo la verifica dell'identità effettua un cambio della password dell'utente comunicando di persona il nuovo codice.

Durata dell'accreditamento

Le credenziali rimangono attive per tutta la durata dell'iscrizione ad un corso di laurea dell'Ateneo nel repository A.D.A. .

Disabilitazione utente

Attualmente non è prevista la disabilitazione temporanea delle credenziali assegnate.

Cancellazione definitiva utente

La cancellazione definitiva dell'utente avviene 1 anno dopo la conclusione del percorso formativo. La cancellazione è gestita da una procedura automatica.

Rischi specifici associati alla categoria di utenti

Possibilità di violazione della password.

La procedura di cambio della password prevede il rispetto dell'attuale normativa e pertanto l'utente deve scegliere un codice con complessità validata dal sistema.

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

Nessuna.

Il processo di accreditamento per la categoria di utenti **affiliate**

Il processo

Accreditamento di un utente "esterno"

Modalità di riconoscimento della persona

Compilazione della modulistica cartacea predisposta per la richiesta e accreditamento dell'utente mediante verifica del documento d'identità valido presso gli uffici dei Centri Informatici di Ateneo (N.I.A. – Ce.S.M.I.).

Caratteristiche dell'identità digitale

Gli attributi associati alla persona in fase di inserimento della scheda sono relativi ai dati anagrafici:

1. Matricola
2. Cognome
3. Nome
4. Sesso
5. Data di nascita
6. Provincia di nascita
7. Comune di nascita
8. Stato
9. Codice fiscale
10. Indirizzo di residenza
11. Provincia di residenza
12. Comune di residenza
13. Cap
14. Ruolo
15. Facoltà
16. Email
17. Recapito telefonico

Gli attributi che possono essere considerati pubblici sono:

1. Nome
2. Cognome
3. Indirizzo e-mail
4. Ruolo

Gestione del ciclo di vita

L'utente non può aggiornare i dati anagrafici del suo profilo.

Formato e regole delle credenziali

Le credenziali assegnate sono basate su userID/password.
La password iniziale sarà modificabile dall'utente mediante una funzione disponibile nell'area riservata del portale dell'Ateneo.

Eventuale presenza di credenziali multiple per la stessa persona

Nessuna.

Modalità di consegna delle credenziali

Lo username e la password sono consegnati di persona dall'operatore autorizzato che procede con la registrazione della scheda.

Modalità di recupero delle credenziali smarrite

I centri servizi possono procedere con il cambio della password. Il personale verifica mediante riconoscimento della persona e del documento di identità la richiesta.

Modalità di gestione smarrimento smartcard/token

Il personale dietro richiesta e dopo la verifica dell'identità della persona effettua un cambio della password dell'utente comunicando di persona il nuovo codice.

Durata dell'accreditamento

Le credenziali rimangono attive per tutta la durata del rapporto di lavoro.

Disabilitazione utente

Attualmente non è prevista la disabilitazione temporanea delle credenziali assegnate.

Cancellazione definitiva utente

La cancellazione definitiva dell'utente avviene al momento della conclusione del rapporto lavorativo mediante procedura manuale di cancellazione delle credenziali.

Rischi specifici associati alla categoria di utenti

Possibilità di violazione della password.

La procedura di cambio della password prevede il rispetto dell'attuale normativa e pertanto l'utente deve scegliere un codice con complessità validata dal sistema.

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

Nessuna.

Il sistema di autenticazione e autorizzazione interno

Il sistema di gestione delle identità interno all'Ateneo è utilizzato principalmente per:

- l'accesso ad applicazioni web che richiedano l'autenticazione dell'utente;
- l'accesso ai servizi di connettività alla rete Internet (wired, wireless);
- il logon delle postazioni utente dove presenti postazioni iscritte a dominio (principalmente nei laboratori informatici).

Gli identificativi principali di ogni persona sono univoci una volta assegnati e non vengono riutilizzati.

Partecipazione ad altre federazioni

Attualmente l'Università Politecnica delle Marche non partecipa ad altre federazioni di Autenticazione e Autorizzazione.