Documento descrittivo del processo di accreditamento degli utenti dell'Università degli studi di Napoli "Parthenope"

Le informazioni fornite in questo documento sono accurate alla data del ***01-12-2010***

1 Gestore dell'accreditamento

L'accreditamento è gestito dalle seguenti strutture:

- Per il **personale docente e tecnico-amministrativo**, dai rispettivi uffici (uff. Personale docente ed uff. personale Tecnico-amministrativo), all'atto della firma del contratto.

- Per gli **studenti**, dalla segreteria studenti, all'atto dell'immatricolazione.

Inoltre in occasione di eventi, quali convegni, dibattiti, mostre, etc... qualora vi fosse bisogno di accesso all'infrastruttura di rete (principalmente servizio wireless) la struttura organizzatrice dell'evento è responsabile di tali operazioni.

Il processo completo delle procedure di accreditamento per le diverse tipologie è descritto in dettaglio nei paragrafi dedicati.

2 Utenti gestiti

Di seguito l'elenco delle categorie di utenti gestite e la loro mappatura nella classificazione di IDEM

Categoria	Cardinalità	Affiliazione IDEM
Personale docente e ricercatore	500	Staff
Personale Tecnico-amministrativo	500	Staff
Collaboratori alla ricerca	100	Staff
Studenti delle lauree primo e secondo livello	15.000	Staff
Dottorandi	100	Staff
Studenti dei master	1.000	Student

3 Mappatura degli utenti sulle affiliazioni IDEM

Vedi paragrafo precedente

4 Visione di insieme del processo di accreditamento degli utenti

I dati degli studenti sono immagazzinati nel database della segreteria studenti (GISS) mentre le restanti identità sono immagazzinate in un LDAP. Queste due fonti sono usate per alimentare un servizio RADIUS.

Attraverso l'autenticazione RADIUS gli studenti ed il personale, possono accedere alla wireless e gli studenti alle postazioni della biblioteca ed alla piattaforma e-learning.

Inoltre l'accesso alla rete dalle postazioni "pubbliche" (punti rete nelle aule e nei corridoi) è assicurato tramite captive portal, alimentato dal servizio RADIUS.

Il database degli studenti è sottoposto ad una politica di backup, secondo le modalità operative richieste da GISS. La directory ove sono immagazzinati i dati LDAP è su uno storage NAS configurato in RAID 5 ed inoltre è implementato un meccanismo di backup s del server basato su rsync.

5 Il processo di accreditamento per il personale, collaboratori di ricerca e dottorandi

5.1 Il processo

L'ufficio competente dopo la stipula del contratto accompagna l'utente presso il Centro di Calcolo che fisicamente crea l'identità.

Per il personale, gli uffici competenti sono (rispettivamente): personale docente oppure personale tecnico-amministrativo;

Per i dottorandi, l'ufficio competente è Affari Generali

Per i collaboratori di ricerca, agli uffici sopraelencati si aggiungono i dipartimenti.

5.2 Modalità di riconoscimento della persona

Il riconoscimento della persona avviene presso l'ufficio del personale, con le modalità necessarie per la stipula del contratto (usualmente documento di identità).

5.3 Caratteristiche dell'identità digitale

Ad una identità digitale sono associati i dati anagrafici, i dati fiscali, i dati samba, i dati relativi alla struttura (nome struttura, sede, carica, tel.,fax.) ed ovviamente la mail.

Vengono considerati dati pubblici il nome, cognome, il tel, la mail e la struttura di appartenenza.

5.4 Gestione del ciclo di vita

Le informazioni nel database vengono aggiornate dal CCE a seguito di richiesta scritta (o via email istituzionale). L'utente può cambiare la password autonomamente usando l'apposita interfaccia web. Quando un dipendente cessa, la entry viene impostata "non attiva".

5.5 Formato e regole delle credenziali

Le credenziali fornite sono del tipo: userID/password

Lo UserID è formato da caratteri alfanumerici e coincide con la convenzione *nome.cognome*. La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri.

5.6 Eventuale presenza di credenziali multiple per la stessa persona

Le credenziali multiple servono per servizi diversi e non interagiscono.

5.7 Modalità di consegna delle credenziali

All'atto di creazione dell'entità viene comunicata all'utente la sua username e consegnata brevi manu allo stesso la password in busta chiusa.

5.8 Modalità di recupero delle credenziali smarrite

Attualmente non è previsto un recupero della password, bensì un suo RESET da parte del CCE a seguito di richiesta scritta. La procedura per la consegna della nuova password è la stessa descritta innanzi.

5.9 Modalità di gestione smarrimento smartcard/token

Non vi è utilizzo di token/smartcard

5.10 Durata dell'accreditamento

La durata dell'accreditamento coincide con quella del rapporto di lavoro

5.11 Disabilitazione utente

Quando un dipendente cessa, la entry viene impostata "non attiva" a seguito della comunicazione di uno dei due uffici del personale (docente e tecnico-amministrativo) dopo circa un mese. Quando la entry viene impostata a "non attiva" non vi è alcuna possibilità di accesso ai servizi.

5.12 Cancellazione definitiva utente

Non è prevista la cancellazione definitiva.

5.13 Rischi specifici associati alla categoria di utenti

[Dove si descrivono i rischi e i problemi associati a questa categoria e le misure in fase di attuazione per superare le criticità]

Il maggior rischio è rappresentato dalla scelta di password poco sicure da parte dell'utente. E' stato notato che meccanismi di obbligo al cambio password frequente e/o di password complicate (lunghezza eccessiva, forzatura a combinazioni maiuscolo-minuscolo-numero-simbolo) producevano l'effetto opposto,ossia proliferare di pwd del tipo XXX1, XXX2... XXXn oppure Qwerty123 .. etc.

Per cui si è scelto come compromesso una lunghezza minima di 8 caratteri alfanumerici composta almeno da maiuscole-minuscole ed un numero.

Minore rischio rappresenta l'evento (pur accaduto) di un ritardo nella segnalazione di disattivazione di un utente, in quanto le operazioni eventualmente compiute sono comunque tracciabili.

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

Non vi è utilizzo di token/smartcard

6 Il processo di accreditamento per gli studenti

6.1 Il processo

L'accreditamento avviene con la immatricolazione delle studente. L'identità è gestita attraverso la procedura GISS di Kion da parte della segreteria studenti e dello studente stesso (limitatamente ad anagrafica e pwd).

Questo processo è applicato agli studenti delle lauree di primo e secondo livello, nonché agli studenti dei master.

6.2 Modalità di riconoscimento della persona

Il riconoscimento avviene al momento dell'iscrizione al primo anno del corso di studi. In quell'occasione, previo controllo dei documenti d'identità, la segreteria effettua l'inserimento nel database oppure conferma lo stesso qualora lo studente abbia effettuato una pre-immatricolazione on-line. in questo secondo caso, fino alla conferma da parte della segreteria, lo studente non può accedere a nessuno dei servizi dell'ateneo.

6.3 Caratteristiche dell'identità digitale

Ad una identità digitale sono associati i dati anagrafici (inclusa la mai istituzionale), i dati fiscali, e i dati relativi al corso di appartenenza (facoltà, corso, anno, esami, etc..)

Nessun dato è considerato pubblico.

6.4 Gestione del ciclo di vita

Il ciclo di vita è relazionato alla carriera didattica dello studente e le sue evoluzioni sono tracciate con lo strumento GISS di Kion.

6.5 Formato e regole delle credenziali

Le credenziali fornite sono del tipo: userID/password

Lo UserID è formato da caratteri numerici e coincide con la matricola.

La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri.

6.6 Eventuale presenza di credenziali multiple per la stessa persona

Le credenziali multiple (caso studente-lavoratore) non interagiscono.

6.7 Modalità di consegna delle credenziali

Nel caso di pre-immatricolazione, lo studente si sceglie autonomamente la pwd dal form di nel rispetto delle regole che tale pwd deve avere.

Nel caso di immatricolazione "allo sportello", viene assegnata una password temporanea 8primi 19 caratteri del codice fiscale).Tale password permette esclusivamente l'accesso al portale studenti, il quale, al primo accesso, obbliga al cambiamento della stessa.

6.8 Modalità di recupero delle credenziali smarrite

E' prevista una procedura recupero automatico, che invia la password ad una mail indicata dallo studente.
E' possibile il RESET da parte della segreteria.

6.9 Modalità di gestione smarrimento smartcard/token

Non vi è utilizzo di token/smartcard

6.10 Durata dell'accreditamento

La durata dell'accreditamento e' indefinita.

6.11 Disabilitazione utente

La disabilitizazione dell'utente è prevista limitatamente alla fruizione dei servizi di ateneo (es. wireless) ed è attuata dagli uffici preposti a seguito di comunicazione da parte del segreteria o di altri uffici autorizzati (es. Presidenze, etc..).

6.12 Cancellazione definitiva utente

Non è prevista la cancellazione definitiva dell'utente

6.13 Rischi specifici associati alla categoria di utenti

Non si evidenziano rischi specifici per la categoria di utenti trattata

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

Non vi è utilizzo di token/smartcard

7 Il sistema di autenticazione e autorizzazione interno

Attualmente i sistemi interni usano l'autenticazione diretta sulla base dati LDAP (eventualmente attraverso RADIUS).

L'implementazione dell'IDP federato è comunque il primo tassello del progetto di rivisitazione del sistema di identity management e implementazione del SSO in atto.

Gli username utilizzati per l'identificazione per la loro definizione (matricola e nome.cognome) e per il fatto di essere sempre residenti (anche se disabilitati) sono univoci e non riutilizzabili.

Per il server IDP è stata adottata la politica di gestione che contraddistingue tutti gli altri server ossia quella dell'aggiornamento allo stato dell'arte sia del SO (linux) che di tutti i software in esso installati.

Per quel che riguarda le impostazioni dei timeout e la terminazione delle

sessioni non si è modificato il valore predefinito dell'installazione Shibboleth.

8 Partecipazione ad altre federazioni

Questo Ateneo non partecipa ad altre federazioni,

E' in programma l'adesione alla federazione Eduroam successivamente al completamento dell'adesione ad IDEM-All.