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

Le informazioni fornite in questo documento sono accurate alla data del 06 Maggio 2010

1) Sommario

2) Revisioni

Data	Versione	Descrizione modifica	Autori
06/05/2010	1.0	Versione finale 2010	M. Boeretto, P. Ghezzo, C. Palermo

3) Abbreviazioni

AAI:	Authentication Authorization Infrastructure
AI:	Area Infrastrutture
ASD:	Area Servizi alla Didattica
ARUO:	Area Risorse Umane ed Organizzazione
AUP:	Acceptable User Policy
EDUROAM:	Educational Roaming
GARR:	Gestione Ampliamento Rete Ricerca
GTSRA:	Gestione Tecnica dei Sistemi, delle Reti e delle Applicazioni
IDEM:	Identity Management
IDP:	Identity Provider
PIN:	Personal Identification Number
PUK:	Personal Unblocking Key
RFID:	Radio Frequency IDentification
SP:	Service Provider

4) Gestore dell'accreditamento

L'accreditamento è gestito dalle seguenti strutture:

- **Area Risorse Umane e Organizzazione**, Servizi "Gestione personale docente e ricercatore" e "Gestione personale docente e ricercatore", per il personale e per tutti gli altri soggetti che stipulano con Iuav un contratto di collaborazione o insegnamento, all'atto della firma del contratto.
- **Area Servizi alla didattica,** "Segreterie Studenti" per gli studenti immatricolati a qualsiasi titolo presso Iuav, all'atto dell'immatricolazione.
- **Area Infrastrutture,** Servizio "Gestione Tecnica dei Sistemi, delle Reti e delle Applicazioni" per il personale e per tutti gli altri soggetti che hanno titolo all'utilizzo dei servizi Internet e posta elettronica Iuav, a seguito di identificazione personale

La raccolta dei dati, il filtraggio e l'armonizzazione sono in capo all' Area Infrastrutture – Servizio "Gestione Tecnica dei Sistemi, delle Reti e delle applicazioni", d'ora in avanti in questo documento abbreviato in GTSRA.
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; il processo completo è descritto in dettaglio nei capitoli 7-11 "Il processo di accreditamento per le diverse categorie di utenti".

5) 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 categorie utenza d'ateneo	Codice macro categoria
1	Personale docente di ruolo	D
2	Personale ricercatore di ruolo	R
3	Personale tecnico ed amm.vo a tempo indeterminato	P
4	Personale tecnico ed amm.vo a tempo determinato	P
5	Docente supplente esterno	D
6	Collaboratore tecnico/amministrativo	E
7	Collaboratore alla didattica	C
8	Assegnista di ricerca	R
9	Docente a contratto	D
10	Docente con firma digitale per la registrazione esami	D
11	Studente iscritto ai corsi di studio di 1° e 2° livello	S
12	Dottorando (di varie scuole di dottorato)	T
13	Dottorando di università consorziate	T
14	Studente di master	T
15	Laureato di un qualunque corso di studi/ dottorato/ master	L
16	Laureato di un qualunque corso di studi/ dottorato/ master che hanno una qualche forma di collaborazione formale (ad esempio l'iscrizione all'associazione riconosciuta dall'ateneo "Iuav Alumni")	A
17	Ospite (convegnista, ospite occasionale)	G
18	Personale di azienda esterna che lavora presso Iuav	H
19	Personale di azienda/organizzazione esterna che fornisce supporto tecnico sistemistico a qualche servizio ICT d'ateneo	F
20	Personale in quiescenza	I

Tab. 2.1 : Tabella di dettaglio delle categorie di utenza classificate in ateneo

Allo scopo di razionalizzare e semplificare la gestione dell'accreditamento degli utenti sono state definite delle macro categorie che raggruppano le categorie d'utenza con caratteristiche di appartenenza simili ed esigenze operative comuni. Tale suddivisione in macrocategorie è stata successivamente utilizzata per la mappatura degli utenti sulle affiliazioni IDEM.
Nella pagina seguente la loro descrizione.

N.	Codice	Nome macro categoria	Elenco categorie incluse
1	0	Non definito	
2	D	Docente	Personale docente di ruolo, Docente supplente esterno, Docente a contratto
3	R	Ricercatore	Personale ricercatore di ruolo, Assegnista di ricerca
4	P	Dipendente	Personale tecnico ed amm.vo a tempo indet./det.,
5	E	Collaboratore tecnico/amm.vo	Collaboratore tecnico/amm.vo
6	C	Collaboratore alla didattica	Collaboratore alla didattica
7	S	Studente	Studente
8	L	Laureato	Laureato
9	A	Alumni	Alumni
10	T	Dottorando	Dottorandi (di varie scuole di dottorato), Dottorandi di università consorziate, Studenti di master
11	F	Fornitore ICT	Fornitore ICT
12	H	Fornitore servizi diversi	Fornitore servizi diversi
13	I	Pensionato	Pensionato
14	G	Ospite	Ospite

Tab. 2.2 : Tabella delle macro categorie di utenza classificate in ateneo

6) Mappatura degli utenti sulle affiliazioni IDEM

Nella tabella seguente sono riportate le macro categorie mappate in IDEM e quindi a quali utenti viene dato l'accesso ai servizi della federazione. Sono riportate anche la cardinalità di massima per ciascuna macro categoria e la relativa affiliazione.

N.	Codice	Descrizione macro categorie utenza mappate su IDEM	Cardinalità (di massima)	Affiliazione IDEM
1	D	Docente	500	Staff, Member
2	R	Ricercatore	150	Staff, Member
3	P	Dipendente	300	Staff, Member
4	E	Collaboratore tecnico/amministrativo	variabile	Staff, Member
5	C	Collaboratore alla didattica	500	Staff, Member
6	S	Studente	10.000	Student, Member
7	L	Laureato	30.000	Affiliate
8	T	Dottorando	variabile	Student, Staff, Member
9	A	Alumni	20	Affiliate
10	F	Fornitore	40	Affiliate

Tab. 3.1 : Tabella mappature delle macro categorie di utenza sulle affiliazioni IDEM

7) Visione di insieme del processo di accreditamento utenti

La base dati degli utenti e le informazioni associate alle identità digitali vengono conservate all'interno di un database MySQL e gestite tramite un applicativo Web.

Una procedura lanciata ad intervalli regolari effettua gli aggiornamenti sul database LDAP, che alimenta Shibboleth e RADIUS, sul server Active Directory, che gestisce il dominio IUAV.IT per i computer desktop e il VDI, e infine su Google Apps per la gestione delle caselle di posta elettronica.

Un'altra procedura sincronizza invece le informazioni di tutti gli studenti presenti nel database di Esse3 con quelle presenti nel database MySQL; le password sono escluse dal processo di sincronizzazione in quanto il rilascio delle credenziali viene gestito direttamente da Iuav.

Il link di cambio password di tutte le applicazioni Web punta alla parte pubblica del software di gestione degli utenti, che tra le altre cose permette anche il pre-accreditamento degli ospiti di eventi programmati dall'Ateneo.

L'utente utilizza le proprie credenziali su Shibboleth, sui captive portal che permettono l'accesso alla rete da aule informatiche e postazioni pubbliche dell'Ateneo e su tutti i servizi che utilizzano il server LDAP per autenticare i propri utenti. Al momento tra le applicazioni più importanti ed utilizzate di questa ultima categoria abbiamo Titulus (gestione dell'archivio dell'Ateneo), IRIS (gestione delle presenze), VPN (accesso sicuro da reti esterne, ammesso al momento per lo più agli amministratori dei servizi), i servizi bibliografici oltre ovviamente la procedura di cambio password.

Il grafico nella pagina seguente illustra il flusso dei dati ed evidenzia in rosso le connessioni sicure.

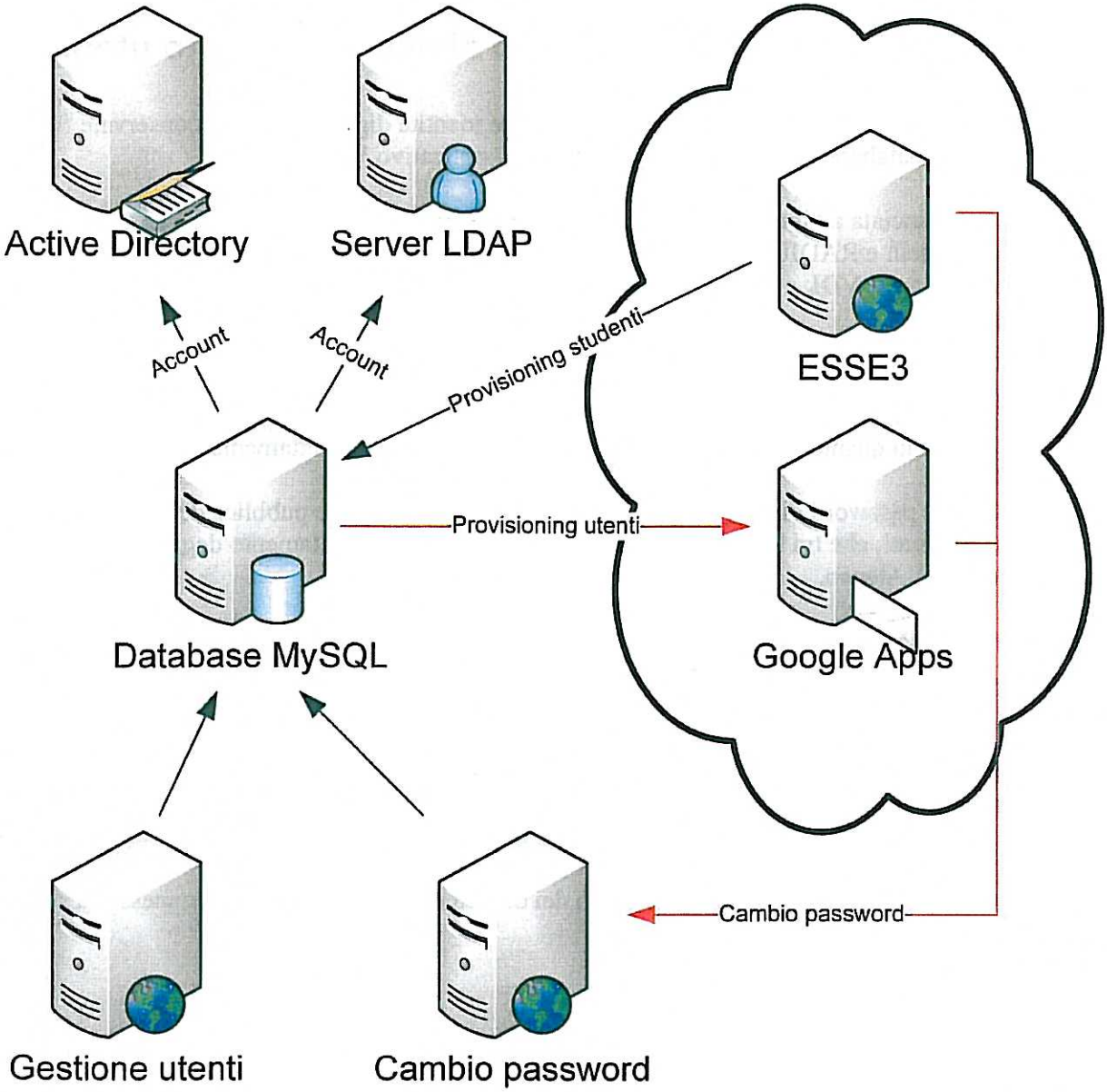

Fig. 1 : Diagramma dell'architettura di provisioning degli utenti

8) Il processo di accreditamento per la categoria di utenti:

- **Personale Tecnico Amministrativo a tempo determinato ed indeterminato**
- **Personale Docente e Ricercatore di ruolo e a contratto**
- **Collaboratori tecnico amministrativi**
- **Collaboratori alla didattica**
- **Assegnisti di ricerca**

Il processo

Struttura organizzativa di riferimento: ARUO - Area Risorse Umane e Organizzazione
Responsabile accreditamento: Responsabili di Servizio "Gestione personale docente e ricercatore" e "Gestione personale tecnico e amministrativo".
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 "Gestione personale docente e ricercatore" e ufficio "Gestione personale tecnico e amministrativo".
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 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, la matricola, il numero del badge e i dati dell'inquadramento (area e struttura di appartenenza, afferenza didattica, inquadramento ad esempio: D2, 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.
Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:
- eduPersonAffiliation : staff, member

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 di attribuzione dell'identità digitale.
Quando nel db MySql un utente subisce variazioni, queste vengono recepire da LDAP ed AD entro un'ora dalla modifica.

Formato e regole delle credenziali

Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici. La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri. La durata temporale delle password rispetta i vincoli normativi.
A tutti i dipendenti viene inoltre rilasciata una tessera con banda magnetica utilizzata per rilevare le presenze. Il sistema di rilevazione presenze è in via di sostituzione e le nuove tessere saranno di tipo RFID (identificazione in radiofrequenza).

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 brevi manu dall'ufficio gestore alla persona in busta chiusa separatamente dal codice di sblocco PUK.

Modalità di recupero delle credenziali smarrite
Lo userID smarrito può essere richiesto all'ufficio preposto.
Per il recupero della password è prevista una procedura web basata su codice di sblocco PUK. Lo smarrimento del codice di sblocco comporta la rigenerazione di entrambe i codici password e PUK. Tale operazione può essere eseguita solo dall'ufficio preposto nel rispetto delle modalità di consegna sopra indicate.

Modalità di gestione smarrimento smartcard/token
Il personale docente può utilizzare smartcard con lettore o token business key per la firma digitale con validità legale. In caso di smarrimento è revocato il precedente ed emesso uno nuovo; si gestisce in aggiunta il processo di revoca presso l'ente erogatore.

Durata dell'accreditamento
Gli utenti di queste categorie sono accreditati per tutto il tempo in cui sussiste il rapporto di lavoro ed almeno fino a 1 anno oltre la scadenza risultante dal db dell'ufficio risorse umane e organizzative.

Disabilitazione utente
Per le categorie caratterizzate da un rapporto di lavoro a termine la disabilitazione avviene in modo automatico alla data di fine rapporto impostata nel db utenti mysql. Di norma questa data corrisponde alla scadenza del contratto aumentato di 6 mesi. Per le altre categorie del personale l'eventuale disabilitazione viene fatta manualmente dall'ufficio preposto a necessità 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 preposto decorso 1 anno dalla data di disabilitazione ed in assenza di attribuzione di una nuova scadenza. 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 incrociata a cadenza annuale con il db dell'ufficio contratti ARUO.

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.

9) Il processo di accreditamento per la categoria di utenti: - "Studenti"

Il processo

Struttura organizzativa di riferimento: ASD - Area Servizi alla Didattica
Responsabile accreditamento: Responsabile di Servizio "Segreteria studenti – Front office"
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali della categoria "Studenti" dell'ateneo.

Modalità di riconoscimento della persona

Ufficio di riferimento: Segreteria studenti – Front office
Modalità di riconoscimento della persona: il riconoscimento avviene presso l'ufficio preposto con la presenza fisica della persona al momento dell'iscrizione al primo anno del corso di studi. In quell'occasione viene effettuato il controllo dei documenti d'identità personale e trattenuta copia agli atti. Contestualmente l'ufficio preposto consegna alla persona la documentazione relativa al consenso per il trattamento dei dati personali e alle acceptable user policy 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 l'apposita applicazione web Esse3 di Kion.

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.
Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:
- eduPersonAffiliation : student, member

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. La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri. La durata temporale delle password rispetta i vincoli normativi.

Eventuale presenza di credenziali multiple per la stessa persona

Esistono alcuni casi particolari della categoria studenti per i quali è prevista la generazione di due identità digitali. Si tratta degli studenti dottorandi e degli studenti di master. Questi utenti hanno un'identità digitale con validità permanente per la carriera universitaria ed un'identità digitale con validità determinata per il solo periodo di durata del corso di dottorato o di master.

Modalità di consegna delle credenziali

Le credenziali sono consegnate brevi manu dall'ufficio gestore alla persona in busta chiusa separatamente dal codice di sblocco PUK.

Modalità di recupero delle credenziali smarrite

Lo userID smarrito può essere richiesto all'ufficio preposto.
Per il recupero della password è prevista una procedura web basata su codice di sblocco PUK. Lo smarrimento del codice di sblocco comporta la rigenerazione di entrambe i codici password e PUK. Tale

operazione può essere eseguita solo dall'ufficio preposto nel rispetto delle modalità di consegna sopra indicate.

Modalità di gestione smarrimento smartcard/token

Non sono utilizzati smartcard/token.

Durata dell'accreditamento

La durata dell'accreditamento e' indefinita.

Disabilitazione

Sono previsti due livelli di disabilitazione dell'identità digitale: il primo riguarda la gestione della carriera universitaria dello studente, il secondo riguarda l'accesso ai servizi di ateneo.
Il primo livello viene ereditato dalla base dati Kion e fornisce l'informazione se lo studente è in regola con il pagamento delle tasse e/o se si e' laureato. Nel caso lo studente si sia laureato il passaggio di stato avviene automaticamente dopo 6 mesi dalla data di conclusione del corso di studi. Lo studente in stato "non attivo" può accedere all'applicativo di gestione della sua carriera ma non ai servizi di ateneo.
Il secondo livello di disabilitazione viene gestito dagli uffici preposti attraverso una specifica procedura applicativa. Come sopra dall'avvenuta disabilitazione lo studente non potrà più condurre con successo la procedura di autenticazione ai servizi d'ateneo.

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 la categoria di utenti trattata.

10) Il processo di accreditamento per la categoria di utenti:

- **Dottorandi di varie scuole di dottorato**
- **Studenti di master**
- **Dottorandi di università consorziate**

Il processo

Struttura organizzativa di riferimento: AI - Area Infrastrutture
Responsabile accreditamento: Responsabile Ufficio GTSRA
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 GTSRA
Modalità di riconoscimento della persona: la richiesta di accreditamento per queste categorie proviene dalle strutture organizzative d'ateneo che hanno attivato i corsi di dottorato e/o i master ed avviene attraverso la compilazione di un modulo sottoscritto dal direttore della struttura. Il riconoscimento della persona avviene al momento della consegna delle credenziali 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 protetta.

Caratteristiche dell'identità digitale

Elenco degli Attributi associati all'identità digitale: i dati anagrafici, il codice fiscale, l'eventuale matricola e i dati della facoltà, del corso di dottorato/master.
Elenco degli Attributi associati all'identità digitale considerati pubblici: Gli unici dati pubblici sono nome e cognome, corso di dottorato/master.
Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:
- eduPersonAffiliation : staff, student, member

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 di attribuzione dell'identità digitale.
Quando nel db MySql un utente subisce variazioni, queste vengono recepire da LDAP ed AD entro un'ora dalla modifica.

Formato e regole delle credenziali

Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici. La password è una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri. La durata temporale delle password rispetta i vincoli normativi.

Eventuale presenza di credenziali multiple per la stessa persona

Eventuali credenziali multiple servono per servizi diversi e non interagiscono.

Modalità di consegna delle credenziali

Le credenziali sono consegnate brevi manu dall'ufficio gestore alla persona in busta chiusa separatamente dal codice di sblocco PUK.

Modalità di recupero delle credenziali smarrite

Lo userID smarrito può essere richiesto all'ufficio preposto.
Per il recupero della password è prevista una procedura web basata su codice di sblocco PUK. Lo smarrimento del codice di sblocco comporta la rigenerazione di entrambe i codici password e PUK. Tale operazione può essere eseguita solo dall'ufficio preposto nel rispetto delle modalità di consegna sopra indicate.

Modalità di gestione smarrimento smartcard/token

Il personale docente può utilizzare smartcard con lettore o token business key per la firma digitale con validità legale. In caso di smarrimento è revocato il precedente ed emesso uno nuovo; si gestisce in aggiunta il processo di revoca presso l'ente erogatore.

Durata dell'accreditamento

Gli utenti di queste categorie sono accreditati per tutto il tempo in cui sussiste il rapporto di lavoro ed almeno fino a 1 anno oltre la scadenza risultante dal db utenti mysql.

Disabilitazione utente

La disabilitazione avviene in modo automatico alla data di conclusione del corso di dottorato/master impostata nel db utenti mysql. Di norma questa data corrisponde alla scadenza del contratto aumentato di 6 mesi. Dall'avvenuta disabilitazione la persona non potrà più condurre con successo la procedura di autenticazione.

Cancellazione definitiva utente

La cancellazione definitiva viene fatta manualmente dall'ufficio preposto decorso 1 anno dalla data di disabilitazione ed in assenza di attribuzione di una nuova scadenza.

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 a cadenza annuale del db utenti mysql.

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.

11) Il processo di accreditamento per la categoria di utenti: - Alumni

Il processo
Struttura di riferimento: AI - Area Infrastrutture
Responsabile accreditamento: Responsabile di Servizio GTSRA
Le strutture di riferimento sono responsabili dell'assegnazione, del mantenimento e della cancellazione delle identità digitali dell'ateneo. La gestione dell'accreditamento riguarda esclusivamente il ciclo di vita delle identità digitali e quindi non la definizione e la formalizzazione del rapporto di lavoro dell'individuo con l'ente che ne è semmai un prerequisito.

Modalità di riconoscimento della persona
Ufficio responsabile: Area Infrastrutture - GTSRA
Ufficio preposto (con delega scritta del responsabile): Segreteria associazione Iuav Alumni
Modalità di riconoscimento della persona: avviene 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 l'ufficio preposto consegna 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 provvisorio del record personale all'interno del database delle identità digitali mediante apposita applicazione web protetta. L'ufficio responsabile successivamente procede alla convalida dell'accreditamento.

Caratteristiche dell'identità digitale
Elenco degli Attributi associati all'identità digitale: Tutti quelli definiti al paragrafo "Una visione d'insieme"
Elenco degli Attributi associati all'identità digitale considerati pubblici: Tutti quelli definiti al paragrafo "Una visione d'insieme"
Elenco delle coppie attributo/valore che caratterizzano la categoria di utenti:
- eduPersonAffiliation : affiliate

Gestione del ciclo di vita
L'aggiornamento del database delle identità digitali è a carico dell'ufficio preposto. Gli strumenti di gestione e le modalità di accesso all'applicazione sono i medesimi del processo di attribuzione dell'identità digitale. L'unico cambiamento relativo a questa categoria è relativo alla disabilitazione. L'identità digitale viene automaticamente disabilitata alla scadenza inserita in database ed eliminata definitivamente decorsi i 30 giorni in assenza di attribuzione di una nuova scadenza da parte dell'ufficio preposto.

Formato e regole delle credenziali
Le credenziali fornite sono del tipo: userID/password
Lo UserID è formato da caratteri alfanumerici. La password e' una sequenza casuale di caratteri alfanumerici di lunghezza pari almeno ad 8 caratteri. La durata temporale delle password rispetta i vincoli normativi.

Eventuale presenza di credenziali multiple per la stessa persona
Le persone incluse nella categoria Alumni sono studenti laureati dell'ateneo. Per questo motivo hanno due identità digitali delle quali solo quella qui trattata consente l'accesso alle rete dati d'ateneo ed alle risorse federate mentre l'altra identità, presente per ragioni storiche, consente unicamente l'accesso alla piattaforma applicativa della segreteria studenti.

Modalità di consegna delle credenziali
Le credenziali sono consegnate brevi manu dall'ufficio gestore alla persona in busta chiusa separatamente dal codice di sblocco PUK.

Modalità di recupero delle credenziali smarrite

Lo userID smarrito può essere richiesto all'ufficio preposto.
Per il recupero della password è prevista una procedura web basata su codice di sblocco PUK. Lo smarrimento del codice di sblocco comporta la rigenerazione di entrambe i codici password e PUK. Tale operazione può essere eseguita solo dall'ufficio preposto nel rispetto delle modalità di consegna sopra indicate.

Modalità di gestione smarrimento smartcard/token

Non sono utilizzati smartcard/token

Durata dell'accreditamento

La durata dell'accreditamento coincide con la durata dell'iscrizione all'associazione.

Disabilitazione utente

La disabilitazione avviene automaticamente alla data di scadenza dell'iscrizione presente in base dati oppure può essere esegiuta dall'ufficio preposto attraverso una specifica procedura applicativa. Dall'avvenuta disabilitazione la persona non potrà più condurre con successo la procedura di autenticazione.

Cancellazione definitiva utente

La cancellazione definitiva avviene decorsi i 30 giorni dalla data di disabilitazione in assenza di attribuzione di una nuova scadenza da parte dell'ufficio preposto.

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 la categoria di utenti trattata.

12) Il sistema di autenticazione e autorizzazione interno

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

Applicazioni	SSO	LDAP/AD
Accessi pubblici alla rete dati d'ateneo (attraverso un Portale web)		X
Accessi sicuri in VPN da internet alla rete dati d'ateneo		X
Gestione amministrativa del personale (IRIS-superve)		X
Protocollo elettronico (Titulus)		X
Servizi bibliotecari di consultazione e prestito		X
Servizi di posta elettronica/mailing list del personale e degli studenti	X	
Gestione VoIP d'ateneo		X
Applicazioni web d'ateneo per gestione votazioni, iscrizioni ad eventi, ecc.		X
Servizi di consultazione cartografie e materiali fotografici		X
Servizi di streaming archivi multimediali		X
Servizio di accounting stampa e fax centralizzati		X

Tab. 11.1 : Tabella delle applicazioni interne e relativo metodo di autenticazione

Come si evince dalla tabella 11.1, Iuav mette a disposizione dei fornitori di servizi interni un sistema di autenticazione basato su LDAP e un sistema di "single sign-on" (SSO) basato su una versione di Shibboleth patchata per poter gestire anche il logout. Mette inoltre a disposizione le conoscenze acquisite per migrare più applicazioni possibili ad un meccanismo di SSO, forte della possibilità di utilizzarlo anche per l'accesso a risorse federate.

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.

13) Partecipazione ad altre federazioni

- L'università Iuav di Venezia partecipa 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.
  Lo scopo della doppia partecipazione alle federazioni Eduroam e IDEM-AAI è garantire che qualsiasi persona accreditata presso una delle organizzazioni federate possa accedere ad internet ed usufruire delle risorse federate connettendosi all'infrastruttura WiFi di una qualsiasi delle organizzazioni federate solamente con l'impiego delle credenziali fornite dalla propria organizzazione.
  Per assicurare la piena mobilità a tutti coloro che hanno una "identità", anche a livello internazionale, ed assicurate l'accesso anche a tutti gli altri servizi che IDEM mette a disposizione è fondamentale condividere la medesima base dati d'identità digitali.