

Iniziativa “Università Digitale” – Tavolo tecnico di coordinamento.

Autenticazione Federata

Allegato Tecnico alle Linee Guida

Sommario

Premessa

Scopo e contenuti del documento

Scenario e principi generali

Obiettivi di servizio agli utenti finali

Conferimento delle identità digitali

Realizzazione dei servizi federati

Amministrazione delle infrastrutture tecnologiche

Livelli di servizio

Adozione coordinata di soluzioni tecnologiche

Comunicazione

Allegato – Schema funzionale esemplificativo

Allegato – Esempio di DOPAU per l’adesione alla Federazione Idem

Premessa

Le presenti indicazioni tecniche sono orientate all’implementazione delle soluzioni di *Federated Identity and Access Management* immediatamente funzionali alla Federazione delle Università partecipanti ai fini dell’accesso ad Internet e propedeutiche alla fruizione e allo sviluppo di servizi federati a valore aggiunto.

Nel testo seguente sono utilizzati i seguenti acronimi:

AAA Authentication, Authorization, Accounting

AAI Authentication and Authorization Infrastructure

DOPAU Documento sul Processo di Accreditamento degli Utenti

DPS Documento Programmatico sulla Sicurezza

FIAM Federated IAM

IAM Identity and Access Management

IdP Identity Provider

NREN National Research and Education Network

OSS Open Source Software

PII Personally Identifiable Information

RADIUS Remote Authentication Dial-In User Service

SP Service Provider

SAML Security Assertion Markup Language

SSO Single Sign On

UMS User Management System

URL Uniform Resource Locator

Scopo e contenuti del documento

Il presente documento contiene le indicazioni tecnico-operative di carattere generale finalizzate all’adesione delle Università partecipanti alla Federazione Italiana Eduroam e alla Federazione IDEM – entrambe coordinate dal Consortium GARR – seguendo modalità per quanto possibile omogenee.

Il documento contiene inoltre uno schema funzionale esemplificativo di una possibile implementazione e una traccia di DOPAU utilizzabile per l'adesione alla Federazione IDEM.

Il presente documento NON contiene:

- le indicazioni procedurali finalizzate al rispetto delle indicazioni normative in materia, che sono oggetto di un altro lavoro prodotto dal Tavolo Tecnico di coordinamento dell'iniziativa Università Digitale, e al quale si rimanda;
- le indicazioni procedurali di dettaglio di adesione alle federazioni, in quanto la documentazione di riferimento è mantenuta dal Consortium GARR ed è accessibile ai seguenti URL (verificati il 2 luglio 2010):

Per la Federazione Italiana Eduroam:

Regolamento

http://www.servizi.garr.it/index.php/it/eduroam/documenti/doc_download/18-regolamento-della-federazione-italiana-eduroam-

Cookbook

http://www.servizi.garr.it/index.php/it/eduroam/documenti/doc_download/17-eduroam-cookbook-

Per la Federazione IDEM

Requisiti e attività preliminari all'adesione

<https://www.idem.garr.it/index.php/it/idem/190-sei-pronto-per-partecipare-alla-federazione>

Regolamento, Norme di Partecipazione, Specifiche Tecniche e Specifiche Tecniche per la Compilazione e l'uso degli Attributi:

<https://www.idem.garr.it/index.php/it/come-partecipare>

Richiesta di Adesione, Richiesta di Registrazione IDP, Modello DOPAU, Richiesta di Registrazione SP (necessaria per la registrazione dell'accesso Wi-Fi):

<https://www.idem.garr.it/index.php/it/come-partecipare>

Guide di installazione più aggiornate per l'IDP:

https://www.idem.garr.it/index.php/it/documenti/doc_download/134-installare-lidp-2x-su-debian-lenny-con-solo-tomcat

http://www.garr.it/eventiGARR/idem-day/docs/conte-monticini_pres_idemday09.pdf

Scenario e principi generali

Il paradigma dell'autenticazione federata, allo stato, ha raggiunto un livello di notevole maturità tecnologica; il consolidamento del protocollo SAML, del formato eduPerson e di varie soluzioni OSS (in particolare Shibboleth), l'orientamento alla collaborazione caratteristico della comunità universitaria, la presenza diffusa di personale con *skills* tecnici adeguati e il ruolo dei NREN sono fattori che rendono irrinunciabile e sostenibile l'adozione di soluzioni di FIAM.

Il Consortium GARR, che è il NREN italiano, coordina la Federazione Italiana Eduroam e la Federazione IDEM. La prima, basata sullo standard IEEE 802.1X e su un sistema gerarchico di *server* RADIUS, è orientata all'accesso Wi-Fi in *roaming* alla rete Internet; la seconda è orientata all'accesso ai servizi e si basa su SAML. Considerate le finalità diverse ma complementari delle due Federazioni, considerata l'evoluzione tecnologica in atto, viste le esperienze di alcune Università che utilizzano soluzioni *Shibboleth-based* anche per l'accesso a Internet, le presenti linee guida non intendono forzare le politiche delle Università verso l'adesione all'una o all'altra Federazione ma si limitano a suggerire l'adesione ad entrambe nei limiti strettamente necessari:

- alla realizzazione di un insieme minimo, omogeneo e garantito di servizi di accesso;
- alla non preclusione verso opportunità di fruizione e realizzazione di servizi a valore aggiunto che possono beneficiare, economicamente e funzionalmente, della dimensione e delle caratteristiche proprie di una Federazione.

Obiettivi di servizio agli utenti finali

Le Università partecipanti adotteranno le soluzioni tecnico–organizzative necessarie a garantire almeno i seguenti servizi federati:

- Accesso in *roaming* alla rete Internet attraverso la propria struttura tecnologica Wi-Fi, esteso ad una o più zone e consentito agli utenti accreditati presso le organizzazioni afferenti alla Federazione Italiana Eduroam, secondo le modalità tecnico–operative stabilite dalla Federazione stessa;
- Accesso alla rete Internet mediato da *Captive Portal* (o soluzione funzionalmente equivalente) consentito agli utenti accreditati presso le organizzazioni afferenti alla Federazione IDEM, secondo le modalità tecnico–operative stabilite dalla Federazione stessa;

Conferimento delle identità digitali

Le Università partecipanti, in sede di adesione alle Federazioni IDEM ed Eduroam, conferiranno almeno le identità digitali degli utenti appartenenti alla categoria “studenti”, anche con eventuali limitazioni qualora i sistemi informativi localmente utilizzati non consentano un’agevole gestione dell’intera popolazione studentesca.

Le Università partecipanti adotteranno le soluzioni tecnico–organizzative necessaria a garantire nel tempo la qualità delle identità digitali conferite e dei processi di *user provisioning* al fine di onorare i principi di fiducia e affidabilità che sono a base della Federazione. A titolo meramente esemplificativo, quanto sopra si potrebbe raggiungere con l’impiego di un sistema UMS dedicato e opportunamente gestito che alimenti il servizio di *directory*.

Realizzazione di servizi federati

Le Università partecipanti, in fase di definizione di nuovi servizi da conferire nella Federazione IDEM, adotteranno soluzioni che limitino allo stretto necessario il trasferimento di PII privilegiando, ad esempio, autorizzazioni *role-based* anziché *user-based*.

Restano ferme le responsabilità degli IdP come indicato nelle linee guida normative richiamate in precedenza.

Amministrazione delle infrastrutture tecnologiche

I livelli di sicurezza dei sistemi informatici di accesso alla rete mediante autenticazione federata sono conformati, sotto la responsabilità dell’amministratore di sistema designato, alle specifiche generali stabilite per la presenza sulla rete GARR e alle specifiche particolari previste per la partecipazione alle Federazioni. Il Consortium GARR fornisce se necessario assistenza tecnica.

La parte di processo AAA gestito presso l’Università ospitante può costituire trattamento di dati dell’Università di provenienza, in particolare per quanto riguarda le informazioni trasferite per la gestione dell’accesso. Per tale motivo, quando necessario, le Università adeguano di conseguenza i propri DPS.

Livelli di servizio

Le Università partecipanti adottano le misure tecnico–organizzative necessarie affinché i servizi di validazione delle identità digitali conferite in Federazione siano affidabili, sicuri e operativi con continuità.

Per quanto riguarda presenza, durata, efficacia ed efficienza del servizio le Università partecipanti garantiscono, per la copertura conferita in Federazione, livelli di servizio non inferiori a quelli garantiti per l'utenza locale.

Adozione coordinata di soluzioni tecnologiche

Le Università partecipanti, nell'attuazione delle proprie politiche di IAM si impegnano allo studio di soluzioni compatibili con lo standard SAML e possibilmente con l'implementazione Shibboleth dello stesso.

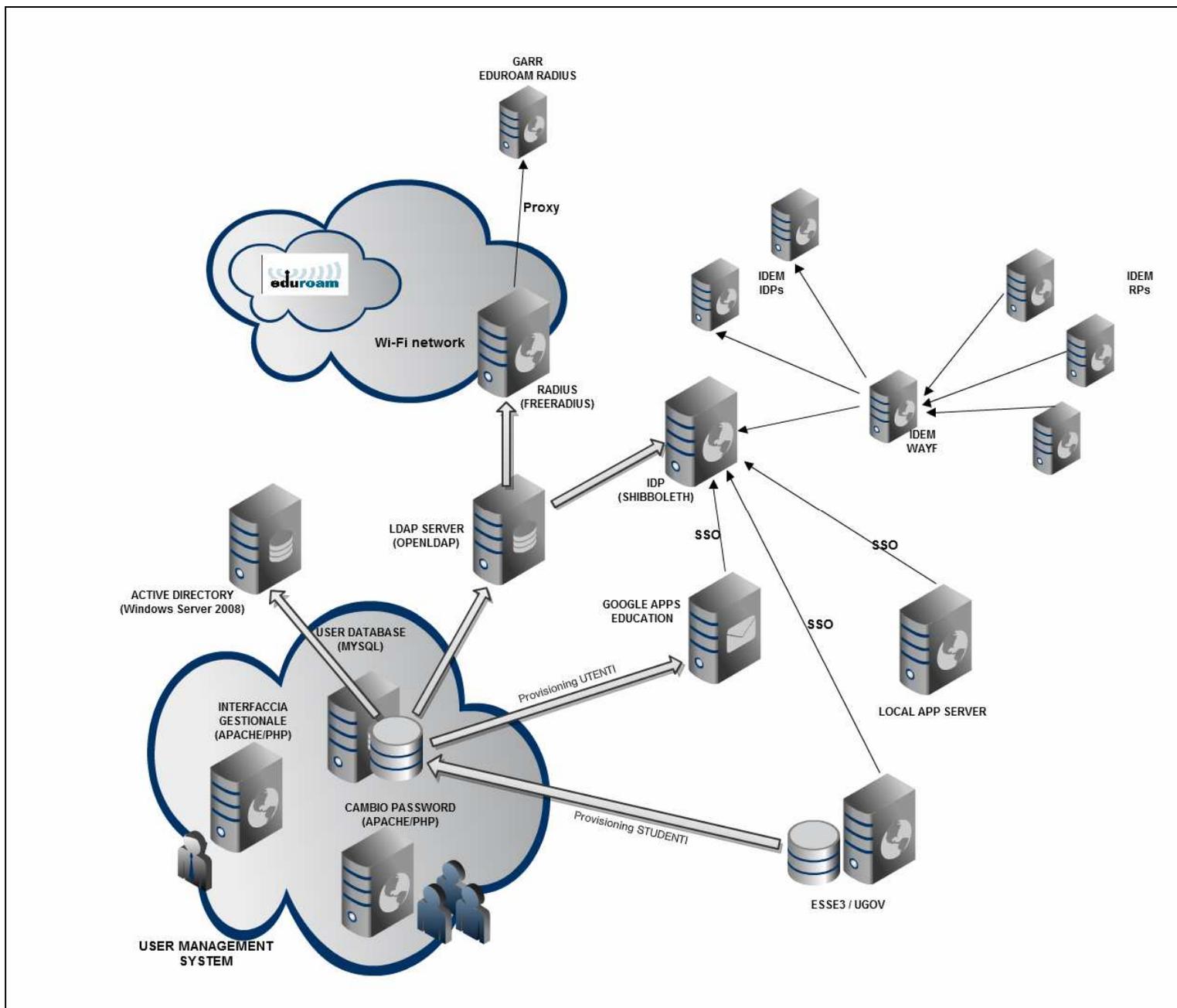
Le Università partecipanti utilizzano, per quanto possibile, prodotti OSS nell'implementazione delle soluzioni IAM e FIAM.

Comunicazione

Le modalità di comunicazione e i contenuti della comunicazione sono per quanto possibile resi omogenei per le Università partecipanti all'iniziativa. Oltre alle informative stabilite nelle linee guida normative più volte richiamate, le Università comunicano:

- l'adesione alle iniziative Eduroam e IDEM e i tempi previsti per l'attivazione dei servizi minimi;
- i livelli di servizio garantiti;
- le modalità operative per l'utilizzo dei servizi;
- l'elenco e le caratteristiche delle risorse conferite in Federazione;
- i riferimenti per l'assistenza agli utenti federati; in linea generale un *ticket* viene preso in carico in prima istanza dall'*identity provider* (riferimento diretto per l'utente finale) che eventualmente, effettuate le verifiche del caso, coinvolge il gestore della Federazione (Servizio IDEM GARR AAI o Eduroam).

Allegato – Schema funzionale esemplificativo



La figura riporta uno schema funzionale esemplificativo dell'implementazione di una soluzione AAI scalabile e compatibile con le indicazioni tecniche.

La soluzione suggerisce:

- 1) L'impiego di un UMS nell'ottica dell'economicità e affidabilità dei processi di user provisioning.
- 2) La gestione integrata delle infrastrutture di IAM e FIAM
- 3) L'impiego per quanto possibile di OSS nei componenti infrastrutturali.

Allegato – Esempio di DOPAU per l’adesione ad IDEM

Documento descrittivo del processo di accreditamento degli utenti dell’Università XYZ

Le informazioni fornite in questo documento sono accurate alla data del XX/XX/XXXX

Sommario

Abbreviazioni.....
Gestore dell’accREDITamento
Mappatura degli utenti sulle affiliazioni IDEM.....
Visione di insieme del processo di accREDITamento utenti
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
Il processo di accREDITamento per la categoria di utenti: Studenti
Il processo di accREDITamento per la categoria di utenti: Dottorandi interni, Studenti di master, Dottorandi di Università consorziate
Il processo di accREDITamento per la categoria di utenti: Alumni
Il sistema di autenticazione e autorizzazione interno.....
Partecipazione ad altre federazioni

Revisioni

Data	Versione	Descrizione modifica	Autori
XX/XX/XXXX	1.0	Versione finale	Verdi, Bianchi, Rossi

1) Abbreviazioni

AAI:	Authentication Authorization Infrastructure
AUP:	Acceptable User Policy
EDUROAM:	Educational Roaming
GARR:	Gestione Ampliamento Rete Ricerca
IDEM:	Identity Management
IDP:	Identity Provider
PIN:	Personal Identification Number
PUK:	Personal Unblocking Key
RFID:	Radio Frequency IDentification
SP:	Service Provider

2) Gestore dell'accreditamento

L'accreditamento è gestito dalle seguenti strutture:

- **Divisione servizi al Personale**, 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.
- **Divisione servizi alla Didattica**, "Segreterie Studenti" per gli studenti immatricolati a qualsiasi titolo presso l'Università XYZ, all'atto dell'immatricolazione.
- **Divisione servizi Informatici**, per il personale e per tutti gli altri soggetti che hanno titolo all'utilizzo dei servizi Internet e posta elettronica erogati dall'Università XYZ, a seguito di identificazione personale

La raccolta dei dati, il filtraggio e l'armonizzazione sono in capo alla Divisione Servizi Informatici, d'ora in avanti in questo documento abbreviato in DSI.

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".

3) Utenti gestiti

Nelle 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 dotato di dispositivo di firma digitale per la registrazione d. esami	D
11	Studente iscritto ai corsi di studio di 1° e 2° livello	S
12	Dottorando	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 titolare di una collaborazione a qualsiasi titolo (quale ad esempio l'iscrizione all'associazione "Alumni" riconosciuta dall'Ateneo)	A
17	Ospite (convegnista, ospite occasionale)	G
18	Personale di azienda esterna che presta attività lavorativa presso l'Università XYX	H
19	Personale di azienda/organizzazione esterna che fornisce servizi ICT	F
20	Personale in quiescenza	I

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, 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

Tabella delle macro categorie di utenza classificate in ateneo

4) 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

Tabella mappature delle macro categorie di utenza sulle affiliazioni IDEM

5) Visione di insieme del processo di accreditalmento 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.

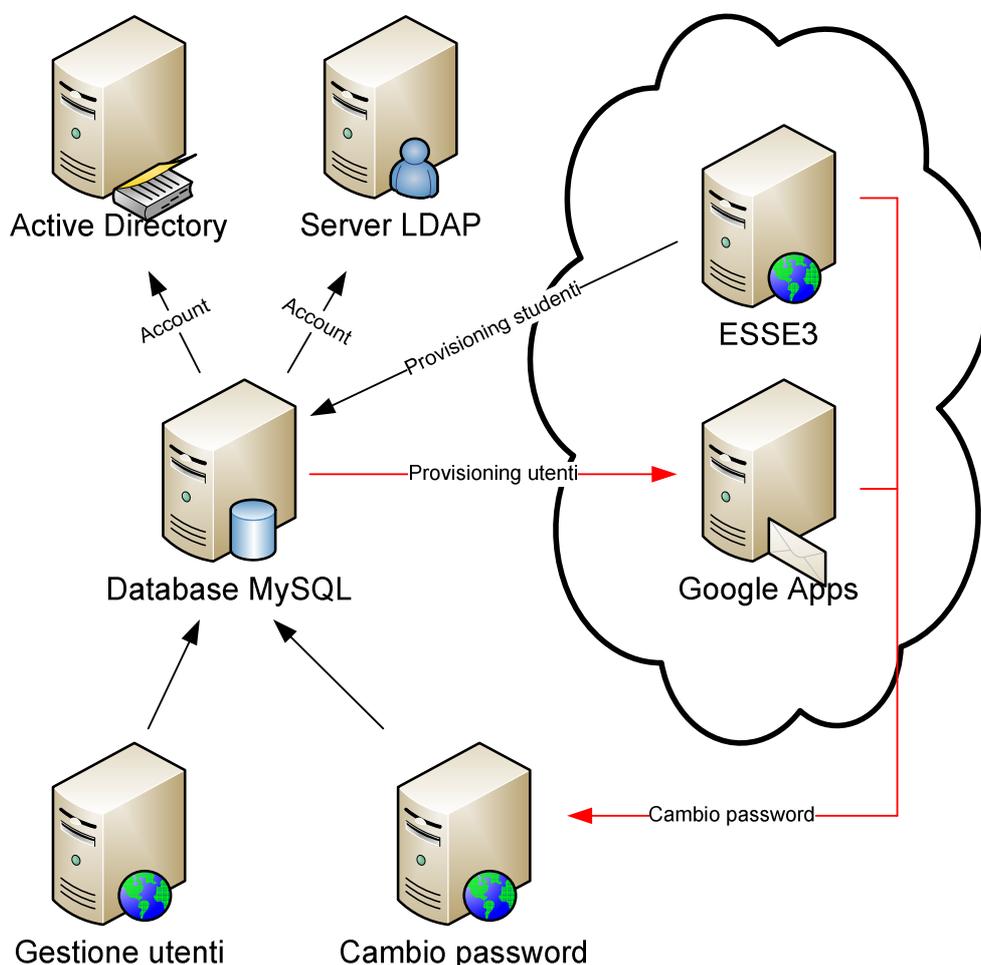
Una procedura eseguita ad intervalli regolari effettua gli aggiornamenti sul database LDAP (che alimenta i servizi Shibboleth e RADIUS) sul server Active Directory (che gestisce il dominio XYZ.IT per i computer desktop e il VDI) e infine su Google Apps Education (per la gestione delle caselle di posta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

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

Il link di cambio password di tutte le applicazioni Web punta alla parte pubblica del software di gestione degli utenti, che tra le altre funzioni prevede anche il pre-accreditalmento degli ospiti (in caso di eventi, iniziative ecc.).

L'utente utilizza le proprie credenziali presso i servizi Shibboleth, presso i captive portal (che permettono l'accesso alla rete dalle aule informatiche e dalle postazioni pubbliche dell'Ateneo) e presso tutti i servizi locali che utilizzano il server LDAP per autenticare i propri utenti. Al momento tra le principali di questa ultima categoria vi sono la gestione dell'archivio e protocollo, la gestione delle presenze, l'accesso VPN sicuro da reti esterne, i servizi bibliografici oltre ovviamente la procedura di cambio password.

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



6) 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: Divisione servizi al Personale

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, 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 recepite 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 annuale con il database dei contratti detenuto dalla Divisione dei Servizi al 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.

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

Il processo

Struttura organizzativa di riferimento: Divisione 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.

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

- Dottorandi interni
- Studenti di master
- Dottorandi di Università consorziate

Il processo

Struttura organizzativa di riferimento: Divisione Servizi Informatici

Responsabile accreditamento: Responsabile Ufficio Sistemi

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 Sistemi

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 recepite 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.

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

Il processo

Struttura organizzativa di riferimento: Divisione Servizi Informatici

Responsabile accreditamento: Responsabile Ufficio Sistemi

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: Ufficio Sistemi

Ufficio preposto (con delega scritta del responsabile): Segreteria dell'Associazione 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 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

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 eseguita 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.

10) 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		X
Protocollo elettronico		X
Servizi bibliotecari di consultazione e prestito		X
Servizi di posta elettronica/mailling 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
CMS di Ateneo		X
Piattaforma di E-Learning Moodle		X

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 con patch per la gestione ottimizzata del 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.

11) Partecipazione ad altre federazioni

- L'Università XYZ 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 assicurare l'accesso anche a tutti gli altri servizi che IDEM mette a disposizione è fondamentale condividere la medesima base dati d'identità digitali.