



*Ministero dell'Istruzione, dell'Università e della Ricerca*  
**DIPARTIMENTO PER L'UNIVERSITÀ, L'ALTA FORMAZIONE ARTISTICA, MUSICALE E COREUTICA E  
PER LA RICERCA**  
DIREZIONE GENERALE PER L'UNIVERSITÀ, LO STUDENTE E IL DIRITTO ALLO STUDIO UNIVERSITARIO

**Al Rettore  
Al Direttore Amministrativo  
Università ed Istituzioni Universitarie  
LORO SEDI**

*e p.c.* **CINECA**

Prot. n. 26/SEGR/DGUS/2011  
del 01/02/2011

**Oggetto: Diffusione linee guida per la digitalizzazione dei servizi**

Nell'ambito del progetto "Università digitale" previsto dal Piano eGov 2012 del Ministro per la pubblica amministrazione e l'innovazione e attuato con protocollo di intesa con il Ministro dell'istruzione, dell'università e della ricerca del 30 ottobre 2008, è stato realizzato un accurato lavoro di analisi e di sperimentazione su alcuni temi legati alla digitalizzazione, che credo sia utile condividere anche con le università che non hanno preso parte all'iniziativa.

Il Progetto era finalizzato ad accelerare e sostenere il processo di digitalizzazione e semplificazione amministrativa delle Università, con l'introduzione, il potenziamento e la standardizzazione di servizi quali, l'iscrizione online e la verbalizzazione elettronica degli esami, il fascicolo personale dello studente, l'automazione dei flussi informativi, nonché l'adozione di servizi VoIP e l'intera copertura dei campus con reti wifi.

Le Università partecipanti al progetto, il Dipartimento per la Digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei ministri e il Ministero dell'istruzione, dell'università e della ricerca, hanno elaborato e approvato apposite linee guida per la digitalizzazione dei principali processi e servizi considerati:

- implementazione del processo di verbalizzazione elettronica degli esami
- definizione del fascicolo dello studente
- realizzazione della cooperazione applicativa
- adozione di sistemi VoIP
- autenticazione federata per l'accesso a internet e risorse in rete

Le linee guida che sono disponibili sul sito <http://www.ict4university.gov.it/temi-universita-digitale.aspx> sono il risultato di una preziosa attività di definizione degli ambiti di applicazione dell'Università digitale, di analisi dei contesti normativi di riferimento e di proposta di soluzioni minime che consentono di realizzare infrastrutture e servizi a supporto per ognuno dei temi considerati.

Al fine di gestire il processo di digitalizzazione dei servizi con un approccio di sistema, le Università sono invitate a recepire le indicazioni contenute nelle linee guida per la fase di implementazione dei servizi che sono stati analizzati dal Tavolo Tecnico "Università Digitale".

Si ringrazia per la preziosa collaborazione.



*Ministero dell'Istruzione, dell'Università e della Ricerca*  
**DIPARTIMENTO PER L'UNIVERSITÀ, L'ALTA FORMAZIONE ARTISTICA, MUSICALE E COREUTICA E  
PER LA RICERCA**

F.to Ing Paolo Donzelli

Direttore Generale  
Ufficio studi e progetti per l'innovazione digitale  
Dip. Digitalizzazione PA ed innovazione Tecnologica

F.to Dott Marco Tomasi

Direttore Generale  
Direzione generale per l'università, lo studente e il diritto allo studio universitario

**IL DIRETTORE GENERALE**  
Dott. Marco Tomasi

Inviata ai seguenti atenei:

Università degli Studi di BARI

Politecnico di BARI

Università degli Studi della BASILICATA

Università degli Studi di BERGAMO

Università degli Studi di BOLOGNA

Università degli Studi di BRESCIA

Università degli Studi di CAGLIARI

Università della CALABRIA

Università degli Studi di CAMERINO

Università degli Studi di CASSINO

Università degli Studi di CATANIA

Università degli Studi "Magna Graecia" di CATANZARO

Università degli Studi "G. d'Annunzio" CHIETI-PESCARA

Università degli Studi di FERRARA

Università degli Studi di FIRENZE

Università degli Studi di FOGGIA

Università degli Studi di GENOVA

Università degli Studi INSUBRIA Varese-Como

Università degli Studi de L'AQUILA

Università degli Studi del SALENTO

Università degli Studi di MACERATA

Università degli Studi di MESSINA

Università degli Studi di MILANO

Università degli Studi di MILANO-BICOCCA

Politecnico di MILANO

Università degli Studi di MODENA e REGGIO EMILIA

Università degli Studi del MOLISE

Università degli Studi di NAPOLI "Federico II"

Seconda Università degli Studi di NAPOLI

Università degli Studi di NAPOLI "Parthenope"

Università degli Studi di NAPOLI "L'Orientale"

Università degli Studi di PADOVA

Università degli Studi di PALERMO

Università degli Studi di PARMA

Università degli Studi di PAVIA

Università degli Studi di PERUGIA

Università per Stranieri di PERUGIA

Università degli Studi del PIEMONTE ORIENTALE "Amedeo Avogadro"-Vercelli

Università degli Studi di PISA

Scuola Normale Superiore di PISA

Scuola Sup. di Studi Univ. e Perfezionamento S.Anna di PISA

Università Politecnica delle MARCHE

Università degli Studi "Mediterranea" di REGGIO CALABRIA  
Università degli Studi di ROMA "La Sapienza"  
Università degli Studi di ROMA "Tor Vergata"  
Università degli Studi ROMA TRE  
Istituto Universitario di Scienze Motorie di ROMA  
Università degli Studi di SALERNO  
Università degli Studi del SANNIO di BENEVENTO  
Università degli Studi di SASSARI  
Università degli Studi di SIENA  
Università per Stranieri di SIENA  
Università degli Studi di TERAMO  
Università degli Studi di TORINO  
Politecnico di TORINO  
Università degli Studi di TRENTO  
Università degli Studi di TRIESTE  
Scuola Internazionale Superiore di Studi Avanzati di TRIESTE  
Università degli Studi della TUSCIA  
Università degli Studi di UDINE  
Università "Ca' Foscari" di VENEZIA  
Università IUAV di VENEZIA  
Università degli Studi di VERONA  
SUM - Istituto Italiano di SCIENZE UMANE di FIRENZE  
Scuola IMT - Istituzioni, Mercati, Tecnologie - Alti Studi - LUCCA  
I.U.S.S. - Istituto Universitario di Studi Superiori - PAVIA  
Università degli Studi di URBINO "Carlo BO"  
LUM "Jean Monnet"  
Libera Università di BOLZANO  
Università "Carlo Cattaneo" - LIUC  
Università Commerciale "Luigi Bocconi" MILANO  
Università Cattolica del Sacro Cuore  
Libera Università di lingue e comunicazione IULM-MI  
Libera Università "Vita Salute S.Raffaele" MILANO  
Università degli Studi Suor Orsola Benincasa - NAPOLI  
Università "Campus Bio-Medico" ROMA  
Libera Univ. Inter.le Studi Sociali "Guido Carli" LUISS-ROMA  
Libera Università degli Studi "S. Pio V" ROMA  
Libera Univ. degli Studi "Maria SS.Assunta" - LUMSA - Roma  
Università della VALLE D'AOSTA  
Università Telematica "LEONARDO da VINCI"  
Università Telematica "E-CAMPUS"  
Università Telematica "GIUSTINO FORTUNATO"  
Università Telematica GUGLIELMO MARCONI  
Università Telematica Internazionale - UNITEL  
Università Telematica Internazionale UNINETTUNO

Università Telematica "ITALIAN UNIVERSITY LINE" - IUL  
Università Telematica PEGASO  
Università Telematica TEL.M.A.  
Università Telematica delle SCIENZE UMANE - UNISU  
Università Telematica "Universitas MERCATORUM"  
Università degli Studi di SCIENZE GASTRONOMICHE  
UKE - Università Kore di ENNA  
Università per Stranieri "Dante Alighieri" di REGGIO CALABRIA  
Università degli Studi EUROPEA di ROMA



Ministero dell'Istruzione, dell'Università e della  
Ricerca  
Direzione generale per l'università, lo studente e il  
diritto allo studio universitario



Presidenza del Consiglio dei Ministri  
Dipartimento per la digitalizzazione della Pubblica  
Amministrazione e l'Innovazione tecnologica  
Ufficio studi e progetti per l'Innovazione digitale

Ai Rettori

e p.c. ai Direttori Amministrativi

**Oggetto: Diffusione linee guida per la digitalizzazione dei servizi.**

Nell'ambito del progetto "Università digitale" previsto dal Piano eGov 2012 del Ministro per la pubblica amministrazione e l'innovazione e attuato con protocollo di intesa con il Ministro dell'istruzione, dell'università e della ricerca del 30 ottobre 2008, è stato realizzato un accurato lavoro di analisi e di sperimentazione su alcuni temi legati alla digitalizzazione, che credo sia utile condividere anche con le università che non hanno preso parte all'iniziativa.

Il Progetto era finalizzato ad accelerare e sostenere il processo di digitalizzazione e semplificazione amministrativa delle Università, con l'introduzione, il potenziamento e la standardizzazione di servizi quali, l'iscrizione online e la verbalizzazione elettronica degli esami, il fascicolo personale dello studente, l'automazione dei flussi informativi, nonché l'adozione di servizi VoIP e l'intera copertura dei campus con reti wifi.

Le Università partecipanti al progetto, il Dipartimento per la Digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei ministri e il Ministero dell'istruzione, dell'università e della ricerca, hanno elaborato e approvato apposite linee guida per la digitalizzazione dei principali processi e servizi considerati:

- implementazione del processo di verbalizzazione elettronica degli esami
- definizione del fascicolo dello studente
- realizzazione della cooperazione applicativa
- adozione di sistemi VoIP
- autenticazione federata per l'accesso a Internet e risorse in rete

Le linee guida che sono disponibili sul sito <http://www.ict4university.gov.it/temi-universita-digitale.aspx> sono il risultato di una preziosa attività di definizione degli ambiti di applicazione dell'Università digitale, di analisi dei contesti normativi di riferimento e di proposta di soluzioni

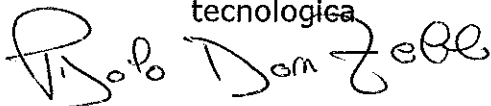
minime che consentono di realizzare infrastrutture e servizi a supporto per ognuno dei temi considerati.

Al fine di gestire il processo di digitalizzazione dei servizi con un approccio di sistema, le Università sono invitate a recepire le indicazioni contenute nelle linee guida per la fase di implementazione dei servizi che sono stati analizzati dal Tavolo Tecnico "Università Digitale".

Si ringrazia per la preziosa collaborazione.


Ing. Paolo Donzelli

Direttore Generale  
Ufficio studi e progetti per l'innovazione  
digitale  
Dip. Digitalizzazione PA ed Innovazione  
tecnologica



Dott. Marco Tomasi

Direttore Generale  
Direzione generale per l'università, lo  
studente e il diritto allo studio  
universitario





**Presidenza del Consiglio dei Ministri**  
Dipartimento per la digitalizzazione della  
Pubblica Amministrazione e l'innovazione  
tecnologica



**Ministero dell'Istruzione, dell'Università e  
della Ricerca**

## **Università digitale**

# **Linee guida per la digitalizzazione dei servizi**

**Piano eGov 2012 – Obiettivo Università**



**Ottobre 2010**

## Sommario

Presentazione del documento.....	4
Capitolo 1. Contesto di riferimento e sintesi.....	5
1.1 Premessa.....	5
1.2 Sintesi delle linee guida .....	6
1.3 Università partecipanti al progetto “Università digitale”.....	8
1.4 Documentazione di riferimento .....	9
Capitolo 2. Implementazione del processo di verbalizzazione elettronica degli esami.....	10
2.1 Premessa.....	10
2.2 Linee guida.....	10
Capitolo 3. Fascicolo personale dello studente .....	13
3.1 Premessa.....	13
3.2 Terminologia e riferimenti normativi .....	13
3.3 Uso del fascicolo studente negli atenei – stato dell’arte .....	15
3.4 Linee guida.....	15
3.5 Modello di riferimento .....	16
Capitolo 4. Realizzazione della cooperazione applicativa.....	18
4.1 Premessa.....	18
4.2 Terminologia.....	18
4.3 Cooperazione Applicativa - linee guida.....	18
4.4 Cooperazione applicativa: caso d’uso foglio di congedo.....	19
4.4.1 Definizione di un glossario di termini.....	20
4.4.2 Condivisione del processo .....	21
4.4.3 Definizione e condivisione del formato di interscambio dati .....	22
4.4.4 Definizione e condivisione delle modalità di interazione.....	23
4.4.5 Definizione e condivisione del protocollo di comunicazione.....	23
Capitolo 5. Adozione di sistemi VoIP .....	25
5.1 Individuazione di standard aperti per l’interoperabilità.....	25
5.2 Infrastruttura di trasporto e visibilità .....	25
5.3 Mobilità e servizi a valore aggiunto innovativi .....	25
5.4 Sistemi e tecnologie Open Source per il VoIP.....	25
5.5 Ricadute sull’Organizzazione .....	26
Capitolo 6. Autenticazione Federata per l’accesso a Internet e a risorse in rete.....	27
6.1 Descrizione generale del servizio e ambito di applicazione .....	27
6.2 Modalità operative: i casi eduroam ed IDEM - autenticazione federata per il Wi-Fi in ambito universitario .....	28
Appendici .....	30
Appendice A. Allegato tecnico alle linee guida per la realizzazione della cooperazione applicativa .....	31
A.1. Web services a supporto della cooperazione applicativa finalizzata al trasferimento degli studenti .....	31
A.1.1. Riepilogo dei servizi .....	31
A.1.2. Dettaglio dei servizi .....	32
A.2. Esempificazione del processo di trasferimento basato sulla cooperazione applicativa .....	38
A.2.1. Uscita: gestione della domanda di trasferimento da parte dell’Ateneo di provenienza .....	38
A.2.2. Ingresso: gestione della domanda di trasferimento da parte dell’Ateneo di destinazione .....	42
A.2.3. Foglio excel.....	45
A.2.4. Schema xsd .....	45

A.2.5. Note.....	56
Appendice B. Specifiche tecniche di riferimento per l’implementazione di infrastrutture VoIP interoperabili .....	57
B.1. Premessa.....	57
B.2. Requisiti .....	58
Appendice C. Normativa sul VoIP .....	68
Appendice D. Allegato tecnico alle linee guida per l’autenticazione federata per l’accesso a Internet e risorse in rete .....	70
D.1. Premessa.....	70
D.2. Scopo e contenuti del documento .....	70
D.3. Scenario e principi generali.....	71
D.4. Obiettivi di servizio agli utenti finali .....	71
D.5. Conferimento delle identità digitali .....	72
D.6. Realizzazione di servizi federati .....	72
D.7. Amministrazione delle infrastrutture tecnologiche.....	72
D.8. Livelli di servizio .....	72
D.9. Adozione coordinata di soluzioni tecnologiche .....	73
D.10. Comunicazione.....	73
D.11. Allegato – Schema funzionale esemplificativo.....	74
D.12. Allegato – Esempio di DOPAU per l’adesione ad IDEM .....	75
D.12.1. Abbreviazioni.....	75
D.12.2. Gestore dell’accreditamento .....	75
D.12.3. Utenti gestiti .....	76
D.12.4. Mappatura degli utenti sulle affiliazioni IDEM.....	77
D.12.5. Visione di insieme del processo di accreditamento utenti .....	78
D.12.6. 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 .....	79
D.12.7. Il processo di accreditamento per la categoria di utenti: Studenti .....	82
D.12.8. Il processo di accreditamento per la categoria di utenti: Dottorandi interni, Studenti di master, Dottorandi di Università consorziate.....	84
D.12.9. Il processo di accreditamento per la categoria di utenti: Alumni .....	86
D.12.10. Il sistema di autenticazione e autorizzazione interno.....	88
D.12.11. Partecipazione ad altre federazioni .....	88
Appendice E. Data di approvazione delle linee guida .....	89
E.1. Tabella di sintesi .....	89

## Presentazione del documento

Le Linee guida sono state realizzate nell’ambito del progetto “Università digitale” previsto dal Piano eGov 2012 del Ministro per la pubblica amministrazione e l’innovazione e attuato con protocollo di intesa con il Ministro dell’istruzione, dell’università e della ricerca del 30 ottobre 2008.

Le linee si rivolgono a tutte le università italiane statali e non statali legalmente riconosciute e gli Istituti di Alta Formazione Artistica e Musicale con l’intento di chiarire gli ambiti di applicazione, analizzare i contesti normativi di riferimento e fornire le indicazioni su “come” realizzare infrastrutture e servizi per l’università digitale.

Il documento è strutturato come delineato nel seguente schema.



## Capitolo 1. Contesto di riferimento e sintesi

### 1.1 Premessa

Il Piano eGov 2012 promosso dal Ministro per la pubblica amministrazione e l'innovazione definisce un insieme di progetti di innovazione digitale che, nel loro complesso, si propongono di modernizzare, rendere più efficiente e trasparente la Pubblica Amministrazione, migliorando qualità ed efficienza dei servizi erogati a cittadini e imprese.

Tra gli obiettivi prioritari del Piano vi è l'Università: “entro il termine della legislatura tutte le università italiane disporranno di servizi avanzati per studenti, docenti e personale amministrativo, a partire da una completa copertura WiFi e disponibilità di servizio VoIP in tutte le sedi”.

Il progetto “Università digitale” si inserisce tra le iniziative previste dal Piano e attivate con il protocollo di intesa del 30 ottobre 2008 tra il Ministro per la pubblica amministrazione e l'innovazione e il Ministro dell'istruzione, dell'università e della ricerca.

Il progetto “Università digitale”, in fase avanzata di realizzazione in 27 università, intende accelerare il processo di digitalizzazione e semplificazione amministrativa delle università, con l'introduzione, il potenziamento e la standardizzazione di servizi quali, l'iscrizione online e la verbalizzazione elettronica degli esami, il fascicolo personale dello studente, l'automazione dei flussi informativi, nonché l'adozione di servizi VoIP e l'intera copertura dei campus con reti wifi.

Per favorire la diffusione dei risultati conseguiti all'intero sistema universitario, le università partecipanti al progetto, il Dipartimento per la Digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei ministri e il Ministero dell'istruzione, dell'università e della ricerca, hanno elaborato e approvato apposite linee guida per la digitalizzazione dei principali processi e servizi considerati:

- 1) Linee guida per l'implementazione del processo di verbalizzazione elettronica degli esami
- 2) Linee guida per il fascicolo dello studente
- 3) Linee guida per la realizzazione della cooperazione applicativa
- 4) Linee guida per l'adozione di sistemi VoIP
- 5) Linee guida per l'autenticazione federata per l'accesso a internet e risorse in rete

## 1.2 Sintesi delle linee guida

### Linee guida per l'implementazione del processo di verbalizzazione elettronica degli esami

Le linee guida definiscono i requisiti minimi che caratterizzano un sistema per la completa digitalizzazione del processo di gestione degli esami: dall'iscrizione da parte degli studenti, alla definizione degli appelli, alla notifica del risultato, fino alla firma e conservazione dei verbali, esaminandone gli aspetti più critici da un punto di vista normativo, organizzativo e implementativo. Le fasi principali del processo di verbalizzazione analizzate sono le seguenti:

- 1) definizione degli appelli e delle commissioni di esame;
- 2) gestione delle liste di esame;
- 3) svolgimento dell'esame (eventualmente con prove multiple);
- 4) definizione del voto e sua comunicazione allo studente;
- 5) accettazione/rifiuto del voto da parte dello studente (opzionale);
- 6) redazione del verbale;
- 7) firma del verbale;
- 8) consultazione del voto da parte dello studente.

### Linee guida per il fascicolo dello studente

Le linee guida delineano il percorso di creazione del “dossier digitale” degli atti di carriera dello studente (dall'immatricolazione, ai piani di studio, ai verbali di esame) in un formato condiviso e in linea con gli standard europei. Il documento definisce inoltre le modalità per realizzare l'integrazione tra i sistemi di gestione documentale ed i sistemi gestionali in uso presso gli atenei, a partire dal sistema di gestione delle carriere studenti, al fine di:

- semplificare il processo di apertura del fascicolo dello studente nel sistema di gestione documentale di ateneo rendendo automatica l'attività, in sostituzione dell'attivazione manuale;
- ridurre il carico di lavoro del personale consentendo l'inserimento automatico nel fascicolo studente dei documenti più rilevanti relativi alla sua carriera e l'utilizzo *online* degli stessi, nel rispetto della *privacy*, per assolvere compiti istituzionali;
- rendere disponibile a ciascun studente il proprio fascicolo ai fini della trasparenza amministrativa.

### Linee guida per la realizzazione della cooperazione applicativa

Al fine di definire efficientemente le modalità di cooperazione tra una molteplicità di sistemi e di permettere un facile adattamento degli stessi rispetto all'evoluzione dei servizi, le linee guida forniscono delle raccomandazioni generali su cui basare la cooperazione applicativa.

Tali raccomandazioni sono poi state declinate su uno specifico caso di studio, il “foglio di congedo”, che rappresenta un tipico esempio di cooperazione tra due atenei che devono scambiarsi informazioni relative a uno studente che inoltra una domanda di trasferimento per lasciare l'ateneo di provenienza e giungere presso l'ateneo di destinazione.

Le linee guida sono state inoltre progettate in modo da essere utili anche nella definizione di moderni scenari di cooperazione applicativa con le anagrafi centrali.

### Linee guida per l'adozione di sistemi VoIP

Le linee guida forniscono indicazioni e suggerimenti su come realizzare un'infrastruttura completamente integrata per l'istadamento su rete della ricerca di tutte le chiamate telefoniche interne alle università e tra le università e il MIUR, anche integrando le applicazioni con i servizi VoIP.

Le linee guida si focalizzano sui seguenti punti:

- individuare protocolli e standard aperti per garantire la migliore interoperabilità;
- condividere le scelte relative ai problemi di visibilità dei numbering plan locali e “indirizzamento” telefonico attraverso soluzioni condivise quali NRENUM (“pagine bianche” del VoIP);
- utilizzare infrastrutture di rete pubbliche a resa prestazionale elevata e costi contenuti;
- adottare il VoIP anche e soprattutto per fornire agli utenti servizi innovativi quali mobilità, presenza, instant-messaging, comunicazione unificata, operatore automatico, rubrica on-line, conference call, per rispondere ai più moderni bisogni di comunicazione e interazione per l'intera comunità universitaria.

### Linee guida per l'autenticazione federata per l'accesso a internet e risorse in rete

Le linee guida indicano quali scenari e tecnologie si devono implementare nelle università per giungere all'obiettivo di rendere sempre disponibili agli utenti i servizi digitali a prescindere dalla locazione fisica degli utenti stessi, nel rispetto delle indicazioni normative vigenti. Il documento si articola in due parti: in una prima parte vengono indicati ambito di applicazione e presa in considerazione la normativa di riferimento; nella seconda si affrontano casi specifici di applicazione.

### 1.3 Università partecipanti al progetto “Università digitale”

Denominazione Rete	Università	Denominazione Progetto
U4U- University 4 University	<ol style="list-style-type: none"> <li>1) Politecnico di TORINO (Capofila)</li> <li>2) Politecnico di MILANO</li> <li>3) Università degli Studi di CATANIA</li> <li>4) Università degli Studi di FERRARA</li> <li>5) Università degli Studi di URBINO "Carlo BO"</li> </ol>	U4U- University 4 University
R.U.P. Rete delle Università Pugliesi	<ol style="list-style-type: none"> <li>1) Università degli Studi del SALENTO (Capofila)</li> <li>2) Politecnico di BARI</li> <li>3) Università degli Studi di BARI</li> <li>4) Università degli Studi di FOGGIA</li> </ol>	K-Student
UNI22	<ol style="list-style-type: none"> <li>1) Università degli Studi di BOLOGNA (Capofila)</li> <li>2) Università degli Studi di TRENTO</li> <li>3) Università degli Studi di VERONA</li> </ol>	Ubiversitas
DuecentoSuQuattro	<ol style="list-style-type: none"> <li>1) Università degli Studi di NAPOLI "Federico II" (Capofila)</li> <li>2) Università degli Studi "G. d'Annunzio" CHIETI – PESCARA</li> <li>3) Università degli Studi di MACERATA</li> <li>4) Università degli Studi di TORINO</li> </ol>	DIGIT@UNI:Infrastrutture e servizi per il sistema universitario
Atenei Veneziani	<ol style="list-style-type: none"> <li>1) Università IUAV di VENEZIA (Capofila)</li> <li>2) Università "Cà Foscari" di VENEZIA</li> </ol>	Venice Wide Campus
Uni5Net	<ol style="list-style-type: none"> <li>1) Università degli Studi di PAVIA (Capofila)</li> <li>2) Università degli Studi di BERGAMO</li> <li>3) Università degli Studi di FIRENZE</li> <li>4) Università degli Studi di MILANO-BICOCCA</li> <li>5) Università degli Studi INSUBRIA VARESE - COMO</li> </ol>	Uni5Net4Student
	Università degli Studi di ROMA "Tor Vergata"	Tor Vergata - Università digitale
	Università degli Studi di ROMA "La Sapienza"	La Sapienza - Università digitale
	Università degli Studi "ROMA TRE"	Roma Tre - Università digitale
	Università degli Studi dell'AQUILA	Università degli Studi dell'Aquila - Università digitale

## 1.4 Documentazione di riferimento

- ❑ Piano eGovernment 2012 disponibile al link:  
<http://www.e2012.gov.it/egov2012/?q=content/universit%C3%A0-digitale>
  
- ❑ Protocollo di intesa del 30/10/2008 disponibile al link:  
<http://www.innovazionepa.gov.it/comunicazione/notizie/2008/ottobre/notizia-del-30102008-2.aspx>
  
- ❑ Programma ICT4University disponibile al link: <http://www.ict4university.gov.it>

## Capitolo 2. Implementazione del processo di verbalizzazione elettronica degli esami

### 2.1 Premessa

Le fasi principali del processo di verbalizzazione sono le seguenti:

- 1) Definizione degli appelli e delle commissioni di esame
- 2) gestione delle liste di esame
- 3) svolgimento dell'esame (eventualmente con prove multiple)
- 4) definizione del voto e sua comunicazione allo studente
- 5) accettazione/rifiuto del voto da parte dello studente (opzionale)
- 6) redazione del verbale
- 7) firma del verbale
- 8) consultazione del voto da parte dello studente

Nel seguito, fase per fase, sono definiti i requisiti minimi che il sistema deve soddisfare.

### 2.2 Linee guida

#### *1) Definizione degli appelli e delle commissioni di esame*

In questa fase si devono definire gli appelli e la composizione della commissione di esame. Queste informazioni devono essere pubblicate sul web e devono essere recuperate in modo automatico a partire dall'offerta formativa; l'applicazione di gestione esami (di seguito sistema) deve essere integrata con gli applicativi esistenti.

#### *2) gestione delle liste di esame*

Il sistema deve permettere la gestione di tutte le modalità di esame previste dall'ateneo: ad esempio, solo orali, solo scritti, scritto più orale, molti scritti molti orali, prove di laboratorio, anche considerando corsi integrati e modulari.

Il sistema deve consentire al docente di gestire le liste di esame e di visionare le liste degli studenti registrati. Il sistema deve consentire allo studente di iscriversi, ovvero cancellarsi, da una lista.

Poiché il sistema è integrato con il sistema di gestione delle carriere studenti, sarà possibile eseguire automaticamente dei controlli volti a verificare che lo studente abbia tutti i titoli per iscriversi a un esame (per esempio se è in regola con il pagamento delle tasse universitarie, o se sono rispettate eventuali propedeuticità).

#### *3) svolgimento dell'esame (eventualmente con prove multiple)*

Il sistema deve supportare il docente nella gestione dell'esame, anche su prove multiple. In caso di prove multiple il docente deve poter inserire le votazioni parziali riportate e comunicare tali esiti agli studenti (operazioni che possono essere svolte esattamente come nel punto 4, descritto nel seguito).

#### ***4) definizione del voto e sua comunicazione allo studente***

Completato l'esame, il docente procede a inserire nel sistema il voto riportato da ogni studente (eventualmente frutto di prove multiple).

Successivamente all'inserimento dei voti, il sistema renderà disponibili gli esiti pubblicandoli sul portale dell'Ateneo, al quale gli studenti potranno accedere previa autenticazione.

Il sistema provvede inoltre a notificare automaticamente agli studenti la pubblicazione degli esiti degli esami, anche in caso di esami svolti in presenza (per i quali il docente potrebbe già aver comunicato a voce l'esito) con le seguenti modalità: tramite invio di una email alla casella di posta elettronica istituzionale ovvero di un sms ovvero di PEC che avvisi lo studente della disponibilità dell'esito dell'esame sostenuto o dell'esito stesso. In seguito al ricevimento della notifica, lo studente si potrà collegare al portale di Ateneo, dove potrà consultare il voto riportato nell'esame (previa autenticazione).

#### ***5) accettazione/rifiuto del voto da parte dello studente (opzionale)***

Nel caso di esami in presenza, il docente comunica il risultato allo studente, che può decidere se accettare/rifiutare il voto. Nel caso di esami con esito non immediato, lo studente, che con le modalità di cui al punto 4) è stato informato del voto conseguito, può accedere al sistema per accettarlo oppure rifiutarlo. Nel primo caso il voto verrà registrato e verbalizzato, nel secondo no.

Occorre informare lo studente del tempo massimo (indicativamente non superiore a 5 giorni solari consecutivi) a disposizione per prendere visione del voto e quindi eventualmente rifiutarlo. La mancata presa visione ovvero il mancato rifiuto del voto da parte dello studente entro tale tempo massimo equivale alla sua accettazione.

#### ***6) redazione del verbale***

Il sistema deve supportare il docente nella compilazione del verbale, guidandolo nelle operazioni richieste e minimizzando la quantità di informazioni da inserire (è auspicabile che il docente debba inserire solo il voto).

Dati del verbale "obbligatori" : codice e denominazione dell'insegnamento, identificativo dell'appello, data dell'esame che può o meno coincidere con quella di verbalizzazione, informazioni sui membri della commissione di esame, identificativo del docente verbalizzante, identificativo dello studente, voto. Dati del verbale "addizionali": argomenti di esame (che potrebbero essere selezionati automaticamente da un insieme di domande precaricate), note.

Ciascun verbale può contenere le registrazioni relative a più studenti.

I verbali devono essere redatti in formati appropriati sia alla gestione che alla conservazione, per consentire la lettura del verbale nel tempo con le stesse caratteristiche estrinseche (ad esempio, modalità di impaginazione, logo, etc) che il documento aveva al momento della sua firma. Il formato suggerito è PDF/A1.

### ***7) firma del verbale***

Il verbale deve essere firmato digitalmente dal solo docente verbalizzante. Non è prevista la firma da parte dello studente.

La firma può essere eseguita dal docente sia con dispositivi personali di firma (ad esempio, smart card o token usb), sia mediante l'uso di tecniche di firma remota.

La remotizzazione della firma si basa sulla possibilità di utilizzare degli Hardware Security Module (HSM), eliminando la necessità di distribuire a tutti i docenti un dispositivo personale di firma. I certificati per la firma possono inoltre contenere le limitazioni d'uso previste dalla normativa (ad esempio essere limitati alla firma dei verbali ovvero all'uso nell'ambito universitario).

Una volta eseguita la firma, il voto entra nella carriera dello studente e il verbale va in conservazione. Inoltre il verbale viene trasmesso alla casella di posta elettronica istituzionale degli altri membri della commissione.

### ***8) consultazione del voto da parte dello studente***

Il sistema deve consentire agli studenti in ogni momento la visualizzazione dei propri voti.

### ***Note conclusive***

#### ***Modalità di autenticazione degli utenti:***

Il sistema deve prevedere almeno le seguenti modalità di autenticazione degli utenti:

- autenticazione docente: autenticazione basata solo su username e password (ulteriori livelli di sicurezza possono essere previsti per l'inserimento dei voti e sono necessari per l'utilizzo della firma digitale);
- autenticazione studente: autenticazione basata su username e password.

#### ***Conservazione dei verbali di esame***

I verbali di esame non richiedono marca temporale contestualmente alla sottoscrizione.

## Capitolo 3. Fascicolo personale dello studente

### 3.1 Premessa

Il fascicolo dello studente costituisce una particolare specie di fascicolo; al suo interno infatti si conservano documenti relativi a diversi procedimenti amministrativi correlati fra loro dal solo vincolo di essere relativi ad un'unica persona fisica, lo studente.

Principale obiettivo dell'iniziativa Università Digitale in tale contesto è quello di realizzare l'integrazione tra i sistemi di gestione documentale ed i sistemi gestionali in uso presso gli atenei, a partire dal sistema di gestione delle carriere studenti, al fine di:

- semplificare il processo di apertura del fascicolo dello studente nel sistema di gestione documentale di ateneo rendendo automatica l'attività, in sostituzione dell'attivazione manuale;
- ridurre il carico di lavoro del personale consentendo l'inserimento automatico nel fascicolo studente dei documenti più rilevanti relativi alla sua carriera e l'utilizzo *online* degli stessi, nel rispetto della *privacy*, per assolvere compiti istituzionali;
- rendere disponibile a ciascun studente il proprio fascicolo ai fini della trasparenza amministrativa.

Quanto appena descritto indurrebbe immediatamente a focalizzare l'attenzione su valutazioni e scelte di tipo tecnologico; tuttavia si ritiene necessario dover affrontare prima l'argomento da un punto di vista più ampio, ponendo l'attenzione su altre componenti quali la:

- condivisione ed armonizzazione del linguaggio
- rilevazione dei modelli organizzativi adottati negli atenei
- definizione di un modello di riferimento.

L'integrazione tra il sistema di gestione documentale ed i sistemi gestionali, a partire dal sistema di gestione delle carriere studenti, non esaurisce quanto deve essere realizzato al fine di una completa dematerializzazione del fascicolo studente. L'obiettivo finale resta infatti la reingegnerizzazione ed automazione di tutti processi interni agli atenei relativi al ciclo di vita dello studente, analogamente a quanto realizzato per la verbalizzazione degli esami.

### 3.2 Terminologia e riferimenti normativi

#### **Documento informatico:**

(Art.1, comma 1, lettera p [decreto legislativo n. 82 del 7 marzo 2005 – Codice dell'Amministrazione digitale – CAD 2005]) “La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”.

(Art.20 comma 1 [CAD 2005]) “Il documento informatico, da chiunque formato, la registrazione su supporto informatico e la trasmissione con strumenti telematici sono validi e rilevanti a tutti gli effetti di legge se conformi alle disposizioni del presente codice ed alle regole tecniche di cui all'articolo 71”.

#### **Procedimento e fascicolo informatico:**

(Art. 41 comma 2 [CAD 2005]) “La pubblica amministrazione titolare del procedimento può raccogliere in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da qualunque formati; all'atto della comunicazione dell'avvio del procedimento ai sensi dell'articolo 8 della legge 7 agosto 1990, n. 241, comunica agli interessati le modalità per esercitare in via telematica i diritti di cui all'articolo 10 della citata legge 7 agosto 1990, n. 241”.

(Art. 41 comma 2-bis [CAD 2005]) “Il fascicolo informatico è realizzato garantendo la possibilità di essere direttamente consultato ed alimentato da tutte le amministrazioni coinvolte nel procedimento. Le regole per la costituzione e l’utilizzo del fascicolo sono conformi ai principi di una corretta gestione documentale ed alla disciplina della formazione, gestione, conservazione e trasmissione del documento informatico, ivi comprese le regole concernenti il protocollo informatico ed il sistema pubblico di connettività, e comunque rispettano i criteri dell’interoperabilità e della cooperazione applicativa; regole tecniche specifiche possono essere dettate ai sensi dell’articolo 71, di concerto con il Ministro della funzione pubblica”.

(Art. 41 comma 2-ter [CAD 2005]) “Il fascicolo informatico reca l’indicazione:

- a) dell’amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
- b) delle altre amministrazioni partecipanti;
- c) del responsabile del procedimento;
- d) dell’oggetto del procedimento;
- e) dell’elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater”.

(Art. 41 comma 2-quater [CAD 2005]) “Il fascicolo informatico può contenere aree a cui hanno accesso solo l’amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti; è inoltre costituito in modo da garantire l’esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990”.

### **Sistema di gestione dei flussi documentali:**

(art. 64 [decreto del Presidente della Repubblica n. 445 del 28 dicembre 2000 – DPR 445])

“1. Le pubbliche amministrazioni provvedono in ordine alla gestione dei procedimenti amministrativi mediante sistemi informativi automatizzati, valutando i relativi progetti in termini di rapporto tra costi e benefici, sulla base delle indicazioni fornite dall’Autorità per l’informatica nella pubblica amministrazione.

2. I sistemi per la gestione dei flussi documentali che includono i procedimenti amministrativi di cui al comma 1 e’ finalizzata al miglioramento dei servizi e al potenziamento dei supporti conoscitivi delle amministrazioni secondo i criteri di economicità, di efficacia dell’azione amministrativa e di pubblicità stabiliti dalla legge.

3. Il sistema per la gestione dei flussi documentali include il sistema di gestione informatica dei documenti.

4. Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d’archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo”.

### **Gestione informatica dei documenti:**

(Art.1, comma 1, lettera u, del CAD 2005) “L’insieme delle attività finalizzate alla registrazione e segnatura di protocollo, nonché alla classificazione, organizzazione, assegnazione, reperimento e conservazione dei documenti amministrativi formati o acquisiti dalle amministrazioni, nell’ambito del sistema di classificazione d’archivio adottato, effettuate mediante sistemi informatici”.

### **Area Organizzativa Omogenea (AOO):**

(DPCM 31 ottobre 2000) “Un insieme di funzioni e di strutture, individuate dall’amministrazione che opera su tematiche omogenee e che presenta esigenze di gestione della documentazione in modo unitario e coordinato ai sensi dell’Articolo 2, comma 2, del decreto del Presidente della Repubblica n. 428/1998”;

**Unità organizzativa responsabile (UOR):**

Una struttura operativa dell'AOO costituita da un complesso di risorse umane e strumentali, cui sono affidate competenze omogenee nell'ambito delle quali il personale dipendente assume la responsabilità della trattazione di affari o procedimenti amministrativi.

**3.3 Uso del fascicolo studente negli atenei – stato dell'arte**

Dalla rilevazione condotta tra gli atenei che partecipano ai progetti di Università Digitale risulta che i modelli organizzativi adottati per la gestione dei processi che riguardano la carriera dello studente sono profondamente diversi tra loro. Al livello più basso della struttura organizzativa si trova sempre la segreteria studenti, una per ciascuna facoltà; differiscono invece le aggregazioni organizzative ai livelli superiori e quelle per la gestione di specifiche attività (es. immatricolazione, collaborazioni studentesche, etc). Altrettanto dicasi dei modelli organizzativi per l'archiviazione dei documenti nel sistema di gestione documentale e per la loro eventuale protocollazione.

Non esiste pertanto una *policy* uniforme e condivisa dagli atenei per la formazione del fascicolo studente; talvolta questa differisce anche tra le segreterie dello stesso ateneo. È inoltre sempre più diffusa la tendenza a sostituire con appositi servizi web autenticati la presentazione da parte degli studenti di istanze cartacee. In questi casi il documento/modulo tradizionale quasi sempre viene rimpiazzato da un insieme di dati registrati nel *data base* del sistema informativo di ateneo.

Il sistema di archiviazione documentale di norma non è integrato con il sistema di gestione delle carriere studenti. Esiste inoltre un insieme di documenti/atti interni all'amministrazione universitaria (es. decreti, delibere), spesso di natura collettiva, che circolano ancora in forma cartacea.

**3.4 Linee guida**

In conformità a quanto stabilito dal bando, i progetti devono mirare alla semplificazione del processo di apertura e chiusura del fascicolo studente nei sistemi di gestione documentale in uso presso gli atenei attraverso la realizzazione di opportuni servizi automatizzati che supportino l'interoperabilità tra il sistema di gestione delle carriere studenti e quello documentale. Analogamente anche l'inserimento di documenti nel fascicolo deve essere semplificato e non implicare aggravii gestionali al personale coinvolto nel processo.

Considerato che molte delle istanze presentate dallo studente sono state ormai sostituite da servizi web autenticati, eliminando così la necessità di presentare modelli cartacei, i documenti informatici da inserire nel fascicolo studente, anch'esso informatico, devono essere necessariamente limitati a quelli di legge ed eventualmente a quelli che si riferiscono ad eventi con effetti sulla carriera, sia che essi vengano innescati dallo studente sia che vengano generati dall'ateneo.

Tutti i documenti informatici dovranno essere generati in formati aperti standard (es. PDF/A, XML).

Vale la pena ricordare che la conferma dei dati inseriti tramite un servizio web previa autenticazione con credenziali di accesso costituisce sottoscrizione elettronica ai sensi dell'art. 65, comma 1, lettera c, del CAD/2005. Non è quindi necessario in questi casi presentare una istanza cartacea con firma autografa. Inoltre, se l'istanza è singolarmente individuabile in qualche modo (ad es. mediante un numero univoco), ai sensi dell'art. 53, comma 5, del D.P.R. 445/2000, si può prevedere di escluderla dalla registrazione di protocollo in quanto “già soggetta a registrazione particolare dell'amministrazione”. Le credenziali di accesso devono tuttavia essere quelle di un soggetto identificato e non semplicemente autoregistrato.

Nella fase transitoria, in cui alcuni processi connessi al ciclo di vita dello studente in ateneo saranno ancora manuali, prevedendo quindi il trattamento di documenti cartacei, sarà cura del personale

amministrativo dell'unità organizzativa che ha in carico il procedimento inserire, quando necessario, anche questa tipologia di documenti nel fascicolo informatico dello studente avvalendosi dei servizi offerti dal proprio sistema documentale. Rientrano in questa specie, ad esempio, le delibere degli organi ed i decreti del rettore. È comunque auspicabile che si operi in tempi brevi, sia a livello organizzativo che a livello tecnico, per dematerializzare il processo di generazione delle delibere e decreti, rendendo automatico il loro inserimento nel fascicolo informatico dello studente, almeno nei casi in cui gli atti hanno valenza individuale, e consentendo così alle segreterie studenti di averne visibilità diretta ed immediata dai sistemi di gestione delle carriere studenti.

È altresì auspicabile che la consultazione da parte dello studente del contenuto del proprio fascicolo informatico possa essere attuata tramite un apposito servizio web.

Per quanto attiene infine la definizione del contenuto del fascicolo studente, oltre ai criteri sopra enunciati, devono essere tenute in considerazione anche le regole di conservazione (di scarto) documentale. Essendo tuttavia la materia già oggetto di studio e di definizione da parte di progetti nazionali ed internazionali (es. Cartesio), si ritiene conveniente non duplicare le attività concentrando invece l'attenzione sugli aspetti tecnologici dell'integrazione tra sistemi. Pertanto, al solo scopo di consentire l'avvio dell'operatività del fascicolo dello studente entro i termini stabiliti dal bando, in allegato viene fornito un elenco di tipologie di documenti informatici che si ritiene debbano essere inseriti nel fascicolo studente, classificati secondo la seguente scala di priorità: obbligatorio, consigliato, opzionale. Ciascun ateneo è comunque libero di stabilire priorità diverse.

### 3.5 Modello di riferimento

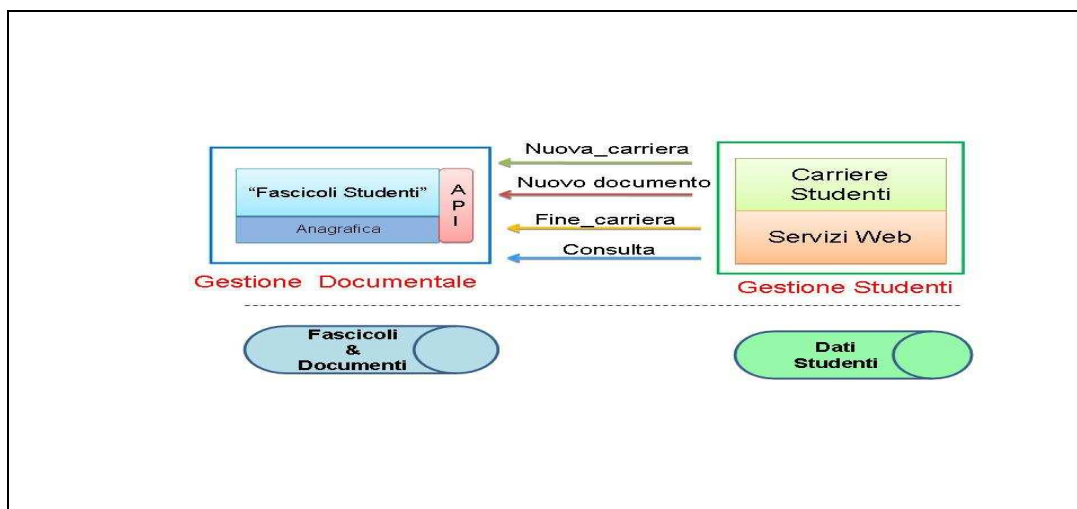
L'analisi delle piattaforme software in uso presso gli atenei e le modalità di utilizzo del sistema di gestione documentale e di protocollo da parte delle segreterie studenti, determina la necessità di individuare una soluzione tecnico-funzionale che soddisfi i seguenti requisiti:

- piena adattabilità alle diverse strutture organizzative degli atenei
- indipendenza dai sistemi coinvolti
- rispetto e adozione degli standard.

Ai fini della realizzazione della soluzione operativa si prevede pertanto che ogni sistema di gestione documentale sia in grado di esporre dei servizi tramite un'interfaccia in grado di gestire i principali eventi inerenti il ciclo di vita e di alimentazione del fascicolo studente.

Analogamente i sistemi di gestione delle carriere studenti, i servizi Web ed eventualmente altri sistemi, dovranno essere in grado di integrare le attuali funzionalità chiamando tali servizi.

L'interazione tra i sistemi, ad esempio tra segreterie studenti, servizi web e gestione documentale, è schematicamente rappresentata dal seguente modello ad eventi/processi:



<b>Evento</b>	<b>Processo nel sistema di gestione carriere studenti</b>	<b>Azioni nel sistema di gestione documentale (servizi invocati/usati)</b>
Nuova_carriera	Invocato all'atto della immatricolazione-iscrizione di un nuovo studente nell'ateneo	- crea o aggiorna anagrafica - crea fascicolo informatico
Nuovo_documento	Inserisce un nuovo documento nel fascicolo informatico di uno studente (protocollandolo o meno) es. domanda di laurea	- inserisci
Fine_carriera	a) per trasferimento: inserisce il foglio di congedo b) per conseguimento del titolo: inserisce il diploma supplement c) per rinuncia o decadenza : inserisce il relativo atto	- inserisci - chiudi fascicolo
Consulta	Permette alla segreteria studenti di elencare e visualizzare i documenti contenuti in un fascicolo informatico di carriera dello studente.	- lista

Resta inteso che l'apposizione del protocollo ai documenti ed il personale da abilitare ai sistemi/servizi dipende dai modelli organizzativi adottati nei singoli atenei.

### **Elenco tipologie di documenti da inserire nel fascicolo studente e di serie documentali ad esso correlate**

- Domanda di immatricolazione / abbreviazione di corso / trasferimento in ingresso - **OBBLIGATORIO**
- Passaggio di corso – **OPZIONALE**
- Conferma titolo di studio – **OBBLIGATORIO** (auspicata integrazione con banca dati titoli scuola media superiore)
- Delibera passaggio di corso – **OBBLIGATORIO**
- Attestazione ISEE/ISEU – **CONSIGLIATO**
- Domanda esonero/benefici – **CONSIGLIATO**
- Domanda piano di studio individuale – **OPZIONALE**
- Delibera approvazione piano di studio individuale – **OBBLIGATORIO**
- Verbali di esame – **OBBLIGATORIO** (non necessariamente nel fascicolo studente - conservazione sostitutiva in presenza di processo dematerializzato)
- Contratto di Learning Agreement – **CONSIGLIATO**
- Transcript of Records – **CONSIGLIATO**
- Istanze – **OPZIONALE**
- Decreti di annullamento esame, contratto collaborazione studentesca, riconoscimento esami, etc. - **OBBLIGATORIO**
- Domanda di laurea /trasferimento – **OPZIONALE**
- Diploma supplement / Foglio di congedo / Rinuncia / Decadenza – **OBBLIGATORIO**
- Tesi di laurea – **OBBLIGATORIO** (ma non necessariamente nel fascicolo studente)
- Domanda esame di stato – **CONSIGLIATO**
- Abilitazione – **OBBLIGATORIO**

## Capitolo 4. Realizzazione della cooperazione applicativa

### 4.1 Premessa

Il presente documento fornisce delle linee guida utili alla definizione di un sistema che consenta l'integrazione di servizi e l'allineamento di informazioni tra diversi Atenei Italiani.

Al fine di definire efficientemente le modalità di cooperazione tra una molteplicità di sistemi e di permettere un facile adattamento degli stessi rispetto all'evoluzione dei servizi, in questo documento verranno inizialmente definite delle linee guida generali su cui basare la cooperazione applicativa. Tali linee guida saranno poi declinate, nella seconda parte del documento, su uno specifico caso di studio, il caso d'uso "foglio di congedo".

### 4.2 Terminologia

Le parole chiave "DEVE", "CONSIGLIATO" in queste linee guida devono essere interpretate nel seguente modo:

- **DEVE:** significa che l'indicazione è un requisito assoluto della linea guida;
- **CONSIGLIATO:** significa che possono esistere delle valide ragioni in circostanze particolari per ignorare l'indicazione ma è richiesta una attenta valutazione prima di scegliere di seguire una strada alternativa.

### 4.3 Cooperazione Applicativa - linee guida

Si elencano di seguito le linee guida utili alla realizzazione della cooperazione applicativa.

1. *Definizione di un glossario di termini:* è necessario ("DEVE") innanzitutto condividere con gli Atenei coinvolti nella cooperazione applicativa, un glossario di termini relativo al dominio specifico su cui si sta lavorando, ciò al fine di non lasciare alcun margine di interpretazione a concetti basilari che dovranno essere poi gestiti dai singoli sistemi informativi.
2. *Condivisione del processo:* la cooperazione applicativa prevede la capacità di due o più sistemi di utilizzare, ciascuno nella propria logica applicativa, le informazioni scambiate. La condivisione del processo, in questo contesto, non implica obbligatoriamente che gli Atenei coinvolti nella cooperazione applicativa debbano gestire le informazioni scambiate secondo un medesimo processo interno, bensì implica che gli Atenei prendano accordi ("DEVE") sul formato di interscambio dati, sulle modalità di interazione e sul protocollo di comunicazione: si parla dunque di condivisione del processo *esterno*.
3. *Definizione e condivisione del formato di interscambio dati:* è necessario ("DEVE") che gli Atenei coinvolti nella cooperazione applicativa si accordino sul formato di interscambio dati intendendo con ciò:
  - a. Informazioni da scambiare ("DEVE") (preferibilmente suddivise in sezioni ("CONSIGLIATO") che raggruppano informazioni omogenee legate al contesto applicativo di riferimento);
  - b. Tabelle di transcodifica ("CONSIGLIATO") utili a consentire agli Atenei di decodificare le informazioni codificate (si preferisce ("CONSIGLIATO"), laddove possibile, utilizzare delle informazioni codificate accompagnate da un campo descrittivo testuale);

- c. Opzionalità di ciascuna informazione (“DEVE”): per ciascun dato che gli Atenei devono scambiarsi è importante stabilire se esso è opzionale o obbligatorio (“DEVE”) per consentire una maggiore conformità ai differenti scenari applicativi dei singoli atenei.
4. *Definizione e condivisione delle modalità di interazione*: è necessario (“DEVE”) che gli Atenei stabiliscano in che termini dovrà avvenire la comunicazione (se sincrona, asincrona o mista) e quali informazioni possono/devono essere scambiate ad ogni interazione (“DEVE”). Inoltre, gli Atenei, nel realizzare la cooperazione applicativa, devono poter definire quali sezioni di informazione devono essere scambiate sequenzialmente (perché esistono dei vincoli di precedenza) e quali, invece, possono essere scambiate parallelamente (“DEVE”).
5. *Definizione e condivisione del protocollo di comunicazione*: Gli Atenei devono accordarsi (“DEVE”) sul protocollo di comunicazione da utilizzare. E’ preferibile che si preveda:
  - a. Una *fase di negoziazione* (“CONSIGLIATO”) in cui le parti comunicano l’intenzione di volersi scambiare delle informazioni relativamente ad un contesto ben preciso;
  - b. Una *fase di sincronizzazione* (“CONSIGLIATO”) in cui gli Atenei si scambiano un identificativo del processo esterno che si sta condividendo da utilizzare per tutte le comunicazioni che seguiranno;
  - c. Una *fase di interscambio dati* (“DEVE”) in cui vi è lo scambio effettivo dei dati tra gli Atenei: in funzione delle modalità di interazione concordate (singola, asincrona, mista, sequenziale, parallela) si avrà lo scambio di dati vero e proprio;
  - d. Una *fase di chiusura* (“CONSIGLIATO”) in cui, concluso lo scambio di messaggi, il processo termina con la distruzione dell’identificativo. Naturalmente, nel caso in cui la cooperazione applicativa ha come obiettivo quello di lavorare una certa pratica, è fondamentale che l’attore di pertinenza indichi l’esito della pratica.

Si consiglia vivamente (“CONSIGLIATO”) a tutti gli Atenei di tenere traccia dello storico delle informazioni scambiate tra gli attori della cooperazione applicativa al fine di consentire una corretta e sicura gestione di eventuali messaggi di ri-invio e messaggi di errata corrige.

Si consiglia (“CONSIGLIATO”), ove possibile, ai singoli Atenei di predisporre dei servizi utili a rendere quanto più possibile trasparenti i processi interni a tutti gli attori coinvolti che non dovessero avere visibilità su tali processi (es. studenti, altri Atenei, etc).

#### **4.4 Cooperazione applicativa: caso d’uso foglio di congedo**

In riferimento alle linee guida delineate nel paragrafo precedente, si riporta di seguito l’applicazione delle stesse ad un caso d’uso specifico: il foglio di congedo.

Il foglio di congedo è un tipico esempio di cooperazione applicativa in quanto vede coinvolti due Atenei (di seguito Ateneo di destinazione ed Ateneo di provenienza) nello scambio di informazioni relative ad un preciso studente che inoltra una domanda di trasferimento per lasciare l’Ateneo di provenienza e giungere presso l’Ateneo di destinazione. Il processo di trasferimento è molto articolato e ciascun Ateneo è libero di gestire il processo in completa autonomia; tuttavia, è presente nel processo una forte interazione tra i due Atenei pertanto è possibile definire un processo *esterno* che gli Atenei possono condividere indipendentemente dalle modalità operative di gestione proprie di ciascun ateneo.

#### 4.4.1 Definizione di un glossario di termini

I termini ritenuti particolarmente significativi nell'ambito del processo foglio di congedo sono i seguenti:

- **Ateneo di provenienza:** Ateneo presso cui lo studente è iscritto e dal quale si avvia il processo di trasferimento;
- **Ateneo di destinazione:** Ateneo presso cui lo studente richiede l'iscrizione al fine di proseguire, in seguito ad eventuale convalida di crediti, con la propria carriera;
- **Convalida di crediti:** Presso l'Ateneo di destinazione lo studente può vedersi convalidati dei crediti e/o delle attività formative già concluse presso l'Ateneo di provenienza o presso Enti o Istituti esterni. La convalida dei crediti viene realizzata dalla commissione didattica presso l'Ateneo di destinazione grazie alle informazioni indicate sul foglio di congedo (*e ad ulteriori informazioni non in possesso dell'Ateneo di provenienza, fornite dallo studente direttamente all'Ateneo di destinazione*).
- **Foglio di congedo:** documento (cartaceo o elettronico) articolato in più sezioni contenente tutte le informazioni relative allo studente: dati anagrafici, dati di carriera, attività extracurricolari, etc.
- **Carriera:** Comprende tutto ciò che lo studente ha fatto a partire dalla prima immatricolazione e fino al momento in cui lo studente chiede di trasferirsi presso altro Ateneo. Nella carriera sono indicati sia gli esami sostenuti (o convalidati se lo studente ha fatto trasferimenti multipli *o ha ottenuto il riconoscimento di altre attività curricolari*) che eventuali altre attività extra curricolari che lo studente intende inserire nella sua carriera. La carriera dello studente è suddivisa in tratte.
- **Prima immatricolazione:** rappresenta il primo ingresso dello studente nel Sistema Universitario Italiano.
- **Tratta:** Indica gli esami sostenuti (o convalidati) dallo studente nell'ambito di uno stesso corso di studi. In ciascuna tratta lo studente ha un proprio numero di matricola. Lo stesso numero di matricola potrebbe riferirsi a differenti tratte (nel caso per esempio di un passaggio di corso interno allo stesso Ateneo).
- **Domanda di trasferimento:** domanda presentata dallo studente presso l'Ateneo di provenienza che avvia l'intero processo di trasferimento dello studente dall'Ateneo di provenienza all'Ateneo di destinazione.
- **Corso di Studi ad accesso programmato:** Corso di Studi per il quale è previsto un numero massimo di iscritti. L'accesso a tali corsi di studio prevede una prova di ammissione.
- **Corso di Studi ad accesso libero:** Corso di Studi per il quale non è previsto un numero massimo di iscritti.
- **Corso singolo:** ogni studente, nell'ambito del corso di studi, può iscriversi a corsi singoli che costituiscono attività extra-curricolari che dovranno essere eventualmente convalidati per essere riconosciuti come crediti che concorrono al conseguimento del titolo. All'atto dell'iscrizione a tali corsi singoli, lo studente ha un numero di matricola (lo studente può pertanto avere in uno stesso istante due numeri di matricola, uno relativo alla iscrizione al corso di studi ed uno relativo all'iscrizione al corso singolo): le iscrizioni ai corsi singoli sono indicate in una specifica tratta.
- **Agreement:** Accordo sul numero di sezioni del foglio di congedo che l'Ateneo di destinazione si aspetta di ricevere.

## 4.4.2 Condivisione del processo

Il processo “foglio di congedo” è articolato in diversi step ciascuno dei quali svolto in completa autonomia da parte di ciascun Ateneo. Risulta importante, ai fini della condivisione del processo tra gli Atenei che potranno poi utilizzare la cooperazione applicativa, individuare e descrivere brevemente gli step principali. E' evidente che tali step non vogliono rappresentare tutti i dettagli del processo, ma sono quelli che vedono coinvolti i due Atenei.

1. Identificazione Corso di Studi: Lo studente identifica il Corso di Studi presente nell'Ateneo di destinazione verso il quale è interessato a trasferirsi (l'offerta è fornita dall'Ateneo di destinazione per ciascun corso attivo includendo anche informazioni relativamente ai Corsi ad accesso programmato);
2. Negoziazione tra Atenei: L'Ateneo di destinazione e l'Ateneo di provenienza definiscono l'Agreement relativo al foglio di congedo indicando le relative tempistiche;
3. Presentazione della domanda di trasferimento: Lo studente presenta presso il proprio Ateneo (Ateneo di provenienza) la domanda di trasferimento indicando il Corso di Studi e l'Ateneo presso cui è intenzionato a trasferirsi;
4. Verifiche amministrative e di completezza delle informazioni: l'Ateneo di provenienza effettua una serie di verifiche interne di tipo amministrativo (regolarità tasse, regolarità posizione biblioteche, presenza di tutte le registrazioni di esami, delibere, etc);
5. Preparazione foglio di congedo: l'Ateneo di provenienza prepara tutte le informazioni utili alla compilazione del foglio di congedo e procede con l'invio (elettronico) dello stesso. Il foglio di congedo deve contenere le seguenti informazioni:
  - Anagrafica studente;
  - Informazioni sul trasferimento ossia informazioni relative all'Ateneo ed al Corso di Studi presso cui lo studente intende iscriversi;
  - Informazioni sui titoli di studio posseduti dallo studente;
  - Carriera studente;
6. Scambio del foglio di congedo e identificazione del processo: L'Ateneo di provenienza procede con l'invio del foglio di congedo e comunica all'Ateneo di destinazione il proprio identificativo univoco associato alla domanda di trasferimento (ID Pratica). L'ID Pratica dovrà essere comunicato allo studente per consentirgli di accedere ad eventuali servizi messi a disposizione dall'Ateneo di destinazione o dall'Ateneo di provenienza.
7. Acquisizione del foglio di congedo: l'Ateneo di destinazione acquisisce il foglio di congedo giunto dall'Ateneo di provenienza. A questo punto è possibile avviare, all'interno dell'Ateneo di destinazione, il processo di convalida crediti che si concluderà con una delibera a favore dello studente in cui sono indicate le tabelle di conversione tra esami/attività sostenute ed esami/attività convalidate;

8. **Verifica Stato Trasferimento:** Ogni Ateneo predispone un servizio attraverso il quale è possibile monitorare lo stato di avanzamento della pratica relativamente alle attività di propria competenza.
9. **Iscrizione dello studente:** lo studente (al quale è stato notificato il trasferimento dall'Ateneo di provenienza) procede con la regolarizzazione della propria posizione presso l'Ateneo di destinazione in base alle modalità da questo stabilite (può procedere con l'iscrizione prima o dopo la definizione della delibera di convalida degli esami/attività).
10. **Conclusione del Processo di Trasferimento:** l'Ateneo di destinazione comunica all'Ateneo di provenienza la conclusione del processo di trasferimento confermando la regolarizzazione della posizione dello studente presso l'Ateneo di destinazione.

### **Osservazione 1**

E' possibile che l'Ateneo di provenienza non disponga immediatamente di tutte le informazioni relative allo studente ed utili alla definizione del foglio di congedo: in tal caso può limitarsi ad inviare le informazioni relative all'anagrafica studente e le informazioni relative al trasferimento riservandosi di inviare informazioni sul titolo di studio e sulla carriera studente in un invio successivo.

### **Osservazione 2**

Nel caso di trasferimento da Corsi di Studio ad accesso libero verso Corsi di Studio ad accesso programmato per cui è necessario il superamento di un test di ammissione, il processo di trasferimento, qualora lo studente non sia in possesso dei requisiti di ammissibilità, può essere concluso dall'Ateneo di destinazione attraverso una comunicazione verso l'Ateneo di provenienza della non ammissibilità della richiesta di trasferimento.

### **Osservazione 3**

Nel caso di trasferimento da Corsi di Studio ad accesso programmato verso Corsi di Studio ad accesso programmato (ad es. da Medicina a Medicina) per cui è indispensabile la disponibilità del posto, il processo di trasferimento può essere concluso, qualora non ci sia disponibilità di posto, dall'Ateneo di destinazione attraverso una comunicazione verso l'Ateneo di provenienza della non ammissibilità della richiesta di trasferimento.

## **4.4.3 Definizione e condivisione del formato di interscambio dati**

Si riporta di seguito una sintesi delle informazioni che gli atenei dovranno scambiarsi.

Per il processo foglio di congedo le informazioni scambiate possono essere suddivise nelle seguenti sotto sezioni:

**SEZ 1. TRASFERIMENTO:** vengono riportati qui le informazioni relative al trasferimento intendendo con ciò gli estremi della domanda che lo studente ha presentato presso l'Ateneo di provenienza e le informazioni sull'Ateneo di destinazione e sul corso di studi specifico all'interno dell'Ateneo di destinazione.

**SEZ 2. DATI IDENTIFICATIVI STUDENTE:** si intendono i dati che consentono di identificare lo studente quali codice fiscale, nome, cognome, data e luogo di nascita etc. In questa sezione sono presenti anche informazioni di contatto quali residenza e domicilio ed informazioni relative ad altre forme di contatto possibili (e-mail, skype etc).

SEZ 3. TITOLI CONSEGUITI: in questa sezione sono riportati tutti i titoli di studio conseguiti dallo studente a partire dal diploma di scuola media superiore fino ad eventuali titoli di tipo universitario. Per i titoli universitari è importante riportare la descrizione della prova finale.

SEZ 4. CARRIERA UNIVERSITARIA: La Carriera Universitaria riporta innanzitutto informazioni sulla prima immatricolazione e successivamente, per ciascuna tratta, sono riportate le iscrizioni effettuate e gli esami sostenuti (o convalidati) nell'ambito della tratta. Per ciascun esame si indica se esso è stato sostenuto o convalidato e tutti i dettagli di interesse (votazione, CFU, SSD etc). Per ciascuna tratta si indicano i motivi per cui essa è stata chiusa (Chiusa per Conseguimento titolo, Chiusa per trasferimento, ecc.). Nella Carriera Universitaria si indicano anche le attività extra curriculari che lo studente ha svolto. Esse sono indicate come "altre attività".

Facendo riferimento alle tabelle di transcodifica da utilizzare si fa presente che:

- I comuni e gli stati esteri sono rappresentati dal relativo codice ISTAT che li identifica;
- Gli istituti superiori che rilasciano il diploma di maturità sono identificati da Codice\_scuole\_superiori ANS;
- Codice diploma identificato da codice\_titolo\_diploma ANS
- Codice Ateneo identificato da Codici\_Universita ANS;
- Codice Tipo Corso di Studi identificato da Codici\_Tipo\_Laurea ANS;
- Codice Classe del Corso di Studi identificato da Codici\_Classe ANS;
- Codice Corso di Studi identificato da Chiave\_corso fornito da ANS;
- Codice Attività Formativa identificate dalla codifica ANS per le attività formative;
- I programmi relativi ad ogni insegnamento sono strutturati secondo quanto indicato nel diploma supplement.

La maggior parte delle informazioni di dettaglio sono opzionali. Ulteriori informazioni sull'opzionalità delle informazioni possono essere trovate nell'allegato tecnico.

#### **4.4.4 Definizione e condivisione delle modalità di interazione**

Nello specifico caso d'uso selezionato la comunicazione sarà sincrona ed avverrà attraverso la predisposizione di appositi servizi su entrambi gli Atenei al fine di supportare il processo precedentemente descritto. Inoltre, le informazioni relativamente al foglio di congedo potranno essere inviate in modo parziale (Sezione 1 e 2) o completo (Sezioni 1,2,3 e 4). Gli Atenei che decidano di inviare in una prima fase informazioni relative alle sezioni 1 e 2, dovranno completare la trasmissione delle sezioni 3 e 4 entro i termini indicati dall'Ateneo di destinazione in fase di negoziazione.

#### **4.4.5 Definizione e condivisione del protocollo di comunicazione**

Nello specifico caso d'uso selezionato, saranno previsti dei servizi propedeutici rispetto alle fasi indicate nelle linee guida (Par 4.2), ed in particolare:

L'Ateneo di destinazione dovrà predisporre un servizio che consenta all'Ateneo di provenienza di poter reperire l'Offerta Formativa dell'Ateneo di destinazione.

### **Fase di Negoziazione:**

L'Ateneo di destinazione dovrà predisporre un servizio che consenta all'Ateneo di provenienza di ottenere l'Agreement relativo al foglio di congedo, ossia la possibilità di gestire, da parte dell'Ateneo di destinazione, un invio completo del foglio di congedo (Sezioni 1,2,3 e 4) o un invio parziale (Sezioni 1 e 2) indicando contestualmente le tempistiche per l'invio delle sezioni 3 e 4.

### **Fase di Sincronizzazione e di Interscambio Dati:**

L'Ateneo di destinazione dovrà predisporre un servizio che consenta l'attivazione del processo di trasferimento attraverso l'invio parziale o completo del foglio di congedo e dell'identificativo della pratica (ID Pratica), generato dall'Ateneo di provenienza, utile a monitorare lo stato della pratica.

L'Ateneo di destinazione dovrà predisporre un servizio che consenta all'Ateneo di provenienza di ritrasmettere o la prima parte (Sezione 1 e 2) o la seconda parte (Sezione 3 e 4) a partire dall'identificativo della pratica (ID Pratica).

Sia l'Ateneo di destinazione che l'Ateneo di provenienza dovrà predisporre un servizio che consenta attraverso l'ID Pratica di verificare lo stato di elaborazione della stessa relativamente ai processi interni di propria competenza.

L'Ateneo di provenienza dovrà predisporre un servizio che consenta all'Ateneo di destinazione di poter richiedere una ritrasmissione del foglio di congedo a partire dall'identificativo della pratica (ID Pratica).

### **Fase di Chiusura:**

L'Ateneo di provenienza dovrà predisporre un servizio che consenta all'Ateneo di destinazione di notificare la conclusione del processo di trasferimento dello studente a seguito della regolarizzazione dello stesso (Conclusione del processo di trasferimento con esito positivo) o per mancanza di requisiti di idoneità dello studente (Conclusione del processo di trasferimento con esito negativo).

## **Capitolo 5. Adozione di sistemi VoIP**

### **5.1 Individuazione di standard aperti per l'interoperabilità**

Al fine di garantire che le infrastrutture VoIP realizzate siano facilmente interfacciabili sia fra loro che con qualsiasi altro sistema telefonico è necessario che le stesse siano implementate sulla base di soluzioni tecnologiche aperte e standardizzate, ampiamente diffuse e disponibili sul mercato, garantendo l'investimento in termini di scalabilità e garanzie di mantenimento nel tempo della validità tecnologica dell'iniziativa. E' inoltre necessario che tali soluzioni siano perfettamente in linea con le tecnologie VoIP utilizzate sulla rete nazionale dai principali operatori di telecomunicazione.

### **5.2 Infrastruttura di trasporto e visibilità**

Per supportare adeguatamente i servizi avanzati di comunicazione e per ottimizzare gli investimenti effettuati, si suggerisce di utilizzare infrastrutture di rete pubbliche a resa prestazionale elevata e costi contenuti (es. la rete nazionale della ricerca GARR ed eventuali altre reti metropolitane/regionali a disposizione del mondo della ricerca e della PA) per veicolare il traffico audio/video tra le Università.

E' auspicabile che tutti gli atenei intenzionati a esporre (anche in maniera selettiva) le proprie utenze telefoniche, rendendo visibile a livello globale uno spazio di numerazione pubblico, raggiungibile via IP, si registrino presso il servizio NRENum.net (gestito in Italia dal consortium GARR) per identificare gli utenti VoIP e i servizi associati e permettere quindi di veicolare le relative chiamate sulle reti pubbliche (azzerando i costi delle chiamate inter-ateneo).

### **5.3 Mobilità e servizi a valore aggiunto innovativi**

Si suggerisce di adottare il VoIP anche e soprattutto per fornire agli utenti servizi innovativi quali mobilità, presenza, instant-messaging, messaggeria unificata, operatore automatico, rubrica on-line, conference call, per rispondere ai più moderni bisogni di comunicazione e interazione per l'intera comunità universitaria. E' auspicabile che tali servizi possano essere resi disponibili indipendentemente dalla localizzazione e in pieno regime di mobilità sia in ambito intra- che inter-ateneo, sfruttando tecnologie di trasmissione wireless/mobile e logiche di autenticazione federata (EduRoam, IDEM etc.).

### **5.4 Sistemi e tecnologie Open Source per il VoIP**

In aggiunta/complemento alle numerose soluzioni commerciali disponibili sul mercato, si evidenzia la disponibilità di tecnologie Open Source ormai più che mature, stabili e scalabili. La scelta Open Source può permettere di tagliare in modo significativo i costi, sia per la tipologia di apparati telefonici che possono essere adottati, sia per le soluzioni software che beneficiano dell'adozione di standard aperti e della riusabilità. Inoltre tali soluzioni consentono di adattare facilmente il sistema alle proprie esigenze seguendone l'evoluzione nel tempo, e di estenderne le funzionalità, anche beneficiando delle estensioni rilasciate da attive comunità di sviluppatori.

## **5.5 Ricadute sull'Organizzazione**

L'introduzione della tecnologia VoIP si deve accompagnare a una rivisitazione consapevole dei processi e dell'organizzazione. Il VoIP è un servizio della rete e come tale richiede competenze informatiche per un corretto ed efficace inserimento e utilizzo in una organizzazione. Come tutti i servizi informatici, anche il VoIP sottolinea l'importanza di garantire la continuità del servizio, un tema che porta l'attenzione delle organizzazioni verso la progettazione di infrastrutture stabili e affidabili, in termini di reti e sistemi di supporto.

Inoltre si deve segnalare che il servizio VoIP non è un servizio "universale" di comunicazione, poiché è significativamente dipendente dalla disponibilità di energia elettrica, basato su un trasporto non pienamente affidabile e la mobilità degli utenti intrinseca ai sistemi VoIP non ne garantisce la localizzazione.

Infine, un sistema VoIP permette di introdurre nuove possibilità ed elementi innovativi nonché risparmi sui costi dell'infrastruttura, e di facilitare la fruizione di servizi telefonici a condizioni particolarmente competitive, erogati, attraverso reti di trasporto basate su IP, da molteplici operatori.

## Capitolo 6. Autenticazione Federata per l'accesso a Internet e a risorse in rete

Queste linee guida indicano quali scenari e tecnologie si devono implementare nelle università per giungere all'obiettivo nel rispetto delle indicazioni normative vigenti; esse pertanto sono articolate in due parti, una che contiene la descrizione generale, l'ambito di applicazione e la normativa, ed un'altra che contiene la esemplificazione in casi specifici.

### 6.1 Descrizione generale del servizio e ambito di applicazione

L'utente, registrato presso un soggetto, detto "Organizzazione di appartenenza" (OdA), che gli ha fornito un'identità digitale e le relative credenziali (username e password, o certificato), utilizza le credenziali fornite dall'OdA per accedere ad Internet attraverso le risorse di rete di un secondo soggetto, detto "Fornitore di servizio" (FdS).

#### Condizioni d'uso:

1. **registrazione**: la procedura di registrazione adottata dall'OdA per assegnare e/o abilitare le credenziali all'utente deve garantire l'integrità, la disponibilità e la riservatezza delle credenziali e l'identificazione certa dell'utente nel rispetto della normativa vigente in materia di antiterrorismo e di protezione dei dati personali. Sono ammesse:
  - a. procedure di registrazione a seguito di identificazione diretta *de visu* attraverso l'acquisizione dei dati di un documento di identità personale,
  - b. procedure di registrazione a seguito di identificazione indiretta basata sull'acquisizione dei dati di una carta di credito o di una SIM card rilasciata in Italia,
  - c. procedure di registrazione a seguito di identificazione indiretta basata sull'acquisizione di token o la verifica di credenziali precedentemente rilasciati dalla OdA stessa con modalità di tipo a) o b).
2. **gestione dell'identità digitale**: l'OdA deve garantire il trattamento dei dati e delle credenziali dell'utente nel rispetto della normativa vigente in materia di protezione dei dati personali e, nel caso in cui l'identità digitale comprenda username e password, l'OdA deve mettere a disposizione dell'utente procedure sicure per modificare o reimpostare la propria password.
3. **autenticazione**: la procedura di autenticazione deve prevedere l'utilizzo di canali sicuri per la trasmissione delle credenziali, attraverso opportune tecnologie, e evitare di esporre le credenziali al FdS o a terzi.
4. **accesso**: la procedura di accesso deve prevedere lo scambio tra l'OdA e il FdS dei dati minimi indispensabili a permettere: l'identificazione dell'utente presso l'OdA, la verifica del possesso dei requisiti di accesso, l'erogazione del servizio nel rispetto della normativa vigente e delle usage policies della rete del FdS e della rete (ad esempio NREN) a cui questo è connesso;
5. **tracciamento**: l'OdA e il FdS devono collaborare ai fini del tracciamento e dell'identificazione dell'utente, nel rispetto della normativa vigente in materia di antiterrorismo e di protezione dei dati personali. A tal fine l'OdA e il FdS devono condividere riferimenti univoci associati alle tracce mantenute dal FdS e all'identità dell'utente mantenuta dall'OdA.

6. **fiducia:** l'OdA e il FdS devono darsi garanzie reciproche di rispetto delle condizioni espresse ai precedenti punti 1), 2), 3), 4) e 5). Tali garanzie possono essere formalizzate da un accordo bilaterale tra OdA e FdS, o dalla adesione dell'OdA e del FdS ad una federazione o confederazione che preveda il rispetto delle suddette condizioni.
7. **informazione:** l'utente deve essere informato in modo chiaro e compiuto:
  - delle finalità e delle modalità di trattamento dei propri dati personali eventualmente richiesti;
  - dei servizi, delle federazioni e delle confederazioni a cui le credenziali danno accesso;
  - dell'identità del soggetto che fornisce il servizio (FdS) e dell'identità del soggetto che opera la validazione delle credenziali all'atto dell'autenticazione (OdA);
  - dello scambio di informazioni tra OdA e FdS ai fini della fornitura del servizio, nei casi in cui ciò sia indispensabile ai fini dello stesso;
  - delle condizioni di utilizzo del servizio di accesso;
  - delle modalità di interruzione dell'accesso (logout).
8. **consenso:** prima di effettuare l'accesso l'utente deve acconsentire, caso per caso o una tantum allo scambio di informazioni tra OdA e FdS eventualmente necessarie ai fini della fornitura del servizio.
9. **controllo:** l'utente deve avere controllo della durata della connessione ad Internet e deve poterne verificare in ogni momento la sussistenza o la cessazione.

## 6.2 Modalità operative: i casi eduroam ed IDEM - autenticazione federata per il Wi-Fi in ambito universitario

Le linee guida generali di cui sopra si riferiscono all'autenticazione federata per accesso ad Internet in qualsiasi ambito e con qualsiasi tecnologia. Nel presente paragrafo si dà invece una particolareggiata esemplificativa, riferita all'autenticazione federata per il Wi-Fi in ambito universitario. In questo specifico ambito, le due modalità suggerite per implementare quanto espresso nel paragrafo "Descrizione generale del servizio e ambito di applicazione" sono le federazioni **IDEM** ed **eduroam**.

**Eduroam** (education roaming) è il servizio di accesso sicuro e globale (mondiale) alla rete Internet in modalità Wi-Fi per gli utenti mobili, a disposizione della comunità internazionale della ricerca e della formazione universitaria. eduroam permette agli studenti, ai ricercatori e al personale universitario di sfruttare la connettività Internet nei propri campus e presso ogni altra istituzione partecipante che si ha l'occasione di visitare senza ulteriori necessità di registrazione o configurazione (<http://www.eduroam.org>).

**IDEM** è la Federazione Italiana di Infrastrutture di Autenticazione e Autorizzazione dedicata alla comunità della ricerca e della formazione universitaria (<https://www.IDEM.garr.it>). La federazione IDEM permette l'accesso a molteplici risorse web, utilizzando profili SAML. L'utente beneficia anche del Single Sign On e mediante l'unica identità fornita dalla sua organizzazione di appartenenza accede a molteplici risorse (contenuti, dati, applicazioni) della propria organizzazione e delle altre organizzazioni della federazione.

Mediante le tecnologie messe in opera dalla federazione IDEM è possibile realizzare speciali Service Provider per autorizzare l'accesso alla rete in modalità Wi-Fi gli utenti della Federazione che si trovano presso la propria Organizzazione di appartenenza o presso altre Organizzazioni della

Federazione. Questa particolare configurazione permette una modalità di accesso alla rete Internet per gli utenti mobili analoga, ma non alternativa, a quella fornita da eduroam.

È auspicato che ogni Università aderisca ad entrambe le federazioni seguendo una roadmap personalizzata che conduce alla realizzazione di:

- un sistema di Identity Management (IM)
  - è a carico di questo componente dare garanzia del rispetto delle condizioni 1. e 2. prima definite
  - il sistema di IM non è un componente tecnologico né della Federazione IDEM, né della Federazione eduroam
  - ciascuna università stabilisce in autonomia come realizzarlo
  - il sistema di IM dovrebbe essere unico per l'università e ad esso dovrebbero attingere le informazioni sulle identità digitali sia l'Identity Provider di IDEM che l'Identity Provider di eduroam.
- un Identity Provider (IDP) in IDEM
  - le condizioni 3., 5. sono garantite dall'implementazione tecnologica del componente
- un Identity Provider (IDP) in eduroam
  - le condizioni 3., 5. sono garantite dall'implementazione tecnologica del componente
- un Servizio di accesso alla rete (Resource Provider, RP) in modalità wireless tramite la Federazione eduroam
  - le condizioni 4., 5., 9. sono garantite dall'implementazione tecnologica del componente
- un Servizio di accesso alla rete in modalità wireless tramite la Federazione IDEM
  - le condizioni 4., 5. sono garantite dall'implementazione tecnologica del componente
  - la condizione 9. è fattibile, ma richiede esplicita configurazione

L'adesione ufficiale di una università a ciascuna delle 2 federazioni attua la condizione 6.

Rimane a carico dell'Università stabilire come attuare le condizioni 7. e 8., con la precisazione che quest'ultima può essere acquisita in forma tradizionale, oppure in modalità informatica con l'implementazione tecnologica di un modulo aggiuntivo (uApprove).

# Appendici

## Appendice A. Allegato tecnico alle linee guida per la realizzazione della cooperazione applicativa

### A.1. Web services a supporto della cooperazione applicativa finalizzata al trasferimento degli studenti

#### A.1.1. Riepilogo dei servizi

	Denominazione	Descrizione sintetica
1	Get_Offerta()	Richiesta all'Ateneo di destinazione dei Corsi di Studio offerti
2	Get_InfoWorkflowTrasferimento()	Richiesta all'Ateneo di destinazione delle specifiche di ricezione Foglio di Congedo
3	Put_ProcessoTrasferimento()	Avvio del workflow di trasferimento presso l'Ateneo di destinazione
4	Require_RefreshDatiTrasferimento ()	Richiesta all'Ateneo di provenienza di re-invio/completamento del Foglio di Congedo
5	Put_DatiTrasferimento()	Re-invio all'Ateneo di destinazione del Foglio di Congedo
6	Change_StatusProcessoTrasferimento()	Notifica (all'Ateneo di provenienza o di destinazione) del cambio di stato di una domanda di trasferimento
7	Get_StatusProcessoTrasferimento()	Richiesta (all'Ateneo di provenienza o di destinazione) dello stato di avanzamento di una domanda di trasferimento

**A.1.2 Dettaglio dei servizi****A.1.2.1. Servizio Get\_Offerta()**

Denominazione	Get_Offerta
Descrizione	Il servizio viene invocato per chiedere all'Ateneo di destinazione l'offerta dei Corsi di Studio attivi in un determinato AA ed utilizzabili per un trasferimento in ingresso
Input	<ul style="list-style-type: none"> <li>- Anno Accademico di trasferimento</li> <li>- Tipo di Corso (Laurea, Laurea Magistrale, Laurea Quinquennale, ...)</li> </ul>
Output	<ul style="list-style-type: none"> <li>- Set di Facoltà e, per ciascuna di esse, set di Corsi di Studio offerti con indicazione di: <ul style="list-style-type: none"> <li>- Denominazione</li> <li>- Tipo di Corso</li> <li>- Sede di erogazione</li> <li>- Data ultima di presentazione della domanda di ammissione/trasferimento</li> <li>- Presenza di numero chiuso e/o di procedure di selezione</li> <li>- Link alla pagina web, dell'Ateneo di destinazione, riportante ulteriori dettagli sul Corso di studi</li> <li>- Note</li> </ul> </li> </ul>
Attivazione	Invocazione da parte dell'Ateneo di partenza
Esecutore	Ateneo di destinazione (o MIUR.OFF)
Note	<ul style="list-style-type: none"> <li>- Va definito il domino del parametro Tipo di Corso</li> <li>- Per i Corsi di Studio va utilizzata la codifica OFF/ANS</li> <li>- Valutare l'ipotesi che il servizio sia esposto centralmente da MIUR.OFF</li> </ul>

**A.1.2.2. Servizio Get\_InfoWorkflowTrasferimento()**

Denominazione	Get_InfoWorkflowTrasferimento
Descrizione	Il servizio viene invocato per conoscere dall'Ateneo di destinazione le modalità di avvio del processo di trasferimento, ovvero le modalità di trasmissione del Foglio di Congedo
Input	Nessuno
Output	<ul style="list-style-type: none"> <li>- Modalità di trasmissione del Foglio di Congedo: <ul style="list-style-type: none"> <li>- Completa = sezione amministrativa + sezione descrittiva della carriera</li> <li>- Parziale = ammessa la trasmissione della sola sezione amministrativa</li> </ul> </li> <li>- Altre info workflow: l'Ateneo di destinazione può fornire ulteriori informazioni relative al proprio processo di gestione della domanda di trasferimento</li> </ul>
Attivazione	Invocazione da parte dell'Ateneo di provenienza
Esecutore	Ateneo di destinazione
Note	Dettagliare l'articolazione delle informazioni aggiuntive sul workflow

**A.1.2.3 Servizio Put\_ProcessoTrasferimento()**

Denominazione	Put_ProcessoTrasferimento
Descrizione	Il servizio viene invocato dall'Ateneo di provenienza per avviare il processo di trasferimento all'Ateneo di destinazione.
Input	<ul style="list-style-type: none"> <li>- Foglio di Congedo: <ul style="list-style-type: none"> <li>- Sezione amministrativa (sempre obbligatoria)</li> <li>- Sezione descrittiva della carriera (opzionale al primo invio, se così previsto dalle modalità di trasmissione dell'Ateneo di destinazione)</li> </ul> </li> <li>- IdPratica: Identificativo univoco della pratica di trasferimento assegnato dall'Ateneo di provenienza ed utilizzato nel seguito dai due Atenei coinvolti per individuare il processo avviato e condiviso</li> </ul>
Output	<ul style="list-style-type: none"> <li>- Esito della richiesta di avvio del trasferimento: <ul style="list-style-type: none"> <li>- OK</li> <li>- NOT_OK per:</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>- mancanza nel Foglio di Congedo di almeno una sezione o sottosezione obbligatoria</li> <li>- prerequisiti di ammissione non soddisfatti, ad esempio perché lo studente ha richiesto/avviato il trasferimento ad un Corso a numero programmato per il quale l’Ateneo di destinazione richiede il preventivo superamento di un test di ingresso</li> <li>- Token: Password provvisoria che insieme al CF (codice fiscale) andrà a costituire la coppia di credenziali d’accesso utilizzate dallo studente in trasferimento per farsi riconoscere dal sistema informativo dell’Ateneo di destinazione.</li> </ul>
Attivazione	Invocazione da parte dell’Ateneo di provenienza
Esecutore	Ateneo di destinazione
Note	<ul style="list-style-type: none"> <li>- Nel caso in cui Get_InfoWorkflowTrasferimento() dichiarasse ammissibile per l’Ateneo di destinazione un passaggio in due fasi dei dati a supporto del trasferimento, verrebbe accettata la mancanza della sezione descrittiva della carriera.</li> <li>- Ciascuna sezione inviata (dati amministrativi o dati di carriera) deve comunque includere tutte le sottosezioni indicate come obbligatorie nelle specifiche. La mancanza di una sezione/sottosezione marcata come obbligatoria determinerebbe il rifiuto della richiesta e genererebbe una corrispondente risposta con esito NOT_OK.</li> <li>- Nel caso di Corso di studio a numero programmato, il non aver superato il test di ammissione potrebbe generare un esito NOT_OK nel caso in cui l’Ateneo di destinazione considerasse tale superamento un prerequisito per l’avvio del trasferimento</li> <li>- E’ da valutare se le richieste con esito NOT_OK debbano comunque essere protocollate dall’Ateneo di arrivo (l’avvenuta presentazione potrebbe essere comunque rilevante a ridosso delle scadenze).</li> </ul>

#### A.1.2.4 Servizio Require\_RefreshDatiTrasferimento()

Denominazione	Require_RefreshDatiTrasferimento
Descrizione	<p>Il servizio viene invocato dall'Ateneo di destinazione per chiedere all'Ateneo di provenienza la ritrasmissione di un Foglio di Congedo:</p> <ul style="list-style-type: none"> <li>- per ottenere il completamento dello stesso con la Sezione descrittiva della carriera (non trasmessa all'avvio della pratica di trasferimento)</li> <li>- per ottenere la valorizzazione di informazioni opzionali</li> <li>- a fronte di condizioni di errore rilevate a livello applicativo nell'elaborazione del Foglio di Congedo ricevuto con la Put_ProcessoTrasferimento()</li> </ul>
Input	<ul style="list-style-type: none"> <li>- IdPratica: identificativo della pratica di trasferimento</li> <li>- Causale (CompletamentoCarriera, CompletamentoInfoOpzionali, Errore, .... )</li> <li>- Note</li> </ul>
Output	Nessuno
Attivazione	Richiesta, da parte dell'Ateneo di destinazione, di ritrasmissione di un Foglio di Congedo da parte dell'Ateneo di provenienza
Esecutore	Ateneo di provenienza
Note	<ul style="list-style-type: none"> <li>- Valutare la strutturazione delle causali di richiesta di ritrasmissione</li> <li>- Definire le condizioni di errore che potrebbero determinare la necessità di ritrasmissione del Foglio di Congedo.</li> </ul>

#### A.1.2.5 Servizio Put\_DatiTrasferimento()

Denominazione	Put_DatiTrasferimento
Descrizione	<p>Il servizio viene invocato dall'Ateneo di provenienza per:</p> <ul style="list-style-type: none"> <li>- ritrasmettere un Foglio di Congedo in risposta ad una richiesta notificata dall'Ateneo di destinazione mediante Require_RefreshDatiTrasferimento()</li> <li>- completare la trasmissione di un Foglio di Congedo del quale era stata trasmessa la sola sezione amministrativa</li> </ul>
Input	<ul style="list-style-type: none"> <li>- Foglio di Congedo</li> <li>- IdPratica: identificativo della pratica di trasferimento</li> <li>- Causale (Completamento, RitrasmissioneSuRichiesta, .... )</li> <li>- Note</li> </ul>

Output	<ul style="list-style-type: none"> <li>- Esito della riacquisizione del Foglio di Congedo:                             <ul style="list-style-type: none"> <li>- OK</li> <li>- NOT_OK per mancanza nel Foglio di Congedo di almeno una sezione o sottosezione obbligatoria</li> </ul> </li> </ul>
Attivazione	Invocazione da parte dell'Ateneo di partenza
Esecutore	Ateneo di destinazione
Note	A differenza di Put_ProcessoTrasferimento(), questo servizio non genera un nuovo workflow, ma si limita ad integrare di dati descrittivi un processo di trasferimento già avviato

#### A.1.2.6 Servizio Change\_StatusProcessoTrasferimento()

Denominazione	Change_StatusProcessoTrasferimento
Descrizione	<p>Il servizio viene invocato da uno dei due Atenei coinvolti nel trasferimento per propagare una transizione di stato del processo.</p> <p>Ad esempio per:</p> <ul style="list-style-type: none"> <li>- la notifica all'Ateneo di provenienza (da parte dell'Ateneo di destinazione) dell'avvenuta conclusione del trasferimento in ingresso dello studente (per consentire all'Ateneo di provenienza la chiusura della corrispondente pratica)</li> <li>- la richiesta all'Ateneo di destinazione (da parte dell'Ateneo di provenienza) di annullare un processo di trasferimento in precedenza avviato con Put_ProcessoTrasferimento().</li> </ul>
Input	<ul style="list-style-type: none"> <li>- IdPratica: identificativo della pratica di trasferimento</li> <li>- Nuovo stato del processo di trasferimento</li> <li>- Note</li> </ul>
Output	Nessuno
Attivazione	Invocazione da parte di uno dei due Atenei coinvolti nel trasferimento
Esecutore	Ateneo al quale viene notificata la transizione di stato
Note	

**A.1.2.7 Servizio Get\_StatusProcessoTrasferimento()**

Denominazione	Get_StatusProcessoTrasferimento
Descrizione	Il servizio viene invocato per chiedere, rispetto ai workflow attivati negli Atenei di provenienza e destinazione, lo stato di una richiesta di trasferimento.
Input	IdPratica: identificativo della pratica di trasferimento
Output	<ul style="list-style-type: none"><li>- Set di passi seguiti dal workflow gestito internamente all'Ateneo con indicazione, per ciascuno di essi, di:<ul style="list-style-type: none"><li>- Stato</li><li>- Data della transizione di ingresso in tale stato</li><li>- Note</li></ul></li></ul>
Attivazione	Invocazione da parte di uno dei due Atenei coinvolti nel trasferimento
Esecutore	Ateneo al quale viene chiesto lo stato di avanzamento del processo di trasferimento
Note	Il servizio può essere utilizzato per dare visibilità allo studente dell'avanzamento del processo di trasferimento.

## **A.2. Esempificazione del processo di trasferimento basato sulla cooperazione applicativa**

### **A.2.1. Uscita: gestione della domanda di trasferimento da parte dell’Ateneo di provenienza**

#### **A.2.1.1. Presentazione della domanda di trasferimento in uscita**

Dal portale di Ateneo lo studente accede all’area dei servizi personalizzati (WebPoliSelf nel caso PoliMI) e, dopo essersi autenticato con le proprie credenziali, seleziona il servizio di presentazione della domanda di trasferimento.

Il servizio richiede allo studente di selezionare l’Ateneo di destinazione, scegliendolo da un catalogo predefinito.

Il sistema invoca poi il servizio<sup>1</sup> Get\_Offerta(), esposto dall’Ateneo scelto dallo studente, per ottenere l’elenco dei Corsi di Studio offerti ed utilizzabili ai fini del trasferimento nell’AA specificato.

I Corsi di Studio vengono presentati raggruppati per Facoltà tramite una struttura ad albero navigabile, ed a ciascuno di essi vengono associate le seguenti informazioni:

- denominazione, tipo, durata, sede di erogazione
- eventuale obbligo di test di ammissione
- data limite per la presentazione della richiesta di trasferimento
- link alla pagina dell’Ateneo erogante il Corso di Studio.

I Corsi di Studio a numero programmato, che richiedono il superamento di una prova di ammissione, sono opportunamente evidenziati nell’elenco presentato.

Nel caso in cui uno studente dovesse scegliere uno di tali Corsi un opportuno messaggio provvederebbe a ricordare il requisito di ingresso, tuttavia il sistema non effettuerebbe alcun controllo vincolante sulla compatibilità tra la data di presentazione della domanda e la data di scadenza dell’iscrizione alla prova.

Ciò perché lo studente potrebbe aver già superato il test di ammissione prima di presentare la domanda di trasferimento o addirittura essersi già immatricolato presso l’Ateneo di destinazione per evitare di perdere il posto ottenuto in graduatoria. Allo studente è dunque lasciata libertà di presentare la domanda di trasferimento senza vincoli temporali rispetto allo svolgimento del test di ammissione.

Acquisiti i dati di destinazione, il servizio mostra allo studente le informazioni relative alla sua carriera (ovvero una bozza del suo Foglio di Congedo): elenco degli esami superati/convalidati/con idoneità, eventuali esami sospesi con la relativa causale di sospensione, elenco degli insegnamenti frequentati presenti nel piano degli studi, ecc.

Lo studente controlla la completezza e la validità delle informazioni riportate e può, qualora lo ritenesse necessario, compilare un campo note per segnalare eventuali anomalie.

Lo studente potrebbe inoltre confermare la domanda o riservarsi di completarla in un secondo momento; in questo caso la domanda verrebbe salvata nello stato di “bozza” e il sistema non effettuerebbe ulteriori controlli.

---

<sup>1</sup> Un’alternativa rispetto alla lettura dell’offerta di Corsi mediante un servizio esposto dall’Ateneo di destinazione potrebbe l’uso di un servizio condiviso ed esposto da MIUR.OFF; in tal caso andrebbe però valutata l’adeguatezza (in termini di aggiornamento e di grado di dettaglio) delle informazioni disponibili su tale sistema.

In caso invece di conferma della domanda da parte dello studente, il sistema effettuerebbe la verifica di condizioni prestabilite (regolarità pagamenti, assenza di registrazioni sospese, ecc.) e segnalerebbe allo studente le eventuali irregolarità; in base alle decisioni assunte da ciascun Ateneo, alcune di queste potrebbero condizionare il salvataggio della domanda.

Allo studente viene mostrata anche l’informativa per l’autorizzazione al trattamento dei dati personali da parte dell’Ateneo di destinazione che lo studente stesso dovrà confermare.

La conferma della domanda determina, mediante cooperazione applicativa con il sistema di protocollo informatico (Titulus nel caso PoliMI), l’assegnazione del numero di protocollo e il salvataggio della domanda nello stato di “presentata”.

Contestualmente il sistema provvede alla generazione della ricevuta di presentazione (in formato PDF), che lo studente può salvare/stampare, sulla quale sono riportate le informazioni relative ad Ateneo e Corso di Studi di destinazione, numero e data di protocollo della domanda ed elenco delle eventuali irregolarità rilevate (esami sospesi, tasse non pagate, etc.).

Il sistema presenta inoltre allo studente il link al quale accedere per scaricare il bonifico di pagamento del contributo di trasferimento e di eventuali pendenze sulle tasse/contributi dell’ultima iscrizione, generato contestualmente al salvataggio della domanda.

Lo studente potrà successivamente accedere al servizio di presentazione della domanda di trasferimento per consultarne lo stato e visualizzare l’elenco delle eventuali irregolarità rilevate non ancora risolte.

Lo stato della domanda visualizzato dallo studente corrisponde a quanto già esposto: “domanda in bozza” se la domanda non è ancora stata completata, “domanda presentata” dopo la conferma.

#### **A.2.1.2. Validazione della domanda di trasferimento in uscita**

La Segreteria studenti visiona l’elenco delle domande di trasferimento da processare, tramite apposita applicazione, e ne attiva l’elaborazione.

L’elaborazione aggiorna i check relativi alle condizioni da verificare e lo stato della domanda da “presentata” a “elaborata”.

La presenza di note dello studente è rappresentata come check non superato e richiede l’aggiornamento manuale da parte della Segreteria, dopo la verifica (ed eventuale rimozione) dell’anomalia segnalata.

La Segreteria effettua le verifiche e gli aggiornamenti necessari, a completamento dei quali autorizza la trasmissione della domanda di trasferimento.

Il sistema invoca il servizio `Get_InfoWorkflowTrasferimento()` reso disponibile dall’Ateneo di destinazione per conoscere le condizioni da rispettare per l’invio del Foglio di Congedo:

- **Completo:** deve essere inviato il Foglio di Congedo completo sia della sezione amministrativa, sia della sezione della carriera;
- **Parziale:** può essere inviata inizialmente la sola sezione amministrativa e, in un secondo tempo, quella della carriera.

A condizione che siano garantite le indicazioni di obbligatorietà specificate dall’Ateneo di destinazione, il sistema dell’Ateneo di provenienza genera il file per l’invio, invoca il servizio per l’assegnazione del numero di protocollo, aggiunge al file i dati della protocollazione e ne effettua l’invio mediante il servizio `Put_ProcessoTrasferimento()` reso disponibile dall’Ateneo di destinazione.

Una volta inviato il Foglio di Congedo all’Ateneo di destinazione la domanda viene salvata nello stato di “validata”.

Sia lo stato “elaborata” che lo stato “validata” corrispondono allo stato “domanda in fase di verifica” visualizzato dallo studente dal servizio di consultazione.

L’Ateneo di destinazione effettua gli opportuni controlli e comunica, come output dell’invocazione del servizio, l’esito della ricezione della domanda - identificata dall’`IdPratica` assegnato dall’Ateneo

di provenienza - unitamente al token che dovrà essere notificato allo studente dall'Ateneo di provenienza per consentirgli il primo accesso al sistema dell'Ateneo di destinazione.

L'esito OK dell'Ateneo di destinazione relativo alla ricezione della domanda induce il cambio di stato della domanda da "validata" a "trasferita".

Dal servizio di consultazione lo studente visualizzerà lo stato di "domanda trasmessa" e il token per accedere al sistema dell'Ateneo di destinazione.

Lo studente visualizzerà ulteriori dettagli sullo stato della domanda, descritti al relativo paragrafo.

Nel caso in cui sia stata effettuata in prima istanza la trasmissione della sola sezione amministrativa, l'Ateneo di provenienza invocherà in un secondo tempo il servizio per inviare il Foglio di Congedo completo della sezione della carriera (AteneoDestinazione.Put\_DatiTrasferimento), citando l'IdPratica, così da permettere il matching con i dati già acquisiti.

In caso di esito NOT\_OK bloccante, il sistema dell'Ateneo di destinazione invierà come risposta esito NOT\_OK con causale opportunamente segnalata (es. obbligatorietà sezioni e/o sottosezioni non rispettata, ...)

Da valutare se già a questo livello sia opportuno verificare la presenza/superamento del test per la richiesta di trasferimento per un Corso di Studio a numero programmato.

L'elaborazione del Foglio di Congedo da parte della Segreteria dell'Ateneo di destinazione può mettere in evidenza altre anomalie (esito NOT\_OK non bloccante) che determinano una richiesta di revisione e conseguente ri-invio.

Tale richiesta viene effettuata tramite invocazione del servizio RequireRefresh\_DatiTrasferimento() reso disponibile dall'Ateneo di provenienza; le anomalie vengono segnalate in un campo note ad inserimento libero, riferite allo specifico ID\_Pratica.

Da valutare l'opportunità di strutturare la comunicazione tramite censimento di un elenco di possibili causali da associare al NOT\_OK.

In questo caso, la domanda viene posta nello stato di "richiesta revisione", presso l'Ateneo di provenienza.

La Segreteria opera le opportune correzioni e/o integrazioni e procede ad un nuovo invio invocando il servizio Put\_DatiTrasferimento() reso disponibile dall'Ateneo di destinazione indicando, in aggiunta all'invio del Foglio di Congedo, la causale della ritrasmissione (revisione su richiesta, revisione per invio errato/incompleto, ...); lo stesso servizio viene invocato anche nel caso di completamento di trasmissione di un Foglio di Congedo per il quale è stata inviata la sola sezione amministrativa.

Ad ogni nuovo invio corrisponde un nuovo numero di protocollo.

### **A.2.1.3. Visualizzazione dello stato della domanda di trasferimento in uscita**

Dal momento della presentazione della domanda fino all'invio all'Ateneo di destinazione, lo studente consulterà lo stato della domanda utilizzando il servizio del proprio Ateneo di provenienza. Fino ad allora, lo stato della domanda presso l'Ateneo di destinazione verrà convenzionalmente mostrato come "Domanda non ancora pervenuta".

Dopo l'invio della domanda all'Ateneo di destinazione, il servizio dell'Ateneo di provenienza oltre a mostrare le proprie informazioni recupererà le informazioni dello stato di avanzamento della domanda di trasferimento invocando il servizio GetStatus\_ProcessoTrasferimento() reso disponibile dall'Ateneo di destinazione indicando l'ID\_Pratica.

Ad ogni richiesta di consultazione, l'Ateneo di provenienza riceve dall'Ateneo di destinazione lo stato di avanzamento del workflow di gestione della pratica rappresentato come un elenco di passi ai quali sono associati una descrizione, uno stato, eventuali note esplicative e l'indicazione di data e ora di quando è avvenuto il passaggio di stato.

Il sistema dell'Ateneo di provenienza mostra in aggiunta il proprio workflow di avanzamento interno, presentandolo affiancato a quello relativo all'Ateneo di destinazione.

Dopo l'assegnazione del token lo studente potrà accedere indifferentemente ai sistemi dell'Ateneo di provenienza o destinazione per consultare lo stato di avanzamento.

#### **A.2.1.4. Annullamento della domanda di trasferimento in uscita**

Lo studente può decidere di rinunciare alla domanda di trasferimento; la richiesta dovrà essere rivolta all'Ateneo di provenienza fino a quando la domanda non sia stata ancora inviata all'Ateneo di destinazione e a quest'ultimo dopo l'invio.

La domanda in stato di "Bozza" (non ancora confermata) può essere annullata direttamente dallo studente accedendo al servizio di gestione della domanda di trasferimento;

La domanda in stato di "Presentata" (confermata dallo studente ed in carico alla Segreteria) può essere annullata solo dalla Segreteria, alla quale si dovrà rivolgere lo studente.

La Segreteria associa lo stato di "Cancellata" alla domanda, tramite l'apposito applicativo di gestione.

La richiesta di annullamento di una domanda già inviata all'Ateneo di destinazione verrà comunicata all'Ateneo di provenienza, tramite il servizio `ChangeStatus_ProcessoTrasferimento()` da questo messo a disposizione, indicando l'`ID_Pratica`, lo stato "Cancellazione", una eventuale causale e la data ed ora della richiesta.

L'Ateneo di provenienza pone la domanda in stato di "Cancellata" e ripristina la posizione dello studente.

#### **A.2.1.5. Chiusura della domanda di trasferimento in uscita**

L'Ateneo di destinazione, al termine dell'iter di valutazione della carriera dello studente, notifica il completamento del trasferimento all'Ateneo di provenienza invocando il servizio `ChangeStatus_ProcessoTrasferimento()` reso disponibile dall'Ateneo di provenienza comunicando l'`ID_Pratica`, lo stato "completamento" o "non accoglimento della domanda" e data e ora del cambio di stato.

Nel caso di pratica chiusa con stato "completamento" l'Ateneo di provenienza pone la domanda nello stato di "chiusa", assegna il numero di archivio e disabilita per lo studente l'accesso ai servizi dell'Ateneo.

Nel caso di pratica chiusa con stato "non accoglimento della domanda", l'Ateneo di provenienza pone la domanda nello stato "respinta", e ripristina la posizione dello studente.

## **A.2.2. Ingresso: gestione della domanda di trasferimento da parte dell’Ateneo di destinazione**

### **A.2.2.1. Ricezione della domanda di trasferimento in ingresso**

Il sistema dell’Ateneo di provenienza contatta il sistema dell’Ateneo di destinazione e richiede la modalità di invio del Foglio di Congedo invocando l’apposito servizio `Get_InfoWorkflowTrasferimento()`.

Il sistema dell’Ateneo di provenienza trasmette quindi il foglio di congedo completo delle sezioni amministrativa e della carriera o della sola carriera invocando l’apposito servizio `Put_ProcessoTrasferimento()`.

In alcuni casi infatti l’Ateneo di destinazione, per snellire e velocizzare il processo di gestione delle domande di trasferimento, potrebbe accettare la sola sezione amministrativa permettendo così allo studente da subito di usufruire di alcuni servizi.

Il sistema dell’Ateneo di destinazione effettua la verifica di conformità dei dati rispetto al tracciato concordato, ai domini e all’obbligatorietà di compilazione di sezioni/singoli elementi.

Da valutare se portare a questo livello la verifica sulla presenza/superamento del test di ingresso per i Corsi di Studio per i quali è obbligatorio.

In questo caso il controllo sarebbe basato sul codice fiscale dello studente.

Nel caso in cui vi siano irregolarità tali da impedire la presa in carico della domanda di trasferimento l’Ateneo di destinazione risponde all’invocazione del servizio `Put_ProcessoTrasferimento()`, notificando l’esito `NOT_OK` con causale opportunamente descritta. Il processo ha fine e non si rende necessario generare e comunicare il token.

In caso di trasmissione effettuata con successo, l’Ateneo di destinazione, tramite risposta all’invocazione del servizio `Put_ProcessoTrasferimento()`, comunica all’Ateneo di provenienza l’esito fornendo in aggiunta il token che dovrà essere comunicato allo studente dall’Ateneo di provenienza per consentirgli il primo accesso al sistema dell’Ateneo di destinazione.

Il sistema procede quindi al salvataggio e alla protocollazione della domanda in ingresso tramite invocazione di opportuno servizio messo a disposizione da Titulus; la domanda viene posta nello stato iniziale di “ricevuta”.

### **A.2.2.2. Validazione della domanda di trasferimento in ingresso**

La Segreteria studenti dell’Ateneo di destinazione verifica, tramite apposita applicazione, la domanda di trasferimento.

Verifica che lo studente abbia i requisiti di ingresso richiesti per il Corso di Studi di destinazione (test di ammissione, sempre che il suo superamento non sia stato già verificato alla ricezione della domanda) e attiva l’elaborazione per aggiornare i check sulla presenza di tutte le sezioni del tracciato.

In caso di esito positivo di entrambe le condizioni, attiva la funzione che modifica lo stato della domanda in “autorizzata immatricolazione”.

Qualora vengano riscontrate delle anomalie, la segreteria dell’Ateneo di destinazione compila un apposito campo note ad inserimento libero e richiede la revisione del foglio di congedo: il sistema dell’Ateneo di destinazione segnala le anomalie, con riferimento allo specifico `IdPratica`, tramite invocazione del servizio `RequireRefresh_DatiTrasferimento()`.

Da valutare l’opportunità di strutturare la comunicazione tramite censimento di un elenco di possibili causali da associare al `NOT_OK`.

La domanda viene posta nello stato di “richiesta revisione”.

### **A.2.2.3. Presentazione della domanda di immatricolazione**

Lo studente accede al portale dell'Ateneo di destinazione utilizzando le credenziali di accesso - codice fiscale e token - valide ai soli fini del primo accesso al sistema dell'Ateneo.

Se la domanda è ancora nello stato di “ricevuta” viene mostrato allo studente un messaggio di cortesia con indicazioni generali.

Se la domanda è nello stato di “autorizzata immatricolazione”, il sistema mostra in successione allo studente le pagine dei servizi che gli consentono sia la registrazione nell'anagrafica di Ateneo che l'immatricolazione, con accesso diretto anche al servizio di pagamento con carta di credito della quota di immatricolazione.

Le pagine sono precompilate con i dati anagrafici e di carriera trasmessi dall'Ateneo di provenienza.

Il sistema procede quindi al salvataggio e alla protocollazione della domanda in ingresso tramite invocazione di opportuno servizio messo a disposizione da Titulus; la domanda viene posta nello stato di “immatricolato”.

Allo studente vengono assegnate le effettive credenziali di accesso - Codice Persona e password (la password dovrà essere modificata dallo studente al primo accesso ai servizi) - e il numero di matricola.

Viene generata la ricevuta di immatricolazione in formato PDF, che lo studente può salvare/stampare.

In caso di trasferimento per un Corso di Studio a numero programmato, è possibile che l'immatricolazione venga effettuata dallo studente prima dell'avvio della domanda di trasferimento, indotto da tempi di conferma del posto a volte molto ristretti.

In questo caso, alla ricezione del Foglio di Congedo sarà necessario procedere alla riconciliazione dei dati dichiarati dallo studente già immatricolato con quelli trasmessi dall'Ateneo di provenienza.

Per acquisire in anticipo l'informazione relativa alla provenienza di un nuovo immatricolato, è utile chiedere allo studente di dichiarare tale condizione.

### **A.2.2.4. Visualizzazione dello stato della domanda di trasferimento in ingresso**

Dal ricevimento del token dall'Ateneo di provenienza lo studente può accedere ai servizi dell'Ateneo di destinazione, tra i quali quello di visualizzazione dello stato della domanda di trasferimento.

Il servizio mostra l'avanzamento degli stati nel processo di gestione della pratica di ciascuno dei due Atenei, di provenienza e destinazione.

Le informazioni vengono scambiate tramite il servizio `GetStatus_ProcessoTrasferimento()`.

### **A.2.2.5. Valutazione della domanda di trasferimento in ingresso**

La Segreteria seleziona la domanda dall'elenco di quelle in stato “immatricolato” e ne autorizza la trasmissione alla Commissione.

Il sistema modifica lo stato della domanda in “autorizzata valutazione”.

La Commissione visiona l'elenco delle domande di trasferimento da valutare, tramite apposita applicazione. La selezione di ciascuna domanda determina l'accesso alle informazioni associate allo studente, in base alle quali la Commissione definirà la delibera contenente le condizioni di ammissione.

Eventuali anomalie rilevate dalla Commissione vengono segnalate alla Segreteria che provvede ad effettuare la richiesta di integrazione all'Ateneo di provenienza, tramite il servizio `RequireRefresh_DatiTrasferimento()` da questo messo a disposizione.

Il consolidamento della delibera da parte della Commissione determina il cambiamento di stato della domanda in “deliberata” e l’associazione ad un numero di protocollo assegnato tramite il servizio messo a disposizione da Titulus (o altro sistema di protocollo informatico).

#### **A.2.2.6. Annullamento della domanda di trasferimento in ingresso**

La richiesta di annullamento di una domanda inviata all’Ateneo di destinazione viene effettuata presso quest’ultimo.

L’annullamento di una domanda nello stato di “Autorizzata Immatricolazione” o successivi può essere richiesto dallo studente alla Segreteria dell’Ateneo di destinazione.

La Segreteria dell’Ateneo di destinazione, attraverso il proprio applicativo di gestione, associa alla domanda lo stato di “Cancellata”.

Tale condizione viene comunicata all’Ateneo di provenienza, tramite il servizio `ChangeStatus_ProcessoTrasferimento()` da questo reso disponibile, indicando l’ID\_Pratica, lo stato “Cancellazione”, una eventuale causale e la data ed ora della richiesta.

L’Ateneo di destinazione provvede quindi alla chiusura della posizione dello studente e alla disabilitazione del suo accesso ai servizi dell’Ateneo.

#### **A.2.2.7. Completamento della domanda di trasferimento in ingresso**

La Segreteria completa le informazioni amministrative associate alla domanda in stato “deliberata” e, al termine, attiva la funzione di conclusione dell’iter di trasferimento.

Tale funzione cambia lo stato della domanda da “deliberata” a “completata” e genera la notifica della conclusione dell’iter cui viene associato il numero di protocollo assegnato dal servizio messo a disposizione da Titulus (o altro sistema di protocollo informatico).

L’Ateneo di destinazione notifica il completamento del trasferimento all’Ateneo di provenienza invocandone il servizio `ChangeStatus_ProcessoTrasferimento()` comunicando l’identificativo della pratica, lo stato “completamento” o “non accoglimento della domanda” e data e ora del cambio di stato.

### A.2.3. Foglio excel

Nel foglio excel disponibile al link <http://www.ict4university.gov.it/temi-universita-digitale/architettura-applicativa.aspx> (FoglioCongedoStruttura.xls) è possibile visionare in forma testuale tutte le informazioni inserite nello schema xsd con i relativi commenti.

### A.2.4. Schema xsd

Si riportano di seguito alcuni screen shot dello schema xsd prodotto.

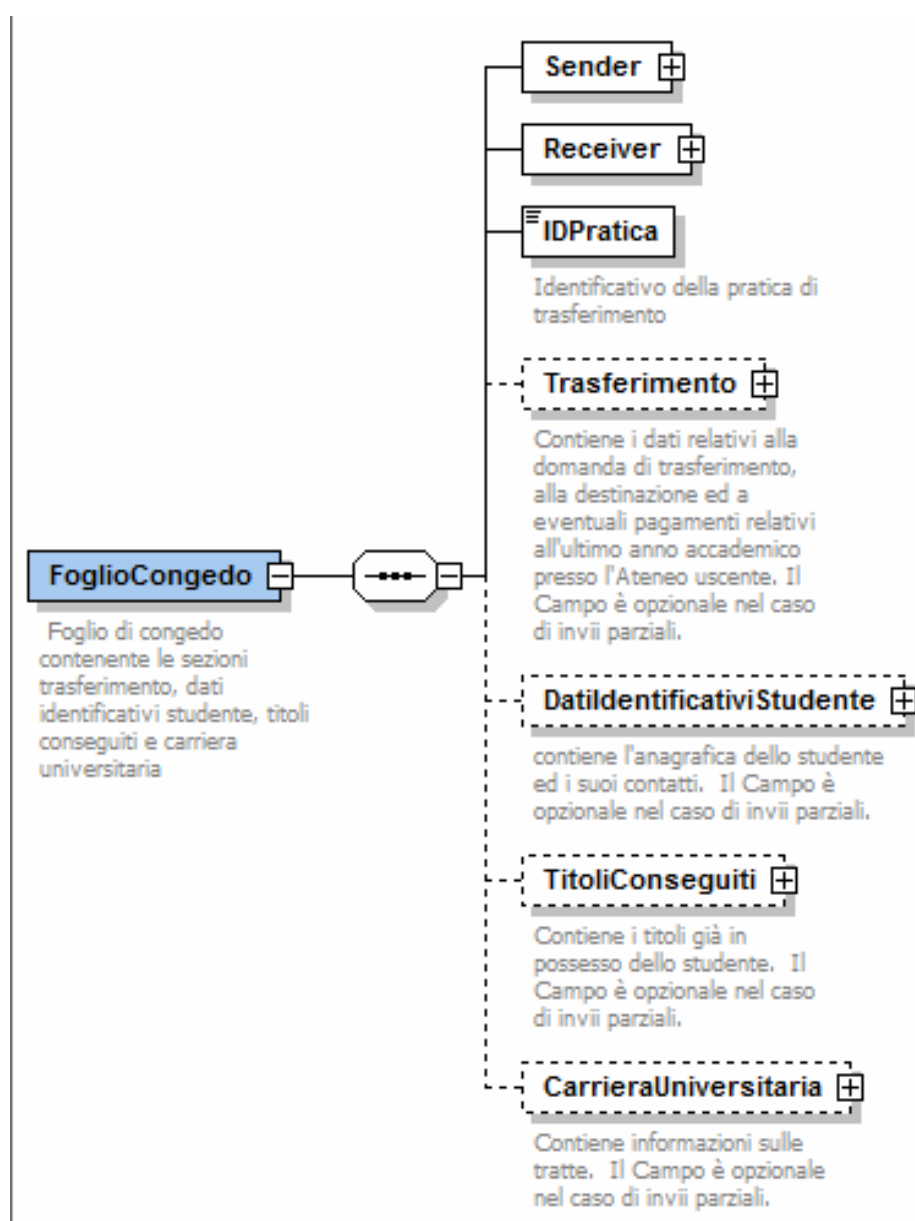


Figura 1 Schema xsd del nodo foglio di congedo

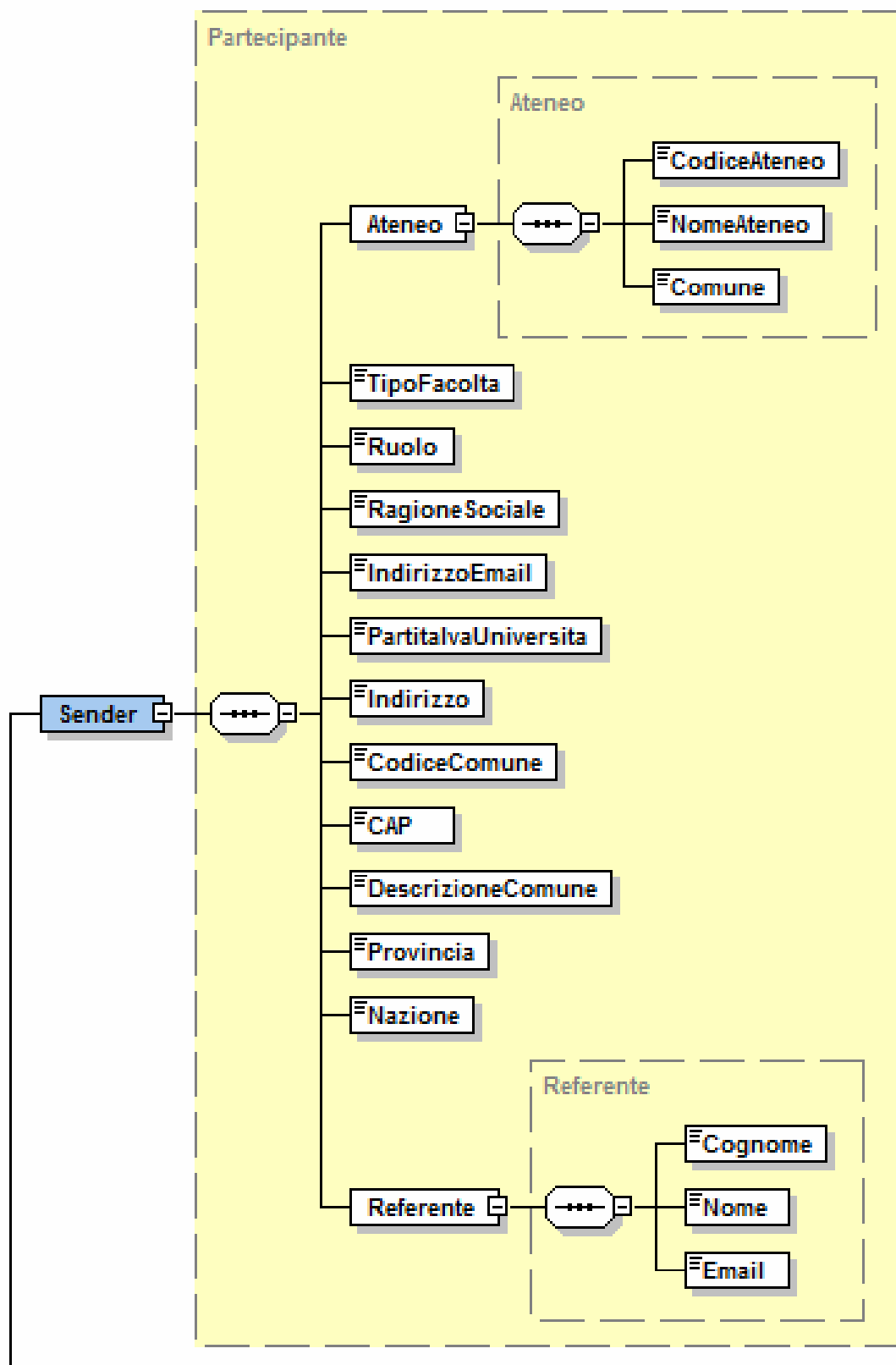


Figura 2 Schema xsd del nodo Sender. Si è utilizzato il tipo complesso “Partecipante”

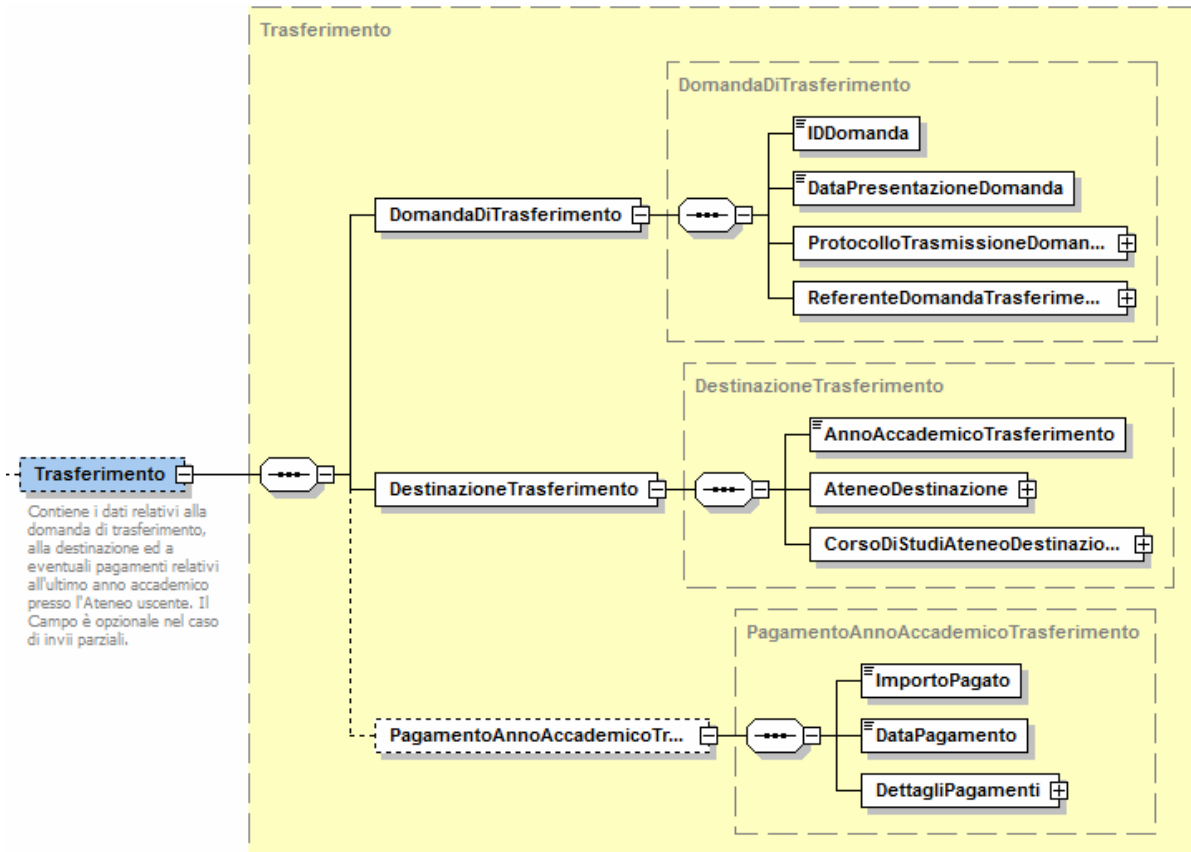


Figura 3 Schema xsd del nodo Trasferimento

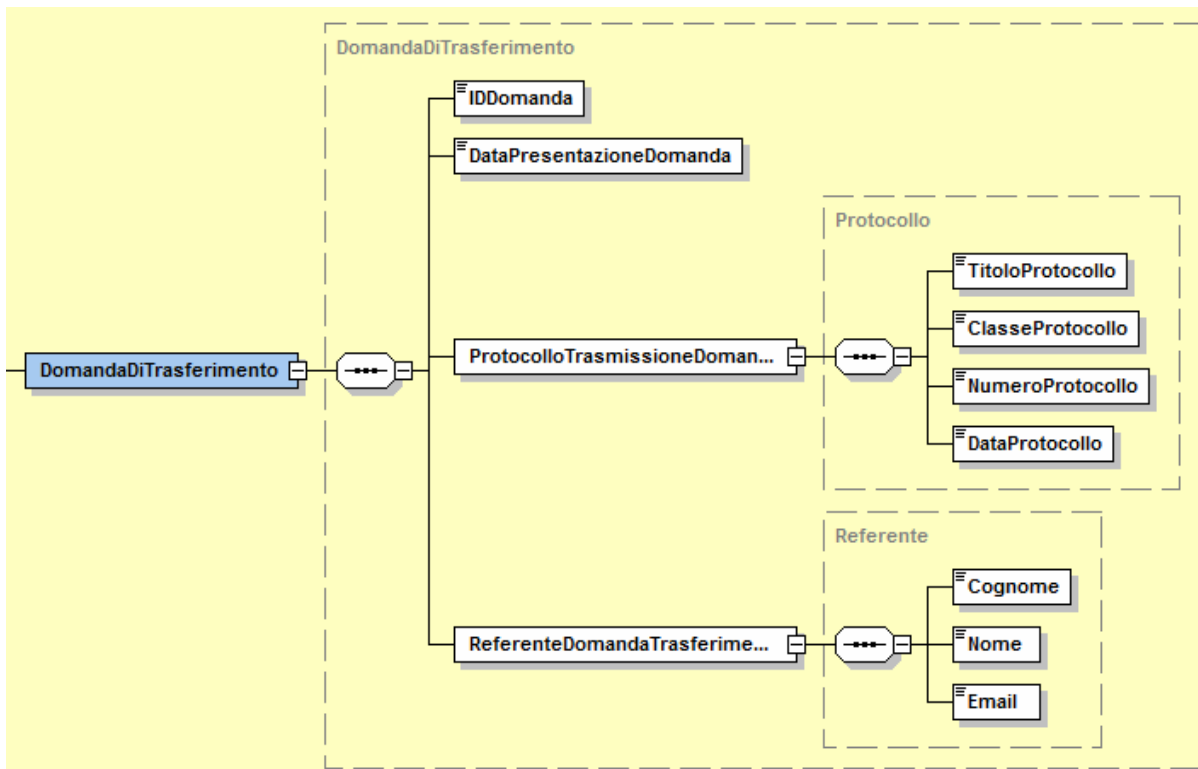


Figura 4 Schema xsd del nodo DomandaDiTrasferimento

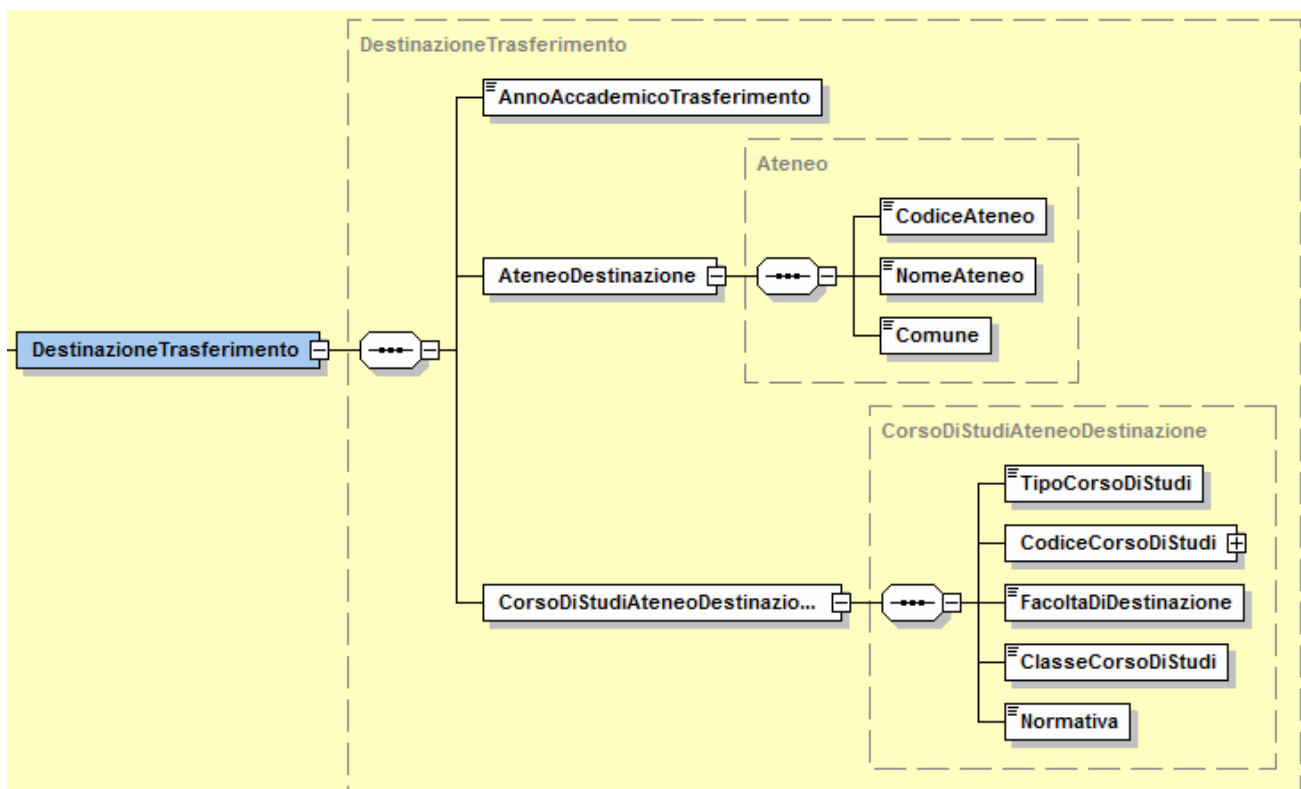


Figura 5 Schema xsd del nodo DestinazioneTrasferimento

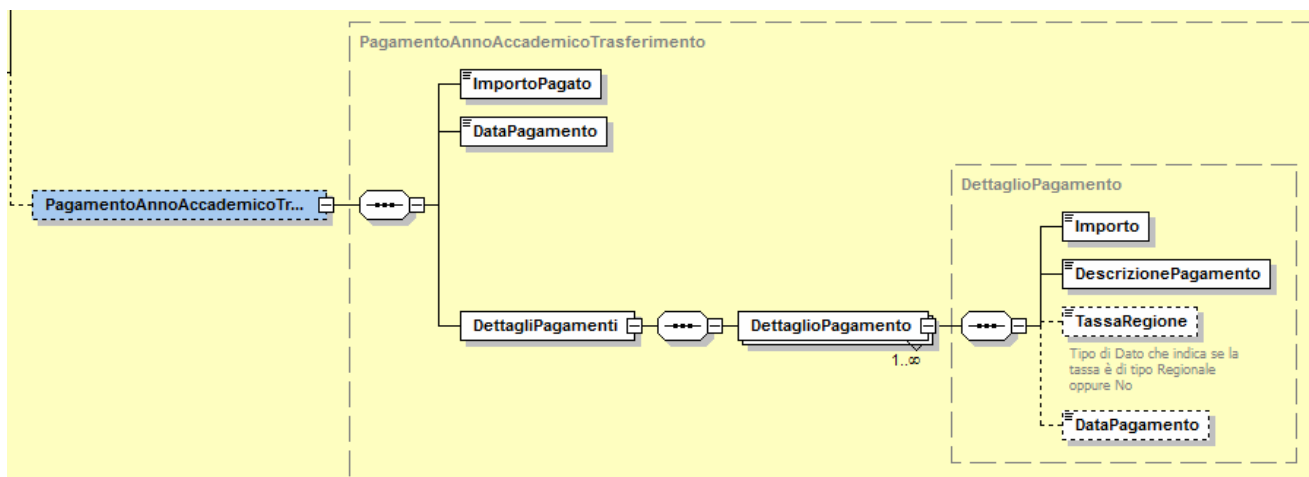


Figura 6 Schema xsd del nodo PagamentoAnnoAccademicoTrasferimento

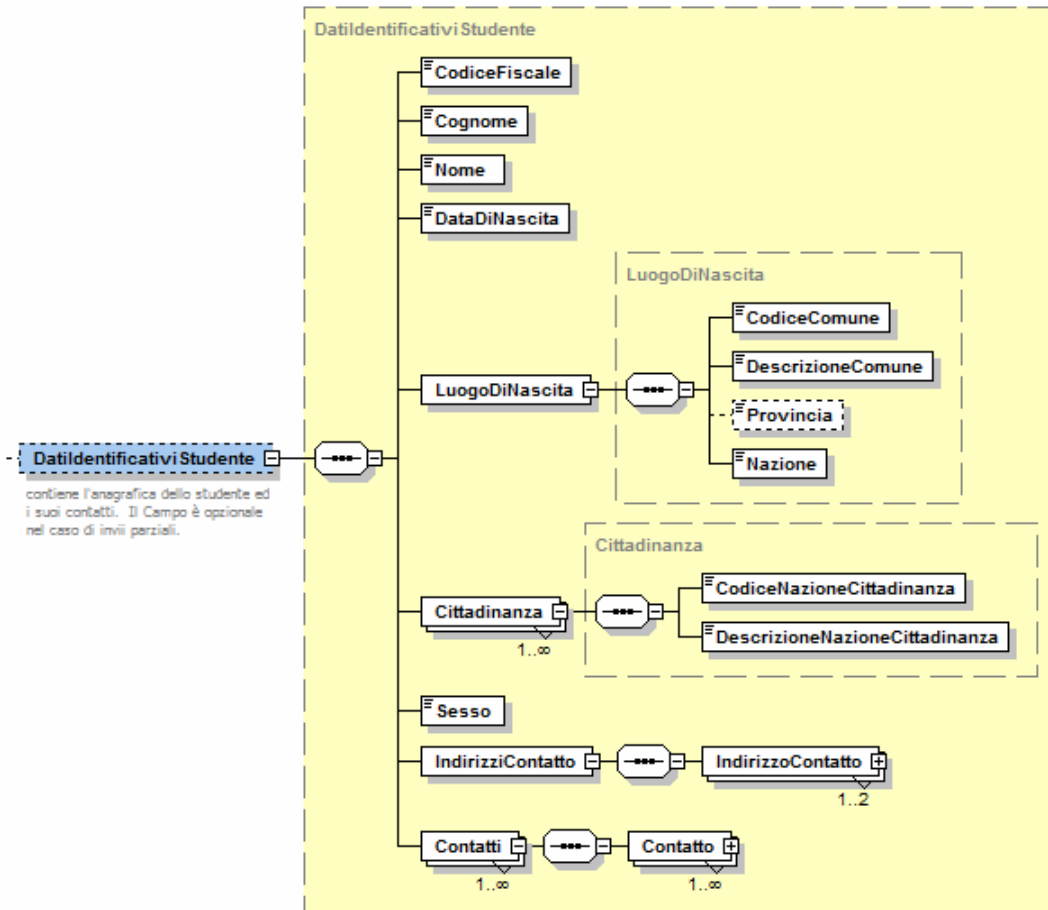


Figura 7 Schema xsd del nodo DatIdentificativiStudiante

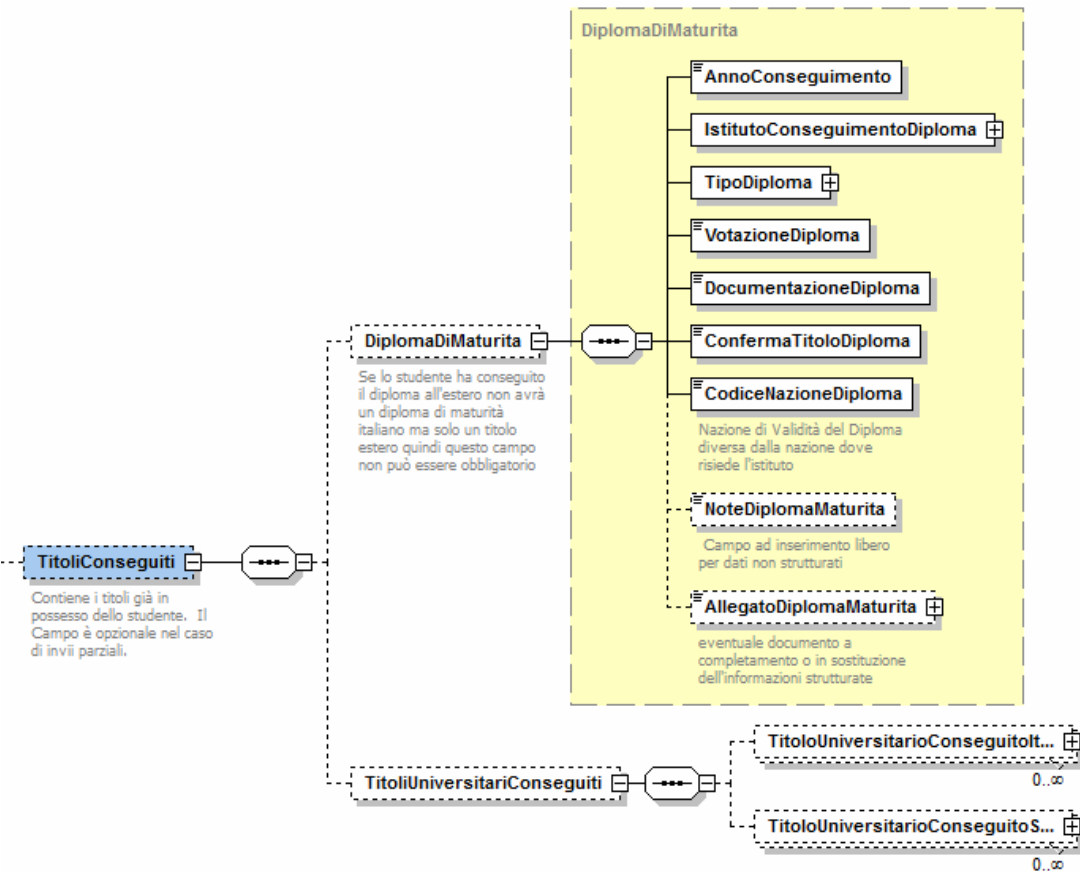


Figura 8 Schema xsd del nodo "TitoliConseguiti"

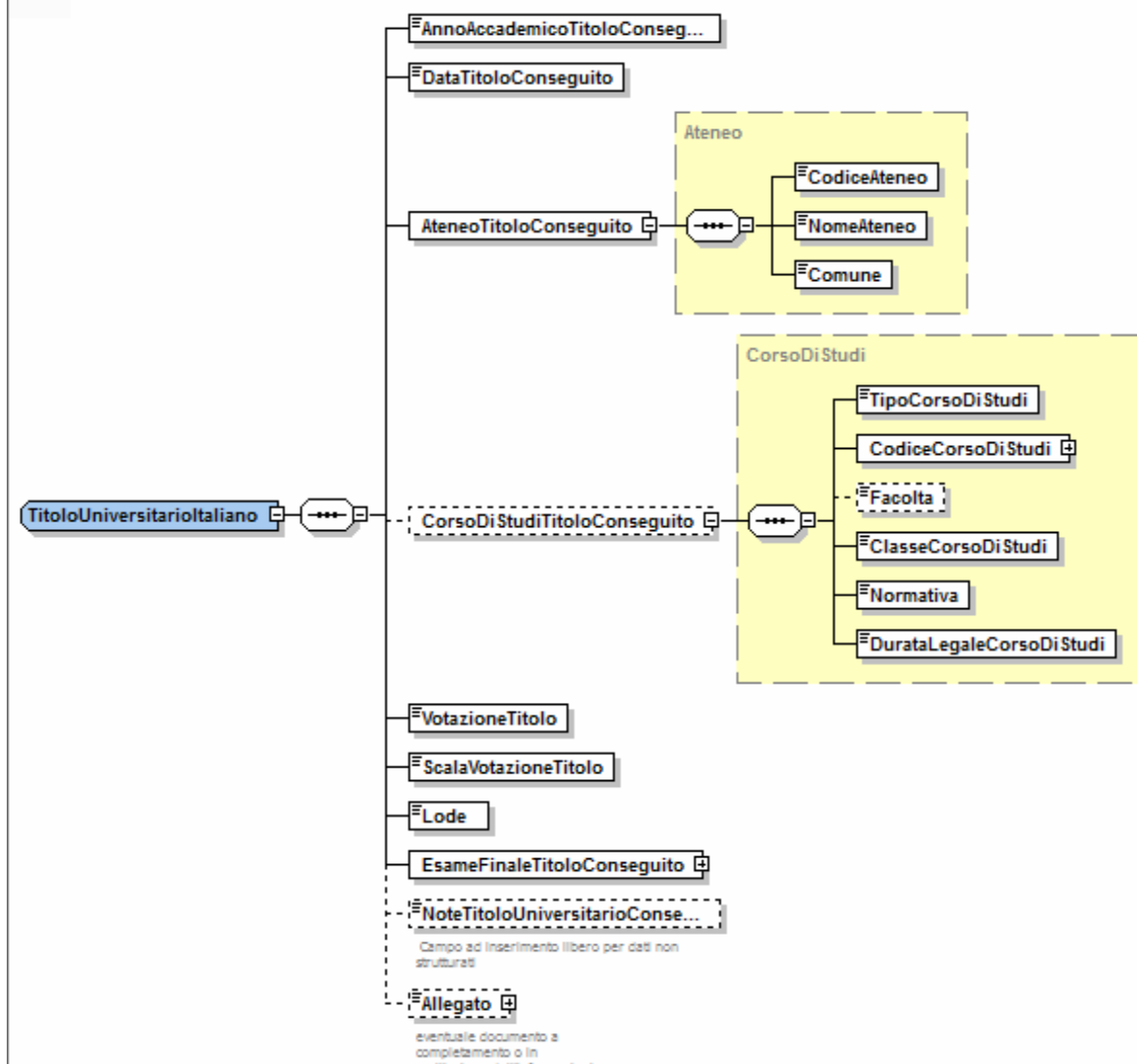


Figura 9 Schema xsd del nodo TitoloUniversitarioItaliano

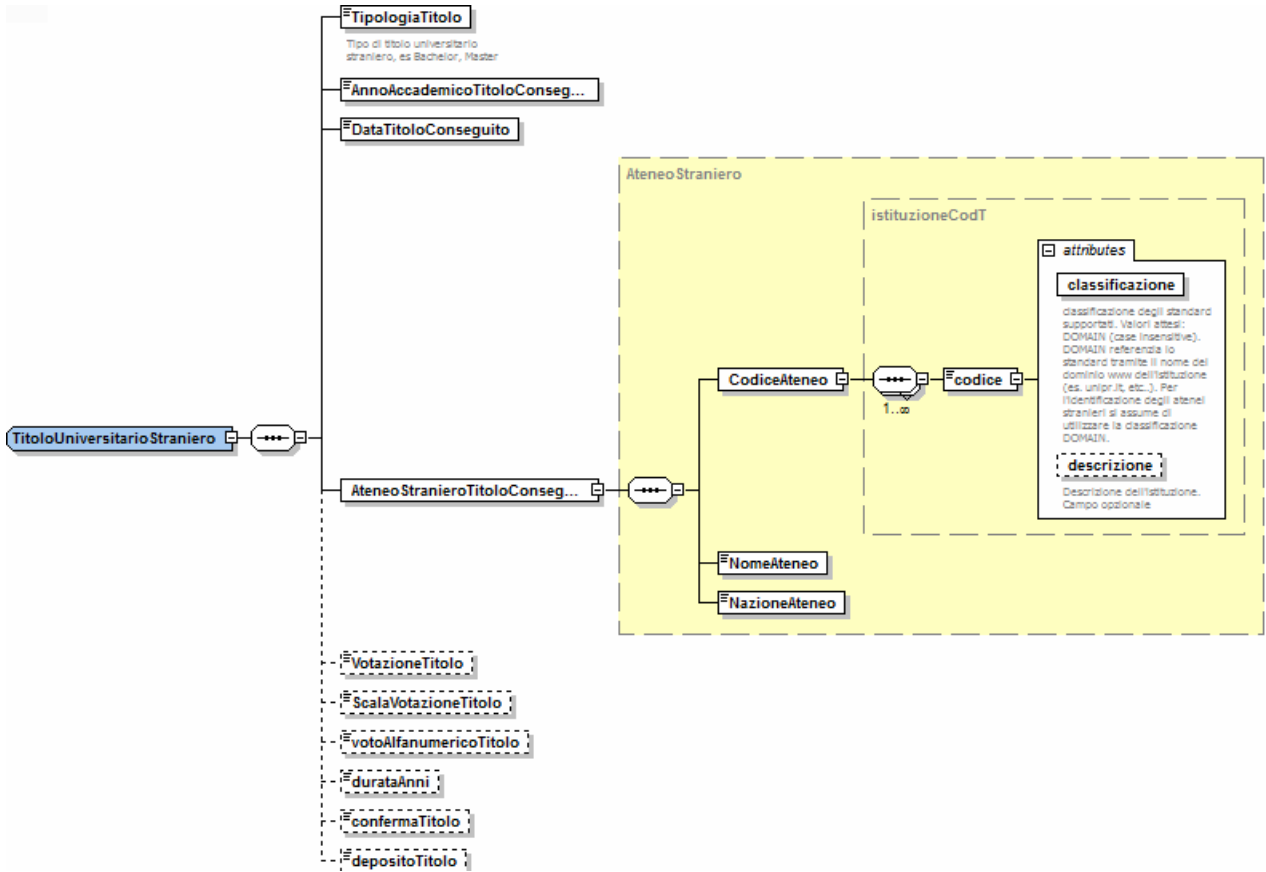


Figura 10 Schema xsd del nodo TitoloUniversitarioStraniero

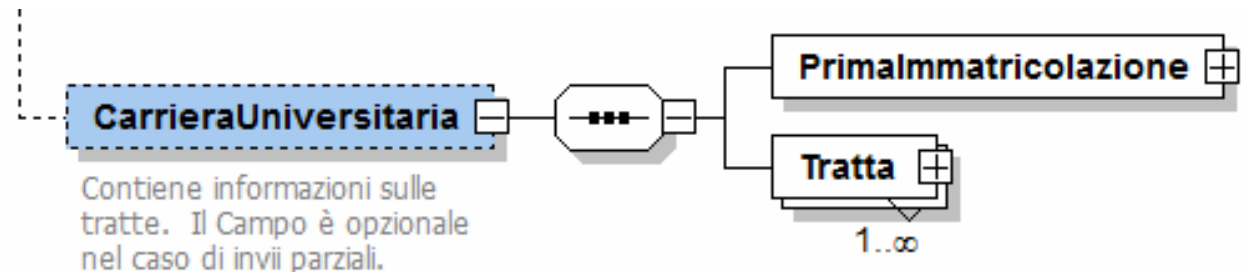


Figura 11 Schema xsd del nodo CarrieraUniversitaria

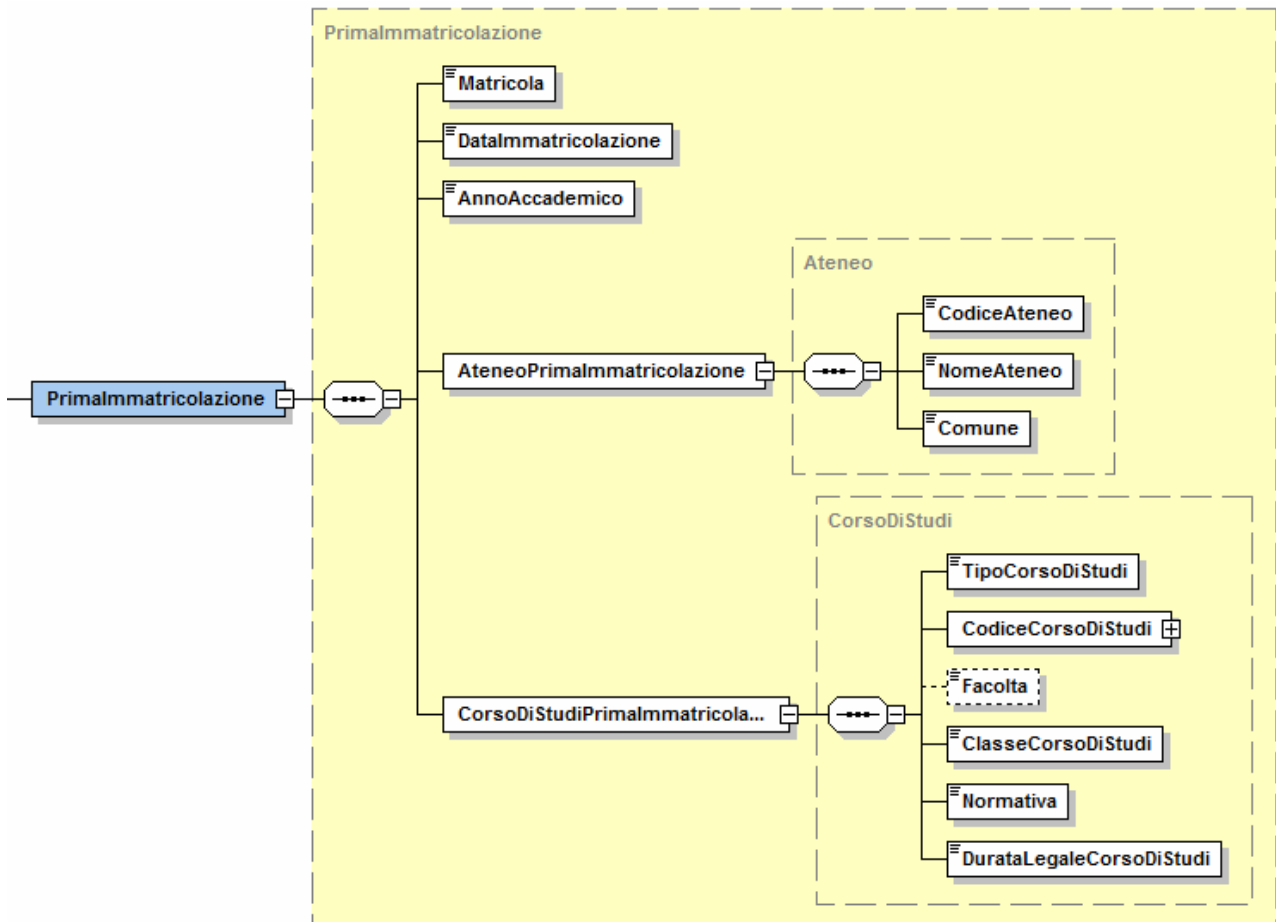


Figura 12 Schema xsd del nodo Primalmmatricolazione

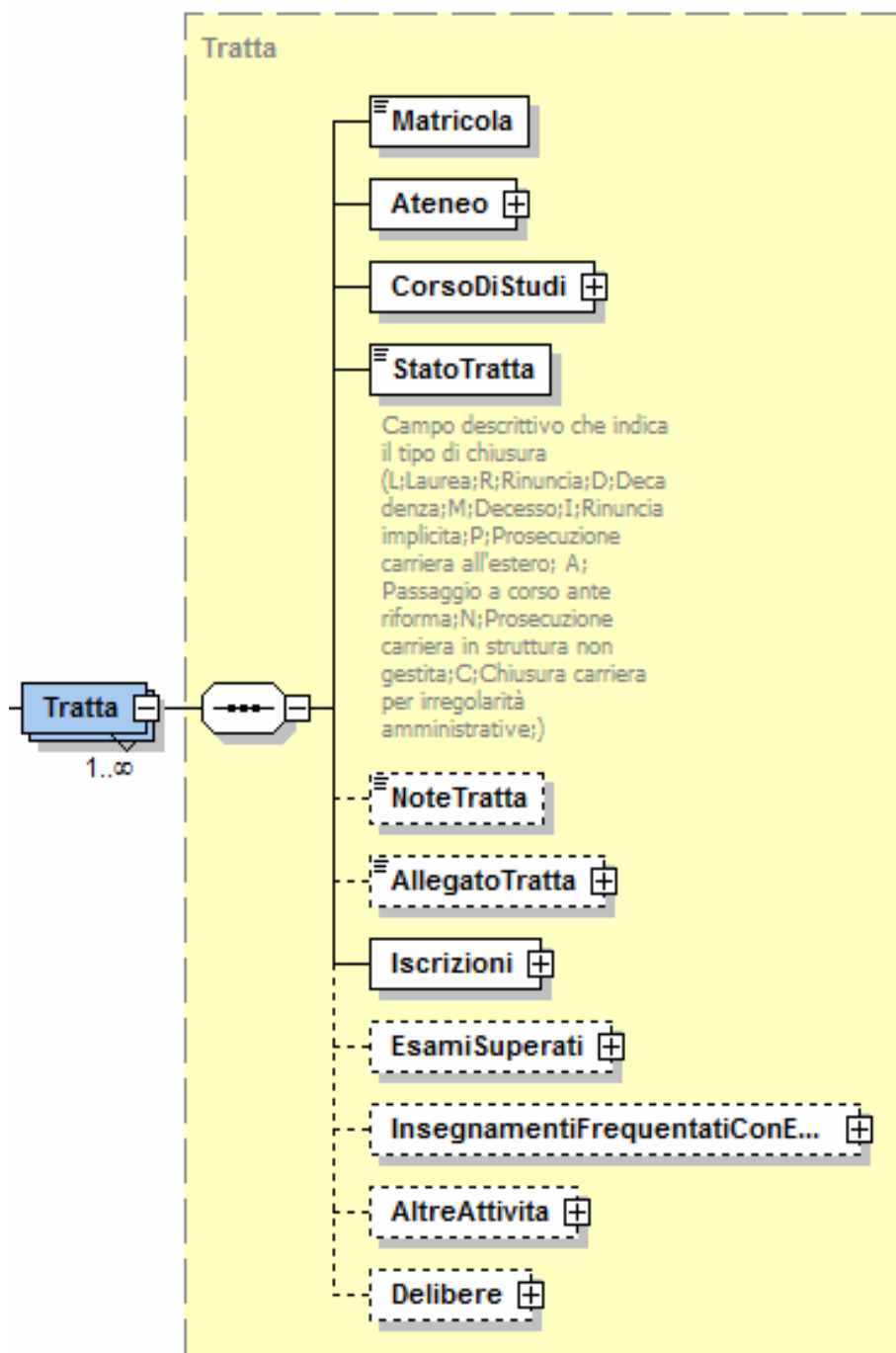


Figura 13 Schema xsd del nodo Tratta

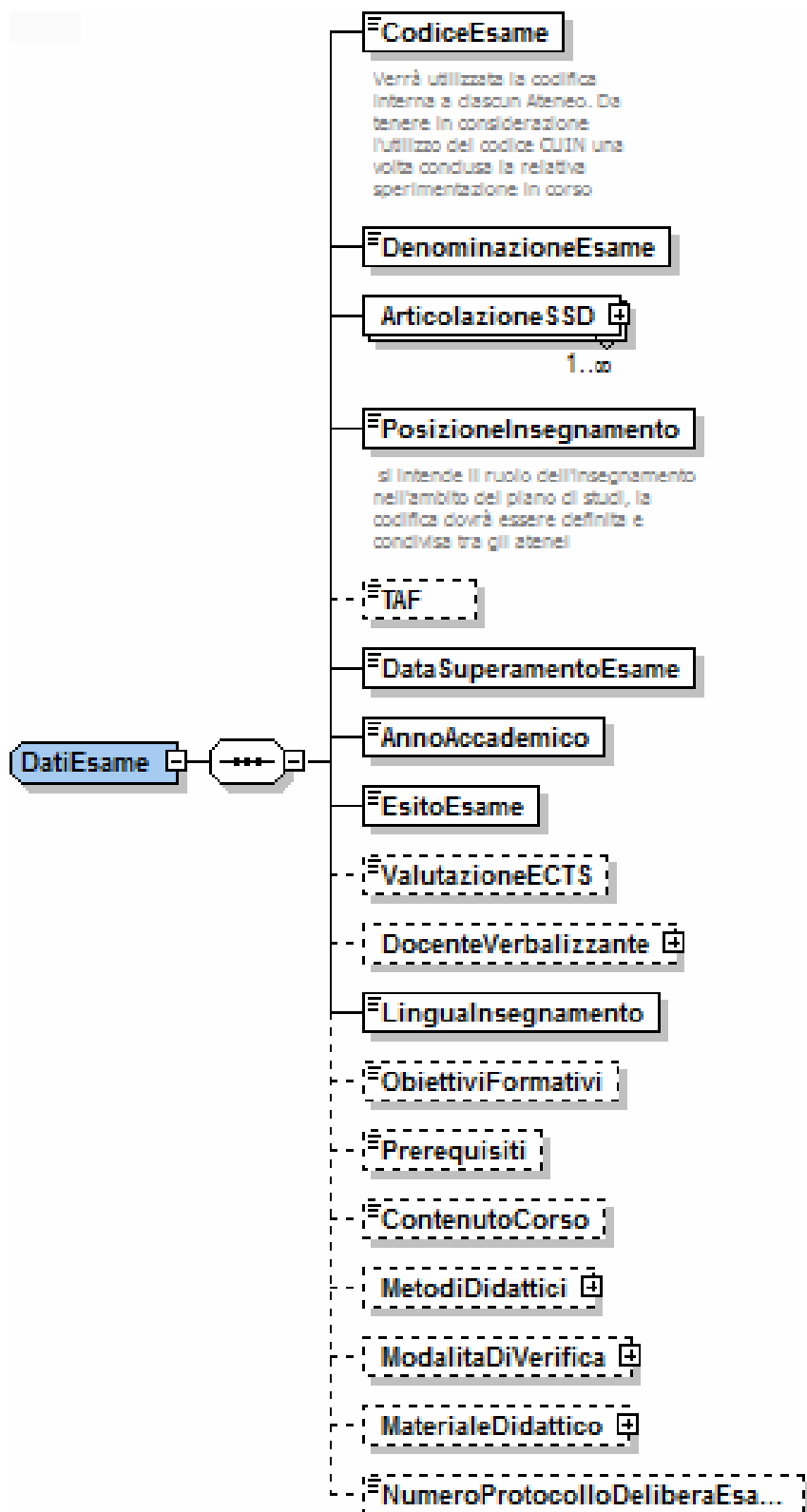


Figura 14 Schema xsd del nodo DatiEsame

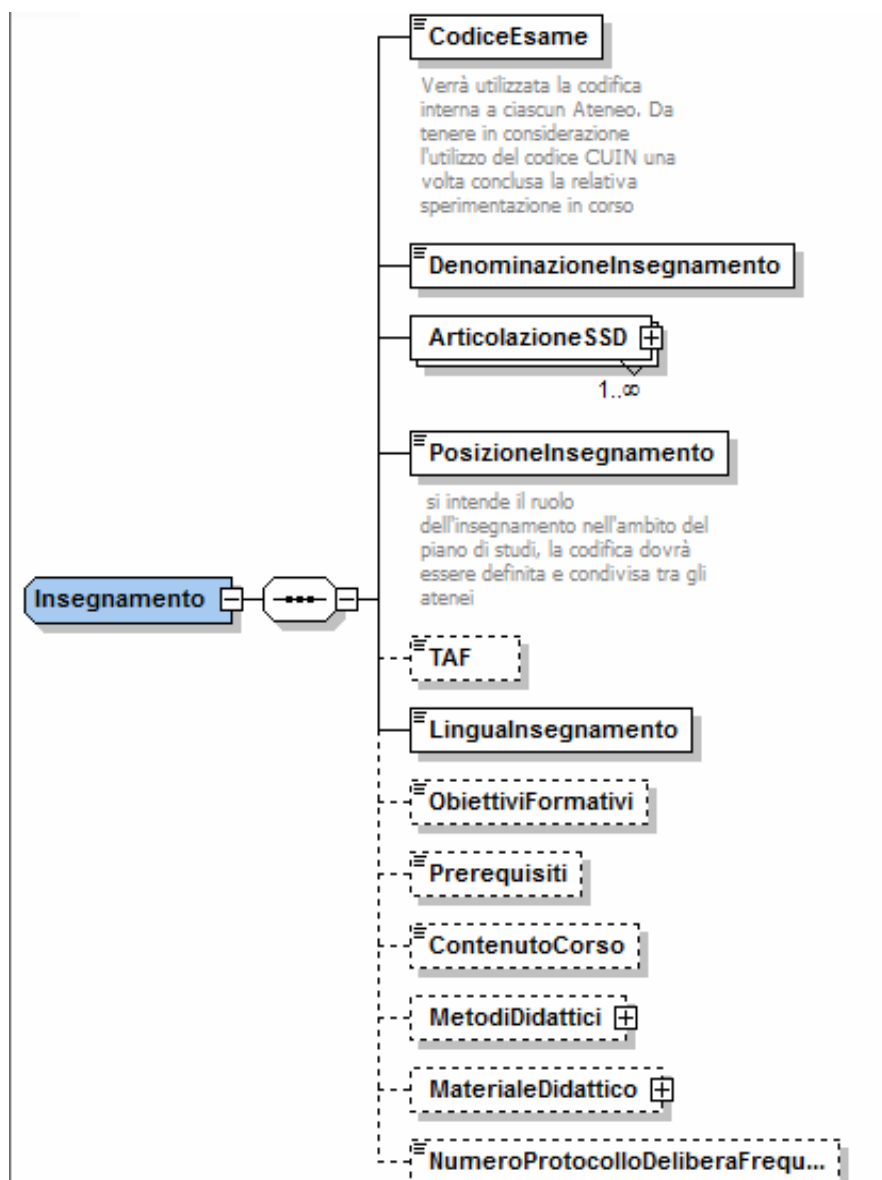


Figura 15 Schema xsd del nodo Insegnamento

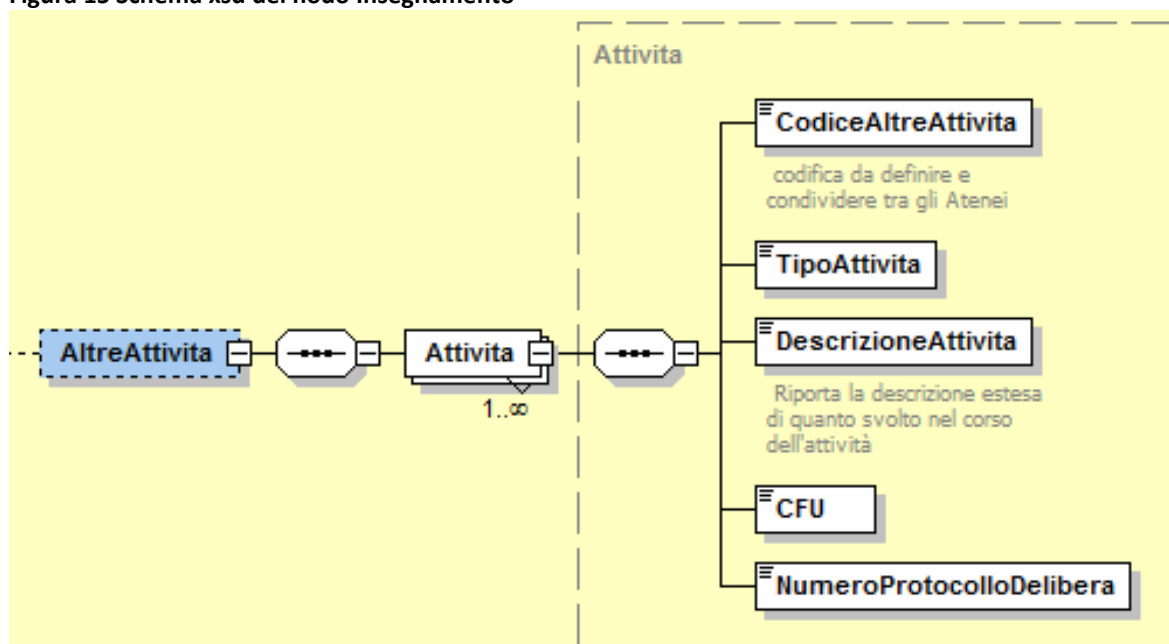


Figura 16 Schema xsd del nodo AltreAttività

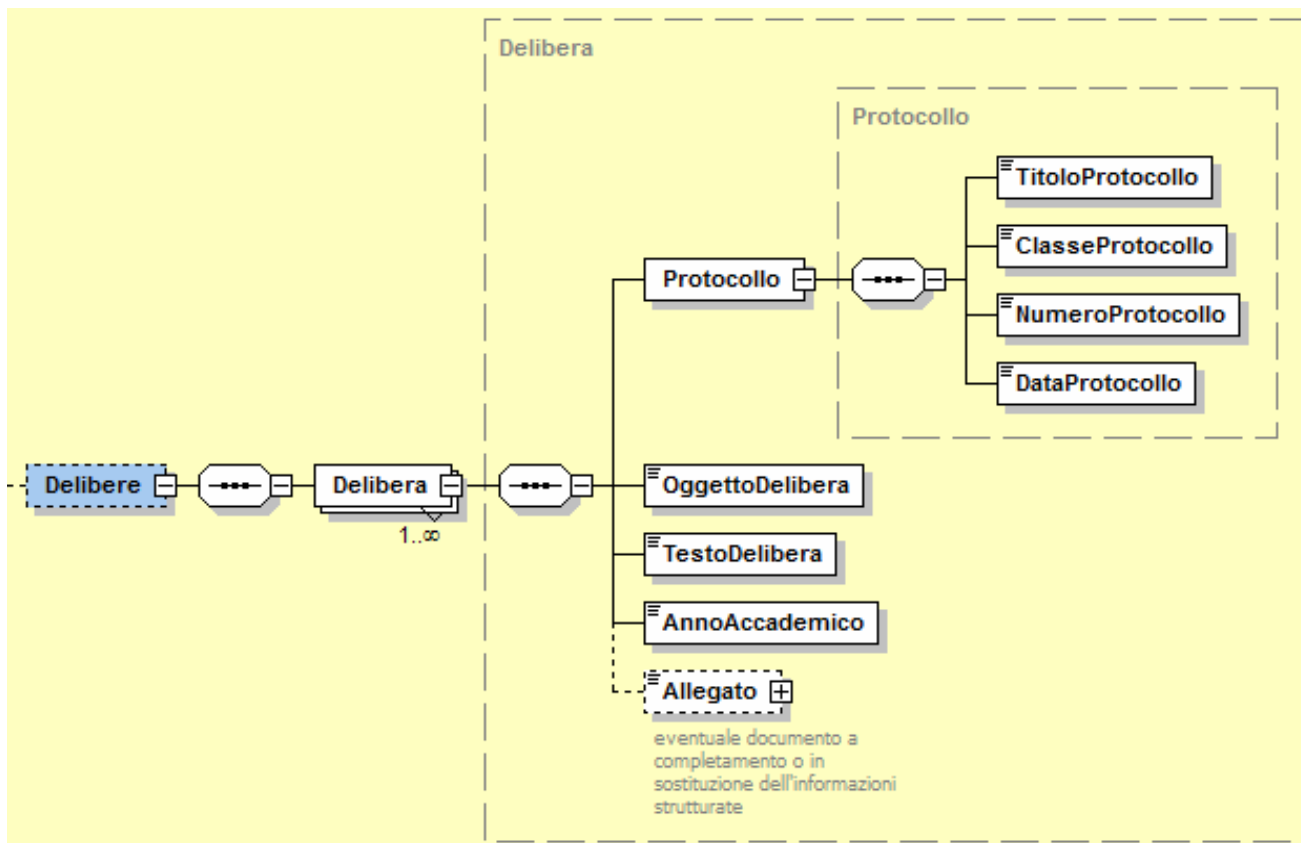


Figura 17 Schema xsd del nodo Delibere

### A.2.5. Note

Laddove possibile, si è preferito utilizzare delle codifiche invece di usare dei campi testuali liberi. Ciascuna codifica è accompagnata dalla relativa descrizione. Alcune codifiche sono state già inserite; altre, come indicato nel file excel, andranno definite e condivise tra gli Atenei nella fase di sperimentazione del sistema.

Si fa notare che, relativamente alla codifica relativa al titolo straniero (TitoliConseguiti->TitoliUniversitariConseguiti(stranieri)->AteneoStranieroConseguimentoTitolo->Codice) rimane da chiarire ancora il tipo di codifica denominato DOMAIN.

## **Appendice B. Specifiche tecniche di riferimento per l'implementazione di infrastrutture VoIP interoperabili**

### **B.1. Premessa**

L'analisi alla base di queste specifiche tecniche è relativa all'individuazione dei requisiti tecnologici di massima di un sistema di IP Telephony tecnologicamente all'avanguardia, con prestazioni e caratteristiche tecniche molto elevate, composto da apparati per la trasmissione e la commutazione di flussi di fonia over IP, in grado di sostituire totalmente o integrarsi gradualmente in un'infrastruttura di fonia legacy TDM- based.

Il sistema in questione deve essere in linea con le più innovative soluzioni tecnologiche oggi disponibili sul mercato e deve essere basato su un'infrastruttura in grado di garantire:

- la protezione degli investimenti già effettuati sulla rete di trasporto
- la stretta integrazione con l'evoluzione delle reti universitarie e della ricerca
- la possibilità di garantire margini di espansione a costi contenuti in accordo con le esigenze che dovessero nascere successivamente alla prima realizzazione.

La soluzione deve essere inoltre totalmente modulare e quindi implementabile in modalità stepwise, facilmente interfacciabile con qualsiasi altro sistema telefonico o dati preesistente; deve essere inoltre implementabile sulla base di soluzioni tecnologiche aperte, ampiamente diffuse e disponibili sul mercato, garantendo l'investimento in termini di scalabilità e garanzie di mantenimento nel tempo della validità tecnologica dell'iniziativa.

La stessa deve consentire di introdurre, all'interno della nuova infrastruttura, servizi e soluzioni in linea con le tecnologie VoIP utilizzate sulla rete nazionale dai principali operatori di telecomunicazione.

Esistono allo stato dell'arte un notevole numero di soluzioni disponibili sul mercato, sia commerciali che open source. Le stesse si differenziano essenzialmente solo per scalabilità, flessibilità e semplicità di uso. In generale, la compliance a protocolli di segnalazione e codifica standard assicura la piena interoperabilità fra tutte le soluzioni disponibili. Il riuso di soluzioni open source abbatta i costi ulteriormente e tende ad evitare il lock-in con un fornitore su soluzioni proprietarie. D'altro canto nel considerare una soluzione open source vanno tenuti in conto i necessari investimenti in termini di know-how necessari per tutte le attività di supporto e manutenzione.

## B.2. Requisiti

Un sistema di telefonia su IP adeguato a rispondere alle moderne esigenze di una struttura universitaria deve rispondere ai seguenti requisiti fondamentali concernenti:

- Affidabilità;
- Modularità;
- Sicurezza.

In quest'ottica, la soluzione ideale deve essere conforme ai seguenti criteri:

- utilizzo esclusivo di protocolli standard o riconosciuti come tali dal mercato;
- compatibilità con i principali protocolli standard supportati dai sistemi telefonici legacy in tecnologia TDM;
- supporto di architetture sia centralizzate che distribuite con possibile ridondanza geografica degli apparati al fine di garantire meccanismi di disaster recovery;
- disponibilità di criteri di sicurezza implementabili a tutti i livelli (accesso, autenticazione e autorizzazione);
- disponibilità di servizi telefonici di base;
- disponibilità di servizi telefonici a valore aggiunto;
- omogeneità dei servizi fruibili da tutti gli utenti e possibilità di profilare l'utenza in base all'accesso condizionato a particolari servizi.

Il sistema deve utilizzare le infrastrutture di rete basate sulla pila protocollare TCP/IP sia per il trasporto della segnalazione sia per il trasporto dei pacchetti voce.

### Caratteristiche architetture

L'architettura del sistema deve prevedere uno schema funzionale che possa supportare criteri di ridondanza e/o bilanciamento del carico (cluster HA centralizzati o architettura totalmente distribuita) e di conseguenza l'alta affidabilità fra i nodi principali per garantire le comunicazioni anche in caso di riconfigurazione o guasto di uno dei principali elementi funzionali.

L'architettura deve inoltre garantire una separazione funzionale tra gli elementi costituenti basata sui seguenti livelli logici.

- Livello di controllo: tutte le funzionalità deputate alla gestione delle chiamate (fase di attivazione, instradamento, controllo e rilascio) e dei servizi telefonici supplementari (trasferimento di chiamata ecc.);
- Livello di trasporto: tutte le funzionalità deputate al trasporto ed al trattamento dei pacchetti voce;
- Livello di servizio: tutte le piattaforme che ospitano la logica dei servizi a valore aggiunto e che hanno in carico le interazioni con le applicazioni.

## **Livello di controllo**

Il Session Control Server o IP PBX è la componente che ha il controllo delle chiamate e della gestione dell'infrastruttura telefonica e che si occupa dell'erogazione dei servizi base ed avanzati quali, ad esempio, la messa in attesa, la richiamata su occupato e la conferenza. È infatti tale elemento che gestisce gli utenti telefonici, la connessione telefonica in ogni sua fase (instaurazione, instradamento, disconnessione), la segnalazione, il piano di numerazione, le operazioni di tariffazione e controllo. Il PBX IP deve garantire il supporto di identificativi di numerazione standard (E.164), di piani di numerazione privati (standard ISO/IEC 11571) e di tutte le funzionalità tipiche di un centralino tradizionale.

Lo stesso deve inoltre garantire meccanismi di ridondanza attivo-attivo o attivo-standby, deve essere inoltre facilmente espandibile ed integrabile con i sistemi esistenti mantenendo i servizi di base presenti sulla rete.

Il Session Control Server deve essere in grado di gestire tutti i terminali IP (telefoni e Media Gateway) che utilizzano protocolli standard (SIP, H.323 e MGCP) o altri protocolli riconosciuti come standard dal mercato.

## **Livello di Trasporto**

A tale livello sono presenti tutti gli elementi necessari per codificare, decodificare, convertire e trasportare la voce in tecnologia VoIP. Essi possono essere distinti in:

Media Gateway;

Media Conference Bridge;

Terminali telefonici, fax ed interfacce di terminazione analogiche.

## **Media Gateway**

Il Media Gateway rappresenta l'interfaccia tra la tecnologia VoIP e le reti legacy in tecnologia a commutazione di circuito (Rete Telefonica Generale (PSTN) e rete di fonia privata in tecnologia legacy). Il suo ruolo principale è trasformare il traffico voce/segnalazione da una tecnologia di trasmissione/rete ad un'altra, generalmente passando da una logica a commutazione di pacchetto basata su datagrammi IP ad una a commutazione di circuito operante in modalità TDM e viceversa.

I Media Gateway devono essere posizionabili in qualsiasi punto della rete di trasporto e devono essere raggiungibili attraverso un indirizzo IP. In particolare potranno essere prese in considerazione le seguenti soluzioni architetturali:

Media Gateway centralizzati su un'unica sede o suddivisi su più siti;

Media Gateway locali alle singole sedi (in ogni sede deve essere previsto un Media Gateway dedicato);

Media Gateway geograficamente distribuiti ma raggruppati 'per aree': in questo caso ogni singolo Media Gateway offrirà l'accesso alla PSTN ad un gruppo di sedi dotate di infrastruttura IP Telephony;

I Media Gateway devono garantire inoltre il supporto di:

interfacce voce tradizionali (analogiche, ISDN BRI/PRI);

interfacce IP (LAN, WAN);

Conversione voce da analogica/TDM a VoIP;

Interlavoro con il Session Control Server.

Il supporto di protocolli standard di segnalazione telefonica tradizionale (Q.931, ISDN, Q.SIG) per l'interazione con sistemi legacy.

### **Media Conference Bridge**

I Media Conference Bridge sono gli apparati che vengono utilizzati per la miscelazione dei flussi vocali per applicazioni di conferenza. Essi devono essere in grado di gestire flussi vocali che utilizzano codec differenti.

Il posizionamento dei Media Conference Bridge, che devono essere raggiungibili attraverso un indirizzo IP, deve poter avvenire in qualsiasi punto della rete. Gli stessi devono essere inoltre in grado di offrire servizi di conference in modalità dedicata o condivisa con piena interazione coi servizi erogati dal Session Control Server.

### **Terminali utente**

I terminali utente ideali devono essere pienamente integrabili con il sistema di comunicazioni basato su IP e supportare le seguenti specifiche di base:

Stack TCP/IP nativo;

Possibilità di acquisire un indirizzo IP in maniera dinamica attraverso un server DHCP oppure di definire un indirizzo IP in maniera statica;

Assegnazione automatica del traffico dati/voce a reti logiche virtuali (VLAN) distinte (Dati e Voce) senza intervento manuale attraverso lo standard IEEE 802.1Q;

Assegnazione automatica del livello di qualità del servizio (QoS) ai pacchetti voce/dati appartenenti a ciascuna delle due VLAN senza intervento manuale;

Supporto dei codec audio standard (es. G.711 e G.729)

Supporto di meccanismi di Voice Activity Detection per ottimizzare il traffico generato e generazione di "Comfort Noise" su silenzio.

Possibilità di ricezione diretta dell'alimentazione dallo switch attraverso la rete LAN secondo lo standard IEEE 802.3af Power over Ethernet (PoE);

Supporto dello standard XML o equivalente per l'implementazione di servizi a valore aggiunto su tutti i dispositivi telefonici;

Supporto di protocolli standard (SIP, H323) o riconosciuti come tali dal mercato;

Suoneria differenziata per telefono e per singola linea telefonica, tramite file audio;

Volume regolabile della suoneria;

### **Servizi telefonici**

I servizi telefonici erogati devono essere distribuibili in maniera omogenea sull'intera infrastruttura VoIP in modalità tale da permetterne l'utilizzo a tutti gli utenti indipendentemente dalla loro dislocazione geografica. E' richiesto il supporto di un portafoglio di servizi evoluto adeguato ai massimi livelli dello stato dell'arte.

## Servizi e funzionalità telefoniche di base

Di seguito sono elencati i servizi telefonici di base che devono essere garantiti da un tipico sistema di telefonia IP:

Gestione completa e flessibile delle chiamate in entrata e in uscita;  
 Gestione chiamate multiple per linea e per telefono;  
 Rubrica globale e personale con chiamata diretta dalla rubrica;  
 Servizio deviazione chiamate a tempo/fisso/variabile;  
 Servizio non disturbare;  
 Servizio conferenza su linee interne/esterne;  
 Servizio attesa;  
 Servizio parcheggio linee;  
 Servizio richiamata;  
 Servizio risposta automatica;  
 Servizio risposta per assente individuale/gruppo;  
 Servizio ripetizione ultimo numero selezionato;  
 Servizio di post-selezione;  
 Servizio di trasferta con offerta /automatica;  
 Impegno diretto e automatico delle linee urbane libere;  
 Possibilità di attivare una conversazione a tre su linee esterne con svincolo del chiamante senza caduta della conversazione stessa;  
 Selezione passante;  
 Servizio documentazione addebiti;  
 Chiamata diretta a gruppi di utenti intercomunicanti;  
 Chiamata diretta a utenti privilegiati;  
 Possibilità di assegnare diverse classi di servizio e livelli di abilitazione ai singoli utenti, attivabili su base identificazione;  
 Possibilità di impegnare le linee uscenti attraverso codici specifici;  
 Cambio classe di servizio a tempo in funzione della fascia oraria;  
 Eseguire, trasferire e rilasciare una chiamata voce;  
 Identificazione del nome chiamante, ove inviato;  
 Identificazione del numero chiamante;  
 Restrizione della chiamata in base al numero;  
 Richiamata su occupato o su non risposta;  
 Musica in Attesa differenziabile per gruppi di utenti;  
 Hunt Group con segnalazione di chiamata in parallelo, circolare, lineare;  
 Trasferimento diretto verso sistemi di messaggistica integrata multicanale;  
 Deviazione totale, su occupato e su non risposta;  
 Direttore Segretaria/multi-segretaria con funzionalità avanzate;  
 Gestione suonerie differenziate per telefono e/o per linea;  
 Esclusione suoneria per linea;  
 Lista delle chiamate perse, effettuate e ricevute;  
 Servizio di mobilità di utente, su telefoni diversi, basato su identificazione utente;  
 Instradamento automatico sulla PSTN anche geograficamente distribuito basato su indisponibilità di risorse;  
 Funzionalità di Call Admission Control (CAC);  
 Blocco delle chiamate in uscita condizionato a classe di servizio, a temporizzazione e a numero chiamato soggetto a codice di sblocco;  
 Avviso acustico configurabile su occupato;  
 Supporto di applicazioni di terze parti tramite interfacce API standard (es. TAPI, JTAPI);

Gestione del Posto Operatore (servizio di centralino);  
 Piena interoperabilità con sistemi esterni Gatekeeper.

### **Servizi accessibili da terminali di telefonia IP**

Un moderno sistema di telefonia su IP deve prevedere un insieme di servizi offribili all'utenza, accessibili direttamente da terminale telefonico, suddivisi in diversi livelli di servizio (ad esempio standard, top-class e advanced) e per tipologia di telefono. L'insieme minimo di servizi utente fruibili attraverso i terminali IP è essenzialmente individuabile in:

Servizio Direttore/Segretaria;  
 Servizio deviazione chiamate a tempo/fisso/variabile;  
 Servizio non disturbare;  
 Servizio conferenza su linee interne/esterne;  
 Servizio attesa;  
 Servizio parcheggio;  
 Servizio richiamata;  
 Servizio risposta automatica;  
 Servizio risposta per assente individuale/gruppo;  
 Servizio ripetizione ultimo numero selezionato;  
 Servizio di Trasferta con offerta/automatica;  
 Impegno diretto delle linee urbane libere;  
 Impegno selettivo a tasto di una linea specifica;  
 Avviso acustico configurabile su occupato;  
 Chiamata intercomunicante;  
 Chiamata Hot Line;  
 Gruppi di utenti intercomunicanti;  
 Chiamata diretta a gruppi di  $N$  utenti intercomunicanti;  
 Cambio classe di servizio;  
 Visualizzazione durata conversazione, numero d'interno, orario, ecc.

### **Servizi opzionali**

Di seguito sono elencati alcuni servizi opzionali particolarmente interessanti che possono essere attivati integrando eventualmente la soluzione di telefonia IP con l'utilizzo di sistemi ausiliari.

Supporto chiamate video;  
 Possibilità della gestione di terminali per videoconferenza, Multipoint Conferencing Unit (MCU), Video Gateway, integrandoli nel piano di numerazione generale e dotandoli dei servizi tipici della fonia (trasferta di videoconferenza, deviazione, parcheggio della chiamata, gruppi di risposta, multiconferenza a più partecipanti, linea condivisa);  
 Riconoscimento chiamate in black list;  
 Service URL- Accesso ai servizi telefonici web, http, directory esterne, etc;  
 Statistiche in tempo reale dei parametri della Qualità del Servizio (QoS) e della qualità della conversazione (MoS) visibili direttamente o sul sistema via interfaccia grafica.

## Servizi a valore aggiunto

E' auspicabile all'interno di un moderno sistema VoIP il supporto o la predisposizione all'attivazione di una serie di servizi non opzionali a valore aggiunto quali:

Mobilità;

Rubrica telefonica e servizi di chiamata attraverso portale voice con interfaccia web;

TeleConferenza;

Messagistica Integrata Multicanale.

Interfacciamento con Applicazioni esterne di Instant Messaging e di presence;

Sistemi per l'erogazione di servizi di IVR e ACD (es. contact center).

## Mobilità

Un moderno sistema di telefonia IP deve essere in grado di supportare in maniera nativa la mobilità degli utenti, conformemente ai criteri di seguito elencati e dettagliati nelle successive sezioni riguardanti:

*Mobilità fisica dell'utente:* Il sistema deve gestire la portabilità del telefono (hardware o software) all'interno della rete su cui è sviluppato il sistema telefonico, mantenendo il numero/classe di servizio del telefono senza modifiche della stessa. La mobilità fisica deve essere gestita attraverso livelli di autenticazione e di registrazione del terminale che assicurino la corretta assegnazione del numero/classe di servizio del telefono.

*Mobilità logica dell'utente.* L'utente deve avere la possibilità di utilizzare qualunque telefono IP e di autenticarsi al sistema attraverso codici univoci. Il servizio deve essere offerto in maniera selettiva a gruppi di utenti e deve essere attivabile/disattivabile da parte dell'utente attraverso codici univoci. Il sistema deve gestire la portabilità del profilo utente tra diversi terminali telefonici mantenendo il numero/classe di servizio dell'utente senza modifiche della stessa. La mobilità logica deve essere gestita attraverso livelli di autenticazione e di registrazione in modo che l'utente possa ricevere ed effettuare telefonate con il proprio numero presso la propria sede oppure presso altre sedi.

## Rubrica telefonica e portale voice

Il sistema deve consentire di gestire una rubrica telefonica a cui sia possibile accedere attraverso i terminali IP oppure tramite interfaccia web. L'accesso agli elenchi telefonici deve avvenire per tutti i telefoni IP via interfaccia XML, per gli utenti esterni attraverso i protocolli HTTP, HTTPS e LDAP.

E' auspicabile inoltre supportare un servizio di tipo "click-to-dial" che permetta agli utenti di effettuare una telefonata dal proprio terminale IP (Handeld o softphone su PC), cliccando su una pagina web il nominativo/numero interno dell'utente.

## Teleconferenza

Il sistema di comunicazioni deve essere dotato di un servizio di teleconferenza audio/video in grado di gestire multiple sessioni (o stanze) con multipli utenti contemporanei sia interni che esterni. Tale servizio deve supportare protocolli e codec standard (ad esempio H.323, H.264, G.711).

Il servizio di Teleconferenza deve essere attivabile:

su invito: Con questa modalità di attivazione del servizio, l'utente che indice la conferenza deve essere in grado attraverso il proprio terminale di:

aggiungere un partecipante;

vedere la lista dei partecipanti;

abbandonare la conferenza lasciando che i restanti partecipanti continuino a fruire del servizio.

su appuntamento: Il sistema definisce un codice di accesso alla stanza virtuale che i partecipanti devono digitare per partecipare alla conferenza e avvisa gli stessi attraverso un messaggio telefonico o via e-mail.

### **Messaggistica Integrata Multicanale (caselle vocali)**

Il servizio di Messaggistica Integrata Multicanale deve essere in grado di gestire la memorizzazione di messaggi vocali e il loro ascolto a posteriori. Esso deve prevedere la possibilità di integrarsi da un lato con il sistema telefonico attraverso protocolli standard SIP, H.323 o con altri protocolli riconosciuti come standard dal mercato e dall'altro lato con i più comuni servizi di posta elettronica/automazione di ufficio (es. Microsoft Exchange, Lotus Notes o comunque servizi standard di posta elettronica). Il sistema di messaggistica integrata deve supportare l'erogazione dei seguenti servizi:

Gestione del messaggio di benvenuto/alternativo configurabile da parte dell'utente;

Possibilità di personalizzare su base utente più messaggi di benvenuto schedulabili in base all'ora, al giorno e all'anno;

Notifica automatica e sincronizzata sul telefono e sul client di posta (es. Outlook) della presenza/cancellazione/ascolto di un messaggio vocale;

Memorizzazione di un messaggio vocale in formato file audio di tipo .wav;

Integrazione del file vocale con la mail elettronica e possibilità di interazione con il sistema di Messaggistica Integrata;

Interazione attiva (ascolto, cancellazione, pausa) del messaggio vocale attraverso il telefono e attraverso il client di posta Outlook;

Possibilità di ricevere le informazioni sul messaggio (ora, data, lunghezza e mittente);

Possibilità di creare alberi di risposta automatica attraverso l'uso dei DTMF.

Altre funzionalità opzionali interessanti sono elencate di seguito:

Text-To-Speech (TTS) utilizzato per la lettura di file testuali tipo e-mail;

Accesso via web da parte dell'utente alla propria casella vocale

Possibilità di cifrare il protocollo di segnalazione e di cifrare il canale comunicativo voce (flusso RTP);

Capacità di controllare lo spazio della casella a disposizione per singolo utente;

Archiviazione/cancellazione dei messaggi per un tempo configurabile;

Possibilità di inoltrare messaggi arrivati sulla propria casella;

Possibilità di inviare messaggi in modalità di broadcast;

Possibilità di notifica di ricezione di un messaggio anche su cercapersone, nella casella e-mail o via SMS;

Possibilità di indicare il messaggio come urgente o come privato;

Possibilità di ricevere la notifica di mancata consegna del messaggio inviato;

Possibilità di integrare e gestire anche messaggi fax.

## **Interfacciamento con Applicazioni esterne di Instant Messaging e di presence**

A fronte dell'evoluzione del mercato che pone il suo sviluppo più rilevante nella messa in opera di servizi per i dispositivi mobili (smart-phone e palm device), un moderno sistema VoIP deve prevedere soluzioni che estendono la fruizione sia del concetto di presence che del concetto di message switching su moderni dispositivi telefonici mobili. L'unione di due tecnologie essenziali, quali la messaggistica in tempo reale e la presenza, all'interno del sistema di comunicazione telefonico VoIP, offre servizi e applicazioni in grado di rispondere ai moderni processi di lavoro e di business di ogni organizzazione. Il sistema deve quindi prevedere la disponibilità di appositi gateways verso i principali servizi di IM e presence (gTalk, MSN, Skype etc) a beneficio dell'integrazione e l'apertura dei servizi alla comunità studentesca.

## **Servizi di Autenticazione, Autorizzazione, Accounting e Billing**

I terminali telefonici introdotti in rete non dovranno funzionare se non preventivamente identificati e registrati attraverso politiche di gestione e controllo accessi. Il sistema deve essere in grado di implementare politiche di:

Autenticazione;  
Autorizzazione;  
Accounting;  
Billing.

### **Autenticazione**

La piattaforma deve garantire servizi di autenticazione dell'utente per tutti gli accessi ai servizi telefonici sia attraverso terminali IP sia attraverso applicazioni. Il sistema deve prevedere l'integrazione con sistemi esterni di tipo LDAP Directory per validare l'utente.

### **Autorizzazione**

Il sistema deve prevedere la possibilità di creare diversi profili di abilitazione ai servizi telefonici garantendo un controllo granulare di tutte le capabilities associate a ogni singolo utente.

### **Accounting**

La piattaforma deve essere in grado di registrare i log di tutte le chiamate effettuate e ricevute in formato tabellare standard (Call Detail Record - CDR), in formato esportabile ad applicazioni esterne al fine di effettuare reportistiche specifiche. La generazione del CDR deve essere effettuata in real-time.

### **Billing**

Il sistema deve essere in grado di gestire tutte le utenze e le relative telefonate relativamente alle seguenti attività:

Generazione di documentazione di addebito sul traffico gestito;

Differenziazione dei diritti di accesso al sistema, tipicamente suddivisi in utente, supervisore ed amministratore. L'utente può solo verificare i propri consumi; il supervisore ha accesso a soli parametri di monitoring e report e l'amministratore ha la visibilità totale;

Gestione delle tariffe sulla base del numero effettuato, della sede e del Media Gateway impiegato;

Gestione delle tariffe secondo i piani di numerazione telefonici italiani e non italiani (ad esempio Nazionale, Europa, USA e Asia);

Gestione e creazione di centri di costo differenziati per utente con relativa documentazione degli addebiti;

Configurazione delle tariffe, ovvero la possibilità di associare dei costi a determinati prefissi, seguendo le specifiche di scatto alla risposta, tariffazione entro un primo intervallo di tempo, tariffazione oltre una soglia temporale configurabile;

Configurazione di report personalizzabili in formato di testo, CSV o PDF;

Scheduling della documentazione di addebito con possibilità di inviare i report in allegato ad una e-mail ai responsabili dei centri di costo e/o all'amministratore;

Priorità in fase di assegnazione delle tariffe ai CDR, qualora esistano casi dubbi;

Gestione sia delle chiamate on-net che off-net con possibilità di effettuare report non solo di costo ma anche di traffico.

## Glossario

ACD=Automatic Call Distribution  
 API=Application Program(ming) Interface  
 BRI=Basic Rate Interface  
 CAC=Call Admission Control  
 CAS=Channel Associated Signaling  
 CDR=Call Detail Record  
 Codec=COmpressor/DECompressor  
 CPU=Central Processing Unit  
 CSV=Comma Separated Values  
 DHCP=Dynamic Host Configuration Protocol  
 DTMF=Dual-Tone Multi-Frequency  
 ETSI=European Telecommunications Standards Institute  
 GSM=Global System for Mobile  
 HTTPS=Hypertext Transfer Protocol Secure  
 IP=Internet Protocol  
 ISDN=Integrated Services Digital Network  
 IT=Information Technology  
 IVR=Interactive Voice Response  
 JTAPI=Java Telephony API  
 LAN=Local Area Network  
 LDAP=Lightweight Directory Access Protocol  
 LCR=Least Cost Routing  
 MAC= Move, Add & Change  
 MCU=Multipoint Conferencing Units  
 MGCP=Media Gateway Control Protocol  
 MOS=Mean Opinion Score  
 MWI=Message Waiting Indicator  
 NAT=Network Address Translation  
 NTP=Network Time Protocol  
 PBX=Private Branch Exchange

PABX=Private Automatic Branch Exchange  
PC=Personal Computer  
PCM=Pulse Code Modulation  
PDA=Personal Digital Assistant  
PDF=Portable Document Format  
PoE=Power over Ethernet  
PRI=Primary Rate Interface  
PSTN=Public Switched Telephone Network  
Q.SIG=Q.Signaling (ISDN)  
QoS=Quality of Service  
RSVP=Resource Reservation Protocol  
RTG=Rete Telefonica Generale  
RTP=Real-time Transport Protocol  
SCS=Session Control Server  
SNMP=Simple Network Management Protocol  
SIP=Session Initiation Protocol  
SMS=Short Message Service  
TAPI=Telephony Applications Programming Interface  
TDM=Time Division Multiplexing  
TTS=Text-To-Speech  
TFTP=Trivial File Transfer Protocol  
UDP=User Datagram Protocol  
UMTS=Universal Mobile Telecommunications System  
VLAN=Virtual Local Area Network  
VoIP=Voice over IP  
WAN=Wide Area Network  
XML=eXtensible Markup Language

## Appendice C. Normativa sul VoIP

### *Descrizione generale del servizio e ambito di applicazione:*

*L'utente, dotato di terminale VoIP collegato su rete IP al centralino dell'Ateneo di appartenenza, si presenta sulla rete telefonica generale (PSTN) con un numero di telefono del piano di numerazione nazionale (PNN) assegnato all'Ateneo da un operatore telefonico.*

### *Condizioni:*

1. **disclaimer:** come previsto dalla normativa vigente (delibera 11/06/CIR) gli utenti devono essere informati di ogni limitazione connessa alla localizzazione delle chiamate di emergenza e alla disponibilità del servizio nel caso di utilizzo nomadico dei servizi VoIP offerti dall'Ateneo nell'ambito dei suoi scopi istituzionali
2. **usage policies:** alle chiamate VoIP verso PSTN si applicano le limitazioni d'uso della rete telefonica eventualmente imposte dall'Ateneo di appartenenza alle diverse categorie di utenti
3. **associazione terminali:** i terminali VoIP devono essere logicamente associati alla rete privata dell'Ateneo di appartenenza, o essere connessi al centralino VoIP attraverso un canale di comunicazione sicuro
4. **autenticazione utenti:** l'associazione del terminale VoIP al centralino dell'Ateneo di appartenenza deve richiedere l'autenticazione dell'utente
5. **chiamate entranti:** le chiamate entranti da rete PSTN (dirette o in selezione passante) devono poter essere ricevute su terminali VoIP in modo trasparente al chiamante
  - gli utenti e i servizi istituzionali devono poter essere raggiunti ai numeri telefonici geografici ad essi associati dall'ente di appartenenza
6. **chiamate uscenti:** le chiamate uscenti verso rete PSTN effettuate da terminali VoIP devono presentarsi al ricevente con un numero del piano di numerazione nazionale assegnato all'ente di appartenenza, preferibilmente con le stesse regole di associazione numero-utente utilizzate per le chiamate entranti
  - se le chiamate uscenti si presentano da numeri geografici soggetti a limitazioni d'uso nomadico nell'ambito del distretto di appartenenza, gli utenti devono essere informati delle limitazioni e responsabilizzati al rispetto delle stesse;
  - se le chiamate uscenti si presentano da numeri nomadici in decade 55 l'utilizzo nomadico può essere esteso al di fuori del distretto di appartenenza;
  - il tavolo tecnico auspica che l'Autorità possa valutare l'estensione fuori distretto dell'utilizzo nomadico dei numeri geografici, ipotizzata all'Art. 7 comma 5 dell'Allegato A alla delibera n. 26/08/CIR, da applicarsi almeno al caso in cui: 1) i numeri telefonici non siano associati agli utenti a titolo personale, ma in base alla funzione che gli utenti svolgono nell'ambito dell'ente di appartenenza, 2) l'uso del servizio telefonico sia limitato alla funzione istituzionale a cui il numero è associato, 3) il nomadismo degli utenti sia gestito a livello IP dall'Ateneo di appartenenza, 4) gli utenti siano informati dell'impossibilità di localizzazione delle chiamate di emergenza e della funzione istituzionale del servizio e del numero telefonico che stanno utilizzando.

7. **tracciabilità:** l'Ateneo deve mettere in atto le misure necessarie a fornire supporto all'Autorità Giudiziaria in materia di tracciamento del traffico e di identificazione degli utenti che usufruiscono del servizio VoIP, anche per chiamate interne
8. **mappatura:** per facilitare e incentivare la comunicazione su reti IP gli Atenei sono invitati ad adottare soluzioni tecniche che supportino il protocollo ENUM e ad aderire all'iniziativa NRENUM
9. **numeri agli studenti:** agli studenti vengono assegnati numeri locali resi accessibili in selezione passante da rete PSTN ed eventualmente mappati su NRENUM
  - è opportuno che i numeri assegnati agli studenti siano indipendenti da altri ID assegnati loro dall'Ateneo per altre finalità (quali i numeri di matricola)
10. **servizi agli studenti:** agli studenti vengono offerti servizi VoIP che non comportano costi variabili per l'Ateneo e non compromettono la disponibilità e l'usabilità del servizio telefonico per scopi istituzionali:
  - chiamate interne, chiamate verso numeri NRENUM, chiamate entranti in selezione passante da rete PSTN (su un sottoinsieme limitato di linee esterne)
  - chiamate verso numeri verdi

## **Appendice D. Allegato tecnico alle linee guida per l'autenticazione federata per l'accesso a Internet e risorse in rete**

### **D.1. 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

### **D.2. 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-](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-](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](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](http://www.garr.it/eventiGARR/idem-day/docs/conte-monticini_pres_idemday09.pdf)

## D.3. 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.

## D.4. 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;

## D.5. 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*.

## D.6. 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.

## D.7. 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.

## D.8. 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.

## **D.9. 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.

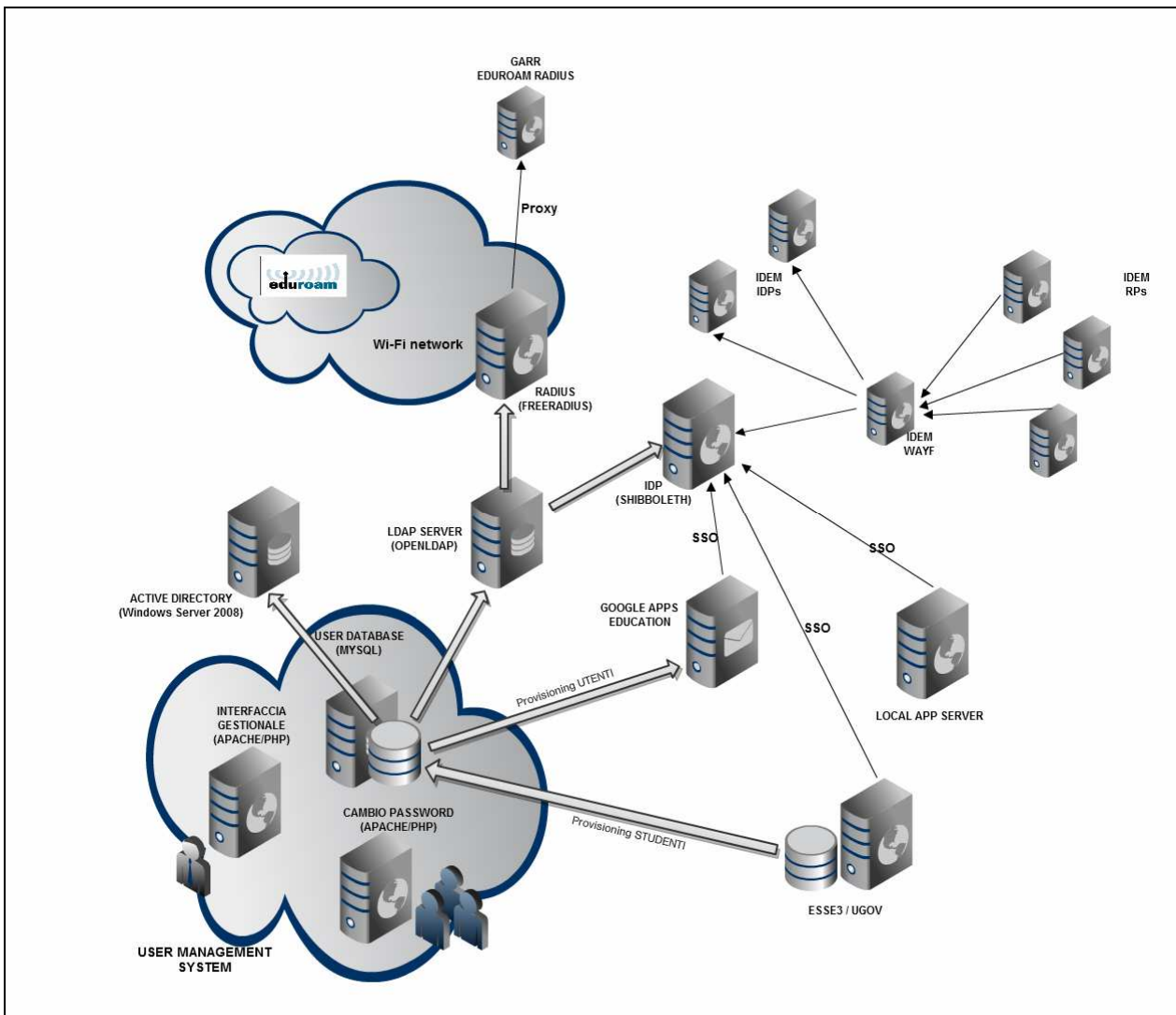
Le Università partecipanti utilizzano, per quanto possibile, prodotti OSS nell'implementazione delle soluzioni IAM e FIAM.

## **D.10. 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).

## D.11. 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 uno 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.

## D.12. 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*

### D.12.1. 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

### D.12.2. 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".

**D.12.3. 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.

<b>N</b>	<b>Descrizione categorie utenza d'ateneo</b>	<b>Codice macro categoria</b>
<b>1</b>	Personale docente di ruolo	D
<b>2</b>	Personale ricercatore di ruolo	R
<b>3</b>	Personale tecnico ed amm.vo a tempo indeterminato	P
<b>4</b>	Personale tecnico ed amm.vo a tempo determinato	P
<b>5</b>	Docente supplente esterno	D
<b>6</b>	Collaboratore tecnico/amministrativo	E
<b>7</b>	Collaboratore alla didattica	C
<b>8</b>	Assegnista di ricerca	R
<b>9</b>	Docente a contratto	D
<b>10</b>	Docente dotato di dispositivo di firma digitale per la registrazione d. esami	D
<b>11</b>	Studente iscritto ai corsi di studio di 1° e 2° livello	S
<b>12</b>	Dottorando	T
<b>13</b>	Dottorando di Università consorziate	T
<b>14</b>	Studente di master	T
<b>15</b>	Laureato di un qualunque corso di studi/ dottorato/ master	L
<b>16</b>	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
<b>17</b>	Ospite (convegnista, ospite occasionale)	G
<b>18</b>	Personale di azienda esterna che presta attività lavorativa presso l'Università XYX	H
<b>19</b>	Personale di azienda/organizzazione esterna che fornisce servizi ICT	F
<b>20</b>	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*

#### **D.12.4. 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*

### D.12.5. 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.

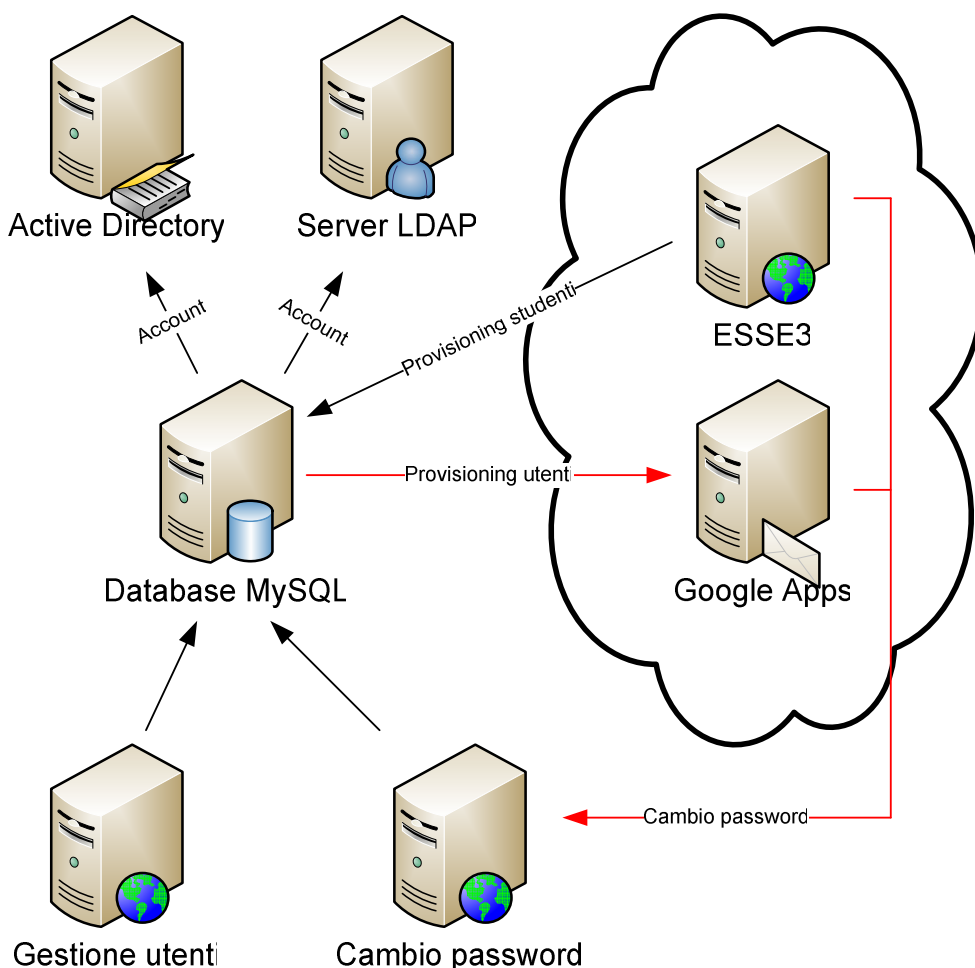
Una procedura eseguita ad intervalli regolari effettua gli aggiornamenti sul database LDAP (che alimenta i servizi Shibboleth e RADIUS) sul server Active Directory (che gestisce il dominio XYZ.IT per i computer desktop e il VDI) e infine su Google Apps Education (per la gestione delle caselle di posta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



## **D.12.6. 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.

## **D.12.7. 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 è 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 è 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.

## **D.12.8. 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.

## **D.12.9. 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.

### D.12.10. 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/ 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
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.

### D.12.11. 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.

## Appendice E. Data di approvazione delle linee guida

### E.1. Tabella di sintesi

<b>Documento</b>	<b>Data di approvazione</b>
Linee guida per l'implementazione del processo di verbalizzazione elettronica degli esami	22 febbraio 2010
Linee guida per il fascicolo dello studente	23 giugno 2010
Linee guida per la realizzazione della cooperazione applicativa	25 maggio 2010
Linee guida per l'adozione di sistemi VoIP	25 maggio 2010
Linee guida per l'autenticazione federata per l'accesso a internet e risorse in rete	8 luglio 2010
Allegato tecnico alle linee guida per la realizzazione della cooperazione applicativa	23 giugno 2010
Specifiche tecniche di riferimento per l'implementazione di infrastrutture VoIP interoperabili	25 maggio 2010
Normativa sul VoIP	23 giugno 2010
Allegato tecnico alle linee guida per l'autenticazione federata per l'accesso a internet e risorse in rete	8 luglio 2010