ICT 4 University

Linee guida Università digitale 2012

Dipartimento per la Digitalizzazione della Pubblica Amministrazione e l'Innovazione Tecnologia

Linee guida

Università digitale

2012

Questo volume è stato curato dal Dipartimento per la digitalizzazione della Pubblica Amministrazione e l'innovazione tecnologica (Presidenza del Consiglio dei Ministri) e dal Ministero dell'Istruzione, dell'Università e della Ricerca, con il coordinamento dell'Università degli Studi del Salento. Le Linee guida sono state realizzate dalle Università partecipanti al progetto "Università digitale" previsto dal Piano eGov 2012.

Pubblicato da

Coordinamento SIBA
UNIVERSITÀ DEL SALENTO
http://siba2.unisalento.it

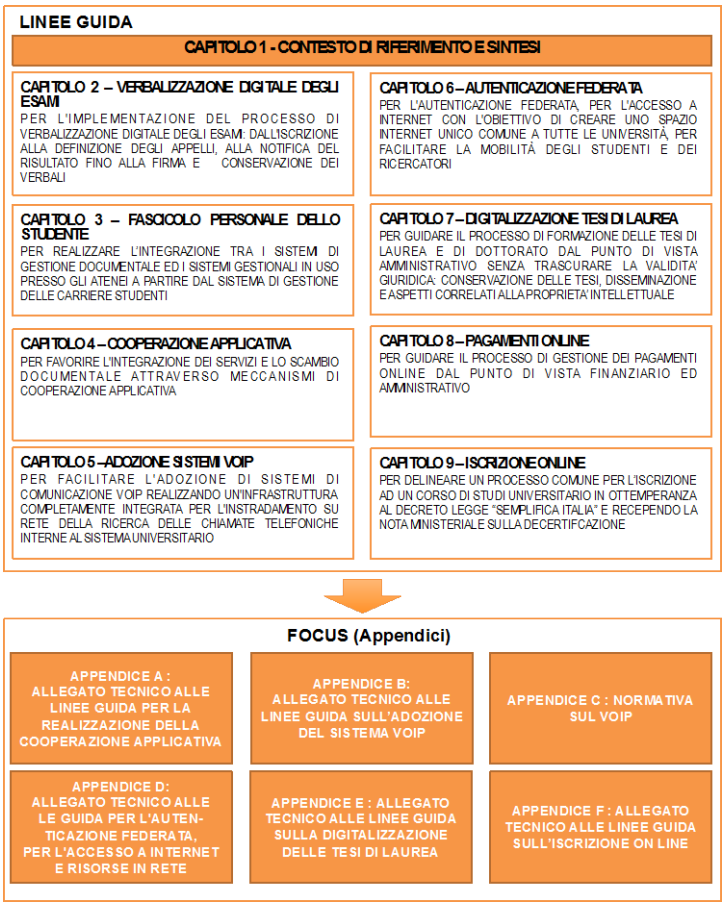
ISBN 978-88-8305-089-3 (electronic version)
http://siba-ese.unisalento.it/index.php/unidig2012/

PRESENTAZIONE DEL DOCUMENTO

LE LINEE GUIDA sono state realizzate nell'ambito del progetto "Università digitale" previsto dal Piano eGov2012.

Le Linee Guida si rivolgono a tutte le università italiane statali e non statali legalmente riconosciute e agli 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 nello schema sottostante.



1 CONTESTO DI RIFERIMENTO E SINTESI

1.1 PREMESSA

IL PIANO EGOV 2012 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 wi-fi e disponibilità di servizio VoIP in tutte le sedi".

Il progetto "Università digitale", curato dal Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica della Presidenza del Consiglio dei Ministri e dal Ministero dell'Istruzione, dell'Università e della Ricerca, si è concluso in ventisette università italiane, consentendo di accelerare il processo di digitalizzazione e semplificazione amministrativa degli atenei con l'introduzione, il potenziamento e la standardizzazione di diversi servizi: l'iscrizione on line e la verbalizzazione digitale 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 wi-fi.
Per favorire la diffusione dei risultati conseguiti all'intero sistema universitario le università partecipanti al progetto, attraverso l'istituzione di un tavolo tecnico coordinato dal Dipartimento per la Digitalizzazione della pubblica amministrazione e l'innovazione tecnologica 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:

- ✓ Linee guida per l'implementazione del processo di verbalizzazione digitale degli esami;
- ✓ Linee guida per il fascicolo dello studente;
- ✓ Linee guida per la realizzazione della cooperazione applicativa;
- ✓ Linee guida per l'adozione di sistemi VoIP;
- ✓ Linee guida per l'autenticazione federata per l'accesso a internet e risorse in rete;
- ✓ Linee guida per la digitalizzazione delle tesi di laurea;
- ✓ Linee guida per i pagamenti online;
- ✓ Linee guida per l'iscrizione online.

1.2 SINTESI DELLE LINEE GUIDA

Linee guida per l'implementazione del processo di verbalizzazione digitale 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, per:

- ✓ 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 on line 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 trasferirsi da una sede universitaria all'altra.

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'istradamento 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 (le "pagine bianche" del VoIP);
- ✓ utilizzare infrastrutture di rete pubbliche a resa prestazionale elevata e a costi contenuti;
- ✓ adottare il VoIP anche e soprattutto per fornire agli utenti servizi innovativi -mobilità, presenza, instant-messaging, comunicazione unificata, operatore automatico, rubrica on-line, conference call - capaci di 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: nella prima parte vengono indicati ambito di applicazione e viene presa in considerazione la normativa di riferimento; nella seconda si affrontano casi specifici di applicazione.

Linee guida per la formazione e conservazione di tesi di laurea magistrali e di dottorato in forma digitale

Le linee guida forniscono alcune indicazioni operative essenziali di natura amministrativa finalizzate a guidare i processi di formazione delle tesi di laurea magistrali e di dottorato in forma digitale nativa. L'attenzione è concentrata sui processi di natura amministrativa e sulla validità giuridica delle tesi, tenendo conto della natura bidimensionale delle tesi (documento amministrativo

all'interno del procedimento finalizzato al conseguimento del diploma di laurea e opera originale dell'intelletto soggetta alla tutela per il diritto d'autore). È stato, inoltre, affrontato l'aspetto della validità giuridica e della conservazione delle tesi oltre che il problema della disseminazione e degli aspetti correlati alla proprietà intellettuale.

Linee guida per i pagamenti online

Le linee guida affrontano il processo di gestione dei "pagamenti online" partendo dall'individuazione delle principali procedure che danno origine a flussi finanziari in entrata e in uscita e che impattano notevolmente sull'organizzazione e la gestione dei servizi degli Atenei. Gli obiettivi principali sono quelli di favorire:

1. la condivisione della terminologia di riferimento;
2. lo snellimento e la semplificazione dei processi e delle procedure;
3. lo snellimento della struttura amministrativa;
4. l'informatizzazione e la razionalizzazione dei processi legati ai pagamenti;
5. il miglioramento dei servizi agli studenti ed in genere agli utenti;
6. l'ottimizzazione e la completezza dei flussi informativi/garanzia di tracciabilità delle transazioni;
7. l'ottimizzazione e la completezza dei dati disponibili relativi ai pagamenti;
8. la riduzione dell'onere della gestione documentale;
9. l'individuazione di standard comuni e "buone pratiche" ("good practice") da replicare.

Linee guida per il processo di iscrizione online

Le linee guida delineano una modalità comune per la gestione del processo di iscrizione e immatricolazione presso gli atenei italiani al fine di adempiere alle disposizione del Decreto Legge "Semplifica Italia" nel rispetto anche di quanto stabilito dal codice dell'amministrazione digitale e dalla recente nota ministeriale sull'abolizione dei certificati nei rapporti fra cittadini e pubblica amministrazione. Si è inoltre tenuto conto degli aspetti legati alla normativa sulla protezione dei dati personali.

1.3 UNIVERSITÀ PARTECIPANTI AL PROGETTO "UNIVERSITÀ DIGITALE"

Denominazione Rete	Università	Denominazione Progetto
U4U- University 4 University	✓ Politecnico di TORINO (capofila) ✓ Politecnico di MILANO ✓ Università degli Studi di CATANIA ✓ Università degli Studi di FERRARA ✓ Università degli Studi di URBINO	U4U – Univertity 4 University
R. U. P. Rete delle Università Pugliesi	✓ Università degli Studi del SALENTO (capofila) ✓ Politecnico di BARI ✓ Università degli Studi diBARI ✓ Università degli studi FOGGIA	K-Student
UNI22	✓ Università degli Studi di BOLOGNA (capofila) ✓ Università degli Studi di TRENTO ✓ Università degli Studi di VERONA	Ubiversitas
Duecento SuQuattro	✓ Università degli Studi di NAPOLI "Federico II" (capofila) ✓ Università degli Studi "G. d'Annunzio" CHIETI-PESCARA ✓ Università degli Studi di MACERATA ✓ Università degli Studi di TORINO	DIGIT@UNI: Infrastrutture e servizi per il sistema universitario
Atenei Veneziani	✓ Università IUAV di Venezia (capofila) ✓ Università "Cà Foscari" di VENEZIA	Venice Wide Campus
Uni5Net	✓ Università degli Studi di PAVIA (capofila) ✓ Università degli Studi di BERGAMO ✓ Università degli Studi di FIRENZE ✓ Università degli Studi di MILANO-BICOCCA ✓ Università degli Studi di INSUBRIA VARESE-COMO	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

2 VERBALIZZAZIONE DIGITALE 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

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

2.2 Linee Guida

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 deve essere integrata con gli applicativi esistenti.

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).

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 ripor tate e comunicare tali esiti agli studenti (operazioni che possono essere svolte esattamente come descritto di seguito nel punto 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 anche 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 mail 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).

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 o rifiutare il voto. Nel caso di esami con esito non immediato lo studente, che con le modalità di cui al punto precedente 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 a diposizione (indicativamente non superiore a cinque giorni solari consecutivi) 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.

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).

Sono considerati dati del verbale "obbligatori" il codice e la denominazione dell'insegnamento, l'identificativo dell'appello, la data dell'esame (che può o meno coincidere con quella di verbalizzazione), le informazioni sui membri della commissione di esame, l'identificativo del docente verbalizzante, l'identificativo dello studente, il voto. Sono considerati dati del verbale come "addizionali" gli

argomenti di esame (che potrebbero esse re selezionati automaticamente da un insieme di domande precaricate) e le 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 consentirne la lettura nel tempo con le stesse caratteristiche estrinseche (ad esempio: modalità di impaginazione, logo, ecc.) che il documento presentava al momento della sua firma. Il formato suggerito è PDF/A1.

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) che 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 verbali 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.

Consultazione del voto da parte dello studente

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

2.3 Note conclusive

Modalità di autenticazione degli utenti:

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

- autenticazione docente - 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 - basata su username e password.

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

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 [CAD 2010]) “La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti”.

(Art.20 comma 1 [CAD 2010]) “Il documento informatico, da chiunque formato, la memorizzazione su supporto informatico e la trasmissione con strumenti telematici conformi alle regole tecniche di cui all'articolo 71 sono validi e rilevanti agli effetti di legge, ai sensi delle disposizioni del presente codice”.

Procedimento e fascicolo informatico: (Art. 41 comma 2 [CAD 2010]) “La pubblica amministrazione titolare del procedimento raccoglie in un fascicolo informatico gli atti, i documenti e i dati del procedimento medesimo da chiunque 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 2010]) “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, l’identificazione 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 2010]) “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;

e-bis) dell’identificativo del fascicolo medesimo”.

(Art. 41 comma 2-quater [CAD 2010]) “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 [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.

- 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.
- Il sistema per la gestione dei flussi documentali include il sistema di gestione informatica dei documenti.
- 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 2010) "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 nel 2010 tra gli atenei che hanno partecipato all'iniziativa Università Digitale è risultato 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; 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 risulta essere 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 in forma cartacea.

3.4 Linee guida

In conformità a quanto stabilito dalle norme gli atenei 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 aggravi 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. Altrettanto dicasi se l'istanza o la dichiarazione viene trasmessa mediante la propria casella di posta elettronica certificata (art. 65, comma 1, lettera c-bis del CAD). In entrambi i casi tuttavia le credenziali di accesso devono essere quelle di un soggetto identificato e non semplicemente auto registrato. 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*".

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, al solo fine di eliminare la presenza del/dei fascicoli cartacei in ateneo, 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, nel paragrafo 6.6 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

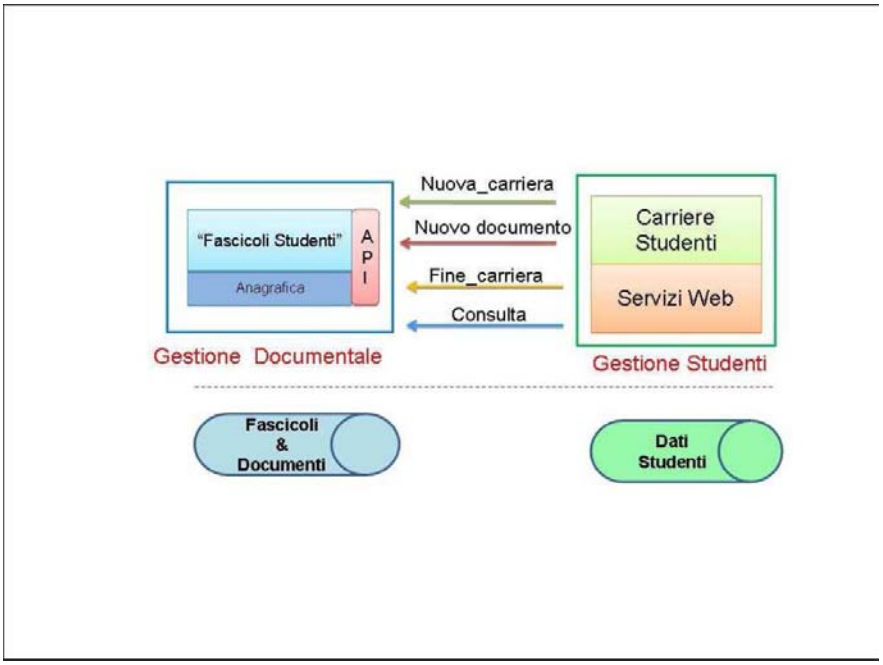
L'analisi delle piattaforme software in uso presso gli atenei e le modalità di utilizzo del sistema di gestione documentale e di protocollo da parte delle segreterie studenti, determina la necessità di individuare una soluzione tecnico-funzionale che soddisfi i seguenti requisiti:

- 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:



Evento	Processo nel sistema di gestione carriere studenti	Azioni nel sistema di gestione documentale (servizi invocati/usati)
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.

3.6 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
- ✓ 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

4 COOPERAZIONE APPLICATIVA

4.1 Premessa

IL PRESENTE documento fornisce alcune 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 alcune 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"), laddo ve 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 con-testo 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 avviene 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

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, ed è pertanto 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 extracurriculari, ecc...

- **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 oppure ha ottenuto il riconoscimento di altre attività curricolari) che eventuali altre attività extra-curriculari 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**: è la 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-curriculari che dovranno essere eventualmente convalidati per essere riconosciuti come crediti che concorrono al conseguimento del titolo. All'atto dell'iscrizione a questi corsi, allo studente viene assegnato un numero di matricola (pertanto, può capitare di averne due contempo raneamente: uno relativo all'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, ecc.).
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.

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 esempio, 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 sottosezioni:

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 (codice fiscale, nome, cognome, data e luogo di nascita, ecc...). 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, ecc.).

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: riporta innanzitutto informazioni sulla prima immatricolazione e successivamente, per ciascuna tratta, sono riportate le iscrizioni effettuate e gli esami sostenuti (o convalidati). Per ciascun esame si indica se esso è stato sostenuto o convalidato e tutti i dettagli di interesse (votazione, CFU, SSD, ecc.). 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, 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 (Appendice A)

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) 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 pro venienza 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 dovranno 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).

5 ADOZIONE SISTEMI VOIP

5.1 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 i servizi di directory disponibili, 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 intrache inter-ateneo, sfruttando tecnologie di trasmissione wireless/mobile e logiche di autenticazione federata (EduRoam, IDEM etc.).

Per quello che riguarda i vincoli normativi per l'uso dei servizi di fonia VoIP, in particolare per utenti nomadici, si rimanda alle specifiche linee guida "Aspetti

normativi delle reti IP e della comunicazione digitale" (disponibile sul sito www.ict4university.gov.it).

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 organizzazione 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 del'infrastruttura, e di facilitare la fruizione di servizi telefonici a condizioni particolarmente competitive, erogati, attraverso reti di trasporto basate su IP, da molteplici operatori.

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. Il capitolo è articolato in due parti: una contiene la descrizione generale, l'ambito di applicazione e la normativa; l'altra 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, 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 dall'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 fornisce invece una particolarizzazione 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 **eduroam ed IDEM**.

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 vi sitare senza ulteriori necessità di registrazione o configurazione (**http://www.eduro- am.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 e 5 sono garantite dall'implementazione tecnologica del componente;
- un Identity *Provider* (IDP) in eduroam
  - ✓ le condizioni 3 e 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 e 9 sono garantite dall'implementazione tecnologica del componente;
- un servizio di accesso alla rete in modalità wireless tramite la federazione IDEM
  - ✓ le condizioni 4 e 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 due 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 (uAp- prove).

7 DIGITALIZZAZIONE TESI DI LAUREA

7.1 Premessa

Le linee guida si limitano a rendere disponibili alcune indicazioni operative essenziali di natura amministrativa finalizzate a guidare i processi di formazione delle tesi di laurea magistrali e di dottorato in forma digitale nativa. L'attenzione è concentrata sui processi di natura amministrativa e sulla validità giuridica delle tesi, pur nella consapevolezza che si tratta di documenti che rispondono a una molteplicità di funzioni tale da rendere necessari in futuro ulteriori approfondimenti, in particolare in relazione agli aspetti bibliografico-documentari delle stesse. Si sottolinea infatti che non è possibile prescindere dalla natura bidimensionale delle tesi (documento amministrativo all'interno del procedimento finalizzato al conseguimento del diploma di laurea e opera originale dell'intelletto soggetta alla tutela per il diritto d'autore) e che oltre ai nodi della validità giuridica e della conservazione delle tesi è indispensabile affrontare il problema della disseminazione e degli aspetti correlati alla proprietà intellettuale.

Per l'analisi e la valutazione della normativa di settore si veda l'appendice E. Lo stato dell'arte, che include anche una sintesi sulle attuali disposizioni e prassi relative al deposito legale delle tesi e alcuni essenziali riferimenti bibliografici.

7.2 Natura giuridica delle tesi di laurea e di dottorato

Le tesi di laurea e di dottorato sono documenti giuridicamente rilevanti secondo la definizione del dpr 445/2000 (articolo 1, comma 1, lettera a): ogni rappresentazione, comunque formata, del contenuto di atti, anche interni, delle pubbliche amministrazioni o, comunque, utilizzati ai fini dell'attività.

In particolare, le dissertazioni ai fini del conseguimento di un titolo di studio universitario di livello magistrale e di dottorato sono identificati nei regolamenti universitari ma anche dalla giurisprudenza come elaborati scritti presentati e discussi dallo studente davanti a una commissione di ateneo in

seduta pubblica e conservati in originale per la consultazione negli archivi universitari[1].

In quanto documenti che svolgono una specifica funzione amministrativa (attestano la regolarità del titolo conseguito) sono riconducibili alle norme generali in materia di documento amministrativo e, in caso di digitalizzazione, alle disposizioni del citato dpr 445/2000 e del dlgs 82/2005 e successive modifiche sia per quanto riguarda la formazione del documento, la produzione di copie, la gestione e la conservazione (cfr appendice E. Lo stato dell'arte).

In particolare, coerentemente con quanto stabilito dalla normativa vigente (nello specifico ai sensi degli articoli 20 e 21 del CAD relativi al documento informatico e al documento informatico sottoscritto con firma elettronica2) e con i risultati della ricerca internazionale e degli standard di settore in materia di archivi digitali3, è necessario che siano documentati e accertabili in fase di formazione e di conservazione oltre ai documenti medesimi quegli elementi costitutivi del documento che garantiscano identificabilità dell'autore, integrità e immodificabilità. Nel caso dei documenti in questione tali elementi in parte riferibili ad informazioni di contesto, possono essere così identificati:

- la *provenienza* intesa come identificabilità dell'autore (colui che si assume la responsabilità del contenuto) o *origine* del documento[4]: l'autore studente deve essere identificato con certezza e in modo persistente

  la riconduzione del documento all'autore deve essere documentata e verificabile; trattandosi di un documento endoprocedimentale, la norma prevede l'utilizzo di qualunque tipo di firma elettronica ovvero l'insieme dei dati in forma elettronica, allegati oppure connessi tramite associazione logica ad altri dati elettronici, utilizzati come metodo di *identificazione informatica* (CAD, articolo 1, comma 1, lettera q)

---

1 Tribunale di Milano, 24 ottobre 1988, Società Zambon chimica contro Società Blaschim (Riv. Dir. Ind., 1990, II, 50, nota).

2 In particolare l'articolo 20 comma 1-bis chiarisce che "L'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità ed immodificabilità", mentre l'articolo 21 comma 1 precisa che "il documento informatico, cui è apposta una firma elettronica, sul piano probatorio è liberamente valutabile in giudizio, tenuto conto delle sue caratteristiche oggettive di qualità, sicurezza, integrità e immodificabilità".

3 Si vedano i risultati del progetto InterPARES (www.interpares.org) con specifico riferimento al profilo di autenticità e di conservazione dei documenti digitali.

4 Il nodo cruciale riguarda l'identificazione informatica dell'autore di un documento, ovvero (ai sensi dell'articolo 1, comma 1, lettera u-ter del CAD approvato con dlgs 235/2010) la validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso. Si tratta della qualificazione di un documento informatico attraverso l'associazione ad esso di alcune informazioni, con la garanzia della loro verificabilità nel tempo.

- *data certa in grado di assicurare al documento nella sua forma finale un riferimento temporale opponibile a terzi*
- *contenuto stabile*: integrità del contenuto e degli elementi identificativi della tesi,
- *persone che intervengono nel procedimento*: docente relatore, presidente e componenti della commissione di laurea; le responsabilità di tutte le persone che intervengono nel procedimento devono essere documentate e verificabili; devono essere pertanto gestite anche dal sistema di gestione documentale
- *contesto amministrativo e documentario*: si tratta degli elementi informativi che identificano l'ambito in cui la tesi è discussa (per le tesi di laurea magistrale: ateneo, facoltà, corso di laurea, intitolazione, anno accademico e data di discussione della tesi, indice di classificazione/fascicolazione, nome dello studente, nome del relatore e dell'eventuale correlatore, indicazione dell'assenso alla pubblicazione, ecc.; per le per le tesi di dottorato intitolazione del dottorato e del relativo ciclo, ateneo di riferimento, intitolazione della tesi, anno accademico e data di discussione, nome dello studente, nome del tutor, indicazioni dei componenti della commissione d'esame finale, eventuale indicazione di embargo, indice di classificazione/fascicolazione, ecc.).

> Un parere del Garante privacy (marzo 2011, n. 88) ricorda l'obbligo di adottare idonee misure per eliminare o ridurre il rischio di cancellazioni, modifiche, alterazioni o *decontestualizzazioni* delle informazioni e dei documenti resi disponibili tramite Internet.

Gli obblighi per la conservazione sono fissati dagli articoli 43, 44 e 44 bis del Codice dell'amministrazione digitale. In sintesi si stabilisce che i documenti di cui sia prescritta la conservazione per legge o regolamento, ove riprodotti su supporti informatici sono validi e rilevanti a tutti gli effetti di legge, se (art. 43, comma 3) "i documenti informatici, di cui è prescritta la conservazione per legge o regolamento, […] sono conservati in modo permanente con modalità digitali, nel rispetto delle regole tecniche stabilite ai sensi dell'articolo 71". I requisiti (articolo 44) stabiliscono:

- l'identificazione di un responsabile per la conservazione dei documenti informatici,
- la cooperazione tra il responsabile per la conservazione e il responsabile del servizio per la tenuta del protocollo informatico dei flussi documentali e degli archivi,
- l'esistenza di un sistema di conservazione che assicuri: l'identificazione certa del soggetto che ha formato il documento e della struttura amministrativa di riferimento (dati di contesto amministrativo), l'integrità del documento, la leggibilità e l'agevole reperibilità dei documenti e delle informazioni identificative, inclusi i dati di

registrazione e di classificazione originari (dati di contesto documentario).

7.3 Indicazioni operative per la formazione, gestione, tenuta e conservazione

Le indicazioni che seguono hanno l'obiettivo limitato di fornire proposte operative, alla luce delle considerazioni che precedono, per la gestione di alcuni aspetti cruciali che hanno finora ritardato l'adozione di strumenti di digitalizzazione delle tesi di laurea magistrale e di dottorato. Non hanno la presunzione di offrire ipotesi di soluzione per gli aspetti, altrettanto cruciali, riguardanti soluzioni organizzative e tecniche quali la gestione dei flussi, l'integrazione con i processi e i metadati necessari ai processi di formazione, gestione e conservazione dei documenti in questione.

Per quanto riguarda la gestione della provenienza e dei profili di responsabilità si propongono le seguenti soluzioni operative:

- **Adozione di sistemi di validazione/identificazione informatica basati sull'utilizzo di firme elettroniche (ad esempio username/password di autenticazione)** che consentano di documentare provenienza e responsabilità nel processo per l'autore della tesi (lo studente) e per tutte le persone che intervengono nelle attività di formazione e tenuta;
- **Data certa** (riferimento temporale opponibile a terzi). Si tratta della data di presentazione della tesi agli uffici di segreteria da effettuare in tempo utile per la discussione in commissione d'esame (da definire nei regolamenti di ateneo in modo da garantire che il documento conservato nei depositi d'archivio corrisponda al documento presentato e discusso in sede di esame finale). La certificazione della data nel tempo (validazione temporale, ai sensi dell'articolo 37 del dpcm 30 marzo 2009) può essere ottenuta e gestita con vari strumenti, quali ad esempio:

- ✓ la segnatura della registrazione di protocollo da effettuare in occasione della presentazione della tesi agli uffici;
- ✓ l'apposizione di una marca temporale (specifica evidenza informatica gestita dai certificatori accreditati ai sensi della delibera Cnipa 17 ottobre 2006);
- ✓ il riferimento temporale ottenuto attraverso la posta certificata**,**
- ✓ il riferimento temporale ottenuto attraverso la procedura di conservazione dei documenti e basato sull'uso di marche temporali

Nel caso delle pubbliche amministrazioni il riferimento temporale ottenuto mediante l'utilizzo della posta elettronica certificata è in ogni caso garantito dall0integrazione con il sistema di protocollo, ai sensi dell'articolo del Codice dell'amministrazione digitale

- **Contenuto stabile**: **integrità**. Valori di impronta/checksum gestiti all'interno del sistema di gestione documentale o del sistema di conservazione
- **Docente relatore**. Comunicazioni anche interne gestite nel sistema di gestione documentale al fine di assicurare il tracciamento degli atti
- **Contesto amministrativo e documentario**. La tesi dovrà essere corredata dei metadati descrittivi, amministrativi e gestionali previsti dai sistemi di gestione documentale e, nel caso delle tesi di dottorato, dalle informazioni che derivano dalle procedure di deposito legale cui le tesi medesime sono soggette per obbligo di legge[5]. Si ritiene peraltro opportuno applicare anche alla gestione delle tesi di laurea magistrale i metadati previsti per il deposito legale delle tesi di dottorato (cfr Appendice E).

Nelle more di una futura standardizzazione dei metadati di natura descrittiva e amministrativa si ricorda che è indispensabile gestire tutti gli elementi rilevanti per la gestione del procedimento amministrativo relativo e le informazioni relative alle aggregazioni documentarie e archivistiche di riferimento (fascicolo studente e serie documentaria delle tesi):

a) per le tesi di laurea magistrale si riportano almeno le seguenti indicazioni: ateneo, facoltà, corso di laurea, tipo di materiale (tesi di laurea magistrale), intitolazione della tesi, nome dell'autore, anno accademico e data di discussione della tesi, nome del relatore e dell'eventuale correlatore, lingua, abstract (eventuale), indicazione dell'assenso alla consultazione e delle sue specifiche modalità (online, offline), dimensione del file, indice di classificazione, numero del fascicolo
b) per le per le tesi di dottorato si riportano almeno le seguenti indicazioni: ateneo, intitolazione del dottorato e del relativo ciclo, intitolazione della tesi, nome dell'autore, anno accademico e data di discussione, nome del tutor, lingua, abstract (eventuale), eventuale indicazione di embargo, dimensione del file, indice di classificazione, numero del fascicolo.

Formati

La tesi deve essere predisposta in formato appropriato sia nella fase di formazione che in quella di conservazione al fine di consentire la lettura nel tempo del documento con le stesse caratteristiche estrinseche originarie

[5] Le tesi di dottorato, in relazione alla normativa sull'obbligo del deposito legale, sono soggette all'esposizione, mediante interfacce web dedicate, dei metadati concordati con le Biblioteche nazionali. Nel prosieguo dei lavori saranno indagate le procedure relative alla conservazione attuate dalle Biblioteche nazionali (in parte descritte nell'allegato E), al fine di accertare in che misura e a quali ulteriori condizioni integrative la conservazione dei documenti (digitali) si possa ritenere esaurita grazie a tali procedure.

(intestazione, modalità di impaginazione, sommario). Il dpcm 30 marzo 2009 conferma che i documenti con firma digitale o firma elettronica qualificata non producono gli effetti della scrittura privata se contengono macroistruzioni e codice eseguibile, dal momento che tale possibilità renderebbe i documenti modificabili.

I formati devono garantire l'integrità della presentazione, l'accesso e la leggibilità nel tempo del documento informatico. Si consiglia l'uso di formati aperti, tra cui per esempio il formato Pdf/A[6].

Si consiglia di valutare l'adozione di altri formati per fini diversi da quello amministrativo (per esempio il formato Open Document Format per facilitare la diffusione e l'accesso)

7.4 Conservazione

Con riferimento a quanto già indicato nel paragrafo 1 e agli obblighi normativi, si prevedono le seguenti attività:

definizione di procedure e flussi di formazione nel manuale di gestione ai sensi del dpcm 31 ottobre 2000 (regole tecniche per il protocollo informatico)

definizione del processo di conservazione e delle relative responsabilità nel manuale di conservazione coerentemente con gli obiettivi previsti dall'articolo 44 del CAD (identificazione del responsabile della conservazione, garanzia di conservazione delle caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità dei documenti conservati, con particolare attenzione per le informazioni relative ai formati utilizzati, ai metadati da associare alle tesi, ai pacchetti di versamento e di archiviazione oltre che di distribuzione, identificazione della logistica anche in caso di delega della funzione di conservazione)

delega esplicita approvata con apposito provvedimento in caso di esternalizzazione di parti del processo di conservazione.

Si specifica che nei processi di conservazione permanente i documenti possono essere oggetto di migrazioni che implicano la modifica dei formati originari. Tali interventi, finalizzati a contrastare i rischi dell'obsolescenza tecnologica e assicurare l'accessibilità e la leggibilità dei documenti conservati, devono essere condotti sotto la diretta responsabilità del responsabile della conservazione (articolo 44 CAD e successive regole tecniche sulla conservazione) ed essere opportunamente documentate sulla base di quanto indicato nel manuale di gestione e nel manuale di conservazione.

[6] Cfr. elenco formati aperti sul sito DigitPA http://www.digitpa.gov.it/sites/default/files/Repertorio%20formati%20aperti%20vers%20%201%200b_1.pdf).

7.5 Elaborati finali di laurea di primo livello

Per quanto riguarda le lauree di primo livello, in considerazione del fatto che la normativa si limita a far riferimento alla predisposizione di elaborati finali[7] e che ogni ateneo ha sviluppato prassi e regolamentazioni specifiche, non si prevedono in questa sede indicazioni univoche. Nel caso in cui l'ateneo optasse per la conservazione si suggerisce comunque

- ✓ la loro produzione in forma digitale, utilizzando formati aperti (PDF/A, Open Document Format),
- ✓ l'utilizzo di interfacce web per la consegna,
- ✓ la conservazione in sistemi Open Archives.

[7] Ai quali non si applicano le prescrizioni previste per le tesi di laurea magistrali e di dottorato.

8 PAGAMENTI ON LINE

8.1 Premessa

Lo scopo del presente documento è quello di definire le linee guida in tema di processi di gestione dei "pagamenti online" partendo dall'individuazione delle principali procedure che danno origine a flussi finanziari in entrata e in uscita e che impattano notevolmente sull'organizzazione e la gestione dei servizi degli Atenei.

Gli obiettivi principali sono quelli di favorire:

- la condivisione della terminologia di riferimento;
- lo snellimento e la semplificazione dei processi e delle procedure;
- lo snellimento della struttura amministrativa;
- l'informatizzazione e la razionalizzazione dei processi legati ai pagamenti;
- il miglioramento dei servizi agli studenti ed in genere agli utenti;
- l'ottimizzazione e la completezza dei flussi informativi/garanzia di tracciabilità delle transazioni;
- l'ottimizzazione e la completezza dei dati disponibili relativi ai pagamenti;
- la riduzione dell'onere della gestione documentale;
- l'individuazione di standard comuni e "buone pratiche" ("good practice") da replicare.

8.2 Definizioni

***PAGAMENTI**:* processi che danno origine a flussi / transazioni di denaro a favore dell'Ateneo da parte di terzi (studenti, fornitori, enti pubblici e privati, nazionali e esteri) e dall'Ateneo a favore di terzi (studenti, fornitori, pubbliche amministrazioni, enti pubblici e privati, nazionali e esteri). I processi analizzati in questo documento sono:

- i flussi in entrata e in uscita della gestione studenti, cioè gli ***incassi*** per contribuzione studentesca ed ***i pagamenti / accrediti*** a favore di studenti
- ***gli ordinativi informatici*** (mandati e reversali, pagamenti ed incassi in genere – *latu sensu*)

PAGAMENTI IN MODALITA' ONLINE: processi che prevedono sia la generazione automatica dei titoli di debito/credito da e verso gli utenti di un Ateneo che la registrazione automatica dei riscontri di pagamento e che di conseguenza

favoriscono l'ottimizzazione della gestione delle risorse (risorse finanziarie, umane, documentali,…).

PAGAMENTI IN MODALITA' CARTACEA: tutto quanto non rientra nella categoria "pagamenti in modalità online".

8.3 Stato dell'arte: incassi/accrediti da/a studenti

8.3.1 Incassi Da Studenti

Per gli incassi di tasse e contributi dovuti dagli studenti vengono usati strumenti differenti; di seguito un prospetto riassuntivo degli stessi con i rispettivi pro e i contro.

INCASSI IN MODALITA' CARTACEA

Sono considerati **incassi in modalità cartacea** quelli effettuati**:**

- allo sportello delle segreterie studenti (tramite contanti, pos,…)
- tramite bollettini, MAV,…, prodotti massivamente e spediti allo studente via posta
- tramite bonifici / bollettini CC postale con riscontro cartaceo.

STRUMENTO	PRO	CONTRO
Pagamento tramite **contanti o POS** presso lo sportello delle segreterie	Nessuno	✓ Difficile il riscontro. ✓ Liquidità, nel caso di contanti, che gli uffici devono gestire e relativi rischi di furto.
Incassi a mezzo **bollettini CC postale** o bonifici **bancari** su "autoliquidazione" da parte dello studente	Non comportano un investimento da parte dell'Ateneo di avvisi agli studenti, invii a scadenze e relativa gestione.	✓ Gli studenti devono sempre e comunque presentare copia cartacea del documento di versamento che attesti il pagamento. ✓ L'Ateneo deve conservare queste copie, con conseguente necessità di conservazione dei documenti cartacei e quindi gestione di spazi/archivi. ✓ Le attività di registrazione, necessariamente manuale, dei dati e di riconciliazione con le comunicazioni di incasso che provengono dal Tesoriere sono causa di percentuali di errore altissime, con elevato dispendio di risorse umane ed economiche.
Incassi a mezzo bollettini, MAV cartacei prodotti massivamente e spediti via posta **(**Pagamento Mediante Avviso**)**	✓ Particolarmente adatto per incassi frazionati (come le tasse e contributi degli studenti). ✓ Facilita la ricostruzione del debito e del debitore. ✓ Regola le scadenze e gli avvisi. ✓ I dati relativi ai crediti possono essere trasmessi alla banca telematicamente oltre che su supporto magnetico o cartaceo.	✓ Il costo di gestione della procedura di emissione e di trasmissione è elevato. ✓ Nei casi di mancata ricezione (recapiti errati) o di perdita del bollettino/MAV, che sono di norma molto frequenti, lo studente ricorrerebbe al pagamento mediante bollettini CC postale o bonifici bancari su "autoliquidazione" (caso precedente).

INCASSI IN MODALITA' ONLINE

Sono considerati **incassi in modalità online** quelli effettuati**:**

- tramite MAV online / bollettini generati online dallo studente durante la richiesta di iscrizione,
- tramite Carta di Credito all'interno della procedura online predisposta dall'Ateneo.

STRUMENTO	PRO	CONTRO
Carta di Credito (Pagamento all'interno della procedura online predisposta dall'Ateneo)	Immediatezza del pagamento direttamente dalla procedura online predisposta dall'Ateneo.	✓ Elevati costi di commissione. ✓ Impossibilità ad utilizzarlo come strumento esclusivo.
MAV online (MAV on demand, creato al momento della richiesta di iscrizione dello studente).	✓ L'emissione è determinata tramite una procedura informatica definita da ogni singolo ateneo. ✓ Il pagamento avvenuto con questa modalità viene acquisito automaticamente dal sistema informatico di gestione delle carriere degli studenti. ✓ Elevati risparmi di risorse finanziarie ed umane. ✓ Maggiore efficienza del sistema: – migliore gestione del servizio al cliente /studente, – miglior analisi/controllo dei dati e conseguente migliore riscossione, – maggior numero di dati disponibili, – maggiore tracciabilità dei pagamenti.	✓ Costo di avvio, principalmente per lo sviluppo delle procedure e delle piattaforme informatiche coinvolte (Tesoriere e SW gestionali degli studenti e contabili/ gestione direzionale).

8.3.2 ACCREDITI AGLI STUDENTI

Gli accrediti che un Ateneo dispone a favore degli studenti sono per:

- rimborsi di tasse e contributi non dovuti (es. restituzioni per merito, per errati pagamenti, per esoneri per reddito)
- pagamento di borse di studio (es. per merito, per reddito, per premi di studio, per collaborazioni studentesche, per mobilità internazionale, per tutela regionale del diritto allo studio)

ACCREDITI IN MODALITA' CARTACEA

Sono considerati **accrediti in modalità cartacea** quelli effettuati **:**

- in contanti presso l'istituto cassiere,
- tramite assegno bancario / circolare a domicilio.

STRUMENTO	PRO	CONTRO
Contanti con ritiro allo sportello	Nessuno	✓ Liquidità che il tesoriere deve gestire e relativi rischi di furti. ✓ Lo studente deve recarsi presso lo sportello del tesoriere e in nessun altro luogo. ✓ Difficile il riscontro.
Assegno bancario all'indirizzo	Nessuno	✓ Oneri di emissione. ✓ Alta percentuale di "mancato buon fine degli assegni". ✓ Costi di gestione dei reincassi

ACCREDITI IN MODALITA' ONLINE

Sono considerati **accrediti in modalità online** quelli effettuati**:**

- su carta prepagata d'Ateneo,
- tramite accredito CC bancario / postale.

STRUMENTO	PRO	CONTRO
Bonifico bancario	✓ Trasferimento su rete bancaria senza spostamento di denaro o altri titoli bancari. ✓ Disponibilità per lo studente nei tempi bancari	✓ Necessità di ottenere le coordinate bancarie dello studente. ✓ Alta percentuale di "mancato buon fine" perché spesso le coordinate bancarie sono errate. ✓ Costi per spese di commissione a carico dello studente.
Carta prepagata multifunzione	✓ Borse di studio e tutti i crediti maturati a qualsiasi titolo dagli studenti di un ateneo possono essere erogate sul "badge". ✓ Immediata" disponibilità della borsa. ✓ Utilizzo della carta come "bancomat" e "carta prepagata" negli esercizi convenzionati in Italia e all'estero, per transazioni via Internet, senza l'obbligo di aprire un conto corrente. ✓ L'operazione di ricarica può essere effettuata agli sportelli automatici bancomat, in tutte le agenzie con bonifico bancario oppure on-line. ✓ La carta può inoltre essere utilizzata come badge e quindi consentire l'identificazione a vista o l'abilitazione ad accedere ai servizi di Ateneo. ✓ L'accredito sulla carta è gratuito e parimenti gratuito è il prelevamento in unica soluzione di quanto accreditato presso uno sportello qualsiasi dell'Istituto Cassiere.	✓ Costo di avvio, principalmente per lo sviluppo delle procedure e delle piattaforme informatiche coinvolte (Tesoriere e S/W gestionali carriera degli studenti).

8.4 Case studies: MAV online, Carta Multifunzione, Conto Corrente Virtuale dello studente

INCASSI ONLINE: MAV online (Università Degli Studi di Milano – Bicocca)

La prima parte del progetto è iniziato, nel luglio 2008, con la realizzazione dei MAV on demand, per la riscossione delle tasse universitarie, suddivise in prima e seconda rata in occasione dell'apertura delle iscrizioni all'a.a. 2008/2009.

Secondo questo processo l'utente compila online la **domanda di immatricolazione** utilizzando per quanto possibile dei menu a tendina per l'inserimento delle informazioni e simultaneamente il sistema provvede a compilare un modulo MAV con le informazioni contenute nella domanda e che servono alla segreteria per individuare quel pagamento: dati anagrafici, corso di studio, ecc.

Al termine della domanda, viene generato un modulo MAV che, grazie ad uno scambio di informazioni in tempo reale tra la banca dati dell'Università e quella dell'Istituto Cassiere, ottiene il codice identificativo necessario per la "pagabilità" immediata del modulo all'interno del circuito ABI.

La disponibilità di questo dato consente all'utente che lo voglia, di pagare il MAV immediatamente online, senza necessità di stamparlo.

L'informazione dell'avvenuto pagamento giunge, mediante un file che contiene tutte le informazioni stampate sul mav, all'Università entro cinque giorni naturali, successivi e continui e si va ad incrociare con la domanda.

I **MAV delle seconde rate** vengono generati su richiesta online dei singoli studenti i quali vengono sollecitati da una mail inviata dall'Università alla casella di posta elettronica di ateneo.

Naturalmente lo studente si limita a richiedere il MAV di seconda rata e questo esce già precompilato. Nel caso in cui lo studente richiede la generazione del MAV oltre il termine di scadenza esso viene prodotto già con un importo che tiene conto della mora da pagare.

L'utilizzo dei MAV siffatti, ha consentito di:

- dematerializzare il processo,
- migliorare la capacità dell'Ateneo di imputare correttamente le riscossioni
- ma, principalmente, di riscuotere di più e meglio.

Con l'introduzione dei MAV è stato inoltre possibile introdurre il blocco delle carriere in caso di mancato o ritardato pagamento.

L'Università adotta un sistema di more il cui ammontare è progressivo con l'aumento del ritardo per cui ove il MAV venga generato con ritardo, come detto, il sistema lo produce tenendo conto delle more maturate fino a quel giorno. Ove venga pagato oltre il termine che fa scattare un'ulteriore mora, il sistema accetta il pagamento ma mantiene il blocco della carriera. In questo caso lo studente deve richiedere l'emissione di un nuovo MAV che gli consenta di pagare l'ulteriore mora.

A partire dall'a.a. 2009/2010 il MAV è stato adottato per tutte le riscossioni.

Tra le altre cose e nell'ottica della semplificazione è stato adottato il MAV anche per la riscossione della tassa di iscrizione e della tassa governativa per gli esami di Stato.

Secondo le disposizioni del MEF la **tassa governativa** deve essere pagata, con bollettino di conto corrente postale a favore di un conto specificamente intestato.

Sollecitati gli uffici territoriali del MEF per individuare una procedura di accredito di tali somme a cura dell'Università evitando agli utenti la necessità di recarsi agli uffici postali per il pagamento e poi in segreteria studenti per la consegna della ricevuta cartacea, questi non hanno minimamente risposto.

L'Università, per agevolare gli utenti e ridurre le code agli sportelli, ha quindi rivisto in autonomia la propria procedura ed ha introdotto nel modulo online della domanda anche la delega all'Università, da parte dell'utente che si iscrive all'esame di Stato, ad effettuare in sua vece il pagamento della tassa governativa. L'utente paga quindi con un unico MAV all'Università l'importo di tutte le tasse ed imposte dovute. L'Università, operando come sostituto d'imposta, versa mensilmente al MEF con un unico mandato e versamento l'ammontare di tutte le tasse governative riscosse ed invia allo stesso Ministero la distinta con tutti i dati anagrafici dei soggetti che hanno pagato. (Ovviamente l'Ateneo procede solo con un mandato informatico con firma digitale, successivamente la banca assolve, per conto dell'Università, al pagamento manuale di un bollettino cumulativo presso un ufficio postale).

L'introduzione di queste innovazioni, oltre a quanto già detto, ha fatto sì che annualmente circa 8000 potenziali matricole evitano di affollare gli uffici delle segreterie per ritirare i documenti cartacei per le immatricolazioni. Inoltre sono state ridotte circa 500 ulteriori presenze annue dovute ai candidati agli esami di Stato che dovevano consegnare la ricevuta dell'avvenuto versamento.

ACCREDITI ONLINE: Carta Multifunzione (Università Degli Studi di Milano – Bicocca)

Dall'inizio dell'a.a. 2009/2010 l'Ateneo distribuisce a tutte le matricole un badge, che oltre a consentire l'accesso ai parcheggi, alla biblioteca,..., è una carta di credito prepagata ricaricabile, nata dalla collaborazione tra l'Università e l'Istituto Cassiere. Se attivata, essa permette di effettuare pagamenti o prelevamenti in Italia e all'estero, di disporre pagamenti relativi ad acquisti su Internet oltre che di consentire il pagamento di piccoli importi, fino a € 15,00 ciascuno, utilizzando la tecnologia contactless (tutti gli esercizi del quartiere Bicocca sono dotati dei necessari terminali).

Libera dal conto corrente, la carta può essere attivata, senza costi aggiuntivi, presso qualsiasi filiale dell'Istituto Cassiere e non comporta l'obbligo di alcun versamento minimo.

In aggiunta, dal 2010 tutte le borse o competenze di natura economica vengono pagate dall'Ateneo agli studenti che ne hanno diritto mediante accredito sulla carta stessa. Gli studenti che devono ricevere accrediti dall'Università devono quindi attivare la funzione di Carta di Credito Prepagata, disponibile sul badge di Ateneo.

Le somme accreditate sulla carta possono anche essere prelevate, dal giorno stesso dell'accredito, attraverso i dispositivi ATM (Bancomat) o presso gli sportelli della banca. Le operazioni di pagamento sono gratuite mentre si paga un euro per ogni prelievo fino a € 250,00. Gli studenti possono comunque decidere di prelevare tutto immediatamente anche in un'unica soluzione presso la rete degli sportelli dell'Istituto Cassiere, senza costo alcuno.

Con questo sistema è possibile quindi raggiungere con il pagamento lo studente ovunque si trovi, senza peraltro dovergli chiedere alcuna informazione aggiuntiva, come le coordinate bancarie che risultano spesso difficili da ottenere e di frequente vengono comunicate erroneamente.

In particolare vengono accreditate anche le borse Erasmus in ratei fin dal primo mese della partenza dello studente. L'accredito viene disposto con il giro stipendi, sulla base della data indicata nell'atto di impegno. In caso di variazioni sulla data di partenza, lo studente la può comunicare entro il giorno 15 del mese di partenza. In caso di mancata comunicazione entro i termini, ove lo studente poi non parta, l'Ateneo è in grado di bloccare l'accredito sulla carta, sebbene sia già disposto sul mandato, entro 48 ore precedenti l'accredito sulla carta (il 25 del mese). Nel caso in cui non si riesca a bloccare l'accredito, si blocca la carriera dello studente e si richiede la restituzione immediata del dovuto.

L'accredito delle competenze mediante la carta di credito, utilizzato finora con soddisfazione quasi unanime richiede, come detto più volte, l'attivazione della funzione di carta di credito del badge universitario. Tale attivazione, che era

facoltativa per lo studente fino all'a.a. 2010/2011, faceva sì che talvolta i pagamenti non andassero subito a buon fine perché la carta di credito era ancora inattiva. Per eliminare questi problemi e stante la gratuità del prodotto, dall'a.a. 2011/2012 è obbligatoria l'attivazione della carta prepagata per tutte le matricole. Siccome l'attivazione richiede un riconoscimento dell'utente ad opera dell'Istituto Cassiere, nel rispetto della normativa antiriciclaggio, e dato che anche l'Università deve a sua volta riconoscere lo studente iscritto, prima che questi faccia esami, si è pensato di rendere obbligatoria l'attivazione della carta fin dal momento dell'immatricolazione utilizzando, d'intesa con l'Istituto Cassiere, il riconoscimento della Banca anche a fini universitari, consentendo così agli studenti di immatricolarsi e poter fare esami anche senza mai recarsi presso gli uffici di segreteria.

Quindi le circa 8000 matricole che venivano in segreteria studenti una o due volte ciascuno per ritirare i moduli (presenza fisica opzionale, in quanto potevano compilare la domanda online, quindi firmarla e spedirla corredata con la copia di un documento ed una fotografia) e poi per farsi riconoscere al momento del ritiro del libretto (presenza fisica obbligatoria), da quest'anno, avendo contestualmente abolito anche il libretto, non devono recarsi fisicamente agli sportelli dell'Ateneo e non devono nemmeno più spedire alcunché all'Università. Per completare l'immatricolazione e per attivare la sua carriera, allo studente viene solo richiesto di recarsi una volta presso lo sportello dell'agenzia dell'Istituto Cassiere, da lui scelta online e su appuntamento (anche e la data e l'ora sono scelte dallo studente con la stessa modalità online) per permettere il riconoscimento e quindi l'attivazione della carta prepagata.

Pertanto le due innovazioni tecnologiche introdotte (**mav online** e **carta prepagata**) hanno consentito di **semplificare** in modo significativo il **flusso delle immatricolazioni** e di ridurlo ai passi di seguito elencati:

- lo studente, ottenute le credenziali provvisorie dopo essersi registrato online, sempre online compila la domanda di immatricolazione, facendo l'upload di una fotografia in formato digitale;
- sempre online produce il MAV della prima rata;
- il flusso della domanda arriva all'Università (in banca dati) e si "ferma" in attesa che giunga il pagamento;
- quando arriva dalla banca il riscontro dell'avvenuto pagamento, l'Università provvede ad attivare una casella e-mail istituzionale per lo studente (lo studente conosce già indirizzo e pwd) e a inviare automaticamente i dati anagrafici e la foto, che lo studente ha fornito nella domanda online, all'Istituto Cassiere, il quale si attiva subito per produrre la carta/badge;
- una volta che la carta/badge è pronta, l'Istituto cassiere lo "comunica" (naturalmente lo scambio di informazioni avviene in modo automatizzato tra gli applicativi s/w dell'Ateneo e della banca) all'Università, che, sempre in modo automatico, invia una mail allo

studente che lo invita a fissare un appuntamento, sempre tramite procedura online, presso una filiale della banca a scelta, per attivare **tutte** le funzioni della carta di Ateneo;

- lo studente si reca in banca, ritira la carta/badge, contestualmente l'impiegato della banca provvede a stampare la domanda di immatricolazione che lo studente ha compilato, lo riconosce, gli fa firmare la stessa domanda e, a parte, tutti i moduli necessari per l'attivazione della carta prepagata.
- Espletata questa formalità, l'Istituto Cassiere comunica, sempre automaticamente, all'Università che lo studente ha completato l'attivazione delle funzionalità della carta e immediatamente viene perfezionata la sua immatricolazione.

I vantaggi economici per l'Ateneo e quelli di semplificazione dell'intero processo di immatricolazione sono molteplici, così come molti sono anche i miglioramenti economici e di qualità del servizio per gli studenti.

INCASSI ONLINE/ACCREDITI ONLINE: Conto Corrente Virtuale dello studente (Politecnico di Torino)

A partire dall'a.a. 2000/01 il Politecnico di Torino ha deciso di adottare lo strumento del conto corrente virtuale dello studente (CCS), come unico "contenitore" per il pagamento delle tasse universitarie.

Il CCS è caratterizzato da un contenitore del tutto simile ad un conto corrente bancario, associato al codice fiscale dello studente, alimentato durante gli anni di carriera dello studente.

In esso vengono inseriti movimenti "a debito" per lo studente, tipicamente: la tassa di immatricolazione, le tasse di iscrizione, le tasse per l'iscrizione all'esame di laurea e movimenti " a credito" che vanno via via a ridurre il debito dello studente. I movimenti " a credito" sono rappresentati dai versamenti che lo studente esegue nelle modalità descritte in premessa. Altri movimenti a credito vengono inseriti in corrispondenza di atti amministrativi che riducono l'importo delle tasse, ad esempio: la riduzione tasse per merito scolastico, le rimanenze di credito di precedenti carriere, altri movimenti in correzione o rimborso.

I debiti che vengono messi nel CCS, dal punto di vista della scadenza, sono di tre tipi:

- Scadenza contestuale al momento dell'assegnazione. Es. tassa di iscrizione esame di laurea, iscrizione PT : se lo studente non lo salda non porta a termine l'operazione.

- Scadenza ad una data prefissata, oltre la quale, in caso di mancato pagamento vengono assegnate delle maggiorazioni : è il caso della 1a e 2a rata di iscrizione.
- Scadenza a chiusura del CCS. Es. le maggiorazioni descritte nel punto precedente: se alla chiusura del CCS (per il 2011/12, a fine giugno 2012) esso risulta in debito, lo studente viene interdetto a qualunque funzionalità informatica, fino a quando il debito non viene saldato.

Sempre alla chiusura del CCS l'eventuale credito residuo può essere rimborsato allo studente su richiesta o, in alternativa, riversato sul nuovo a.a. di carriera dello studente.

La particolarità del CCS è che i debiti relativi alla 1a e 2a rata di iscrizione, vengono caricati nel solo momento in cui lo studente decide di andare a pagare queste tasse. In questo modo vengono minimizzate le fluttuazioni che possono essere dovute a variazioni di livello economico o ad altri eventi di esonero dalle tasse. In ogni caso, lo studente può in qualsiasi momento verificare il debito in essere.

L'utilizzo del CCS ha i seguenti vantaggi specifici, che non si riscontravano nei precedenti modelli di gestione delle tasse:

- minimizzare le fluttuazioni legate a variazioni di livello/idoneità in base alle informazioni che giungono dall'Ente Regionale Diritto allo Studio Universitario;
- minimizzare il numero di rimborsi verso gli studenti;
- gestire la trasportabilità del credito (e in certi casi anche del debito), lungo tutti gli a.a. di carriera dello studente;
- gestire con un conto unico personale più di una posizione di carriera nello stesso a.a. come accade nei passaggi dalla laurea triennale alla laurea magistrale in corso d'anno;
- consentire un'eventuale rateizzazione dei pagamenti per venire incontro alle esigenze degli studenti.

Il principale svantaggio di questo modello risiede nella complessità di gestione della rendicontazione e della reportistica contabile che comporta la ricostruzione degli importi dovuti e degli importi versati nei vari momenti dell'a.a. (per es. a chiusura dell'anno solare) a fronte dei movimenti a debito e credito che avvengono spesso in modo asincrono.

8.5 Ordinativo informatico

Un Ateneo paga e riscuote somme di denaro attraverso mandati e reversali, documenti cartacei che devono essere stampati, firmati (di solito con doppia firma), consegnati all'Istituto Cassiere o Tesoriere, da questi elaborati, caricati a sistema e inviati ai beneficiari (nel caso dei mandati di pagamento) o incrociati

con i documenti “provvisori” di registrazione in entrata e regolarizzati (nel caso delle reversali).

L’ottimizzazione dei processi di gestione di mandati e reversali è rappresentata dall’**ordinativo informatico,** che è un’evidenza elettronica, dotata di validità amministrativa e contabile, in grado di sostituire a tutti gli effetti il mandato di pagamento e la reversale.

In particolare, viene informatizzato l'iter dell'atto amministrativo che intercorre tra l'Amministrazione Universitaria, l’Ente emittente del documento e il pagamento al creditore o la riscossione dal debitore.

L'ordinativo informatico di incasso e pagamento è l'ultimo tassello del processo di automazione dei rapporti tra banche tesoriere e Pubbliche Amministrazioni, che permette a queste ultime di disporre in tempi brevi di informazioni standardizzate e confrontabili.

Le informazioni tra l'Università e la banca vengono di solito trasmesse utilizzando uno specifico **tracciato XML** e le disposizioni inoltrate sono **firmate** da persone legittimate e "conosciute" dal sistema, mediante l'identificazione del certificato elettronico preventivamente consegnato.

La firma digitale garantisce l'autenticità, la riservatezza e l'integrità delle informazioni.

Oltre ad essere firmato digitalmente, il documento contabile deve essere datato con il servizio di **marcatura temporale**: ciò consente di assegnare al documento un riferimento temporale (data ed ora) certo, opponibile ai sensi di legge. Infine il documento deve essere **conservato digitalmente**, secondo le modalità previste dalla normativa (conservazione sostitutiva).

I pro di questa innovazione possono essere così sintetizzati:

- **accelerazione** del processo di pagamento: la procedura automatizzata permette l’emissione e la trasmissione al Tesoriere di mandati informatici in tempo reale. A sua volta il Tesoriere può immettere l’ordine di pagamento sul sistema interbancario senza dover effettuare alcun ulteriore controllo manuale;
- **eliminazione dei flussi cartacei** tra Università e Istituto Cassiere, con conseguente velocizzazione e semplificazione delle operazioni di controllo sui ritorni del Cassiere per singola disposizione e per voci di aggregazione;
- garanzia di **un tempestivo monitoraggio della liquidità** dell’ente grazie alla capacità di una costante verifica dei pagamenti effettuati;
- **conservazione informatica** dei flussi di pagamento/incasso e **semplificazione delle operazioni di consultazione** (sempre disponibili online, secondo le modalità della conservazione sostitutiva);
- risparmio sul consumo di carta e di toner per stampanti.

8.6 CASE STUDY: Realizzazione e introduzione del "mandato informatico"

(Università degli Studi di Milano-Bicocca)

Per la realizzazione del progetto sono state individuate le seguenti fasi:

1. Studio di fattibilità sull'introduzione del mandato informatico in Bicocca e precisamente uno studio della normativa, delle caratteristiche del documento contabile informatico, degli standard tecnologici, delle tecnologie software di interfaccia tra gli applicativi e delle eventuali modifiche alle procedure interne utilizzate.

Queste fasi hanno coinvolto anche il fornitore del software contabile in uso in Ateneo e l'Istituto Cassiere dell'Università.

2. Creazione di un tracciato xml ben definito per la comunicazione e lo scambio di dati tra l'applicativo contabile utilizzato dall'Ateneo e quelli dell' Istituto Cassiere.

Il fornitore del software contabile ha realizzato una serie di implementazioni all'attuale procedura di contabilità finanziaria per produrre lo scarico dei dati relativi ai mandati e alle reversali emesse in formato XML - conforme alle specifiche di DigitPA per l'ordinativo informatico e in collaborazione con l'Istituto Cassiere - e per recepire ed elaborare il corrispondente file relativo alle ricevute applicative contenente gli esiti delle operazioni trasmesse.

3. Approvvigionamento dei certificati di firma digitale (per i Direttori di Dipartimento e i Segretari Amministrativi), installazione di h/w e s/w per poter apporre la firma digitale. La procedura prevede che la trasmissione dei documenti informatici sia sottoscritta con firma digitale, le chiavi di sottoscrizione devono essere rilasciate da un Certificatore accreditato.

Nel caso specifico dell'Università degli Studi di Milano-Bicocca l'Istituto Cassiere ha fornito, gratuitamente, sia le firme digitali che il servizio di conservazione sostitutiva dei documenti.

Attraverso il collegamento telematico l'Università invia i flussi generati e il Cassiere provvede a:

- marcare temporalmente il documento informatico, per assicurare data e ora certe della ricezione e la validità nel tempo del documento;
- verificare la validità formale delle sottoscrizioni e i poteri di firma;
- generare la conferma di ricezione e generare la ricevuta applicativa con indicato, per ciascun documento, l'esito dell'acquisizione ed eventuali errori riscontrati.
- archiviare il documento informatico marcato temporalmente.

4. Test condotto dall'Amministrazione Centrale per un periodo di circa tre mesi operando in parallelo con lo scambio di flussi xml con l'Istituto Cassiere e con il tradizionale invio dei documenti cartacei. In un secondo momento hanno partecipato ai test anche due Dipartimenti.

5. Estensione della procedura, in modo graduale, a tutte le Strutture dell'Ateneo dotate di autonomia contabile (Dipartimenti/Centri).

I tempi di realizzazione del progetto "ordinativo informatico", dallo studio di fattibilità (iniziato nel giugno 2009), all'entrata in produzione a regime per tutte le strutture autonome dell'Ateneo (avvenuto il 1 dicembre 2010) sono stati complessivamente di circa 1 anno e mezzo.

9 ISCRIZIONE ON LINE

9.1 Premessa

Il Decreto Legge 5/2012, entrato in vigore lo scorso 9 febbraio e comunemente noto come "Semplifica Italia", prevede (art. 48, co, 1) che le procedure di iscrizione alle Università debbano avvenire esclusivamente per via telematica.

Obiettivo delle presenti linee guida è quello di delineare una modalità comune per adempiere a tale prescrizione, nel rispetto anche di quanto stabilito dal codice dell'amministrazione digitale (le PA non devono richiedere informazioni già in proprio possesso) e dalla recente nota ministeriale sull'abolizione dei certificati nei rapporti fra cittadini e pubblica amministrazione. Si è inoltre tenuto conto degli aspetti legati alla normativa sulla protezione dei dati personali.

Nel resto del documento si userà il termine *immatricolazione* per intendere la procedura che porta all'avvio di una nuova carriera attraverso l'iscrizione a un corso di studi universitario (CdS).

Molti corsi di studio prevedono l'iscrizione ad una prova di ammissione prima di poter procedere all'immatricolazione: ciò avviene sia per i corsi ad accesso programmato che per i corsi che prevedono una prova preliminare di verifica delle conoscenze.

Data la variabilità nelle modalità di gestione di tali prove non si è ritenuto opportuno inserirne la descrizione all'interno del processo di immatricolazione, limitandosi a citarle quando necessario.

9.2 Struttura del processo

Le fasi principali del processo di immatricolazione on-line sono le seguenti:

- Registrazione al portale dell'Ateneo
- Accesso al servizio di immatricolazione previa autenticazione
- Scelta del corso di studi
- Inserimento/reperimento delle informazioni relative ai titoli di studio
- Inserimento di eventuali altre informazioni
- Calcolo della tassa di immatricolazione e conferma
- Produzione del documento riepilogativo

- Pagamento della tassa di immatricolazione
- Accertamento dell'identità personale
- Apertura fascicolo dello studente
- Verifica dei titoli autocertificati

9.3 Dettaglio delle singole fasi

9.3.1 Registrazione al portale dell'Ateneo

Questa fase è prevista solo se nel caso in cui lo studente non possieda già credenziali dell'Ateneo (tipicamente un'immatricolazione a un corso di primo ciclo).

Si possono presentare tre situazioni:

- Lo studente è in possesso di una carta di identità elettronica (CIE) o di una carta nazionale dei servizi (CNS).
- Lo studente è in possesso della Carta dello studente e delle relative credenziali.
- Lo studente, non possedendo nessuno degli strumenti sopra descritti, inserisce il proprio codice fiscale e una serie di dati anagrafici in modo da consentire al sistema di creare la prima scheda anagrafica.

Nei primi due casi l'identità della persona è da considerarsi accertata, nel terzo si renderà necessario l'accertamento in una fase successiva.

In tutti i casi il sistema, dopo aver verificato l'assenza di situazioni anomale (ad esempio una doppia registrazione), rilascia un set di credenziali (ad esempio username e password) dell'Ateneo.

9.3.2 Accesso al servizio di immatricolazione

L'accesso prevede l'autenticazione, che avviene con le credenziali rilasciate in fase di preregistrazione o con credenziali già in possesso dello studente (rilasciate ad esempio in occasione di una carriera precedente o di una prova di ammissione).

9.3.3 Scelta del corso di studi

Il sistema presenta l'offerta formativa dell'Ateneo e consente allo studente di scegliere a quale corso di studi iscriversi.

9.3.4 Inserimento delle informazioni relative ai titoli di studio

In base al tipo di CdS selezionato, l'Ateneo ha bisogno di entrare in possesso delle informazioni sui titoli di studio posseduti dallo studente, che risultano necessari per l'accesso al corso.

A questo punto si possono presentare tre casi:

- L'identità dello studente è stata accertata e lo studente ha acquisito presso l'Ateneo un titolo di studio compatibile con i requisiti di accesso al corso selezionato: i dati sono già presenti nel sistema e non devono essere richiesti.
- L'identità dello studente è stata accertata ma lo studente non ha acquisito il titolo richiesto presso l'Ateneo: il sistema può interrogare l'Anagrafe Nazionale degli Studenti Universitari (ANSU) per ottenere i dati necessari (relativi al diploma per un'immatricolazione a un corso di primo ciclo, relativi alla laurea per un corso di secondo ciclo). Se non risulta possibile recuperare i dati (ad esempio: studenti stranieri, studenti per cui non sono ancora stati resi disponibili i dati dalla scuola/università di provenienza o scartati da ANSU per qualche errore formale o di coerenza) il sistema richiede allo studente di autocertificare i titoli posseduti, rimandando la verifica a un momento successivo.
- L'identità dello studente non è stata accertata: il sistema chiede di inserire i dati necessari, ricorrendo quindi a un'autocertificazione, e rimandando la verifica a un momento successivo.

Anche nei casi in cui il sistema è in grado di recuperare automaticamente i dati necessari, lo studente dovrà comunque avere la possibilità di inserire un titolo di studio che non è stato rilevato automaticamente, se lo ritiene opportuno.

9.3.5 Inserimento di eventuali altre informazioni

In questa fase vengono richiesti dati utili per determinare le condizioni di immatricolazione.

I dati possono variare da un Ateneo all'altro e possono comprendere, a puro titolo di esempio:

1. Eventuali disabilità,
2. Stato occupazionale,
3. Eventuale tipologia di part-time
4. Questionari statistici
5. Opzioni di rateizzazione

9.3.6 Calcolo tassa di immatricolazione e conferma.

Il sistema utilizza i dati inseriti ai punti precedenti per determinare l'importo della tassa di immatricolazione e lo mostra allo studente assieme ad altri dati riepilogativi.

Lo studente può dare conferma o ritornare ai passi precedenti per apportare eventuali modifiche.

9.3.7 Produzione del documento riepilogativo

Il sistema stampa un documento che nella maggior parte dei casi serve solo come promemoria per lo studente.

Esclusivamente nel caso in cui lo studente abbia dovuto autocertificare il titolo di studio, lo studente dovrà eventualmente consegnare il documento firmato all'ateneo.

9.3.8 Pagamento della tassa di immatricolazione.

Lo studente può procedere al pagamento della rata di immatricolazione con le modalità previste dall'Ateneo. L'avvenuto pagamento ha valore di espressione di volontà relativamente all'immatricolazione.

Si auspica diffusione delle modalità di pagamento on-line oggetto delle relative linee guida.

9.3.9 Accertamento dell'identità personale

In questa fase, se lo studente non è stato identificato in precedenza, l'Ateneo (o un suo delegato), procede a verificarne l'identità.

La verifica può avvenire di persona (de visu) o tramite altre modalità compatibili con le normative relative alla gestione dell'identità personale.

Sulla base di questo riconoscimento le università possono produrre un badge/libretto con foto che servirà anche ad identificare lo studente durante la sua carriera.

Lo studente riceve anche eventuale materiale legato alla sua carriera (ad esempio badge o carta multifunzioni).

9.3.10 Apertura fascicolo dello studente.

L'accertamento dell'identità personale e il pagamento della tassa di iscrizione sanciscono il perfezionamento del processo di immatricolazione, che ha come effetto l'apertura del fascicolo personale dello studente, con le modalità descritte nelle relative linee guida.

9.3.11 Verifica dei titoli autocertificati.

A partire dal momento dell'identificazione dello studente il sistema può provvedere a verificare eventuali dati autocertificati relativi ai titoli di studio posseduti. Per far ciò utilizza le apposite funzionalità messe a disposizione dall'ANSU, sia nel caso di titoli di laurea che di diplomi di scuola secondaria superiore.

La verifica può essere fatta immediatamente dopo l'accertamento dell'identità oppure in momenti successivi secondo le modalità organizzative scelte dall'Ateneo.

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

Riepilogo dei servizi	
Denominazione	**Descrizione sintetica**
Get_Offerta()	Richiesta all'Ateneo di destinazione dei Corsi di Studio offerti
Get_InfoWorkflowTrasferimento()	Richiesta all'Ateneo di destinazione delle specifiche di ricezione Foglio di Congedo
Put_ProcessoTrasferimento()	Avvio del workflow di trasferimento presso l'Ateneo di destinazione
Require_RefreshDatiTrasferimento ()	Richiesta all'Ateneo di provenienza di re-invio/completamento del Foglio di Congedo
Put_DatiTrasferimento()	Re-invio all'Ateneo di destinazione del Foglio di Congedo
Change_StatusProcessoTrasferimento()	Notifica (all'Ateneo di provenienza o di destinazione) del cambio di stato di una domanda di trasferimento
Get_StatusProcessoTrasferimento()	Richiesta (all'Ateneo di provenienza o di destinazione) dello stato di avanzamento di una domanda di trasferimento
Ret_Token()	Notifica (all'Ateneo di provenienza) del token assegnato a una pratica ricevuta in precedenza attraverso il servizio Put_ProcessoTrasferimento()
Get_Allegato()	Accesso dell'Ateneo di destinazione agli allegati specificati all'interno di una pratica ricevuta attraverso il servizio Put_ProcessoTrasferimento()

A.2 Dettaglio dei servizi

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	- Ateneo Chiamante : Codifica MIUR - Anno Accademico di trasferimento (YYYY, es. 2009/2010 --> 2009) - Tipo di Corso (Laurea, Laurea Magistrale, Laurea Quinquennale, …): Codici_Tipo_Laurea ANS oppure "ALL" per tutti i tipi di Corso
Output	- Set di Facoltà (Tipo) e, per ciascuna di esse, set di Corsi di Studio offerti con indicazione di: ✓ Denominazione ✓ Tipo di Corso ✓ Sede di erogazione ✓ Classe ✓ Normativa (509, 270...) ✓ Data ultima di presentazione della domanda di ammissione/trasferimento ✓ Presenza di numero chiuso e/o di procedure di selezione ✓ Link alla pagina web, dell'Ateneo di destinazione, riportante ulteriori dettagli sul Corso di studi ✓ Note
Attivazione	Invocazione da parte dell'Ateneo di partenza
Esecutore	Ateneo di destinazione
Note	I parametri del servizio tengono conto delle informazioni incluse nella struttura del foglio di congedo.

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	✓Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante)
Output	✓Modalità di trasmissione del Foglio di Congedo: ✓ Completa = sezione amministrativa + sezione descrittiva della carriera ✓Token immediato/differito ✓ I= token restituito con il servizio Put_ProcessoTrasferimento() ✓ D = token restituito con il servizio Ret_Token() Altre info workflow: l'Ateneo di destinazione può fornire ulteriori informazioni relative al proprio processo di gestione della domanda di trasferimento
Attivazione	Invocazione da parte dell'Ateneo di provenienza
Esecutore	Ateneo di destinazione
Note	==

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	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ Foglio di Congedo: ✓Sezione amministrativa (sempre obbligatoria) ✓Sezione descrittiva della carriera (opzionale al primo invio, se così previsto dalle modalità di trasmissione dell'Ateneo di destinazione) ✓ 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
Output	✓Esito della richiesta di avvio del trasferimento: ✓OK ✓NOT_OK per: ✓ mancanza nel Foglio di Congedo di almeno una sezione o sottosezione obbligatoria ✓ verifica opzionale sui prerequisiti di ammissione non soddisfatti, ad esempio perché lo studente ha richiesto il trasferimento ad un Corso a numero programmato per il quale l'Ateneo di destinazione richiede il preventivo superamento di un test di ingresso ✓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. **N.B.** L'Ateneo che non fornisce il token attraverso questo servizio dovrà restituirlo successivamente invocando il servizio Ret_Token() dell'Ateneo di provenienza.
Attivazione	Invocazione da parte dell'Ateneo di provenienza
Esecutore	Ateneo di destinazione
Note	✓ Ciascuna sezione inviata (dati amministrativi o dati di carriera) deve 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. ✓ 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. Lo studente potrebbe inoltre essere ammesso ad un Corso di Studi differente da quello richiesto, in base alle regole di ammissione dell'Ateneo di destinazione. In questo caso l'informazione relativa all'effettivo Corso di studi di immatricolazione verrà (opzionalmente) comunicata tramite il servizio Change StatusProcessoTrasferimento. ✓ 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).

Servizio Require_RefreshDatiTrasferimento()	
Denominazione	Require_RefreshDatiTrasferimento
Descrizione	Il servizio viene invocato dall'Ateneo di destinazione per chiedere all'Ateneo di provenienza la ritrasmissione di un Foglio di Congedo: ✓ per ottenere la valorizzazione di informazioni opzionali; ✓ a fronte di condizioni di errore rilevate a livello applicativo nell'elaborazione del Foglio di Congedo ricevuto con la Put_ProcessoTrasferimento().
Input	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ IdPratica: identificativo della pratica di trasferimento ✓ Causale (CompletamentoInfoOpzionali, Errore, ….) ✓ Note
Output	Esito della richiesta di avvio refresh: ✓ OK ✓ NOT_OK
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	✓ Valutare la strutturazione delle causali di richiesta di ritrasmissione ✓ Definire le condizioni di errore che potrebbero determinare la necessità di ritrasmissione del Foglio di Congedo.

Servizio Put_DatiTrasferimento()	
Denominazione	Put_DatiTrasferimento
Descrizione	Il servizio viene invocato dall'Ateneo di provenienza per: ✓ ritrasmettere un Foglio di Congedo in risposta ad una richiesta notificata dall'Ateneo di destinazione mediante Require_RefreshDatiTrasferimento()
Input	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ Foglio di Congedo ✓ IdPratica: identificativo della pratica di trasferimento ✓ Causale (RitrasmissioneSuRichiesta, ….) ✓ Note
Output	- Esito della riacquisizione del Foglio di Congedo: ✓ OK ✓ NOT_OK per mancanza nel Foglio di Congedo di almeno una sezione o sottosezione obbligatoria
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 un processo di trasferimento già avviato

Servizio Change_StatusProcessoTrasferimento()	
Denominazione	Change_StatusProcessoTrasferimento
Descrizione	Il servizio viene invocato da uno dei due Atenei coinvolti nel trasferimento per propagare una transizione di stato del processo. Ad esempio per: ✓ 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); opzionalmente verrà comunicato anche il Corso di immatricolazione, che potrebbe differire da quello originario di destinazione ✓ la richiesta all'Ateneo di destinazione (da parte dell'Ateneo di provenienza) di annullare un processo di trasferimento in precedenza avviato con Put_ProcessoTrasferimento() ✓ la notifica all'Ateneo di provenienza (da parte dell'Ateneo di destinazione) del rifiuto del trasferimento.
Input	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ IdPratica: identificativo della pratica di trasferimento ✓ Nuovo stato del processo di trasferimento (ANNULLA, CHIUDI, RIFIUTA) ✓ Note
Output	✓ Esito della richiesta di change status: ✓ OK ✓ NOT_OK ✓ Corso di Studi di Immatricolazione (Campo opzionale) : Codifica ANS per i Corsi Post Riforma e ISTAT per i Corsi Ante Riforma (CorsoStudioCodD)
Attivazione	Invocazione da parte di uno dei due Atenei coinvolti nel trasferimento
Esecutore	Ateneo al quale viene notificata la transizione di stato
Note	==

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	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ IdPratica: identificativo della pratica di trasferimento
Output	✓ Set di passi seguiti dal workflow gestito internamente all'Ateneo con indicazione, per ciascuno di essi, di: ✓ Stato ✓ Data della transizione di ingresso in tale stato ✓ Note
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.

Servizio Ret_Token()	
Denominazione	Ret_Token
Descrizione	Il servizio viene invocato per fornire all'Ateneo di provenienza il token necessario allo studente per l'autenticazione presso l'Ateneo di destinazione.
Input	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ IDPratica: identificativo della pratica di trasferimento ✓ 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
Output	- OK - NOT_OK
Attivazione	Invocazione da parte dell'Ateneo di destinazione
Esecutore	Ateneo al quale viene inviato il token per il riconoscimento dello studente
Note	Questo servizio supporta la possibilità di restituire il token successivamente, anziché contestualmente, alla ricezione della pratica, in alternativa all'invio diretto attraverso il servizio Put_ProcessoTrasferimento()

Servizio Get_Allegato()	
Denominazione	Get_Allegato
Descrizione	Il servizio viene invocato dall'Ateneo di destinazione per scaricare gli allegati al foglio di congedo trasmesso attraverso il servizio Put_ProcessoTrasferimento() o Put_DatiTrasferimento()
Input	✓ Ateneo Chiamante : Codifica MIUR (MiurAteneoChiamante) ✓ IDPratica : identificativo della pratica di trasferimento ✓ IDAllegato : identificativo del documento che viene inserito all'interno del foglio di congedo da parte dell'Ateneo di provenienza
Output	✓ IDAllegato ✓ Documento allegato
Attivazione	Invocazione da parte dell'Ateneo di destinazione
Esecutore	Ateneo di provenienza che ha fornito il riferimento al documento attraverso il foglio di congedo trasmesso in precedenza
Note	Nella fase di sperimentazione sarà possibile trasferire esclusivamente documenti in formato PDF della dimensione di 200 KB. L'Ateneo di provenienza garantirà l'accesso all'Ateneo di destinazione fino alla data dichiarata nel foglio di congedo.

A.3 Casi d'uso dei Web Services

A titolo esemplificativo (gli XML Namespaces utilizzati non sono significativi), viene riportato di seguito un caso d'uso per ciascuno dei servizi.

Gli errori applicativi sono gestiti tramite l'oggetto "Esito", di ritorno da ogni chiamata del servizio.
L'oggetto è obbligatorio ed è quindi richiesto anche nel caso in cui la chiamata si concluda positivamente.

Servizio Get_Offerta() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Get_Offerta>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <Anno>2010</Anno>
     <Tipo_Tit_Univ>ALL</Tipo_Tit_Univ>
   </pol:Get_Offerta>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Get_Offerta() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Get_OffertaResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Get_OffertaResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
      <Elenco_Facolta>
        <Facolta_Tipo>
         <Cod_Tipo_Facolta>06</Cod_Tipo_Facolta>
         <Desc_Tipo_Facolta>Ingegneria</Desc_Tipo_Facolta>
         <Cdl>
           <CorsoDiStudio>
            <CodiceCorsoStudi>
              <codice classificazione="CODICIONE" descrizione="CIVIL
ENGINEERING FOR RISK MITIGATION">0150207302400006</codice>
            </CodiceCorsoStudi>
            <Classe>LM-23</Classe>
            <Normativa>ord. 270</Normativa>
            <Facolta_Specifica>INGEGNERIA - Facolta' di Ingegneria
Civile, Ambientale e Territoriale</Facolta_Specifica>
            <TipoDiCorso>MS</TipoDiCorso>
```

```
            <Sede>15146</Sede>

<ScadenzaDomandaTrasferimento>01012011</ScadenzaDomandaTrasferimento>
            <NumeroChiuso>SI</NumeroChiuso>
            <ProcedureSelezione>SI</ProcedureSelezione>
            <IndirizzoWeb>http://www.master-
riskmanagement.lecco.polimi.it/</IndirizzoWeb>
            <Note>ATTENZIONE CORSO NON ATTIVO SU TUTTI GLI ANNI. ANNI
DISPONIBILI : 1
CORSO OFFERTO SULLA SEDE DI LECCO</Note>
          </CorsoDiStudio>
       <CodiceCorsoStudi>
                    ……
       </CorsoDiStudio>
        </Cdl>
</Facolta_Tipo>
<Facolta_Tipo>
         <Cod_Tipo_Facolta>07</Cod_Tipo_Facolta>
         <Desc_Tipo_Facolta>Architettura</Desc_Tipo_Facolta>
         <Cdl>
           <CorsoDiStudio>
            <CodiceCorsoStudi>
              <codice classificazione="CODICIONE" descrizione="DESIGN
&amp;amp; ENGINEERING">0150207301300008</codice>
            </CodiceCorsoStudi>
            <Classe>LM-12</Classe>
            <Normativa>ord. 270</Normativa>
            <Facolta_Specifica>DESIGN - Facolta' del
Design</Facolta_Specifica>
            <TipoDiCorso>MS</TipoDiCorso>
            <Sede>15146</Sede>

<ScadenzaDomandaTrasferimento>01012011</ScadenzaDomandaTrasferimento>
            <NumeroChiuso>SI</NumeroChiuso>
            <ProcedureSelezione>SI</ProcedureSelezione>
            <IndirizzoWeb>www.design.polimi.it</IndirizzoWeb>
            <Note>ATTENZIONE CORSO NON ATTIVO SU TUTTI GLI ANNI. ANNI
DISPONIBILI : 1
CORSO OFFERTO SULLA SEDE DI MILANO BOVISA</Note>
          </CorsoDiStudio>
          <CodiceCorsoStudi>
                    ……
       </CorsoDiStudio>
        </Cdl>
</Facolta_Tipo>
</Elenco_Facolta>
     </ns2:Get_OffertaResult>
   </polij:Get_OffertaResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Get_InfoWorkflowTrasferimento() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
```

```
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Get_InfoWorkflowTrasferimento>/
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
   </pol:Get_InfoWorkflowTrasferimento>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Get_InfoWorkflowTrasferimento() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Get_InfoWorkflowTrasferimentoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Get_InfoWorkflowTrasferimentoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
      <InfoWorkflow>
        <ModalitaTrasmissione>Completa</ModalitaTrasmissione>
        <ModalitaToken>I</ModalitaToken>
        <AltreInfo>NESSUNA INFO AGGIUNTIVA</AltreInfo>
      </InfoWorkflow>
     </ns2:Get_InfoWorkflowTrasferimentoResult>
   </polij:Get_InfoWorkflowTrasferimentoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Put_ProcessoTrasferimento() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Put_ProcessoTrasferimento>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>POLIMI20100000052</IdPratica>
     <FoglioCongedo>
          ….
     </FoglioCongedo>
</pol:Put_ProcessoTrasferimento>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Put_ProcessoTrasferimento() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
```

```
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij: Put_ProcessoTrasferimentoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2: Put_ProcessoTrasferimentoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
      <Token>58968742</Token>
     </ns2: Put_ProcessoTrasferimentoResult>
   </polij: Put_ProcessoTrasferimentoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Require_RefreshDatiTrasferimento() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Require_RefreshDatiTrasferimento>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>POLIMI20100000056</IdPratica>
     <Causale>ERRORE</Causale>
     <Note>Richiediamo ritrasmissione per errore</Note>
   </pol:Require_RefreshDatiTrasferimento>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Require_RefreshDatiTrasferimento() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Require_RefreshDatiTrasferimentoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Require_RefreshDatiTrasferimentoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
     </ns2:Require_RefreshDatiTrasferimentoResult>
   </polij:Require_RefreshDatiTrasferimentoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Put_DatiTrasferimento() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Put_DatiTrasferimento>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>POLIMI2010000052</IdPratica>
     <FoglioCongedo>
         ....
     </FoglioCongedo>
     <Causale>ERRORE</Causale>
     <Note>nota</Note>
   </pol:Put_DatiTrasferimento>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Put_DatiTrasferimento() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij: Put_DatiTrasferimentoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2: Put_DatiTrasferimentoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
     </ns2: Put_DatiTrasferimentoResult>
   </polij: Put_DatiTrasferimentoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Change_StatusProcessoTrasferimento() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Change_StatusProcessoTrasferimento>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>POLIMI2010000001</IdPratica>
     <StatoChange>ANNULLA</StatoChange>
     <Note>NOTA</Note>
   </pol:Change_StatusProcessoTrasferimento>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Change_StatusProcessoTrasferimento() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Change_StatusProcessoTrasferimentoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Change_StatusProcessoTrasferimentoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>1</codEsito>
        <descEsito>PRATICA NON TROVATA</descEsito>
      </esito>
     </ns2:Change_StatusProcessoTrasferimentoResult>
   </polij:Change_StatusProcessoTrasferimentoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Get_StatusProcessoTrasferimento() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Get_StatusProcessoTrasferimento>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>POLIMI20100000000462</IdPratica>
   </pol:Get_StatusProcessoTrasferimento>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Get_StatusProcessoTrasferimento() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Get_StatusProcessoTrasferimentoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Get_StatusProcessoTrasferimentoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
      <Passi>
        <Passo>
         <Stato>BOZZA</Stato>
         <DataTransazione>02/12/2010</DataTransazione>
        </Passo>
```

```
      </Passi>
     </ns2:Get_StatusProcessoTrasferimentoResult>
   </polij:Get_StatusProcessoTrasferimentoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Ret_Token() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Ret_Token>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>UNISA20100000053</IdPratica>
     <Token>55555555</Token>
   </pol:Ret_Token>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Ret_Token() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Ret_TokenResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Ret_TokenResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
       </esito>
     </ns2:Ret_TokenResult>
   </polij:Ret_TokenResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

Servizio Get_Allegato() - Esempio chiamata

```
<soapenv:Envelope
xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
xmlns:pol="http://www.ceda.polimi.it/polij/">
  <soapenv:Header/>
  <soapenv:Body>
   <pol:Get_Allegato>
     <MiurAteneoChiamante>16</MiurAteneoChiamante>
     <IdPratica>POLIMI20100000052</IdPratica>
     <IdDocumento>1235892</IdDocumento>
   </pol:Get_Allegato>
  </soapenv:Body>
</soapenv:Envelope>
```

Servizio Get_Allegato() - Esempio risposta

```
<SOAP-ENV:Envelope xmlns:SOAP-
ENV="http://schemas.xmlsoap.org/soap/envelope/" xmlns:SOAP-
ENC="http://schemas.xmlsoap.org/soap/encoding/"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <SOAP-ENV:Body>
   <polij:Get_AllegatoResponse xmlns:jax-
ws="http://www.ceda.polimi.it/polij/jax-ws/"
xmlns:polij="http://www.ceda.polimi.it/polij/">
     <ns2:Get_AllegatoResult
xmlns:ns2="http://www.ict4university.gov.it/">
      <esito>
        <codEsito>0</codEsito>
        <descEsito>OK</descEsito>
      </esito>
      <idPratica>POLIMI20100000000462</idPratica>
      <idAllegato>1235892</idAllegato>
      <allegato>YWFhYQ==</allegato>
     </ns2:Get_AllegatoResult>
   </polij:Get_AllegatoResponse>
  </SOAP-ENV:Body>
</SOAP-ENV:Envelope>
```

A.4 Esemplificazione del processo di trasferimento basato sulla cooperazione applicativa

A.4.1 Uscita: gestione della domanda di trasferimento da parte dell'Ateneo di provenienza

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 Get_Offerta(), esposto dall'Ateneo scelto dallo studente, per ottenere l'elenco del Corsi di Studio offerti ed utilizzabili ai fini del trasferimento nell'AA specificato. Le informazioni possono essere recuperate da una interrogazione contestuale all'inserimento della domanda da parte dello studente o creando una cache attraverso tasks programmati in orari prestabiliti.
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, classe, normativa (509, 270...), sede di erogazione;
- eventuale obbligo di test di ammissione;
- data limite per la presentazione della richiesta di trasferimento;

- link alla pagina web dell'Ateneo di destinazione, riportante ulteriori dettagli sul Corso di studi;
- eventuali note.

I Corsi di Studio a numero programmato, che richiedono il superamento di una prova di ammissione, sono opportunamente evidenziati/corredati di note 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. 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/MAV 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, come già indicato, a: "domanda in bozza" se la domanda non è ancora stata completata; "domanda presentata" dopo la conferma.

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:

- ✓ Modalità di trasmissione del Foglio di Congedo
  - o Completo: deve essere inviato il Foglio di Congedo completo sia della sezione amministrativa, sia della sezione della carriera.
- ✓ Modalità di assegnazione del Token:
  - o Immediato: token restituito con il servizio Put_ProcessoTrasferimento()
  - o Differito: token restituito con il servizio Ret_Token()
- ✓ Altre informazioni:
  - o eventuali ulteriori informazioni relative al proprio processo di gestione della domanda di trasferimento.

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. Nel caso l'Ateneo di destinazione abbia indicato la modalità differita di assegnazione del token, comunicherà, come output dell'invocazione del servizio Put_ProcessoTrasferimento(), solo l'esito della ricezione della domanda; invierà il token in un tempo successivo tramite il servizio Ret_Token(). In entrambi i casi, 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 (se già assegnato) per accedere al sistema dell'Ateneo di destinazione. Se il token non è ancora stato assegnato, gli verrà dato apposito messaggio. Lo studente visualizzerà l'avanzamento dello stato della domanda, come descritto al paragrafo successivo. 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, …).

L'elaborazione del Foglio di Congedo da parte della Segreteria dell'Ateneo di destinazione può mettere in evidenza altre anomalie 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.

Opportuno, dopo la fase di sperimentazione, 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", 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 invio della sezione di carriera a completamento di precedente trasmissione della sola sezione amministrativa di un Foglio di Congedo.

Ad ogni nuovo invio corrisponde un nuovo numero di protocollo.

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.

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.

Chiusura/rifiuto della domanda di trasferimento in uscita

L'Ateneo di destinazione, al termine dell'iter di valutazione della carriera dello studente, notifica il completamento o, in alternativa, il rifiuto 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.4.2 Ingresso: gestione della domanda di trasferimento da parte dell'Ateneo di destinazione

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 invocando l'apposito servizio Put_ProcessoTrasferimento(). 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. Può inoltre verificare già a questo livello la presenza/superamento del test di ingresso per i Corsi di Studio per i quali è obbligatorio, basando il controllo 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. Se la gestione del workflow dell'Ateneo di destinazione prevede l'assegnazione differita del token, questo verrà comunicato successivamente all'Ateneo di provenienza, tramite il servizio Ret_Token().

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”. Il foglio di congedo potrebbe prevedere degli allegati, ciascuno identificato da un IDAllegato, relativi ad esempio ad informazioni non strutturate. L’Ateneo di destinazione può accedere agli allegati del foglio di congedo tramite il servizio Get_Allegato(). L’accesso è garantito fino ad una data limite, anch’essa indicata nel foglio di congedo.

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”.

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 conferma di 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 sia stata effettuata dallo studente prima dell'avvio della domanda di trasferimento, fenomeno 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.

Proprio in relazione agli eventuali vincoli sugli accessi ai Corsi di Studio dell'Ateneo di destinazione, si può verificare che l'immatricolazione venga consentita per un Corso di Studi diverso da quello originario di destinazione. Tale informazione potrà essere comunicata all'Ateneo di provenienza tramite il servizio Change StatusProcessoTrasferimento().

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().

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).

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.

Completamento/rifiuto 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" o "rifiutata"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/rifiuto del trasferimento all'Ateneo di provenienza invocando il servizio ChangeStatus_ProcessoTrasferimento() comunicando l'identificativo della pratica, lo stato "completamento" (valorizzando il parametro StatoChange a "Chiudi") o "non accoglimento della domanda" (valorizzando il parametro StatoChange a "Rifiuta") e data e ora del cambio di stato.

A.5 Foglio excel

Nel foglio excel rilasciato unitamente alle linee guida:

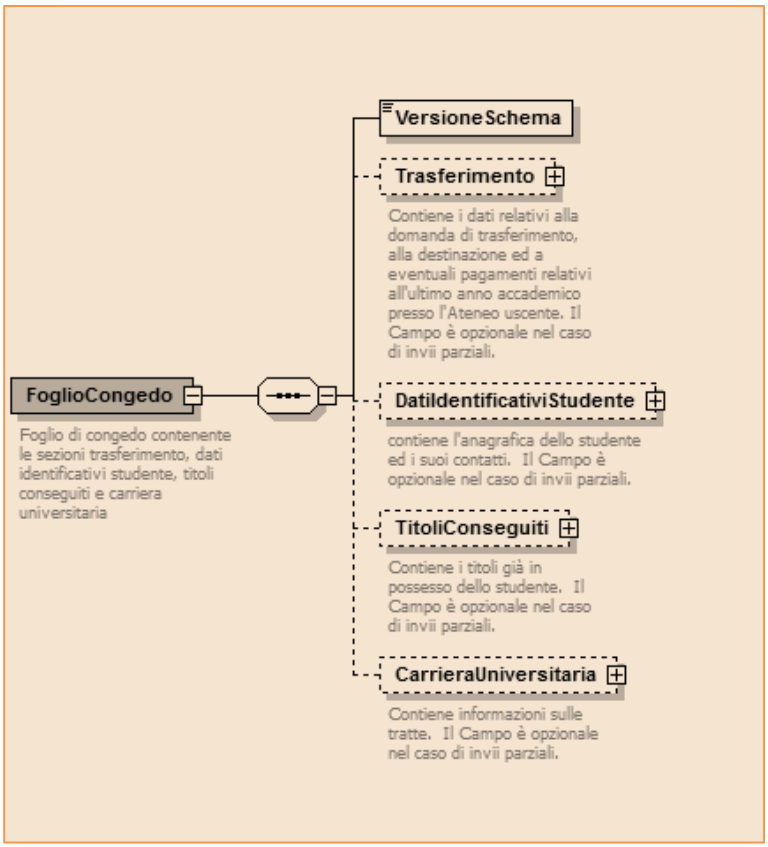
http://www.ict4university.gov.it/temi-universita-digitale/architettura-applicativa.aspx

è possibile visionare in forma testuale tutte le informazioni inserite nello schema xsd con i relativi commenti.

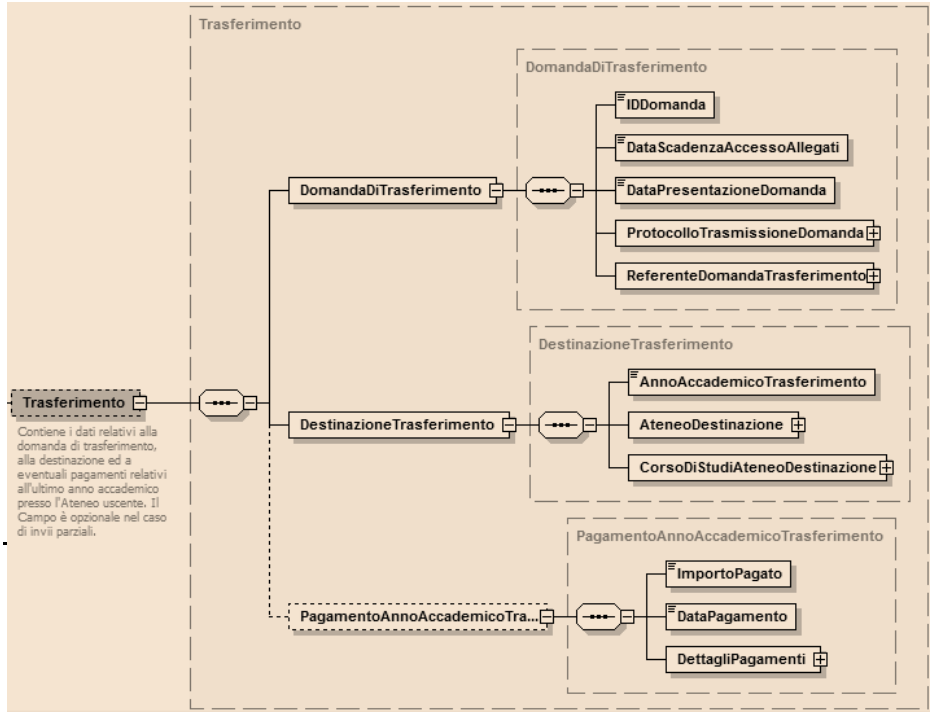
A.6 Schema xsd

Si riportano di seguito alcuni screen shot dello schema xsd prodotto (versione 1.05).

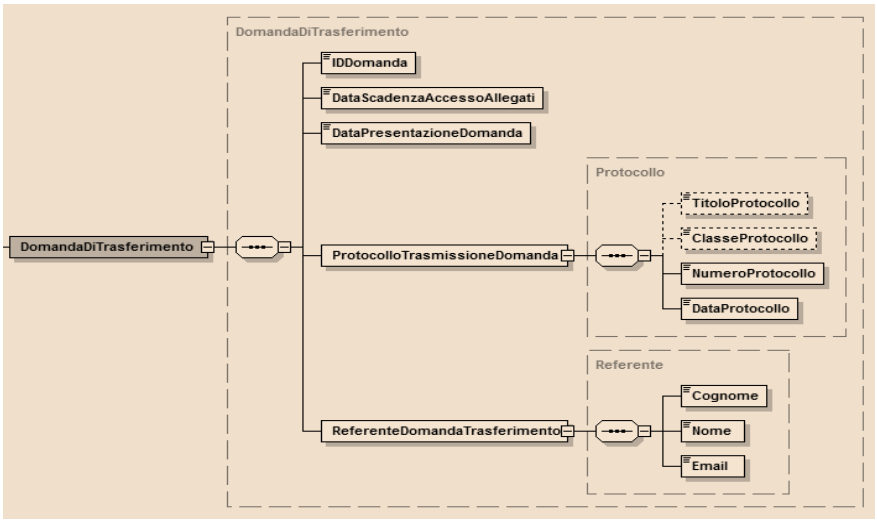
✓ Schema xsd del nodo “FoglioCongedo”



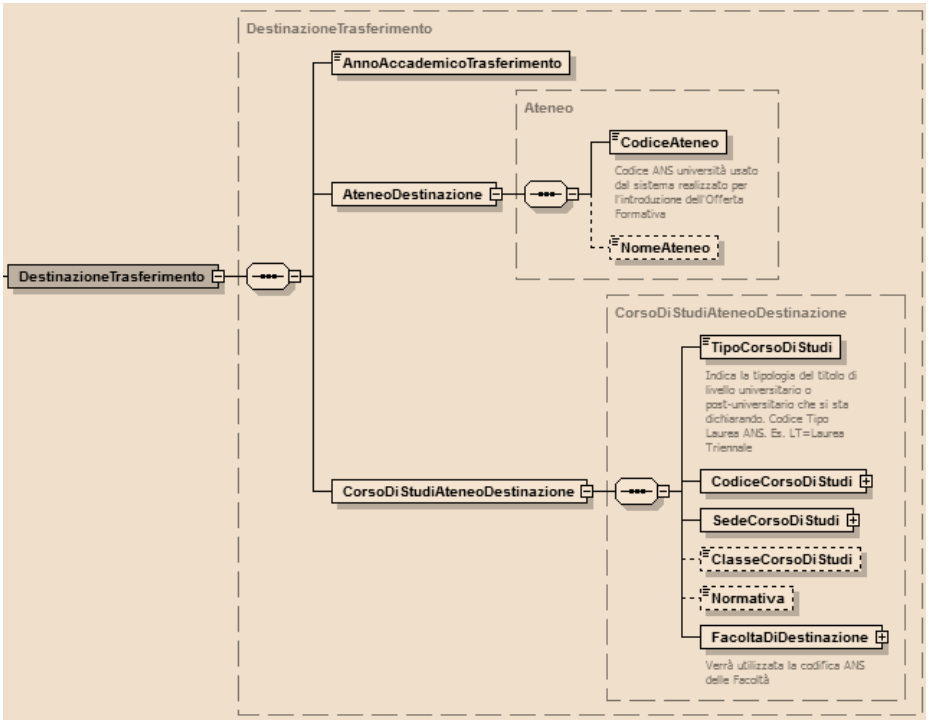
✓ Schema xsd del nodo “Trasferimento”.



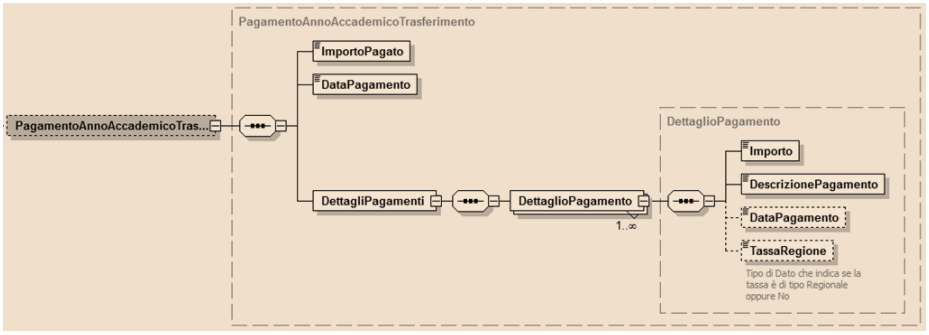
- ✓ Schema xsd del nodo “DomandaDiTrasferimento”.



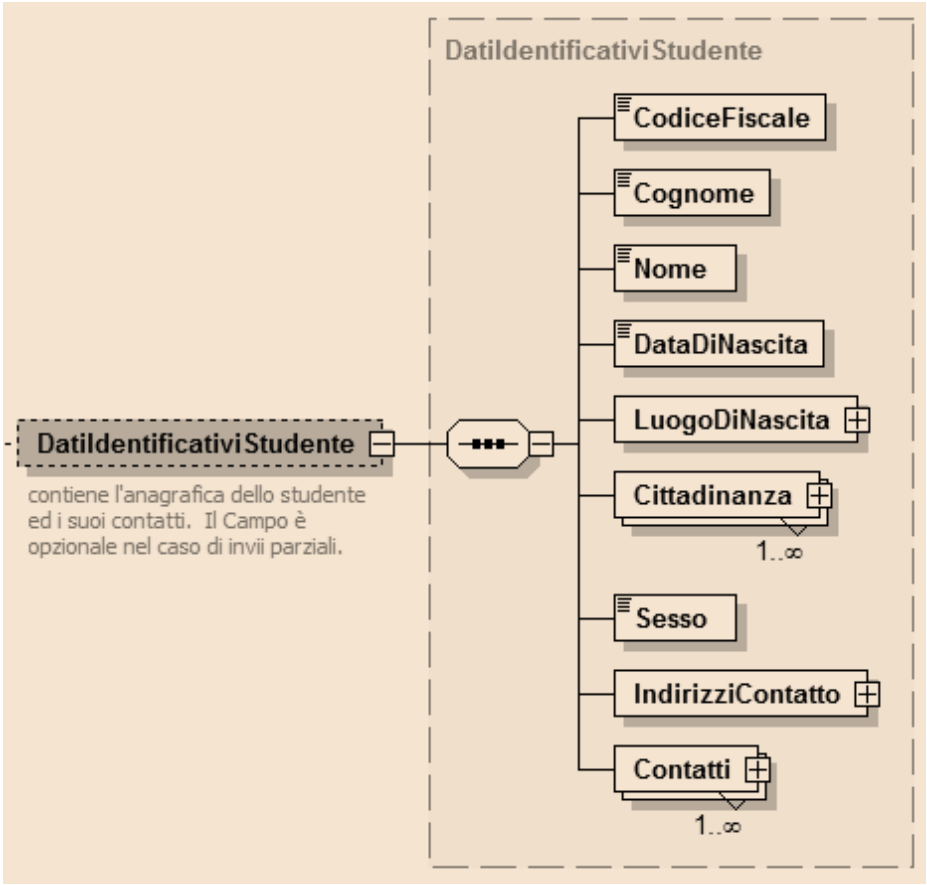
- ✓ Schema xsd del nodo “DestinazioneTrasferimento



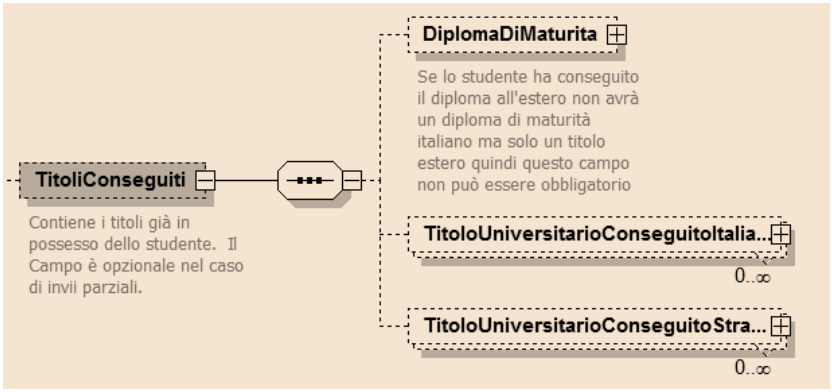
- ✓ Schema xsd del nodo “PagamentoAnnoAccademicoTrasferimento



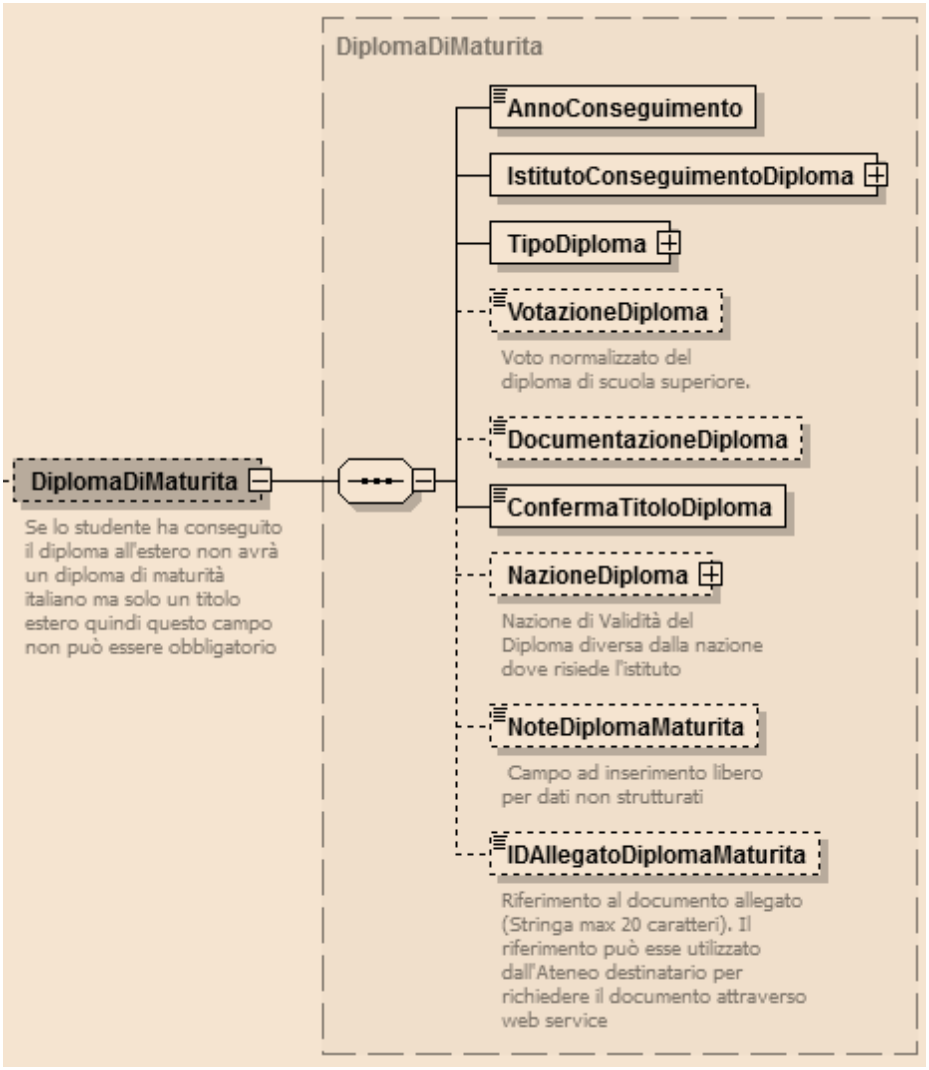
✓ Schema xsd del nodo “DatiIdentificativiStudente”.



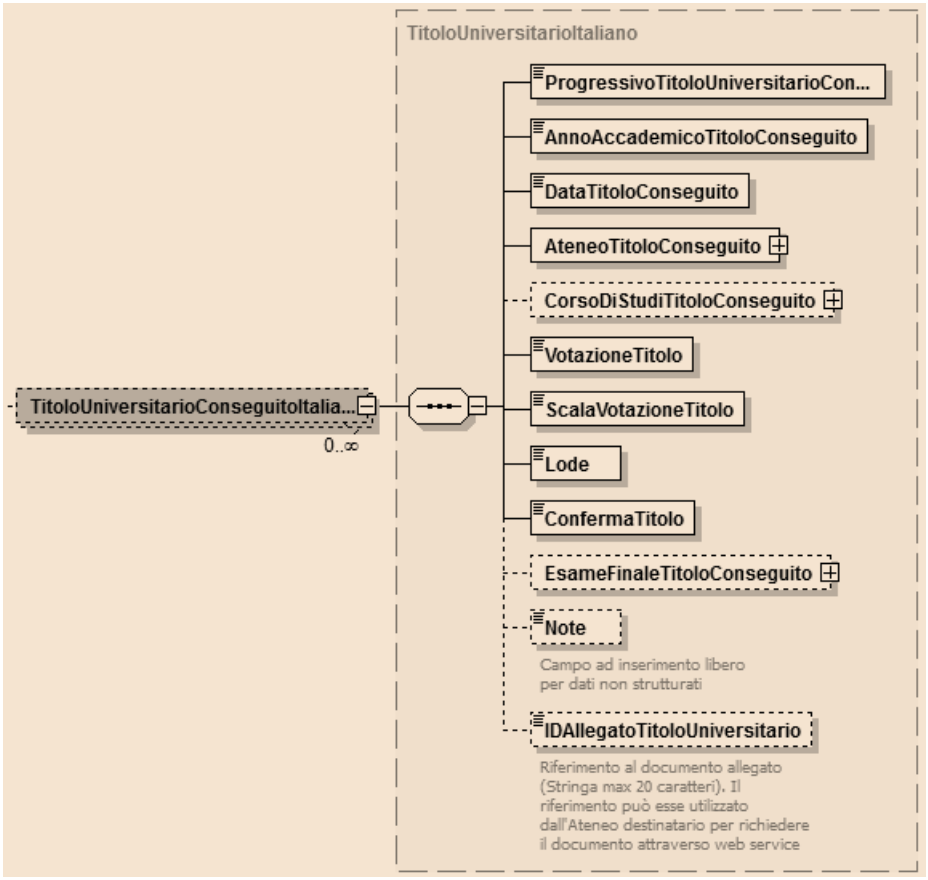
✓ Schema xsd del nodo “TitoliConseguiti”.



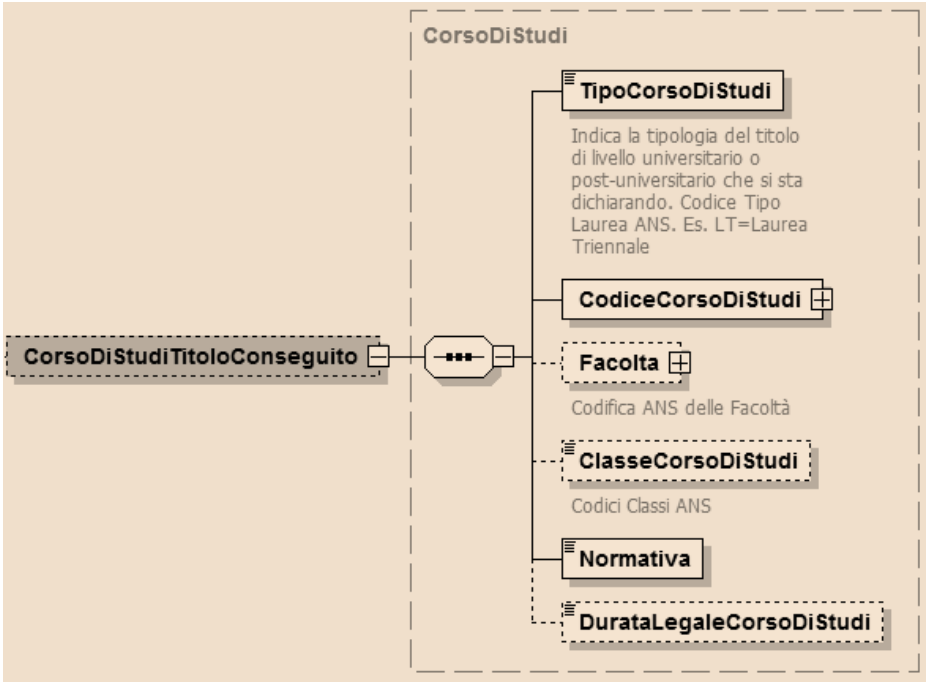
✓ Schema xsd del nodo “DiplomaDiMaturita


DiplomaDiMaturita
AnnoConseguimento
IstitutoConseguimentoDiploma
TipoDiploma
VotazioneDiploma
Voto normalizzato del diploma di scuola superiore.
DocumentazioneDiploma
DiplomaDiMaturita
ConfermaTitoloDiploma
NazioneDiploma
Nazione di Validità del Diploma diversa dalla nazione dove risiede l'istituto
NoteDiplomaMaturita
Campo ad inserimento libero per dati non strutturati
IDAllegatoDiplomaMaturita
Riferimento al documento allegato (Stringa max 20 caratteri). Il riferimento può esse utilizzato dall'Ateneo destinatario per richiedere il documento attraverso web service
Se lo studente ha conseguito il diploma all'estero non avrà un diploma di maturità italiano ma solo un titolo estero quindi questo campo non può essere obbligatorio

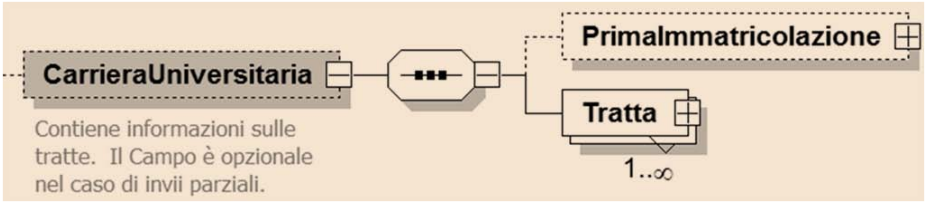
- ✓ Schema xsd del nodo “TitoloUniversitarioConseguitoItaliano”.



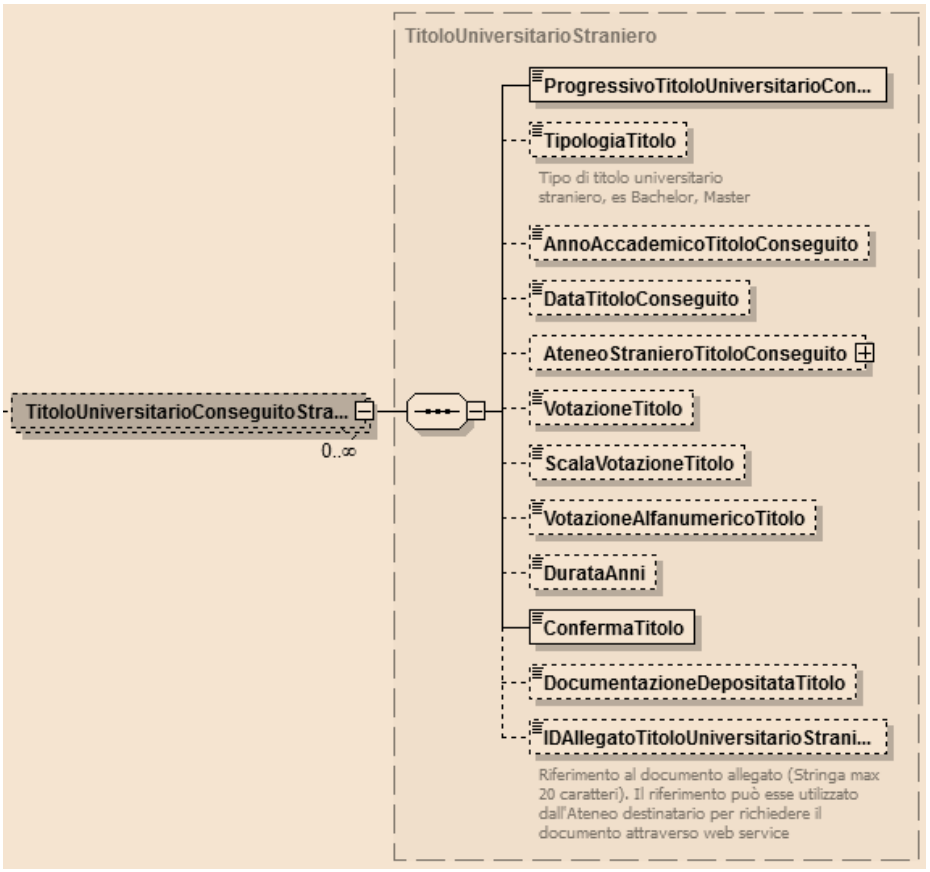
- ✓ Schema xsd del nodo “CorsoDiStudiTitoloConseguito”.



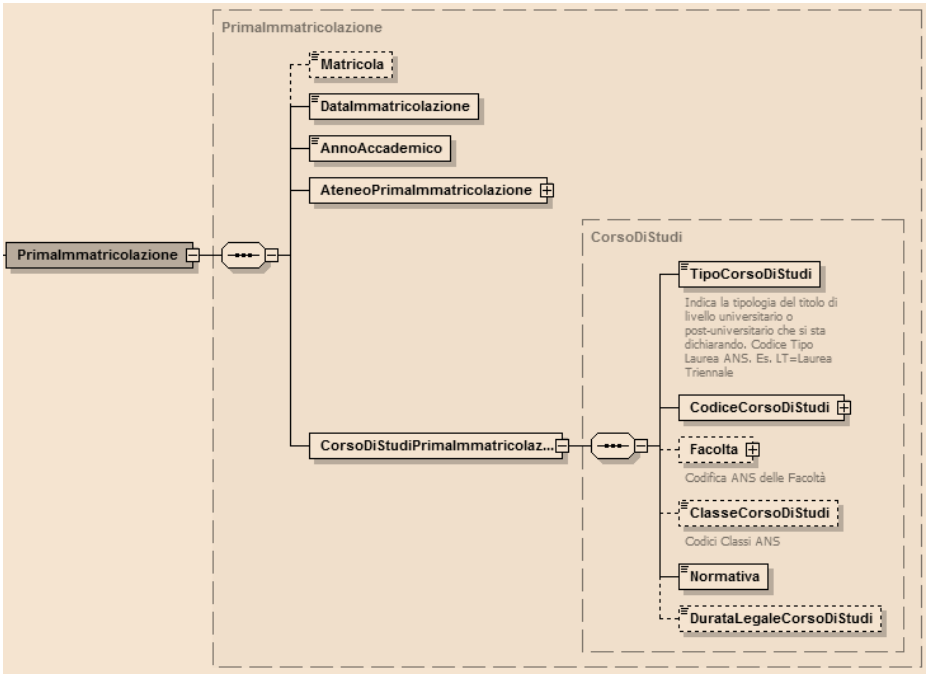
- ✓ Schema xsd del nodo “CarrieraUniversitaria”.



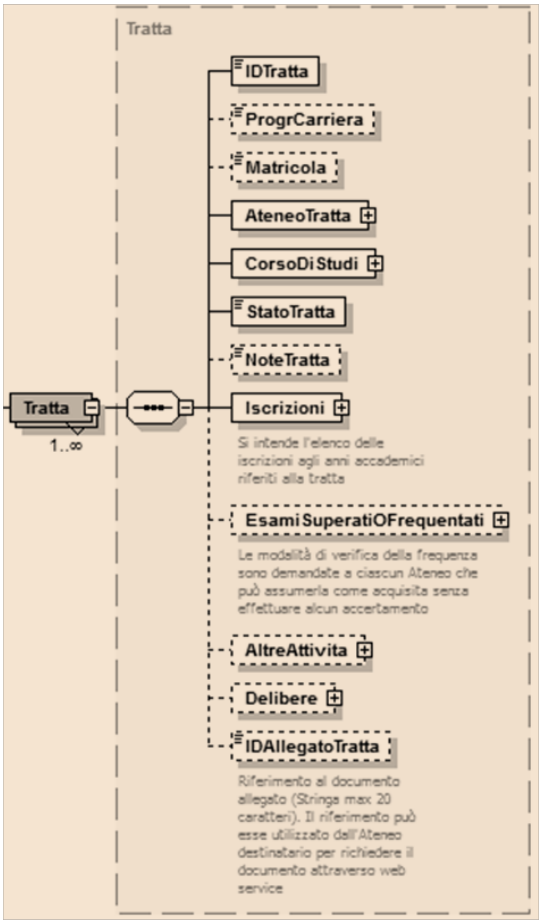
- ✓ Schema xsd del nodo “TitoloUniversitarioConseguitoStraniero”.



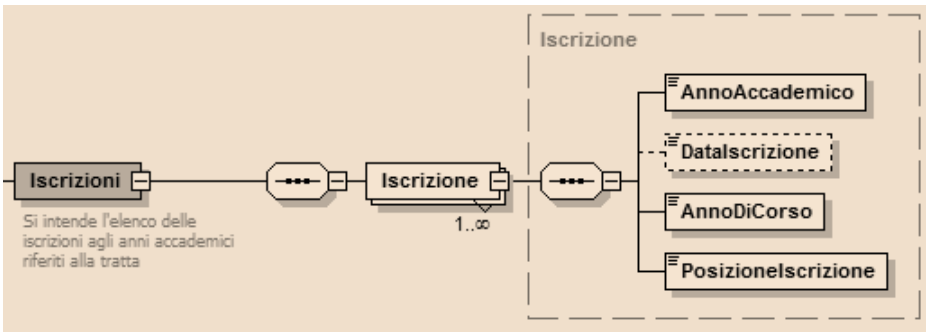
✓ Schema xsd del nodo “PrimaImmatricolazione”.



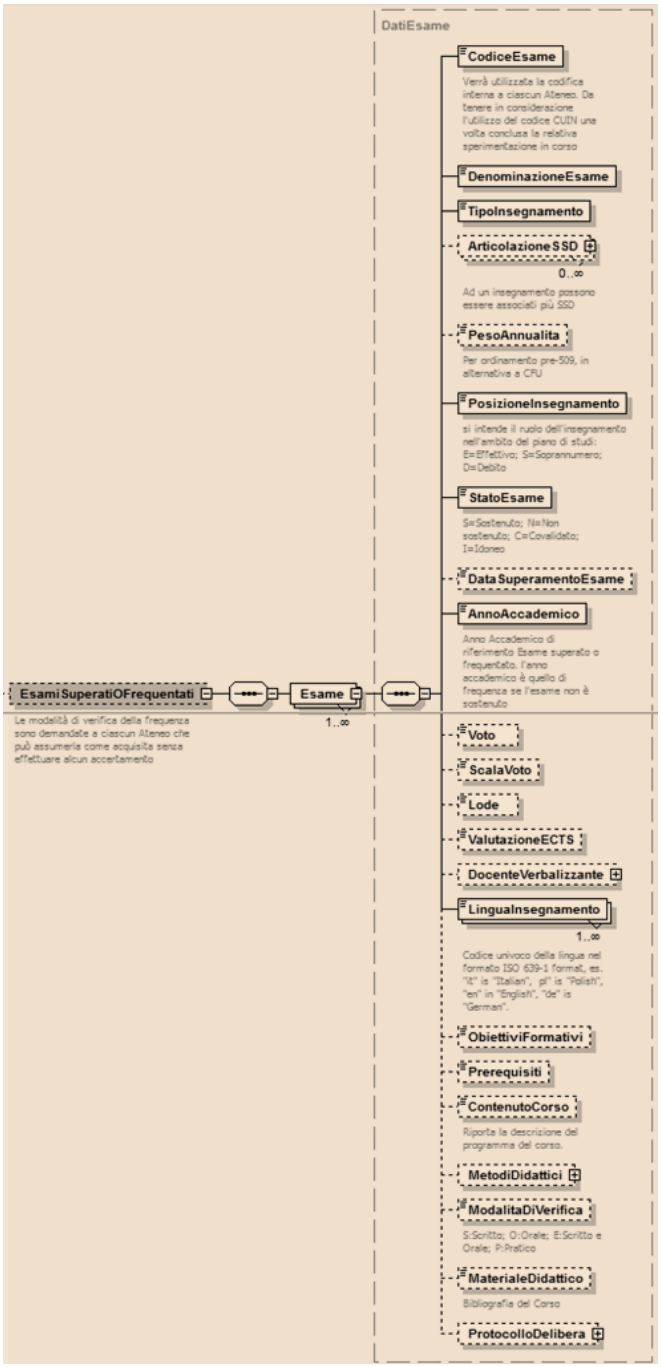
✓ Schema xsd del nodo “Tratta”.



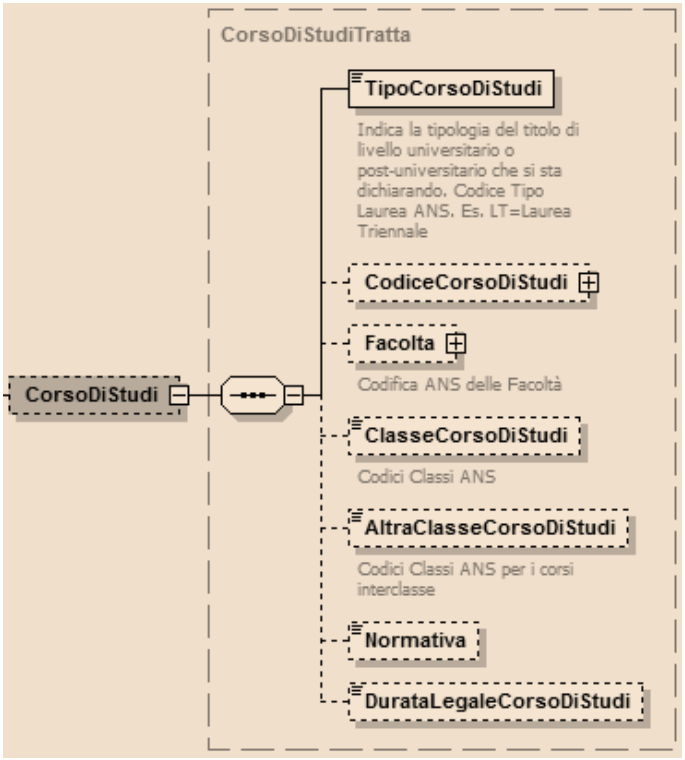
✓ Schema xsd del nodo “Iscrizioni”.



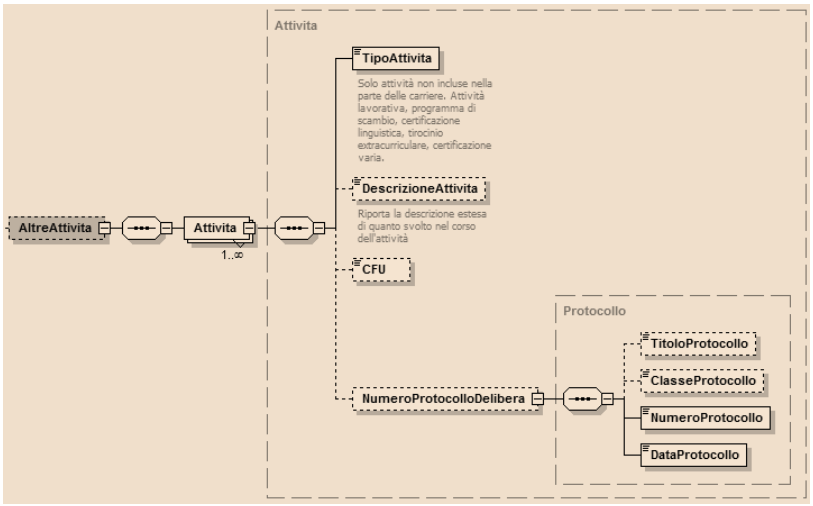
✓ Schema xsd del nodo “EsamiSuperatiOFrequentati”.



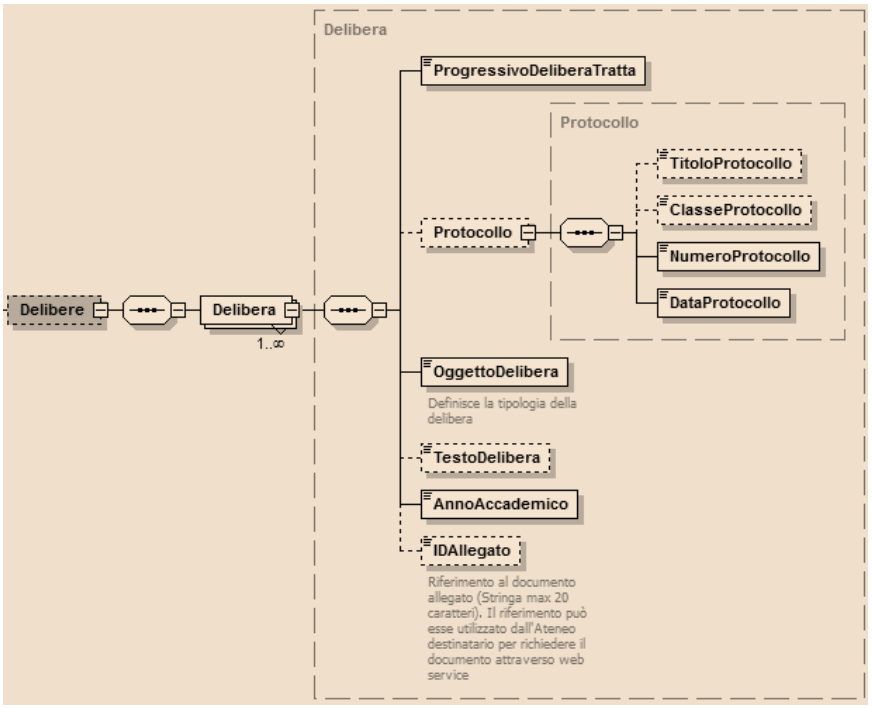
✓ Schema xsd del nodo “CorsoDiStudi”.



- ✓ Schema xsd del nodo “AltreAttivita”.



- ✓ Schema xsd del nodo “Delibere”.



A.7 Schemi WSDL

Dai servizi precedentemente identificati e dalla formalizzazione dei dati del foglio di congedo sono stati desunti rispettivamente lo schema dati dei servizi

(FoglioCongedoDestinazioneSoapService_schema1_Ver1.04.xsd) e il relativo WSDL (FoglioCongedoDestinazioneSoapService_Ver1.04.wsdl).

A.8 Integrazione dei servizi ANS all'interno del processo di trasferimento

I servizi ANS, così come descritti nell'allegato AllegatoTecnicoWebServicesANS.pdf (disponibile al link **http://www.ict4university.gov.it/temi-universita-digitale/architettura-applicativa.aspx)** saranno oggetto di valutazione da parte del gruppo di lavoro al fine di identificare la prassi operativa più adeguata per l'integrazione di tali servizi nel processo di trasferimento.

Appendice B: Allegato tecnico alle linee guida sull'adozione del sistema VOIP

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. 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 abbatte i costi ulteriormente e tende a evitare il lock-in con un fornitore su soluzioni proprietarie.

B.2 Requisiti di progetto

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 e il supporto all'interoperabilità con tutti i più diffusi protocolli di comunicazione aperti;
- ✓ 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 failover automatico e 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.

B.3 Architettura di sistema

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 e 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 telefonia IP e i servizi di fonia tradizionali basati su tecnologie a commutazione di circuito che possono essere sia la Rete Telefonica Pubblica (PSTN) che le preesistenti infrastrutture telefoniche interne basate su centralini legacy.

Il suo ruolo principale è trasformare il traffico voce/segnalazione da una tecnologia di trasmissione/rete a un'altra, generalmente passando da una logica a commutazione di pacchetto basata su datagrammi IP a una a commutazione di circuito operante in modalità TDM e viceversa.

I Media Gateway possono essere parte integrante dell'IP PBX oppure apparati dedicati in grado di comunicare via IP con l'IP PBX stesso; la scelta tra le due possibili modalità di interfacciamento e posizionamento può essere fatta in considerazione delle specifiche esigenze e della topologia di rete presente.

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, con il supporto per tutti i più diffusi codec attualmente disponibili, con particolare attenzione ai più diffusi codec "royalty free" (es: G.711a, G711.u, G.722, GSM, ...);
- ✓ completa interoperabilità con l'IP PBX, di cui possono anche essere parte integrante;
- ✓ il supporto completo sia dei protocolli standard di segnalazione telefonica tradizionale (Q.931, ISDN, Q.SIG), sia degli omologhi protocolli utilizzati nella telefonia IP (SIP, H323).

E' tuttavia fondamentale osservare che la presenza di un Media Gateway è essenziale solo nel caso in cui sia necessario interconnettersi con la PSTN o con un centralino legacy utilizzando tecnologie telefoniche tradizionali; nel caso in cui si rendesse disponibile accesso nativo VoIP alla Rete Telefonica Nazionale, e eventuali centralini legacy fossero in grado di comunicare in tecnologia VoIP (di solito possibile attraverso apposite schede di espansione), la presenza di un Media Gateway risulterebbe del tutto superflua.

E' altresì utile tenere in considerazione il ruolo del Media Gateway nella gestione di failover e disaster recovery, in quanto può facilmente diventare il "single point of failure" dell'intera infrastruttura telefonica.

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 con servizi erogati dal Session Control Server (di cui possono anche essere parte integrante).

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;
- ✓ supporto alla configurazione massiva automatizzata con utilizzo del protocollo HTTP/HTTPS;
- ✓ 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;
- ✓ 2 porte Ethernet per consentire la connessione in serie di un PC in modalità bridge;
- ✓ supporto dei più diffusi codec audio standard (G.711a, G.711u, G722, G.726, GSM, 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 di protocolli standard (SIP, H323) o riconosciuti come tali dal mercato. Nell'ottica di un investimento oculato può essere utile scegliere terminali che supportino i più recenti protocolli di cifratura delle comunicazioni VoIP (SIPS/SRTP);
- ✓ volume regolabile della suoneria.

Livello di servizio

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 dal terminale utilizzato. E' richiesto il supporto di un portafoglio di servizi evoluto adeguato ai massimi livelli dello stato dell'arte.

I servizi VoIP forniti agli utenti posso essere configurati in due modalità: installati direttamente su ogni telefono oppure installati in un server centralizzato e accessibili dagli utenti attraverso un'interfaccia Web da computer. Nel primo caso l'utente può accedere a servizi VoIP evoluti anche se non è dotato di un computer, ma il secondo caso offre altri vantaggi. Infatti, nonostante siano oggi disponibili terminali telefonici IP in grado di fornire autonomamente molte delle funzionalità di fonia evolute rese possibili dal VoIP (tra cui interfacce web di gestione con lista delle chiamate perse e ricevute, click2dial, conferenza a 3, musica d'attesa e molte altre) tuttavia, nell'ottica di un investimento più oculato, può essere opportuno scegliere la soluzione centralizzata che risulterà agli utenti molto più facile da utilizzare, sarà indipendentemente dal terminale che stanno utilizzando (telefoni IP, softphone, smartphone o qualsiasi altro software o apparato in grado di interconnettersi con un sistema VoIP), senza contare che

l'adozione di terminali con un numero ridotto di funzionalità, di solito meno costosi, può portare su larga scala a risparmi considerevoli. Si può considerare come ulteriore vantaggio la possibilità di usare terminali diversi senza vincolarsi a uno specifico modello, rendendo più semplice ed economico potenziare nel tempo la propria infrastruttura e fornire via via nuovi servizi senza dover sostituire i telefoni esistenti.

I servizi telefonici VoIP

Un moderno sistema di telefonia su IP deve prevedere un insieme di servizi fruibili dall'utenza e accessibili direttamente da terminale telefonico o da interfaccia Web dedicata, suddivisi in diversi livelli di servizio (ad esempio standard, top-class e advanced) e per tipologia di telefono.

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;
- ✓ servizio deviazione chiamate a tempo/fisso/variabile;
- ✓ servizio non disturbare;
- ✓ servizio conferenza su linee interne/esterne;
- ✓ servizio attesa;
- ✓ servizio parcheggio linee;
- ✓ 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;
- ✓ selezione passante;
- ✓ servizio documentazione addebiti;
- ✓ possibilità di assegnare diverse classi di servizio e livelli di abilitazione ai singoli utenti, attivabili su base identificazione;
- ✓ impegno diretto delle linee urbane libere;
- ✓ possibilità di impegnare le linee uscenti attraverso codici specifici;
- ✓ 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;
- ✓ gruppi con segnalazione di chiamata in parallelo, circolare, lineare;
- ✓ deviazione totale, su occupato e su non risposta;
- ✓ direttore segretaria/multi-segretaria con funzionalità avanzate;
- ✓ 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) con particolare attenzione al supporto per operatori diversamente abili;
- ✓ piena interoperabilità con sistemi esterni Gatekeeper.

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 (nei limiti e con i vincoli imposti dall'attuale normativa);
- ✓ rubrica telefonica e servizi di chiamata attraverso portale voice con interfaccia web Ill sistema deve consentire di gestire una rubrica telefonica a cui sia possibile accedere attraverso i terminali IP oppure tramite interfaccia web. E' auspicabile inoltre supportare un servizio di tipo "click-to-dial" che permetta agli utenti di effettuare una telefonata dal proprio terminale IP (fisico o softphone su PC), cliccando su una pagina web il nominativo/numero interno dell'utente;
- ✓ 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);
- ✓ supporto alla sicurezza e alla confidenzialità delle comunicazioni, ove necessario, attraverso l'utilizzo di protocolli di comunicazione cifrati;
- ✓ possibilità di integrazione con i più diffusi servizi di comunicazione VoIP esistenti (Skype, Gtalk, Jabber,..).

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.

Per quello che riguarda le problematiche e le limitazioni legali legate all'utilizzo dei servizi di fonia VoIP in mobilità, è possibile riferirsi alle specifiche linee guida redatte in collaborazione con la Polizia Postale e il Ministero competente (disponibili on-line sul sito www.ict4university.gov.it).

B.4 Telefonia IP e sicurezza informatica

Nel progetto e nella gestione di un'infrastruttura telefonica VoIP è necessario tenere in considerazione tutte le problematiche relative alla protezione e alla sicurezza informatica proprie delle reti IP, di cui condivide le risorse e i rischi, prevedendo adeguate misure attive e passive a protezione dei propri sistemi. Pur essendo la telefonia IP un ambito relativamente nuovo nel panorama informatico, oltre a condividere la maggior parte delle "best practices" ben note per ogni sistema informatico, esiste già una nutrita letteratura in materia e adeguati strumenti, anche open source, in grado di garantire un adeguato livello di protezione dei servizi.

B.5 Telefonia IP e servizio Fax

Nonostante gli attuali avanzamenti tecnologici nel campo delle comunicazioni, la tecnologia Telefax resta una componente essenziale e irrinunciabile del servizio di fonia, che deve necessariamente essere garantito nel passaggio alla tecnologia VoIP. Sfortunatamente le caratteristiche tecniche del protocollo di trasmissione dei fax sono inconciliabili con alcune caratteristiche della telefona VoIP, per cui è necessario tenere in considerazione la necessità di mantenere il servizio fax fin dalle prime fasi di progetto di migrazione/creazione di una infrastruttura VoIP. E' possibile fornire agli utenti il servizio di invio e ricezione fax in due modalità distinte, che possono comunque coesistere nello stessa infrastruttura.

B.6 Invio/ricezione fax attraverso apparecchi dedicati

E' possibile continuare a inviare e a ricevere fax utilizzando gli apparecchi fax dedicati tradizionali. In questo caso è necessario un adattatore (ATA) che, con un funzionamento analogo a un Media Gateway, permette di interconnettere apparecchi fax e telefoni analogici all'IP PBX in maniera analoga a quanto avviene per i telefoni IP. Questa soluzione presenta però significative criticità che dovrebbero essere accuratamente valutate. Infatti la trasmissione di fax risulta particolarmente sensibile a funzionalità tipiche della telefonia IP, quali l'utilizzo di codec compressi e meccanismi di cancellazione dell'eco, oltre ai possibili fenomeni tipici di tutte le trasmissioni IP quali ritardi di trasmissione, jitter e perdita di pacchetti. Per quello che riguarda codec e cancellazione dell'eco è sufficiente assicurarsi che le trasmissioni di fax avvengano usando il codec G.711a (lo stesso utilizzato nella PSTN e che non introduce compressione) e che sia l'IP PBX che l'ATA consentano di disattivare la cancellazione dell'eco quando venga riconosciuta la trasmissione di un fax. Fenomeni di elevato jitter o perdita di pacchetti possono invece rendere impossibile l'invio e la ricezione di fax, per cui la garanzia di una elevata QoS è una condizione imprescindibile per poter mantenere il servizio entro standard qualitativi adeguati.

In alternativa è possibile scegliere ATA e IP PBX con supporto per il protocollo T.38 (conosciuto anche come FoIP, acronimo di Fax over IP), pensato appositamente per garantire la funzionalità dei fax su architetture VoIP e che funziona come una sorta di proxy per le trasmissioni fax, mitigando gli effetti di ritardo e di perdita di pacchetti delle reti IP.
In questo caso però è necessario tenere in considerazione alcuni limiti del protocollo, in particolare per quello che riguarda l'uso in modalità "multi-hop", che ancora non offre adeguate garanzie di affidabilità.

B.7 Fax server

In alternativa all'uso di apparecchi tradizionali, è possibile, e anzi decisamente consigliabile, l'uso di un fax server dedicato, in grado di gestire l'invio e la ricezione dei fax. La gestione centralizzata del servizio rende più facile riservare risorse dedicate o comunque ottimizzare le configurazioni, rendendo possibile fornire maggiori garanzie di corretto funzionamento e di elevati standard

qualitativi. La natura del servizio facilita inoltre le pratiche di dematerializzazione dei documenti, permettendo l'archiviazione automatica in formato elettronico e semplificando la gestione dei documenti. L'introduzione di un fax server permette poi diverse modalità di fruizione del servizio da parte degli utenti, tra cui le più diffuse sono:

- ✓ Invio dei fax via Web (con interfaccia dedicata o integrata nel servizio di gestione della fonia VoIP) e ricezione dei fax via mail (come allegato di un messaggio di posta elettronica)
- ✓ Invio e ricezione attraverso messaggi e-mail
- ✓ Client dedicati installabili sul PC dell'utente

Le diverse modalità non sono mutualmente esclusive, ma anzi possono coesistere al fine di fornire un servizio quanto più possibile flessibile e completo.

B.8 Telefonia IP e software open source

Nell'ambito della telefonia IP è opportuno sottolineare il ruolo di rilievo attualmente svolto dal software open source, che ha dapprima favorito la diffusione della tecnologia VoIP e che ora rappresenta un'alternativa più che valida ai sempre più numerosi sistemi proprietari che si sono affacciati al mercato negli ultimi anni. Attualmente esistono prodotti open source, gratuiti e non, in grado di coprire tutte le possibili esigenze relative alla telefonia IP, a partire da IP PBX e fax server, fino ad arrivare ai più complessi sistemi integrati di comunicazione. I principali vantaggi di questi sistemi sono l'utilizzo pressoché esclusivo di standard aperti, che ne garantiscono il massimo livello di interoperabilità e la riduzione dei costi rispetto agli omologhi prodotti proprietari. L'uso di standard aperti garantisce la possibilità di interoperare senza problemi con un enorme numero di apparati e dispositivi di produttori diversi, evitando di legarsi in maniera praticamente indissolubile con un particolare produttore e rendendo più semplice ed economico modificare nel tempo le proprie scelte tecnologiche.

Infine, si ritiene importante evidenziare alcuni punti che possono giocare un ruolo importante nella scelta di una soluzione open source rispetto a una proprietaria: dal punto di vista dei costi, sicuramente le soluzioni open source permettono di ridurli in modo significativo, soprattutto i costi di realizzazione dell'infrastruttura (centralini e apparecchi telefonici); dal punto di vista della gestione del sistema telefonico, l'organizzazione deve decidere se internalizzare il servizio (come avviene per molti servizi informatici) oppure se selezionare un fornitore esterno che si faccia carico della gestione (in un mercato che sta maturando, ma non è certamente così evoluto come quello dei sistemi di fonia proprietaria).

Appendice C: Normativa sul VoiP

C.1 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

C.2 Condizioni

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.

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.

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.

Autenticazione utenti - l'associazione del terminale VoIP al centralino dell'Ateneo di appartenenza deve richiedere l'autenticazione dell'utente.

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

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

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.

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.

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).

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 AAI : Authentication, Authorization, Accounting Authentication and Authorization Infrastructure

DOPAU: Documento sul Processo di Accreditamento degli Utenti

DPS: Documento Programmatico sulla Sicurezza

FIAM

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

Per la Federazione Italiana Eduroam:

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

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

Per la Federazione IDEM
Requisiti e attività preliminari all'adesione
https://www.idem.garr.it/index.php/it/idem/190-sei-pronto-per-partecipare-alla-federazione

Regolamento, Norme di Partecipazione, Specifiche Tecniche e Specifiche Tecniche per la Compilazione e l'uso degli Attributi:
https://www.idem.garr.it/index.php/it/come-partecipare

Richiesta di Adesione, Richiesta di Registrazione IDP, Modello DOPAU, Richiesta di Registrazione SP (necessaria per la registrazione dell'accesso Wi-Fi):
https://www.idem.garr.it/index.php/it/come-partecipare

Guide di installazione più aggiornate per l'IDP:
https://www.idem.garr.it/index.php/it/documenti/doc_download/134-installare-lidp-2x-su-debian-lenny-con-solo-tomcat
http://www.garr.it/eventiGARR/idem-day/docs/conte-monticini_pres_idemday09.pdf

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 dei 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 coordinate 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.

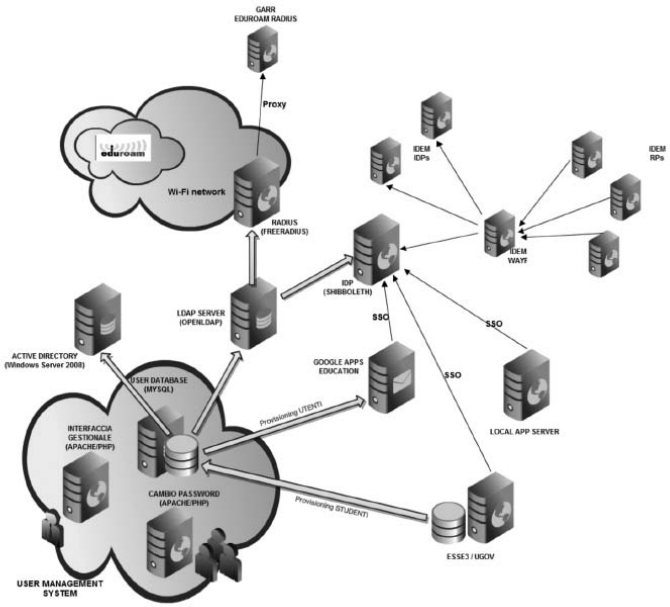
D.10 Comunicazione

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 a 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 "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

Tabella di dettaglio delle categorie di utenza classificate in ateneo		
N.	Descrizione categoria utenza d'ateneo	Cod mac. cat.
1	Personale docente di ruolo	D
2	Personale ricercatore di ruolo	R
3	Personale tecnico ed amm.vo a tempo indeterminato	P
4	Personale tecnico ed amm.vo a tempo determinato	P
5	Docente supplente esterno	D
6	Collaboratore tecnico/amministrativo	E
7	Collaboratore alla didattica	C
8	Assegnista di ricerca	R
9	Docente a contratto	D
10	Docente dotato di dispositivo di firma digitale per la registrazione di esami	D
11	Studente iscritto ai corsi di studio di 1° e 2° livello	S
12	Dottorando	T
13	Dottorando di Università consorziate	T
14	Studente di master	T
15	Laureato di un qualunque corso di studi/ dottorato/ master	L
16	Laureato di un qualunque corso di studi/ dottorato/ master titolare di una collaborazione a qualsiasi titolo (quale ad esempio l'iscrizione all'associazione "Alumni" riconosciuta dall'Ateneo)	A
17	Ospite (convegnista, ospite occasionale)	G
18	Personale di azienda esterna che presta attività lavorativa presso l'Università XYX	H
19	Personale di azienda/organizzazione esterna che fornisce servizi ICT	F
20	Personale in quiescenza	I

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.

Tabella delle macro categorie di utenza classificate in ateneo			
N.	Codice	Nome macro categoria	Elenco categorie incluse
1	O	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

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

Tabella mappature delle macro categorie di utenza sulle affiliazioni IDEM				
N.	Codice	Descrizione Macro categoria di utenza mappate su IDEM	Cardinalità	Affiliazione IDEM
1	D	Docente	500	Staff, Member
2	R	Ricercatore	150	Staff, Member
3	P	Dipendente	300	Staff, Member
4	E	Collaboratore tecnico/amm.vo	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	Fortitore	40	Affiliate

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.

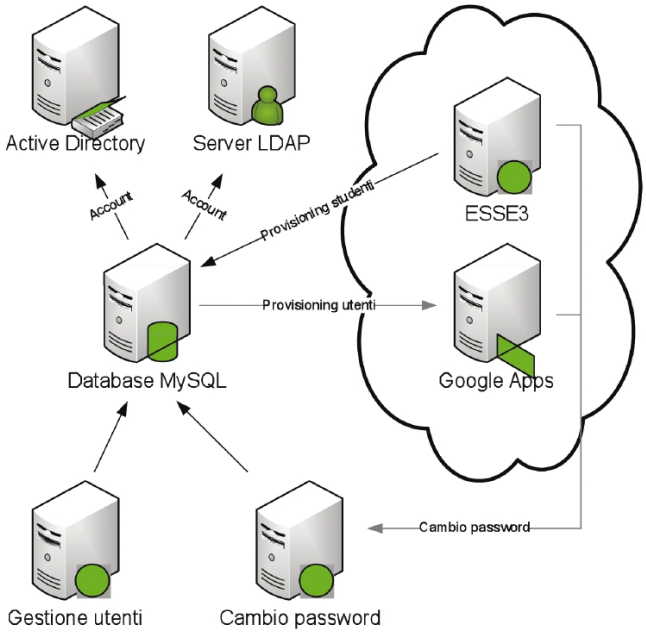
Una procedura eseguita ad intervalli regolari effettua gli aggiornamenti sul database LDAP (che alimenta i servizi Shibboleth e RADIUS) sul server Active Directory (che gestisce il dominio XYZ.IT per i computer desktop e il VDI) e infine su Google Apps Education (per la gestione delle caselle di posta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

Formato e regole delle credenziali
Le credenziali fornite sono del tipo: userID/password

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

A tutti i dipendenti viene inoltre rilasciata una tessera con banda magnetica utilizzata per rilevare le presenze. Il sistema di rilevazione presenze è in via di sostituzione e le nuove tessere saranno di tipo RFID (identificazione in radiofrequenza).

Eventuale presenza di credenziali multiple per la stessa persona

Le credenziali multiple servono per servizi diversi e non interagiscono.

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

Modalità di recupero delle credenziali smarrite
Lo userID smarrito può essere richiesto all'ufficio preposto.

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

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

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

Disabilitazione utente
Per le categorie caratterizzate da un rapporto di lavoro a termine la disabilitazione avviene in modo automatico alla data di fine rapporto impostata

nel db utenti mysql. Di norma questa data corrisponde alla scadenza del contratto aumentato di 6 mesi. Per le altre categorie del personale l'eventuale disabilitazione viene fatta manualmente dall'ufficio preposto a necessità attraverso una specifica procedura applicativa. Dall'avvenuta disabilitazione la persona non potrà più condurre con successo la procedura di autenticazione.

Cancellazione definitiva utente
Per le categorie caratterizzate da un rapporto di lavoro a termine la cancellazione definitiva viene fatta manualmente dall'ufficio preposto decorso 1 anno dalla data di disabilitazione ed in assenza di attribuzione di una nuova scadenza. Per le categorie caratterizzate da un rapporto di lavoro a tempo indeterminato (o di ruolo) non è prevista la cancellazione.

Rischi specifici associati alla categoria di utenti
La procedura manuale di disattivazione e cancellazione dell'utente può essere soggetta a dimenticanze ed errori umani. Al fine di mitigare questo rischio è prevista una verifica 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 e' laureato. Nel caso lo studente si sia laureato il passaggio di stato avviene automaticamente dopo 6 mesi dalla data di conclusione del corso di studi. Lo studente in stato "non attivo" può accedere all'applicativo di gestione della sua carriera ma non ai servizi di ateneo.

Il secondo livello di disabilitazione viene gestito dagli uffici preposti attraverso una specifica procedura applicativa. Come sopra dall'avvenuta disabilitazione lo studente non potrà più condurre con successo la procedura di autenticazione ai servizi d'ateneo.

Cancellazione definitiva utente
Non è prevista la cancellazione definitiva di uno studente.

Rischi specifici associati alla categoria di utenti
Non si evidenziano rischi specifici per la categoria di utenti trattata.

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

Non è prevista interoperabilità tra credenziali deboli e forti per la categoria di utenti trattata.

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 recepire da LDAP ed AD entro un'ora dalla modifica.

Formato e regole delle credenziali

Le credenziali fornite sono del tipo: *userID/password*

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

Eventuale presenza di credenziali multiple per la stessa persona

Eventuali credenziali multiple servono per servizi diversi e non interagiscono.

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

Modalità di recupero delle credenziali smarrite
Lo userID smarrito può essere richiesto all'ufficio preposto.

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

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

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

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

autenticazione.

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

Rischi specifici associati alla categoria di utenti
La procedura manuale di disattivazione e cancellazione dell'utente può essere soggetta a dimenticanze ed errori umani. Al fine di mitigare questo rischio è prevista una verifica periodica a cadenza annuale del db utenti mysql.

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

Non è prevista interoperabilità tra credenziali deboli e forti per le categorie di utenti trattata.

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

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

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

Modalità di recupero delle credenziali smarrite
Lo userID smarrito può essere richiesto all'ufficio preposto.

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

Modalità di gestione smarrimento smartcard/token
Non sono utilizzati smartcard/token

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

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

Cancellazione definitiva utente
La cancellazione definitiva avviene decorsi i 30 giorni dalla data di disabilitazione in as senza 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 trat tata.

D.12.10 Il sistema di autenticazione e autorizzazione interno

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

Come si evince dalla seguente, 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.

Tabella delle applicazioni interne e relativo metodo di autenticazione		
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
Ospite		

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 Wi-Fi di una qualsiasi delle organizzazioni federate solamente con l'impiego delle credenziali fornite dalla propria organizzazione.

Per assicurare la piena mobilità a tutti coloro che hanno una "identità", anche a livello internazionale, ed assicurate l'accesso anche a tutti gli altri servizi che IDEM mette a disposizione è fondamentale condividere la medesima base dati d'identità digitali.

Appendice E: Allegato tecnico alle linee guida sulla digitalizzazione delle tesi di laurea

E.1 Lo stato dell'arte

Premessa[8]

Le linee guida definiscono i processi di digitalizzazione e conservazione dei prodotti della ricerca scientifica in ambito accademico e didattico. Hanno l'obiettivo di fornire indicazioni di massima per la loro produzione in forma digitale nativa in conformità con quanto stabiliscono i requisiti archivistici standard previsti a livello nazionale (delibera CRUI) e internazionale, la più recente normativa italiana (dlgs 235/2010 e regole tecniche ai sensi dell'articolo 71 in corso di approvazione, legge sul deposito legale). Sono escluse dalla trattazione le questioni connesse al diritto d'autore.

Tenendo conto della specificità delle risorse digitali trattate, in particolare della diversità di trattamento prevista dalla normativa italiana e dalle indicazioni internazionali ed europee in materie di tesi di dottorato, le linee guida sono articolate in tre parti: la **prima** dedicata al deposito legale delle tesi di dottorato, per il quale è stata definita (e qui adottata) una specifica regolamentazione finalizzata a consentire il deposito presso le Biblioteche nazionali centrali di Firenze e Roma nella forma di *harvesting*; la **seconda** per tutte le forme di prodotti digitali riconducibili alla produzione di prodotti della ricerca scientifica identificabili come documenti rilevanti dal punto di vista giuridica e archivistico. Rientrano in questa categoria anche le tesi di dottorato per quanto concerne il loro valore giuridico e la loro trattazione archivistica conforme a quanto stabilito dal dpr 445/2000. La terza parte è dedicata a definire – a mero titolo indicativo – scenari operativi di flusso per la formazione e tenuta nell'archivio corrente delle tesi di dottorato e di laurea in forma digitale.

Si sottolinea che gran parte delle fattispecie documentarie qui considerate (in particolare le tesi di laurea e di dottorato) costituiscono per i soggetti produttori

[8] Cfr Biblioteca nazionale centrale di Roma e Fondazione Rinascimento digitale, *Consegna alle Biblioteche nazionali delle Tesi di Dottorato in formato digitale indicazioni tecniche per la raccolta automatica (harvesting:)*; A. Bollini, N. De Paoli, *Harvesting delle tesi di dottorato delle Biblioteche Nazionali tramite DSpace*, Cilea, 14 settembre 2010; MinervaEurope, *Linee guida tecniche per i programmi di creazione di contenuti culturali digitali*, Ministero per i beni e le attività culturali, Edizione italiana 2.0, 2006, www.minervaeurope.org; *Linee guida per il deposito delle tesi di dottorato negli archivi aperti*, https://www.crui.it/HomePage.aspx?ref=1149#) approvate dalla CRUI. Per le indicazioni di dettaglio si veda *Pagina informativa sulle procedure di deposito legale delle tesi di dottorato in formato digitale presso le Biblioteche nazionali centrali,* http://depositolegale.it/oai.html#h2a.

(le Università, in questo caso) documenti giuridicamente rilevanti in quanto "contenuti di atti e fatti prodotti nell'esercizio dell'attività amministrativa" (articolo 1 del dpr 445/2000) e sono quindi sottoposti (per quanto riguarda i processi di informatizzazione e di conservazione digitale) alle disposizioni del dpr 445/2000 sul documento amministrativo, del Codice dell'amministrazione digitale e della successiva regolamentazione tecnica. Hanno infatti **sempre** un duplice profilo, biblioteconomico e archivistico.

Il quadro normativo di riferimento per la produzione e conservazione di documenti informatici

Il quadro normativo di riferimento è alquanto complesso nel caso della produzione digitale nativa di documenti informatici giuridicamente rilevanti. Le principali disposizioni (che qui si riportano sinteticamente e si riferiscono al Codice dell'amministrazione digitale la cui ultima modifica è stata approvata con dlgs 235/2010, al Testo unico 445/2000 e relative regole tecniche e al Codice dei beni culturali, approvato con dlgs 42/2004) riguardano la *definizione dei termini rilevanti*, la *validità giuridica dei documenti* (provenienza/origine, data certa opponibile a terzi, identità, contesto amministrativo e integrità nel tempo dei contenuti e dei metadati che attestano la provenienza, la data, l'identità e il contesto amministrativo) e la loro *conservazione a lungo termine*. Si riportano di seguito le norme di cui è obbligatorio tenere conto nel definire linee guida generali di produzione e tenuta dei documenti in questione.

La definizione dei termini rilevanti (nella regolamentazione tecnica)

- ✓ *autenticità* (caratteristica di un documento informatico che garantisce di essere ciò che dichiara di essere, senza aver subito alterazioni o modifiche; l'autenticità può essere valutata analizzando l'identità del sottoscrittore e l'integrità del documento informatico),
- ✓ *ciclo di gestione* (arco temporale di esistenza del documento informatico, del fascicolo informatico, dell'aggregazione documentale informatica o dell'archivio informatico dalla sua formazione alla sua eliminazione o conservazione nel tempo),
- ✓ *conservazione* (insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo adottato e descritto nel manuale di conservazione),
- ✓ *identificativo univoco* (sequenza di caratteri alfanumerici associata in modo univoco e persistente al documento informatico, al fascicolo informatico, all'aggregazione documentale informatica, in modo da consentirne l'individuazione),
- ✓ *integrità* (insieme delle caratteristiche di un documento informatico che ne dichiarano la qualità di essere completo ed inalterato nei suoi elementi essenziali),

- ✓ *leggibilità* (insieme di caratteristiche in base alle quali le informazioni contenute nei documenti informatici sono fruibili durante l'intero ciclo di gestione dei documenti),
- ✓ *pacchetto di archiviazione* (pacchetto informativo composto dalla trasformazione di uno o più pacchetti di versamento secondo le specifiche contenute nell'allegato 4 del presente decreto e secondo le modalità riportate nel manuale di conservazione),
- ✓ *pacchetto di distribuzione* (pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta),
- ✓ *pacchetto di versamento* (pacchetto informativo inviato dal produttore al sistema di conservazione secondo un formato predefinito e concordato descritto nel manuale di conservazione),
- ✓ *pacchetto informativo* (contenitore che racchiude uno o più oggetti da conservare - documenti informatici, fascicoli informatici, aggregazioni documentali informatiche -, oppure anche i soli metadati riferiti agli oggetti da conservare),
- ✓ *rapporto di versamento* (documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore).

La validità giuridica

Il tema della validità giuridica è molto complesso, poiché riguarda aspetti tecnologici, giuridici e organizzativi che includono tra l'altro l'utilizzo di firme elettroniche per assicurare la provenienza dei documenti ovvero l'imputabilità certa nel tempo dei contenuti del documento e della sua forma a un autore riconosciuto e il riferimento temporale opponibile a terzi (marcatura temporale, protocollazione, posta certificata). In questa sede ci si limiterà a trattare il problema della tipologia di firma elettronica che il Cad consente di utilizzare nel caso della fattispecie documentaria qui considerata e il nodo del riferimento temporale, nelle modalità proposte dal dpcm 30 marzo 2009 e dalla regolamentazione tecnica in corso di approvazione. Poiché i documenti qui considerati sono generalmente a conservazione illimitata, le due questioni sono impegnative non solo sul piano organizzativo e in termini di costi (ad esempio l'impiego massivo di firme digitali da distribuire agli studenti appare in questa fase improponibile sia per ragioni economiche che gestionali), quanto per i rischi di verificabilità della validità della firma e della data nel lungo periodo.

Le regole tecniche sul documento informatico (in corso di approvazione) stabiliscono il principio generale in base al quale **qualunque documento informatico debba essere identificato in modo univoco e persistente e memorizzato all'interno del sistema di gestione documentale**. Stabiliscono inoltre le modalità concrete di memorizzazione che garantiscono il carattere di **immodificabilità** (in termini di non alterabilità nelle fasi di tenuta, accesso e conservazione). Riprendendo precedenti indicazioni (presenti ad esempio nel dpcm 30 marzo 2009) prevedono l'obbligo di "eliminare o rendere statiche, anche attraverso procedure automatiche, tutti gli elementi dinamici, quali

macroistruzioni, riferimenti esterni o codici eseguibili, che possano modificare gli atti, i fatti o i dati nello stesso rappresentati, e le informazioni di ausilio alla redazione, quali annotazioni, revisioni, segnalibri, gestite dal prodotto software utilizzato per la redazione".

Successivamente specificano le modalità operative che garantiscono l'immodificabilità in relazione alla tipologia di formazione del documento. Le indicazioni sono molto flessibili, lasciando i produttori (gli atenei) liberi di scegliere le modalità di gestione del processo: in particolare prescrivono che, nel caso di *redazione tramite l'utilizzo di appositi strumenti software*, l'immodificabilità si ottiene mediante operazioni quali la sottoscrizione con firma digitale ovvero con firma elettronica qualificata o l'apposizione di una validazione temporale o ancora il trasferimento a soggetti terzi con posta elettronica certificata con ricevuta completa o la memorizzazione su sistemi di gestione documentale che adottino politiche di sicurezza o il versamento ad un sistema di conservazione.

A fronte di un così ampio margine di scelta, non si ritiene di dover fornire in questa sede indicazioni tassative. Si richiamano tuttavia le indicazioni specifiche delle nuove regole tecniche:

- ✓ nel caso di documenti amministrativi informatici gestiti dalle pubbliche amministrazioni la caratteristica di immodificabilità è assicurata *anche mediante la registrazione nel registro di protocollo, negli ulteriori registri, ove opportunamente normati, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti,* secondo quanto previsto nel Capo IV del D.P.R. 28 dicembre 2000, n. 445 e come descritti e documentati nel manuale di gestione;
- ✓ si prevede che ai documenti siano associati *riferimenti temporali del tipo UTC* (Tempo Universale Coordinato) in grado di assicurare data certa al contenuto digitale;
- ✓ si stabilisce l'obbligo di utilizzare formati (che saranno indicati in un apposito allegato pubblicato online e aggiornato a cura di DigitPA) da definire a cura del responsabile della conservazione e da esplicitare e motivare nel manuale di conservazione) in grado di assicurare l'indipendenza dalle piattaforme tecnologiche, l'interoperabilità tra sistemi informatici e la longevità dei dati in termini di accesso e di leggibilità; in sostanza l'indicazione generale è quella di evitare formati proprietari e di privilegiare i formati standard;
- ✓ si definisce un nucleo minimo di metadati (indicati anch'essi in un allegato tecnico) che includono un **identificativo univoco e persistente** del documento, la **data nel formato indicato** in precedenza, l'**oggetto**, il **soggetto che ha formato il documento**;
- ✓ si definiscono le modalità di versamento nel sistema di conservazione mediante la creazione di un cosiddetto *pacchetto di versamento* le cui caratteristiche (inclusi i tempi del versamento) sono concordate con il responsabile della conservazione e definite nel manuale di

conservazione oltre che descritte a conclusione del processo nel cosiddetto *rapporto di versamento*.

La conservazione

L'**articolo 43 del Cad** (*conservazione dei documenti*) – fermo restando l'obbligo previsto dall'articolo 40 di produrre i documenti delle pubbliche amministrazioni in forma digitale – ne prescrive la tenuta nel tempo nella medesima modalità per tutti i casi per i quali sia "prescritta la conservazione per legge o regolamento", anche qualora gli originali siano stati formati su altri supporti: la loro validità giuridica e rilevanza è assicurata a condizione che "la riproduzione e la conservazione nel tempo siano effettuate in modo da garantire la conformità dei documenti agli originali nel rispetto della specifica regolamentazione tecnica", fatti salvi i poteri di controllo del Ministero per i beni e le attività culturali sugli archivi tutelati (pubblici o privati dichiarati di notevole interesse storico).

L'**articolo 44 del Cad** (*requisiti per la conservazione dei documenti informatici*), dopo aver confermato quanto già stabilito dal CAD nel 2005 – ovvero che il sistema di conservazione dei documenti informatici garantisce l'identificazione certa del soggetto che ha formato il documento o che lo ha acquisito, l'integrità del documento e la leggibilità e agevole reperibilità dei documenti stessi e delle informazioni identificative inclusi i dati di registrazione e classificazione originari e il rispetto delle misure di sicurezza – introduce due nuovi importanti commi: il comma 1-bis che prescrive la collaborazione tra i responsabili rispettivamente del sistema di conservazione e del servizio per la tenuta del protocollo informatico e il comma 1-ter che stabilisce a livello di norma generale quanto già indicato nella normativa tecnica del 2004 in materia di affidamento della funzione conservativa "ad altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative e tecnologiche".

L'**articolo 44-bis del Cad** (*conservatori accreditati*) prevede la possibilità di richiedere su base volontaria l'accreditamento presso DigitPA per "i soggetti pubblici e privati che svolgono attività di conservazione dei documenti informatici e di certificazione dei relativi processi per conto di terzi ed intendono conseguire il riconoscimento del possesso dei requisiti del livello più elevato, in termini di qualità e sicurezza" (comma 1). I dettagli tecnici, tutt'altro che secondari anche se non esaurienti, sono presenti nel comma seguente allorché si richiamano "in quanto compatibili", gli articoli 26 (requisiti dei certificatori), 27 (certificatori qualificati), 29 (accreditamento, ad eccezione del comma 3, lettera a) e 31 (vigilanza) ovvero gli obblighi e i controlli previsti dal CAD per gli enti certificatori che rilasciano certificati di firma digitale. Nel caso specifico si riconosce che tale funzione possa essere affidata anche a soggetti pubblici e che i soggetti privati (comma 3) che intendano accreditarsi debbano essere "costituiti in società di capitali con capitale sociale non inferiore a euro 200.000". Le regole tecniche in corso d approvazione stabiliscono che le pubbliche amministrazioni possano delegare i servizi di conservazione a soggetti accreditati.

L'**articolo 50 bis** (*continuità operativa*) prevede che "in relazione ai nuovi scenari di rischio, alla crescente complessità dell'attività istituzionale caratterizzata da un

intenso utilizzo della tecnologia dell'informazione, le pubbliche amministrazioni predispongano i *piani di emergenza* in grado di assicurare la *continuità delle operazioni* indispensabili per il servizio e il ritorno alla normale operatività" (comma 1); che il Ministro per la pubblica amministrazione e l'innovazione *assicuri l'omogeneità delle soluzioni* di continuità operativa definite dalle diverse Amministrazioni e ne informi con cadenza almeno annuale il Parlamento (comma 2); che le pubbliche amministrazioni definiscano (sulla base di *studi di fattibilità* valutati da DigitPA):

- ✓ il *piano di continuità operativa*, che fissa gli obiettivi e i principi da perseguire, descrive le *procedure per la gestione* della continuità operativa, anche affidate a soggetti esterni. Il piano tiene conto delle *potenziali criticità* relative a risorse umane, strutturali, tecnologiche e contiene idonee misure preventive. Le amministrazioni pubbliche verificano la funzionalità del piano di continuità operativa con cadenza biennale,
- ✓ il piano di *disaster recovery,* che costituisce parte integrante di quello di continuità operativa di cui alla lettera a) e stabilisce le misure tecniche e organizzative per garantire il funzionamento dei centri di elaborazione dati e delle procedure informatiche rilevanti in siti alternativi a quelli di produzione; si prevede che DigitPA, sentito il Garante per la protezione dei dati personali, definisca le linee guida per le soluzioni tecniche idonee a garantire la salvaguardia dei dati e delle applicazioni informatiche, verifichi annualmente il costante aggiornamento dei piani di *disaster recovery* delle amministrazioni interessate e ne informi annualmente il Ministro per la pubblica amministrazione e l'innovazione.

L'**articolo 51** (*sicurezza dei dati, dei sistemi, delle infrastrutture delle pubbliche amministrazioni*) stabilisce principi generali per le norme di sicurezza (definite in dettaglio nelle regole tecniche di cui all'articolo 71) con riferimento all'esigenza di rispettare criteri di esattezza, disponibilità, accessibilità, integrità e riservatezza dei dati (comma 1); stabilisce l'obbligo di DigitPA di raccordare le iniziative di prevenzione e gestione degli incidenti di sicurezza informatici e promuovere intese con le analoghe strutture internazionali, segnalare al Ministro per la pubblica amministrazione e l'innovazione il mancato rispetto delle regole tecniche da parte delle pubbliche amministrazioni (comma 1-bis) e gli obblighi delle amministrazioni di aggiornare tempestivamente i dati nei propri archivi, non appena vengano a conoscenza dell'inesattezza degli stessi (comma 2-bis).

La regolamentazione tecnica (in via di definitiva approvazione) traduce operativamente gli articoli ora citati, propone – come si è visto – un sistema chiaro ed esaustivo di definizioni e individua le modalità concrete per gestire i documenti digitali, trasferirli a terzi e conservarli, oltre a stabilire un sistema certo di responsabilità, incluse le forme obbligatorie di collaborazione interne alla p.a. (ad esempio tra responsabile dell'archivio e protocollo, responsabile del sistema di sicurezza e responsabile del sistema di conservazione). In particolare prescrive che:

a) le modalità e i tempi per i versamenti nel sistema di conservazione siano concordate con il responsabile della conservazione e siano opportunamente documentate in un **rapporto di versamento**;
b) si predisponga un **manuale di conservazione** (di cui si stabiliscono le componenti principali);
c) si conservino i **metadati essenziali** previsti in sede di formazione della risorsa (**identificativo univoco e persistente** del documento, **riferimento temporale** nel formato indicato, l'**oggetto**, il **soggetto che ha formato il documento, il riferimento al fascicolo di riferimento** che nel caso in questione è riferito al fascicolo dello studente);

Sono inoltre stabilite le fasi e i requisiti minimi del **processo di versamento** (peraltro conformi con i principali standard internazionali):

- ✓ acquisizione da parte del sistema di conservazione del pacchetto di versamento per la sua presa in carico,
- ✓ verifica che il pacchetto di versamento e gli oggetti contenuti siano coerenti con le modalità previste dal manuale di conservazione,
- ✓ rifiuto del pacchetto di versamento, nel caso in cui le verifiche di cui alla lettera b. abbiano evidenziato delle anomalie,
- ✓ generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo Universale Coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione,
- ✓ eventuale sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica qualificata apposta dal responsabile della conservazione, ove previsto nel manuale di conservazione,
- ✓ preparazione e gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati contenute nel pacchetto di archiviazione (definito in allegato alle regole) e secondo le modalità riportate nel manuale della conservazione,
- ✓ preparazione e sottoscrizione con la firma digitale o firma elettronica qualificata, ove previsto nel manuale di conservazione, del pacchetto di distribuzione ai fini dell'esibizione,
- ✓ produzione dei pacchetti di distribuzione coincidenti con i pacchetti di archiviazione al fine di garantire l'interoperabilità tra sistemi di conservazione,
- ✓ produzione dei duplicati informatici o delle copie informatiche effettuati a fini di distribuzione,
- ✓ eliminazione dal sistema di conservazione del pacchetto di archiviazione alla decorrenza dei termini previsti dalla norma dandone informativa al produttore secondo quanto previsto dalla normativa vigente, che, nel caso degli archivi pubblici o archivi privati, che rivestono interesse storico particolarmente importante, implica anche la previa

autorizzazione allo scarto da parte del Ministero per i beni e le attività culturali.

E' inoltre importante sottolineare che in quanto pubbliche amministrazioni gli atenei possono scegliere tra due modelli di conservazione: la gestione interna o l'affidamento a sistemi di conservazione esterni che tuttavia devono essere oggetto di accreditamento presso DigitPA, essere conservati, ai fini della vigilanza da parte di DigitPA sul territorio nazionale e in modo da garantire l'accesso presso la sede del produttore.

Il deposito legale delle tesi di dottorato

Architettura di base

Si riportano in sostanza le indicazioni suggerite dal Ministero per i beni e le attività culturali per il deposito legale mediante *harvesting* da parte delle Biblioteche nazionali centrali di Roma e Firenze. Si tratta di procedure operative già adottate da numerosi atenei che rispettano la conformità al modello stabilito dallo standard ISO 14721 – OAIS.

Si ribadisce che tali indicazioni non sono sufficienti a garantire il valore giuridico delle tesi e la loro conservazione in quanto documento archivistico collegato al contesto amministrativo di ciascun ateneo. Per il trattamento di tali aspetti si rinvia al capitolo relative alla Conservazione presente nelle linee guida.

Formato strutturato dei metadati nel caso di tesi costituite da più file

Si indica come formati per l'impacchettamento lo standard ISO 28500 - WARC (aggregatore di oggetti digitali a fini di stoccaggio in un file system convenzionale) o il contenitore xml MPEG21-DIDL, una modalità semplice e indipendente per acquisire e gestire insiemi di metadati conformi a schemi e a standard diversi, dato che permette di identificare i singoli componenti (didl:Component) della risorsa (didl:Item) e url della pagina web , detta JOP (jump off page) che riporta le informazioni utilii alla consultazione della risorsa mediante un browser. In questo caso il Dublin Core viene utilizzato per identificare (dc:identifier) la JOP che conterrà le ulteriori informazioni sui componenti.

Formato dei file

E' consigliato il PDF-A; sono suggeriti altri formati aperti, tra cui il formato ODS.

Protocollo di rappresentazione per lo scambio dei metadata

Per il servizio di deposito legale attuato con raccolta automatica dei metadati (harvesting) i metadati devono essere esposti da ogni ateneo utilizzando il protocollo OAI-PMH (Open Archives Iniziative Protocol for Metadata

Harvesting)9 in quanto in grado di rappresentare risorse digitali costituite da molteplici file e sostenuto; si suggerisce l'uso di applicativi software open source per la gestione di open archives (Dspace, Eprints).

Accesso
Mantenimento delle scelte di embargo dell'autore per ogni file nella struttura dei metadati; esposizione dei metadati oggetto di validazione da parte degli atenei (segreterie) con particolare riferimento alla presenza di

- ✓ un identificativo univoco (URL del deposito),
- ✓ un profilo di autorizzazione per ogni file depositato al fine di gestire opportunamente le tesi (o parti di esse) soggette a embargo, consentendo in questo caso l'accesso solo presso le sale di consultazione delle Biblioteche nazionali centrali di Roma e Firenze mediante PC privi di periferiche.

Procedura e tempistica
L'Università dichiara alla BNCF la propria disponibilità ad accettare la raccolta automatica dei metadati e dei file relativi alle proprie tesi di dottorato, utilizzando l'applicativo presente sul sito (http://register-oai.depositolegale.it/) per registrare l'url oai-pmh del proprio repository. La BNCF esegue la procedura di raccolta una volta al mese in maniera incrementale.

Procedure di validazione
La BNCF invia, a conferma della ricezione, una mail con allegati due file, in formato xml e xls, contenenti la lista delle URI delle tesi depositate la relativa impronta digitale in formato SHA-1 base32. Meccanismi ulteriori di validazione dipendono dal software utilizzato: ad esempio nel caso di DSpace è possibile prevedere processi di autenticazione di determinati indirizzi IP.

Metadati descrittivi
Si tratta solo delle informazioni di rappresentazione sintattica e semantica utili esclusivamente ai fini del deposito legale e della ricerca online (per i metadati rilevanti a fini archivistici si veda il capitolo 3). È ritenuto obbligatorio il ricorso allo standard Dublin Core secondo lo schema di seguito indicato:

[9] La Open Archives Initiative ha elaborato nel 1999 un quadro di riferimento finalizzato a promuovere la diffusione e l'interoperabilità degli archivi aperti di tipo *e-prints*. Il modello è stato successivamente utilizzato come modello di riferimento per l'architettura della biblioteca digitale.

Dataset	Dublin Core	NOTE
title	DC:title	Titolo della tesi
creator	DC:creator	Autore dell'opera (nel formato cognome, nome); non obbligatorio, ma raccomandato è l'indicazione dell'anno di nascita dell'Autore inserito con la seguente sintassi cognome, nome <anno>
description	DC:description	Abstract (meglio se in inglese)
language	Dc:language	Lingua (nel formato ISO639-1);
identifier	DC: identifier	URL a cui raggiungere il full-text della tesi o a una pagina intermedia
type	DC:type	Tipologia di materiale, da impostare di default come Doctoral Thesis è importante per il recupero dei dati usare la forma inglese
contributor	DC:contributor	Nome del tutor (nella forma cognome, nome)
date	DC:date	Data di discussione della tesi (min. Anno)
publisher	DC:publisher	Nome dell'università (è importante perché l'università di provenienza rende esplicito il valore della tesi)
format	DC:format	Dimensione in byte/MIME type
subjects	DC:subject	Settore scientifico disciplinare MIUR
rights	DC:rights	EMBARGO yy-mm-dd Item availability restricted

E.2 Riferimenti bibliografici

Cristalli di esperienza. Nuove prospettive e scenari per le tesi di dottorato: conservazione, accessibilità, certificazione, formati, integrazione con Open Access, giornata di studio del CNBA, Parma, CNBA, 2008, <http://digital.casalini.it/17240611>.

CRUI, Gruppo di lavoro Open Access, Linee guida per il deposito delle tesi di dottorato negli archivi aperti, 2007, <http://www.crui.it/HomePage.aspx?ref=1149>.

CRUI, Gruppo di lavoro Open Access, Tesi di dottorato e diritto d'autore, <http://www.crui.it/HomePage.aspx?ref=1149#>.

Depositolegale.it, Magazzini digitali, <http://depositolegale.it/>.

Magazzini Digitali: un'infrastruttura per la conservazione permanente, Venezia, Biblioteca Nazionale Marciana, 23 aprile, 2010, <http://marciana.venezia.sbn.it/internal.php?codice=684>.

Marialaura Vignocchi, Linee guida per l'accesso aperto alle tesi di dottorato, in "AIDAInformazioni", 26 (2008), 3-4, <http://www.aidainformazioni.it/pub/arabito-etal342008.pdf>.

G. Penzo Doria, Primi appunti per la gestione, tenuta e tutela delle tesi di laurea, in “Archivi & Computer”, 1998, 1, pp. 9-24.

Appendice F: Allegato tecnico alle linee guida sull'iscrizione on line

Descrizione tecnica del servizio realizzato da CINECA per adempiere alla sperimentazione delle verifiche dei titoli previste dal processo di Iscrizione Online

F.1 Obiettivi dell'allegato

Il presente documento si propone di descrivere un servizio basato sull'uso di web service che consenta la cooperazione a livello applicativo tra Ateneo e Banca Dati ANS per il recupero dei titoli (universitari e di diploma) conseguiti dallo studente.

I web service che verranno descritti sono finalizzati a erogare il servizio di recupero dei titoli conseguiti dallo studente previsto dal processo di immatricolazione.

F.2 I servizi esposti

RicercaTitoloStudente: recupero e verifica dei dati dichiarati dallo studente all'Ateneo riguardo ai Titoli Universitari conseguiti.

RicercaDiplomaStudente: recupero e verifica dei dati dichiarati dallo studente all'Ateneo riguardo il Titolo di Diploma conseguito.

F.3 Dettagli dei servizi erogati

RicercaTitoloStudente
Denominazione: ricercaDatiTitoliUniversitari

Descrizione: il servizio viene invocato dall'Ateneo per il recupero e la verifica dei Titoli Universitari dichiarati dallo studente durante il processo di immatricolazione

Input: Codice Fiscale dello studente

Output: Codice Fiscale dello studente

Codice Ateneo (codifica ANS);

Nazione di conseguimento (codifica ANS);

Tipo Classe del Titolo (codifica ANS);

Tipo del Titolo Universitario (codifica ANS);

Data di Conseguimento (codifica ANS);

Anno Accademico (codifica ANS);

Codice di ritorno; codice dell'esito dell'operazione.

Messaggio di ritorno; descrizione dell'esito dell'operazione.

Attivazione: il servizio viene invocato dagli Atenei.

Erogatore: il sistema ANS.

Descrizione dettagliata del servizio: L'Ateneo accede al servizio tramite BasicAuthentication fornendo le credenziali in suo possesso usate per l'accesso al sito riservato osd.cineca.it.

La richiesta dei titoli di uno studente avviene come previsto dal documento dalle linee guida sull'iscrizione on line inviando l'informazione obbligatoria "Codice Fiscale" dello studente.

Il sistema ANS recupera i Titoli Universitari conseguiti dallo studente (identificato dal Codice Fiscale) e restituisce le informazioni all'Ateneo.

Tracciato record:

Nome campo	*Formato*	*Obbl.*	*Descrizione*
Codice fiscale	CHAR(16)	sì	

Dati di output:

Nome campo	*Formato*	*Obbl.*	*Descrizione*
Codice fiscale	CHAR(16)	sì	
Codice Ateneo	CHAR(3)	sì	Si fa riferimento a codifica Ateneo CINECA
Nazione di conseguimento	CHAR(3)	sì	Per gli stati sono utilizzate le codifiche ISO 3166 (codifica pubblicata sul sito https://osd.cineca.it). Se l'informazione non è disponibile occorre passare 999. Si fa riferimento a codifica Ateneo CINECA
Classe Titolo	NUMBER(5)	sì	I codici sono pubblicati sul sito https://osd.cineca.it
Tipo Titolo	CHAR(2)	sì	**DS** → Diploma di scuola superiore **SF** → Scuola diretta ai fini speciali **DU** → Diploma universitario **DF** → Diploma in educazione fisica **LV** → Laurea vecchio ordinamento **LT** → Laurea triennale **M1** → Master di primo livello **TU** → Laurea a ciclo unico **M2**→ Master di secondo livello **LS** → Laurea specialistica **LM** → Laurea magistrale **AP** → Abilitazione professionale **SI** → Scuola di specializzazione per insegnanti **SM** → Scuola di specializzazione medica **SL**→ Scuola di specializzazione professioni

Nome campo	*Formato*	*Obbl.*	*Descrizione*
			legali **SA** →Altre scuole di specializzazione **DR**→ Dottorato di ricerca **EE** → Laurea estera **DL**→ Diploma mediatore linguistico **DA**→ Diploma accademico quadriennale **CP** → Corso di perfezionamento; **A1** → Diploma accademico di primo livello **A2** → Diploma accademico di secondo livello; **MA** → Altri master **TS** → Titolo generico d'area medica/ospedaliera La tipologia di titolo TS comprende i soli titoli rilasciati da Enti Sanitari che consentano l''ammissione ai corsi di laurea specialistico/magistrale delle professioni sanitarie.
Data di conseguimento	CHAR(8)	sì	Data di conseguimento del titolo
Anno Accademico	NUMBER(4)	sì	Anno Accademico in cui è stato conseguito il titolo
Codice Ritorno	CHAR(1)	sì	Numerico, da definire
Messaggio	CHAR(100)	no	Stringa da definire

RicercaTitoloStudenteService.wsdl (interrogato dall'Ateneo*).*

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions
targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaTitoloStude
nte"
xmlns="http://schemas.xmlsoap.org/wsdl/"
xmlns:intf="http://miur.spcoop.gov.it/servizi/RicercaTitoloStudente"
xmlns:types="http://miur.spcoop.gov.it/servizi/RicercaTitoloStudente/
types"
xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaTitoloStudente.xs
d"
xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/">
<types>
     <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns="http://miur.spcoop.gov.it/servizi/RicercaTitoloStudente.x
sd"
     xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaTitoloStuden
te.xsd"
     targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaTitolo
Studente.xsd"
                    elementFormDefault="qualified"
attributeFormDefault="unqualified">
                    <xs:element
name="ricercaDatiTitoliStudenteElement">
                           <xs:annotation>
                                  <xs:documentation>Comment
describing your root element
                                  </xs:documentation>
                           </xs:annotation>
                           <xs:complexType>
                                  <xs:sequence>
                                         <xs:element
name="codiceFiscale" type="CodiceFiscaleType"
                                                nillable="false" />
                                  </xs:sequence>
                           </xs:complexType>
                    </xs:element>
                    <xs:simpleType name="CodiceFiscaleType">
                           <xs:restriction base="xs:string">
                                  <xs:minLength value="16" />
                                  <xs:maxLength value="16" />
                                  <xs:pattern
                                         value="[A-Z]{6}[0-
9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]"
/>
                           </xs:restriction>
                    </xs:simpleType>
                    <xs:element
name="ricercaDatiTitoliStudenteResponseElement">
                           <xs:complexType>
                                  <xs:sequence>
                                         <xs:element
maxOccurs="unbounded"
```

```
name="result"
type="DatiTitoloStudenteObject"
                                                    nillable="true" />
                                    </xs:sequence>
                            </xs:complexType>
                    </xs:element>
                    <xs:complexType name="DatiTitoloStudenteObject">
                            <xs:sequence>
                                    <xs:element name="codiceFiscale"
type="xs:string"
                                            nillable="true" />
                                    <xs:element name="codiceAteneo"
type="xs:string"
                                            nillable="true" />
                                    <xs:element
name="nazioneConseguimento" type="xs:string"
                                            nillable="true" />
                                    <xs:element
name="tipoClasseTitolo" type="xs:string"
                                            nillable="true" />
                                    <xs:element
name="tipoTitoloUniversitario" type="xs:string"
                                            nillable="true" />
                                    <xs:element
name="dataConseguimento" type="xs:string"
                                            nillable="true" />
                                    <xs:element name="annoAccademico"
type="xs:string"
                                            nillable="true" />
                            </xs:sequence>
                    </xs:complexType>
            </xs:schema>
            <xsd:schema

    xmlns:types="http://miur.spcoop.gov.it/servizi/RicercaTitoloStud
ente/types"
                    xmlns:xsd="http://www.w3.org/2001/XMLSchema"

    xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaTitoloStuden
te.xsd"

    targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaTitolo
Studente/types"
                    elementFormDefault="qualified">
                    <xsd:import

    namespace="http://miur.spcoop.gov.it/servizi/RicercaTitoloStuden
te.xsd"
                             />
                    <xsd:element

    name="richiesta_RichiestaRispostaSincrona_ricercaDatiTitoloStude
nte"

    type="types:Richiesta_ricercaDatiTitoloStudente_Type" />
                    <xsd:element

    name="risposta_RichiestaRispostaSincrona_ricercaDatiTitoloStuden
te"
```

```
    type="types:Risposta_ricercaDatiTitoloStudenteResponse_Type" />
                    <xsd:complexType
name="Risposta_ricercaDatiTitoloStudenteResponse_Type">
                            <xsd:sequence>
                                    <xsd:element
ref="ns1:ricercaDatiTitoliStudenteResponseElement" />
                            </xsd:sequence>
                    </xsd:complexType>
                    <xsd:complexType
name="Richiesta_ricercaDatiTitoloStudente_Type">
                            <xsd:sequence>
                                    <xsd:element
ref="ns1:ricercaDatiTitoliStudenteElement" />
                            </xsd:sequence>
                    </xsd:complexType>
            </xsd:schema>
    </types>
    <message

    name="richiesta_RichiestaRispostaSincrona_ricercaDatiTitoloStude
nte_Msg">
            <part name="parameters"

    element="types:richiesta_RichiestaRispostaSincrona_ricercaDatiTi
toloStudente" />
    </message>
    <message

    name="risposta_RichiestaRispostaSincrona_ricercaDatiTitoloStuden
te_Msg">
            <part name="parameters"

    element="types:risposta_RichiestaRispostaSincrona_ricercaDatiTit
oloStudente" />
    </message>
    <portType name="RicercaTitoloStudente">

    <wsdl:documentation>Intestazione/IntestazioneMessaggio/Servizio=
RicercaTitoloStudente
            </wsdl:documentation>
            <operation name="ricercaDatiTitoliUniversitari">

    <wsdl:documentation>Intestazione/IntestazioneMessaggio/Azione=ri
cercaDatiTitoliUniversitari,

    ProfiloCollaborazione=EGOV_IT_ServizioSincrono</wsdl:documentati
on>
                    <input

    message="intf:richiesta_RichiestaRispostaSincrona_ricercaDatiTit
oloStudente_Msg" />
                    <output

message="intf:risposta_RichiestaRispostaSincrona_ricercaDatiTitoloStu
dente_Msg" />
            </operation>
    </portType>
```

```
    <binding name="RicercaTitoloStudenteBinding"
type="intf:RicercaTitoloStudente">
            <wsdlsoap:binding style="document"
                    transport="http://schemas.xmlsoap.org/soap/http"
/>
            <operation name="ricercaDatiTitoliUniversitari">
                    <wsdlsoap:operation
soapAction="ricercaDatiTitoliUniversitari" />
                    <input>
                            <wsdlsoap:body use="literal" />
                    </input>
                    <output>
                            <wsdlsoap:body use="literal" />
                    </output>
            </operation>
    </binding>
    <service name="RicercaTitoloStudenteService">
            <port name="RicercaTitoloStudenteWS"
binding="intf:RicercaTitoloStudenteBinding">
                    <wsdlsoap:address

    location="http://localhost:8888/RicercaTitoloStudente/RicercaTit
oloStudenteWS" />
            </port>
    </service>
</definitions>
```

RicercaTitoloStudente.xsd

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="http://miur.spcoop.gov.it/servizi/RicercaTitoloStudente.x
sd"
    xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaTitoloStuden
te.xsd"
    targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaTitolo
Studente.xsd"
    elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:element name="ricercaDatiTitoliStudenteElement">
            <xs:annotation>
                    <xs:documentation>Comment describing your root
element
                    </xs:documentation>
            </xs:annotation>
            <xs:complexType>
                    <xs:sequence>
                            <xs:element name="codiceFiscale"
type="CodiceFiscaleType"
                                    nillable="false" />
                    </xs:sequence>
            </xs:complexType>
    </xs:element>
    <xs:simpleType name="CodiceFiscaleType">
            <xs:restriction base="xs:string">
                    <xs:minLength value="16" />
```

```
                    <xs:maxLength value="16" />
                    <xs:pattern
                            value="[A-Z]{6}[0-9LMNPQRSTUV]{2}[A-Z][0-
9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]" />
            </xs:restriction>
    </xs:simpleType>
    <xs:element name="ricercaDatiTitoliStudenteResponseElement">
            <xs:complexType>
                    <xs:sequence>
                            <xs:element maxOccurs="unbounded"
name="result" type="DatiTitoloStudenteObject"
                                    nillable="true" />
                    </xs:sequence>
            </xs:complexType>
    </xs:element>
    <xs:complexType name="DatiTitoloStudenteObject">
            <xs:sequence>
                    <xs:element name="codiceFiscale" type="xs:string"
                            nillable="true" />
                    <xs:element name="codiceAteneo" type="xs:string"
                            nillable="true" />
                    <xs:element name="nazioneConseguimento"
type="xs:string"
                            nillable="true" />
                    <xs:element name="tipoClasseTitolo"
type="xs:string"
                            nillable="true" />
                    <xs:element name="tipoTitoloUniversitario"
type="xs:string"
                            nillable="true" />
                    <xs:element name="dataConseguimento"
type="xs:string"
                            nillable="true" />
                    <xs:element name="annoAccademico"
type="xs:string"
                            nillable="true" />
            </xs:sequence>
    </xs:complexType>
</xs:schema>
<xsd:schema
    xmlns:types="http://miur.spcoop.gov.it/servizi/RicercaTitoloStud
ente/types"
    xmlns:xsd="http://www.w3.org/2001/XMLSchema"
    xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaTitoloStuden
te.xsd"
    targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaTitolo
Studente/types"
    elementFormDefault="qualified">
    <xsd:import

    namespace="http://miur.spcoop.gov.it/servizi/RicercaTitoloStuden
te.xsd"
             />
    <xsd:element

    name="richiesta_RichiestaRispostaSincrona_ricercaDatiTitoloStude
nte"
            type="types:Richiesta_ricercaDatiTitoloStudente_Type" />
    <xsd:element
```

```
    name="risposta_RichiestaRispostaSincrona_ricercaDatiTitoloStuden
te"

    type="types:Risposta_ricercaDatiTitoloStudenteResponse_Type" />
    <xsd:complexType
name="Risposta_ricercaDatiTitoloStudenteResponse_Type">
            <xsd:sequence>
                    <xsd:element
ref="ns1:ricercaDatiTitoliStudenteResponseElement" />
            </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType
name="Richiesta_ricercaDatiTitoloStudente_Type">
            <xsd:sequence>
                    <xsd:element
ref="ns1:ricercaDatiTitoliStudenteElement" />
            </xsd:sequence>
    </xsd:complexType>
</xsd:schema>
```

Il web service sperimentale realizzato da CINECA per il recupero dei Titoli Universitari

L'endpoint del web service realizzato da CINECA per la sperimentazione del workflow descritto nelle linee guida immatricolazione online è:

http://osd.pp.cineca.it/php5/ws/RicercaTitoloStudenteWS.php?wsdl

L'accesso a tale web service avviene con le credenziali fornite agli atenei per la sottomissione dei dati ANS.

L'ateneo può sperimentare il servizio realizzato ed adeguare i propri sistemi informativi usando l'ambiente di demo predisposto

http://osd.pp.cineca.it/php5/ws/RicercaTitoloStudenteWS.php?wsdl, rispettando i criteri definiti in questo documento.

RicercaDiplomaStudente.

Denominazione: ricercaDatiTitoliDiploma.

Descrizione: Il servizio viene invocato dall'Ateneo per il recupero e la verifica del Titolo di Diploma dichiarato dallo studente durante il processo di immatricolazione.

Input: Codice Fiscale dello studente

anno solare di conseguimento del titolo

Output: Codice Fiscale dello studente

Codice ANS della scuola;

Codice ANS della nazione di conseguimento;

Codice ANS del voto di diploma;

Codice ANS della tipologia di diploma

Tipo Diploma e sua descrizione;

Anno solare di conseguimento del titolo;

Codice di ritorno; codice dell'esito dell'operazione.

Messaggio di ritorno; descrizione dell'esito dell'operazione.

Attivazione: il servizio viene invocato dagli Atenei.

Erogatore: il sistema ANS.

Descrizione dettagliata del servizio: l'Ateneo richiede il recupero del titolo come previsto dal documento "Linee_guida_immatricolazione-v005.doc" inviando i dati obbligatori relativi a Codice Fiscale, Anno Solare di conseguimento del Titolo. Il sistema ANS recupera il titolo conseguito dallo studente (identificato dal Codice Fiscale) durante l'anno solare specificato dalla banca dati MIUR-Istruzione interrogando il servizio erogato da HP operante per conto del Ministero dell'Istruzione (MIUR) e restituisce i dati recuperati, codificati ANS, all'Ateneo richiedente.

Tracciato record proposto:

Nome campo	*Formato*	*Obbl.*	*Descrizione*
Codice fiscale	CHAR(16)	sì	
Anno di conseguimento	CHAR(4)	sì	Anno finale dell'anno scolastico: es. 2011 per l'a.s. 2010/11

Nome campo	*Formato*	*Obbl.*	*Descrizione*
Codice fiscale	CHAR(16)	Sì	
Codice Scuola	NUMBER(7)	Sì	Si fa riferimento a codifica Ateneo CINECA
Nazione di conseguimento	CHAR(3)	Sì	Per gli stati sono utilizzate le codifiche **ISO 3166** (codifica pubblicata sul sito https://osd.cineca.it). Se l'informazione non è disponibile occorre passare **999**.
Voto Diploma	CHAR (4)	sì	Voto di diploma normalizzato. I codici sono pubblicati sul sito https://osd.cineca.it
Tipo Titolo Diploma	NUMBER(4)	Sì	La codifica dei titoli è conforme a quella utilizzata dal **MIUR – Istruzione** (codifica pubblicata sul sito https://osd.cineca.it)
Anno Solare conseguimento	CHAR(8)	Sì	Data di conseguimento del titolo
Codice Ritorno	CHAR(1)	sì	Numerico, da definire
Messaggio	CHAR(100)	no	Stringa da definire

Verifica del Titolo di Diploma dalla banca dati ANS MIUR-Istruzione

La richiesta di verifica del Titolo di Diploma proveniente dall'Ateneo viene inoltrata ad HP attraverso l'uso di Porte di Dominio (software SPCoop) ottemperando alle linee guida sulla iscrizione on line inviando i dati obbligatori relativi a Codice Fiscale, Anno Solare di conseguimento.

Il servizio è descritto in dettaglio nel documento “CO-CA-MEM-03052012-Interazione banche dati Istruzione e Università ITC4U-1 0.doc”.

I dati provenienti dalla banca dati dell’Istruzione vengono opportunamente codificati in base alla codifica della banca dati degli Atenei.

RicercaDiplomaStudenteService.wsdl (interrogato dall'Ateneo).

```
<?xml version="1.0" encoding="UTF-8"?>
<definitions

targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStud
ente"
   xmlns="http://schemas.xmlsoap.org/wsdl/"

xmlns:intf="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente"

xmlns:types="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente
/types"

xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente.x
sd"
   xmlns:wsdlsoap="http://schemas.xmlsoap.org/wsdl/soap/"
   xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/" >
  <types>
  <xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente.xsd"
xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente.x
sd"
targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStud
ente.xsd" elementFormDefault="qualified"
attributeFormDefault="unqualified">
    <xs:element name="ricercaDatiDiplomiStudenteElement">
            <xs:annotation>
                    <xs:documentation>Comment describing your root
element</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                    <xs:sequence>
                            <xs:element name="codiceFiscale"
type="CodiceFiscaleType" nillable="false"/>
                            <xs:element name="annoScolastico"
type="AnnoScolasticoType" nillable="false" />
                    </xs:sequence>
            </xs:complexType>
    </xs:element>
    <xs:simpleType name="CodiceFiscaleType">
            <xs:restriction base="xs:string">
                    <xs:minLength value="16"/>
                    <xs:maxLength value="16"/>
                    <xs:pattern value="[A-Z]{6}[0-9LMNPQRSTUV]{2}[A-
Z][0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]"/>
            </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AnnoScolasticoType">
            <xs:restriction base="xs:string">
                    <xs:minLength value="4" />
                    <xs:maxLength value="4" />
```

```
                    <xs:pattern value="[0-9]" />
            </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="UserIDType">
            <xs:restriction base="xs:string">
                    <xs:maxLength value="100" />
            </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="PasswordType">
            <xs:restriction base="xs:string">
                    <xs:maxLength value="15" />
            </xs:restriction>
    </xs:simpleType>
    <xs:element name="ricercaDatiDiplomiStudenteResponseElement">
            <xs:complexType>
                    <xs:sequence>
                            <xs:element maxOccurs="unbounded"
name="result" type="DatiDiplomaStudenteObject" nillable="true" />
                    </xs:sequence>
            </xs:complexType>
    </xs:element>
    <xs:complexType name="DatiDiplomaStudenteObject">
            <xs:sequence >
                    <xs:element name="codiceFiscale" type="xs:string"
nillable="true"/>
                    <xs:element name="codiceScuola" type="xs:string"
nillable="true"/>
                    <xs:element name="nazioneConseguimento"
type="xs:string" nillable="true"/>
                    <xs:element name="votoDiploma" type="xs:string"
nillable="true"/>
                    <xs:element name="tipoTitoloDiploma"
type="xs:string" nillable="true"/>
                    <xs:element name="annoSolareConseguimento"
type="xs:string" nillable="true"/>
                    <xs:element name="codiceRitorno" type="xs:string"
nillable="true" />
                    <xs:element name="messaggio" type="xs:string"
nillable="true" />
            </xs:sequence>
    </xs:complexType>
    </xs:schema>
    <xsd:schema
xmlns:types="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente
/types"

    xmlns:xsd="http://www.w3.org/2001/XMLSchema"

    xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStude
nte.xsd"
    targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaDiplom
aStudente/types" elementFormDefault="qualified">
    <xsd:import
namespace="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente.x
sd" />
    <xsd:element
name="richiesta_RichiestaRispostaSincrona_ricercaDatiDiplomaStudente"
type="types:Richiesta_ricercaDatiDiplomaStudente_Type"/>
```

```
    <xsd:element
name="risposta_RichiestaRispostaSincrona_ricercaDatiDiplomaStudente"
type="types:Risposta_ricercaDatiDiplomaStudenteResponse_Type"/>
    <xsd:complexType
name="Risposta_ricercaDatiDiplomaStudenteResponse_Type">
            <xsd:sequence>
                    <xsd:element
ref="ns1:ricercaDatiDiplomiStudenteResponseElement"/>
            </xsd:sequence>
    </xsd:complexType>
    <xsd:complexType
name="Richiesta_ricercaDatiDiplomaStudente_Type">
            <xsd:sequence>
                    <xsd:element
ref="ns1:ricercaDatiDiplomiStudenteElement"/>
            </xsd:sequence>
    </xsd:complexType>
    </xsd:schema>
  </types>
  <message
name="richiesta_RichiestaRispostaSincrona_ricercaDatiDiplomaStudente_
Msg">
    <part name="parameters"
element="types:richiesta_RichiestaRispostaSincrona_ricercaDatiDiploma
Studente"/>
  </message>
  <message
name="risposta_RichiestaRispostaSincrona_ricercaDatiDiplomaStudente_M
sg">
    <part name="parameters"
element="types:risposta_RichiestaRispostaSincrona_ricercaDatiDiplomaS
tudente"/>
  </message>
  <portType name="RicercaDiplomaStudente">

<wsdl:documentation>Intestazione/IntestazioneMessaggio/Servizio=Ricer
caDiplomaStudente</wsdl:documentation>
    <operation name="ricercaDatiTitoliDiploma">

<wsdl:documentation>Intestazione/IntestazioneMessaggio/Azione=ricerca
DatiTitoliDiploma,
ProfiloCollaborazione=EGOV_IT_ServizioSincrono</wsdl:documentation>
      <input
message="intf:richiesta_RichiestaRispostaSincrona_ricercaDatiDiplomaS
tudente_Msg"/>
      <output
message="intf:risposta_RichiestaRispostaSincrona_ricercaDatiDiplomaSt
udente_Msg"/>
    </operation>
  </portType>
  <binding name="RicercaDiplomaStudenteBinding"
type="intf:RicercaDiplomaStudente">
    <wsdlsoap:binding style="document"
transport="http://schemas.xmlsoap.org/soap/http"/>
    <operation name="ricercaDatiTitoliDiploma">
      <wsdlsoap:operation soapAction="ricercaDatiTitoliDiploma"/>
      <input>
        <wsdlsoap:body use="literal"/>
      </input>
```

```
      <output>
        <wsdlsoap:body use="literal"/>
      </output>
    </operation>
  </binding>
  <service name="RicercaDiplomaStudenteService">
    <port name="RicercaDiplomaStudenteWS"
binding="intf:RicercaDiplomaStudenteBinding">
      <wsdlsoap:address
location="http://localhost:8888/RicercaDiplomaStudente/RicercaDiploma
StudenteWS"/>
    </port>
  </service>
</definitions>
```

RicercaDiplomaStudente.xsd

```
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns=http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente.xsd
xmlns:ns1="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStudente.x
sd"
targetNamespace="http://miur.spcoop.gov.it/servizi/RicercaDiplomaStud
ente.xsd" elementFormDefault="qualified"
attributeFormDefault="unqualified">
<xs:element name="ricercaDatiDiplomiStudenteElement">
            <xs:annotation>
                    <xs:documentation>Comment describing your root
element</xs:documentation>
            </xs:annotation>
            <xs:complexType>
                    <xs:sequence>
                            <xs:element name="codiceFiscale"
type="CodiceFiscaleType" nillable="false"/>
                            <xs:element name="annoScolastico"
type="AnnoScolasticoType" nillable="false" />
                    </xs:sequence>
            </xs:complexType>
    </xs:element>
    <xs:simpleType name="CodiceFiscaleType">
            <xs:restriction base="xs:string">
                    <xs:minLength value="16"/>
                    <xs:maxLength value="16"/>
                    <xs:pattern
value="[A-Z]{6}[0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{2}[A-Z][0-
9LMNPQRSTUV]{3}[A-Z]"/>
            </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="AnnoScolasticoType">
            <xs:restriction base="xs:string">
                    <xs:minLength value="4" />
                    <xs:maxLength value="4" />
                    <xs:pattern value="[0-9]" />
            </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="UserIDType">
            <xs:restriction base="xs:string">
                    <xs:maxLength value="100" />
```

```
            </xs:restriction>
    </xs:simpleType>
    <xs:simpleType name="PasswordType">
            <xs:restriction base="xs:string">
                    <xs:maxLength value="15" />
            </xs:restriction>
    </xs:simpleType>
    <xs:element name="ricercaDatiDiplomiStudenteResponseElement">
            <xs:complexType>
                    <xs:sequence>
                            <xs:element
maxOccurs="unbounded"
name="result"
type="DatiDiplomaStudenteObject" nillable="true" />
                    </xs:sequence>
            </xs:complexType>
    </xs:element>
    <xs:complexType name="DatiDiplomaStudenteObject">
            <xs:sequence >
                    <xs:element name="codiceFiscale" type="xs:string"
nillable="true"/>
                    <xs:element name="codiceScuola" type="xs:string"
nillable="true"/>
                    <xs:element name="nazioneConseguimento"
type="xs:string" nillable="true"/>
                    <xs:element name="votoDiploma" type="xs:string"
nillable="true"/>
                    <xs:element name="tipoTitoloDiploma"
type="xs:string" nillable="true"/>
                    <xs:element name="annoSolareConseguimento"
type="xs:string" nillable="true"/>
                    <xs:element name="codiceRitorno" type="xs:string"
nillable="true" />
                    <xs:element name="messaggio" type="xs:string"
nillable="true" />
            </xs:sequence>
    </xs:complexType>
    </xs:schema>
```

Codici di errore proposti da HP (in fase di definizione).

I codici di errore previsti da HP (ancora in fase di definizione e completamento) sono i seguenti (CODIS, codice fiscale; AAAA, anno; MESS, messaggio di ritorno):

0 = Ricerca effettuata con successo. CODFIS, AAAA

1 = Ricerca effettuata con successo. Non sono stati trovati dati con i parametri specificati in input. CODFIS, AAAA

2 = Ricerca effettuata con successo. Trovate più occorrenze con i parametri specificati : CODFIS, AAAA

3 = Impossibile reperire i dati, problemi di collegamento alla base dati

4 = Errore generico nella ricerca: MESS

12 = Codice Fiscale formalmente non corretto. Impossibile effettuare la ricerca

14 = Anno di Conseguimento non valorizzato correttamente (formato AAAA). Impossibile effettuare la ricerca

15 = Anno di Conseguimento non numerico (formato AAAA). Impossibile effettuare la ricerca

94 = Il Codice Fiscale fornito non è congruente con le credenziali.

95 = Anno di conseguimento non valorizzato o non corretto. Impossibile effettuare la ricerca

96 = Codice Fiscale non valorizzato o non corretto. Impossibile effettuare la ricerca

Il web service sperimentale realizzato da CINECA per il recupero dei Titoli di Diploma

L'endpoint del web service realizzato da CINECA per la sperimentazione del workflow descritto nelle linee guida sull'iscrizione on line è:

http://osd.pp.cineca.it/php5/ws/RicercaDiplomaStudenteWS.php?wsdl

L'accesso a tale web service avviene con le credenziali fornite agli atenei per l'accesso al sito riservato osd.cineca.it.

http://siba2.unisalento.it

ISBN 978-88-8305-089-3 (electronic version)
http://siba-ese.unisalento.it/index.php/unidig2012/

ISBN 978-88-8305-089-3