UNIVERSITÀ
DI TRENTO
Direzione
Didattica e Servizi agli Studenti

Capitolato Prestazionale

Sistema di gestione di credenziali digitali legate all'apprendimento

Servizio di implementazione, gestione e manutenzione di un sistema di gestione di credenziali digitali per l'emissione, condivisione e validazione delle competenze e dei risultati di apprendimento

Sommario

1. Definizioni

Amministratore	Tecnico interno a UniTrento
Ateneo/UniTrento	Il termine è comunemente utilizzato come sinonimo di 'Università di Trento'.
Attività didattiche/formative curricolari	Sono quelle esplicitamente previste in termini di Crediti Formativi Universitari (CFU) dagli ordinamenti e manifesti didattici dei corsi di studio.
Attività didattiche/formative extracurricolari	Sono aggiuntive a quelle previste dagli ordinamenti e manifesti didattici dei corsi di studio.
Badge Digitale o Digital Badge	Tipologia di credenziali digitali che si caratterizzano per il fatto che includono al loro interno metadati che permettono di validare l'evidenza di competenze professionali di diverso tipo.
Badge Class	Rappresenta il "tipo di badge". La Badge Class non contiene informazioni relative al singolo utente che ha conseguito il badge, ma solo le informazioni relative al 'tipo di badge' in sé: le competenze che il badge testimonia, i criteri necessari per conseguirlo, le prove da superare per dimostrare il possesso dei criteri, l'immagine grafica che lo rappresenta, etc. Ogni Badge Class può essere assegnata a molte persone che soddisfano i criteri di assegnazione.
Badge Assertion	Indica la singola istanza di una Badge Class rilasciata ad un determinato learner. Una Badge Assertion è quindi costituita da tutte le informazioni generali sul badge con in aggiunta le informazioni che identificano in modo univoco la persona che lo ha conseguito.
Badge Creator	La persona che all'interno del sistema crea le badge class, ne definisce tutte le caratteristiche e le organizza in raggruppamenti (progetti o milestones).

Badge Issuer	La persona che all'interno del sistema attribuisce i badge ai singoli learner, creando la badge assertion.
Corso di Studio	Tutti quei corsi che prevedono il rilascio di un titolo accademico: corso di laurea, di laurea magistrale, di specializzazione, di dottorato di ricerca e corso per master.
Credenziali di Autenticazione	Consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.
Credenziali digitali o digital credentials	Sono dichiarazioni digitali documentate contenenti affermazioni su una persona, emesse da enti preposti (istituto di istruzione, azienda ecc.) a seguito di un'esperienza di apprendimento.
Crediti Formativi Universitari (CFU)	Sono uno strumento per misurare la quantità di lavoro di apprendimento, compreso lo studio individuale, richiesto allo studente per acquisire conoscenze e abilità nelle attività formative previste dai corsi di studio. Un credito (CFU) corrisponde di norma a 25 ore di lavoro che comprendono lezioni, esercitazioni, etc., ma anche lo studio a casa.
Dipartimento	Il dipartimento è una struttura didattica che svolge funzioni finalizzate allo svolgimento della ricerca scientifica, all'organizzazione delle attività didattiche e formative, nonché delle attività rivolte all'esterno ad esse correlate o accessorie.
Docente	Responsabile di una Attività Didattica
Employer	L'azienda o ente che ricerca competenze

Endorser	L'ente (istituto di formazione o azienda) che manifesta un apprezzamento verso un'iniziativa di apprendimento promossa da un issuer o un traguardo di apprendimento conseguito da un learner;
Gestionale di Ateneo	Sistema informativo di Ateneo per la gestione della didattica, della carriera e dei servizi agli studenti. Il sistema attualmente in uso è Esse3 di Cineca.
Issuer	L'ente che emette credenziali digitali.
Learner	La persona che apprende, all'università o in altri contesti, in una logica di life-long e life-wide learning.
Learning Management System (LMS)	Un learning management system (LMS) è la piattaforma applicativa (o insieme di programmi) che permette l'erogazione dei corsi in modalità e-learning al fine di contribuire a realizzare le finalità previste dal progetto educativo dell'istituzione proponente. Il learning management system presidia la distribuzione dei corsi on-line, l'iscrizione degli studenti, il tracciamento delle attività on-line. Il LMS attualmente in uso presso UniTrento è Moodle.
Learning Record Store (LRS)	Memorizza i dati di apprendimento che vengono raccolti sotto forma di statement in formato xAPI. (maggiori info: https://xapi.com/learning-record-store/)
Manifesto degli Studi	Raccoglie le informazioni fondamentali del corso di studi. In esso sono indicati il piano degli studi ufficiale con l'elenco degli insegnamenti attivati per quell'anno accademico, suddivisi per anni; il periodo didattico in cui si svolgeranno le lezioni, il corrispettivo in crediti formativi per ogni esame.
Offerta Didattica	Insieme delle attività didattiche erogate in un determinato anno accademico.

Orario Lavorativo	Per orario lavorativo si intende la fascia oraria dalle ore 8 alle 17 nei giorni dal lunedì al venerdì.
Percorso di studio	È costituito dalle attività formative che lo studente deve sostenere per completare la propria carriera universitaria e conseguire il titolo di studio.
Piano degli Studi	È il percorso che comprende tutte le attività formative (insegnamenti, laboratori, ecc.) che si devono svolgere per conseguire la laurea. Alcune attività sono obbligatorie. Altre attività sono a libera scelta dello studente e altre ancora devono essere scelte dallo studente entro un elenco specificato nel manifesto degli studi.
Sistema anagrafiche di Ateneo	Sistema di gestione delle anagrafiche di Ateneo nel quale sono censiti i ruoli delle diverse categorie di utenti (cosiddetti "ruoli ADA")
Sistema, Software o Piattaforma	Sistema di gestione di credenziali digitali legate all'apprendimento.
Sistema di ticketing (Ticket System)	Strumento software per ricevere, monitorare, organizzare, assegnare e risolvere le richieste (ticket) di assistenza tecnica.
Servizio CERT (Computer Emergency Response Team)	Il servizio si occupa della gestione degli incidenti di sicurezza informatica per l'Ateneo.
Validator	Ruolo assegnato all'interno della piattaforma agli employers che hanno necessità di verificare le credenziali digitali che i learners hanno condiviso.
xAPI	Il formato xAPI (experience API) definisce la struttura dei dati (statement) raccolti durante l'apprendimento del learner. (maggiori info: https://xapi.com/overview/).

Aggiudicatario	Il Concorrente che ha presentato il miglior preventivo/offerta a UniTrento.
Appaltatore	Il soggetto con il quale UniTrento firmerà il Contratto.
AVCPass	Banca dati nazionale istituita presso l'A.N.A.C. per la verifica del possesso dei requisiti generali e speciali.
Capitolato Prestazionale	Il presente documento che definisce le caratteristiche tecniche del servizio.
Condizioni generali di contratto	Il documento contenente le condizioni generali di Contratto.
Condizioni particolari di Contratto	Il documento contenente le condizioni particolari del Contratto che sarà stipulato tra UniTrento e l'Aggiudicatario.
Concorrente	Ciascuno dei soggetti, siano essi in forma singola o raggruppata, che presenteranno un preventivo per il servizio richiesto
Direttore dell'esecuzione del Contratto	La persona fisica, all'uopo indicata da UniTrento, con il compito di gestire il rapporto contrattuale con l'Appaltatore.
Mandatario	Per i Concorrenti raggruppati o raggruppandi, il componente che assume il ruolo di capofila del gruppo costituito o costituendo.
Offerta	Il preventivo corredato della documentazione amministrativa richiesta economica che ciascun Concorrente deve presentare
Responsabile dell'Appaltatore	La persona fisica indicata dall'Appaltatore per la gestione del Contratto con funzioni di coordinamento e di garanzia al buon funzionamento del servizio.
Responsabile del procedimento	dott. Paolo Zanei
Servizio	L'oggetto dell'appalto.

2. Obiettivi del progetto

Obiettivo del progetto è dotare l'Università degli Studi di Trento (di seguito UniTrento o Ateneo) di un sistema software web based adatto alla gestione di credenziali digitali legate all'apprendimento (di seguito Sistema o Piattaforma).

Le tipologie di credenziali digitali che UniTrento intende gestire sono:

- Titoli di studio e altri attestati rilasciati alla conclusione del percorso universitario: diploma di laurea e laurea magistrale, Master di I e II livello, attestati rilasciati a seguito di percorsi di formazione avanzata (Corsi di Perfezionamento, di Specializzazione, Formazione Insegnanti e Percorsi di Eccellenza);
- Micro Credentials: sono strumenti che si inseriscono nel contesto del lifelong e lifewide learning permettendo di riconoscere e tracciare apprendimenti sia in ambito formale che non formale. La formazione viene resa flessibile e modulare realizzando percorsi formativi brevi che permettano di acquisire competenze orientate al mercato del lavoro. All'interno di questo panorama le micro-credenziali possono essere cumulate per attestare e quantificare il livello di apprendimento di specifiche capacità o competenze, oppure possono essere raggruppate in percorsi, al termine dei quali è possibile riconoscere il raggiungimento di traguardi di più ampio respiro (milestones);
- Attività didattiche e formative: queste attività possono essere singole, oppure articolate in percorsi al termine dei quali è possibile riconoscere il raggiungimento di traguardi di più ampio respiro (milestones);

Il sistema dovrà permettere di:

- Definire le credenziali digitali in tutti i dettagli e organizzarle in percorsi;
- Identificare correttamente le persone alle quali si intende attribuire una credenziale digitale che ne attesti le abilità, competenze o le qualifiche;
- Emettere o revocare una credenziale digitale associata ad una persona specifica. Entrambe queste operazioni possono essere svolte solo da enti riconosciuti e preposti a ciò.
- Memorizzare e gestire le credenziali digitali emesse dagli enti preposti.
- Riferire le credenziali digitali a framework per la referenziazione delle competenze condivisi a livello europeo e internazionale;
- Condividere le credenziali digitali con datori di lavoro e altre organizzazioni. Ciascun individuo può scegliere con chi condividere le proprie credenziali e con chi no.
- Verificare l'autenticità delle credenziali digitali che sono state volontariamente condivise da una persona con un datore di lavoro o altra organizzazione. È auspicabile poter verificare anche l'accreditamento dell'ente preposto all'emissione delle credenziali (ad

es. verificare se un determinato ente è autorizzato ad emettere un determinato tipo di credenziale riguardo ad una specifica qualifica).

Il sistema deve essere sviluppato in modalità web based e tutte le sue funzionalità devono essere disponibili agli utenti autorizzati, previo accesso tramite credenziali di autenticazione di Ateneo da qualsiasi dispositivo connesso alla rete Internet.

Opportune indicazioni in merito verranno fornite durante la fase di configurazione.

3. Oggetto del servizio

L'Appaltatore dovrà fornire a UniTrento i seguenti servizi:

- licenza d'uso dell'applicativo, del database o di quant'altro necessario al funzionamento del sistema. L'applicativo dovrà rispettare i requisiti funzionali e tecnici descritti nel presente capitolato prestazionale;
- il servizio hosting del software: l'Appaltatore ha l'onere della manutenzione ordinaria e straordinaria, della manutenzione dei server, della messa in sicurezza e della gestione dei backup periodici del software e dei dati gestiti;
- l'installazione, la configurazione, secondo i parametri e le caratteristiche del servizio richiesto da UniTrento, ed il collaudo dei software;
- la formazione iniziale e continua, del personale operativo di UniTrento (Operatori);
- il servizio di manutenzione, aggiornamento e assistenza tecnica relativi al software.

4. Destinatari

I destinatari del sistema sono:

- Operatori:
  - Amministratori del sistema: personale di UniTrento che svolge supporto per l'uso dei servizi online.
  - Badge creator: personale di UniTrento che provvede alla creazione delle credenziali digitali all'interno del sistema;
  - Badge issuer: personale di UniTrento che all'interno del sistema provvede al rilascio delle credenziali digitali ai vari learner che ne hanno diritto;
- Utenti:
  - Learners: studenti, laureati, ex studenti, dottorandi, ricercatori, docenti e personale tecnico amministrativo dell'Università di Trento e utenti esterni destinatari di credenziali digitali;

- Employers: enti con i quali i learners condividono le credenziali digitali per certificare i loro traguardi di apprendimento;
- Endorser: enti (istituti di formazione o aziende) che manifestano un apprezzamento verso un'iniziativa di apprendimento promossa da un issuer o un traguardo di apprendimento conseguito da un learner;

5. Requisiti funzionali e tecnici di sistema

Di seguito si riportano le caratteristiche tecniche e funzionali minime che il sistema/software dovrà garantire. Per semplicità di esposizione una parte dei requisiti viene raggruppata per tipologia di utilizzatore. Non potranno essere prese in considerazione offerte condizionate, o che non rispettino i requisiti minimi o nel caso di mancanza anche di uno solo dei suddetti requisiti.

5.1. Accesso al sistema e profilazione utenti

Tutti gli utenti con ruoli che prevedono l'autenticazione, accedono alle funzioni del sistema con Single Sign On d'Ateneo basata su Shibboleth, secondo le modalità indicate al paragrafo *Autenticazione e dati utenti UniTrento*.

Gli utenti devono essere profilati in modo da poter accedere alle funzionalità volute dall'amministratore di sistema e in forme diverse e controllate (es. sola visualizzazione, modifica…) a seconda del profilo. Deve essere possibile individuare l'utente che ha apportato inserimenti e/o modifiche al sistema (tracciabilità delle operazioni).

I profili da attivare sulla piattaforma sono:

- Amministratore,
- Badge Creator (con profili e autorizzazioni diverse),
- Badge Issuer (con profili e autorizzazioni diverse),
- Learner,
- Endorser,
- Validator (senza autenticazione).

Gli utenti di tipo Amministratore possono abilitare o bloccare l'accesso ai sistemi ad altri utenti;

Gli utenti di tipo Amministratore possono assegnare un ruolo ad ogni utente (amministratore, badge creator, badge issuer, endorser...), i ruoli specificano i permessi di accesso alle varie funzionalità.

La verifica dei badge deve essere possibile tramite un'interfaccia web pubblica che non richiede autenticazione.

5.2. Autenticazione e dati utente UniTrento

L'autenticazione dell'utente deve avvenire su pagine protette https utilizzando il protocollo SAML 2.0 nell'implementazione Identity Provider Shibboleth (IDP) in uso presso UniTrento.

Il software, nelle parti riservate, costituisce Service Provider (SP) nel protocollo di autenticazione. Il servizio di Identity Provider (IDP) viene fornito da UniTrento che è membro delle federazioni IDEM/EduGAIN.

UniTrento fornirà il supporto tecnico necessario all'attivazione dell'autenticazione al sistema con Single Sign On d'Ateneo. È a carico dell'Appaltatore la predisposizione del servizio SP sui propri server.

I parametri del servizio saranno concordati durante la fase di configurazione.

5.3. Requisiti generali di Sistema

L'Appaltatore si impegna a garantire l'emissione dei permessi di Amministratore, Creator, Issuer e Endorser a seguito di formale verifica della credibilità dell'ente che emetterà le credenziali digitali. Questo requisito mira ad assicurare la credibilità delle credenziali digitali emesse tramite la piattaforma, deve infatti esserci una formale verifica che credenziali digitali emesse dallo issuer UniTrento siano effettivamente riconducibili allo stesso ente.

Il sistema deve permettere la gestione di diversi tipi di credenziali digitali adatte a diverse esigenze - dalle micro credentials ai titoli notarizzati. In particolare deve permettere la gestione delle seguenti tipologie di credenziale:

- Attestati - credenziali tradizionali, spesso con valore legale, che registrano la partecipazione ad occasioni di apprendimento informale;
- Crediti - attestano la partecipazione a percorsi di apprendimento formale;
- Certificazioni - ottenute a seguito di un'attività di valutazione e verifica delle competenze acquisite.

Il sistema deve rifarsi agli standard internazionali più aggiornati e a tecnologie aperte nella definizione e nella assegnazione delle credentials. Alle credenziali digitali (Badge Assertion) deve essere possibile associare una serie di caratteristiche quali:

- Emittente (inclusa breve descrizione) = Ente Formatore;
- Destinatario = Learner;

- Titolo conseguito;
- Data di conseguimento;
- Criteri di emissione;
- Durata della formazione;
- Contenuti;
- Modalità di Erogazione;
- Coordinatore Scientifico;
- Riferimenti Normativi della formazione;
- Data di fine validità: la credenziale deve risultare valida solo fino al termine indicato dalla data di fine validità; successivamente deve rimanere visibile, ma non più valida;
- Riferimento a sistemi per la gestione e la referenziazione delle competenze.

Il sistema deve registrare le informazioni e garantirne l'integrità in modo assoluto grazie all'uso di sistemi crittografici avanzati. Deve fornire inoltre la garanzia dell'immutabilità dei dati archiviati, la decentralizzazione della rete e la gestione condivisa delle informazioni da parte di tutti i partecipanti alla rete. Tutti i dati devono essere gestiti seguendo i dettami del Privacy By Design, separando quindi identità, persona e contesto.

Il sistema deve integrarsi con sistemi per la gestione e la referenziazione delle competenze condivisi a livello europeo (ad es. ESCO - European Skills, Competences, Qualifications and Occupations) e internazionale, per permettere una interoperabilità e portabilità semantica delle credentials. Ciò consente di progettare le attività formative ponendo l'attenzione non soltanto sul breve termine, ma sull'intero percorso futuro del learner, portandolo a sviluppare competenze più spendibili nel mondo del lavoro.

Per particolari tipi di credenziali digitali che non hanno scadenza (es. titoli di studio) deve essere garantita la completa portabilità delle credenziali digitali: tutte le informazioni rilevanti devono essere incorporate nel badge, eliminando i riferimenti a collegamenti esterni che potrebbero venire meno. In questo modo la verificabilità del badge viene semplificata e i destinatari di un badge non si troveranno di fronte ad un badge "incompleto" se la piattaforma di badge che lo ha emesso cessasse di esistere.

5.4. Requisiti specifici per Amministratori

Oltre a quanto descritto nei paragrafi precedenti, il sistema di gestione delle Credenziali Digitali che si intende acquisire deve rendere disponibili agli Amministratori le seguenti funzionalità:

- Supportare la definizione e personalizzazione del profilo dell'azienda issuer inserendo almeno i seguenti parametri:
    - Nome dello Issuer;

  - Marchio;
  - Descrizione dello Issuer;
- Supportare la gestione di più issuer (ad es. Dipartimenti/Centri) che emettono badges e possono essere tutti raggruppati sotto l'unico cappello di UniTrento.
- Offrire strumenti che permettano all'Ateneo di rendere visibili in rete le attività collegate all'emissione di credenziali digitali, nello specifico:
  - Permettere la presentazione dello issuer su pagine HTML;
  - Permettere la presentazione di progetti e attività su pagine HTML;
  - Permettere la presentazione di specifici badge su pagine HTML;

  Su queste pagine HTML deve essere possibile sia la ricerca semplice che quella avanzata e a testo libero per garantire una adeguata visibilità allo issuer e alle diverse attività promosse.

5.5. Requisiti specifici per Badge Creator

Il sistema di gestione delle Credenziali Digitali che si intende acquisire deve rendere disponibili ai Badge Creator le seguenti funzionalità:

- Offrire strumenti a supporto della progettazione di un sistema di credenziali digitali coerente con gli obiettivi che si intendono raggiungere. Deve essere possibile:
  - definire i criteri di assegnazione delle credenziali;
  - specificare le procedure messe in atto per valutare, assegnare e consegnare le credenziali;
  - definire progetti e aggregare credenziali identificando le connessioni tra i badge singoli in modo da formare collezioni su un tema particolare, oppure percorsi di apprendimento, nei quali i badge devono essere conseguiti in un determinato ordine o in un determinato numero;
  - promuovere le attività più significative sia in termini di progetti che di singole credenziali.
- Permettere la gestione in autonomia delle attività di customizzazione dei badge garantendo quindi la possibilità di personalizzare liberamente le credenziali digitali dal punto di vista grafico e dei metadati contenuti, creando anche dei modelli;
- Permettere la creazione e definizione di un badge in formato HTML;
- Garantire la possibilità di creare badge di tipo "Milestone" che non costituiscono un badge vero e proprio, ma rappresentano il completamento di un percorso durante il quale sono stati collezionati vari badge. Il Badge Milestone racchiude i singoli badge acquisiti durante il percorso.

5.6. Requisiti specifici per Badge Issuer

Il sistema di gestione delle Credenziali Digitali che si intende acquisire deve rendere disponibili ai Badge Issuer le seguenti funzionalità:

- Rilascio delle credenziali digitali (badge assertion) - si configura come inserimento di uno statement all'interno del LRS. Se è presente una regola di assegnazione badge e il Learner è iscritto al sistema, viene contestualmente rilasciata la relativa badge assertion. L'inserimento dello statement può essere fatto:
  - manualmente per il singolo learner;
  - manualmente per un gruppo di learner: il sistema deve mettere a disposizione opportune interfacce per il caricamento massivo dei dati tramite file .csv o .xls.
  - automaticamente attraverso integrazione con il Learning Management System (LMS) di Ateneo (Moodle), il Gestionale di Ateneo e eventuali altri sistemi utilizzati per registrare i traguardi di apprendimento;
- Cancellazione delle credenziali digitali (badge assertion);
- Revoca delle credenziali digitali sia nel caso di modifica dell'indirizzo e-mail del destinatario che per variazione delle date di validità;
- Riemissione delle credenziali digitali;
- Strumenti a supporto dell'archiviazione delle credenziali digitali: il sistema deve permettere di aggregare, pubblicare ed esportare le singole istanze delle credenziali digitali emesse (Badge Assertion). La piattaforma deve essere in grado di importare i badge emessi in diversi formati. Il sistema deve garantire la coerenza e consistenza dei badge sia nella fase di importazione che in quella di esportazione.
- Fornire strumenti che permettano allo issuer di notificare a eventuali persone interessate (ad es. docenti), l'emissione di badge assertion su una specifica badge class;
- Rendere disponibili strumenti per inviare nuovamente la notifica di emissione di una badge assertion al learner che dovesse averla smarrita.

5.7. Requisiti specifici per Learner

Il sistema di gestione delle Credenziali Digitali che si intende acquisire deve rendere disponibile ai learners di UniTrento le seguenti funzionalità:

- Strumenti per collezionare, gestire e verificare le proprie credenziali digitali che devono includere anche le seguenti funzionalità:
  - stampare i propri Attestati/Certificati;
  - gestire email alternative per raccogliere le credenziali ricevute su indirizzi e-mail diversi da quello istituzionale di Ateneo;
  - scaricare link e immagini delle credenziali;

    - definire la visibilità delle proprie credenziali;
- Strumenti per costruire pagine personali per la presentazione di curriculum digitali (e-Portfolio). Ciascun learner può costruire una o più pagine personali che permettano di rappresentare le competenze in maniera differenziata in funzione del contesto in cui devono essere fruite. Le pagine devono poter essere personalizzate inserendo, oltre alle credenziali digitali, anche informazioni personali dell'utente.
- Strumenti per importare Badge rilasciati da qualsiasi piattaforma purché conformi allo standard;
- Strumenti per condividere i propri Badge e la propria pagina di profilo sui Social Networks;
- Strumenti per verificare la validità delle proprie credenziali digitali.

5.8. Requisiti specifici per Endorser

Il sistema deve fornire strumenti di supporto all'endorsment di issuer, di credenziali digitali e di progetti. L'endorsement ha lo scopo di rendere le credenziali più credibili, ricercabili e tracciabili; consente infatti alle organizzazioni di terze parti di indicare pubblicamente quali badge sono allineati ai loro valori o quelli che sono i più significativi e utili per loro. Il sistema deve supportare l'endorsement nei seguenti casi:

- UniTrento può manifestare un endorsement su una specifica tipologia di credenziale di un ente terzo prima che venga rilasciata (endorsement sulla Badge Class);
- UniTrento può manifestare un endorsement su uno specifico progetto di un ente terzo;
- UniTrento può manifestare un endorsement sul profilo di un altro issuer così che l'endorsement possa propagarsi su tutte le sue credenziali digitali, coinvolgendo sia le Badge Class che le Badge Assertion.

La piattaforma permetterà anche ad eventuali enti terzi (aziende, altri istituti di formazione ecc.) che dispongano del ruolo di endorser di esprimere apprezzamenti riguardo a UniTrento in generale, a un particolare progetto che UniTrento propone oppure ad una specifica credenziale che UniTrento rilascia.

5.9. Requisiti specifici per Validator

Il sistema di gestione delle Credenziali Digitali che si intende acquisire deve rendere disponibile ai validators di UniTrento o di altri Employers le funzionalità necessarie per verificare la validità delle credenziali digitali condivise dai learners tramite e-mail o altri social networks.

Queste funzionalità devono essere messe a disposizione senza necessità di autenticarsi al sistema.

5.10. Strumenti di analisi dei dati e reportistica

Il sistema deve mettere a disposizione delle differenti tipologie di utenti operatori (Amministratore, Badge Creator e Badge Issuer) i seguenti dati relativi all'attività di emissione di credenziali digitali:

- il numero totale e la lista di badge class e di badge assertion emesse, con la possibilità di raggrupparle sulla base del Progetto a cui appartengono;
- per ciascuna badge class:
    - il numero e la lista delle badge assertion emesse, includendo i dettagli dei learner;
    - informazioni aggregate sul numero di condivisioni effettuate dai learner;
- per ciascun learner: il numero e la lista di badge assertion attribuite, comprensiva di tutti i dettagli relativi ai metadati contenuti nel badge;

UniTrento si riserva di richiedere ulteriori report in funzione delle necessità dell'Ateneo.

5.11. Generazione delle credenziali digitali

Nel momento in cui il Learner si iscrive al sistema di credenziali digitali, vengono elaborati gli statement presenti nel LRS che lo riguardano (per le quali si trova una corrispondenza di indirizzo email) e se sono presenti delle regole (definite dal Badge Creator) allora viene emessa la corrispondente badge assertion. Fintanto che il Learner non si iscrive al sistema di credenziali digitali, accettando le relative privacy policy, gli statement rimangono all'interno dell'LRS.

5.12. Interoperabilità

Il sistema deve offrire una infrastruttura che possa essere richiamata ed integrata nei sistemi che gestiscono il ciclo di attività che precede e segue il rilascio di credenziali digitali. Deve essere garantita l'interoperabilità tramite API con strumenti già presenti in Ateneo quali il Gestionale di Ateneo (Esse3) e il Learning Management System (Moodle).

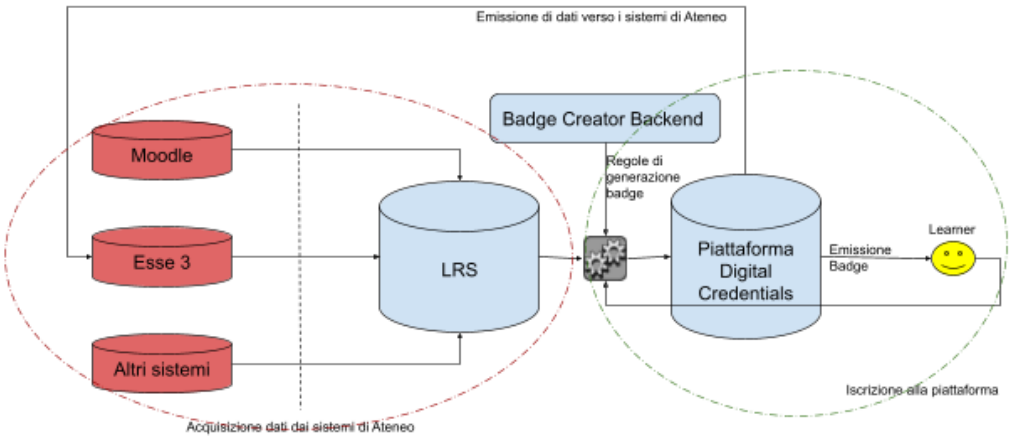

Diagramma di integrazione dei sistemi

5.12.1. Acquisizione dati dai sistemi di Ateneo

Il sistema deve essere in grado di registrare all'interno del proprio LRS, gli statements ricevuti dai sistemi di Ateneo in formato xAPI (https://github.com/adlnet/xAPI-Spec).

I principali statement che alimenteranno il LRS saranno:

- statement da parte del Gestionale di Ateneo (Esse3): per lo più inerenti al conseguimento di un titolo da parte del learner - verranno emessi in formato xAPI;
- statement da parte del Learning Management System (Moodle): inerenti al completamento di un corso da parte del learner. Verranno trasmessi tramite plugin Logstore xAPI (https://moodle.org/plugins/logstore_xapi, release v4.6.0 o successive;
- statement da parte di eventuali altri sistemi presenti in Ateneo: verranno emessi rispettando lo standard xAPI

Il sistema deve inoltre permettere al personale UniTrento che possiede il ruolo di *Badge Issuer* (vedi paragrafo *Requisiti specifici per Badge Issuers*), l'acquisizione massiva nel LRS di statements tramite importazione di file CSV, riportante le informazioni essenziali per il rilascio di un badge (nome, cognome e indirizzo mail del learner, oggetto del completamento, data completamento).

5.12.2. Emissione di dati verso i sistemi di Ateneo

Il sistema deve essere configurabile affinché al momento del rilascio di un badge al learner, possa comunicare l'evento ai sistemi di Ateneo tramite:

- chiamata web service al sistema Gestionale di Ateneo (Esse3), indicando le informazioni sul badge emesso (soggetto ricevente il badge, oggetto del badge, data conseguimento)
- chiamata web service/webapi ad eventuali altri sistemi presenti in Ateneo, indicando le informazioni sul badge emesso (soggetto ricevente il badge, oggetto del badge, data conseguimento)

5.13. Multicanalità e Multipiattaforma

La consultazione della piattaforma deve essere consentita senza alcuna limitazione, in maniera indipendente dal sistema operativo e dal tipo di browser utilizzato dagli utenti per le piattaforme di uso corrente nelle versioni diffuse. Non deve prevedere plug-in o estensioni specifiche o supportate da una sola piattaforma.

In particolare si deve prevedere il supporto per diverse versioni di browser: a titolo esemplificativo e non esaustivo Chrome, Edge, Firefox, Safari. L'interfaccia web del sito dovrà essere fruibile anche su dispositivi mobili dotati dei sistemi operativi più diffusi sul mercato, in particolare:

- Android v.5.1 e superiori;
- IoS v.11 e superiori.

5.14. Gestione Multilingua

Il sistema deve supportare la presentazione di contenuti o parte di essi, in due lingue, italiano e inglese, selezionabili direttamente da parte degli utenti del sistema.

Selezionando una lingua, devono essere presentate all'utente del sistema unicamente le informazioni tradotte in quella lingua. Le lingue richieste sono italiano e inglese.

La scelta della lingua può essere fatta in qualsiasi punto della navigazione e conservarsi per l'intera sessione (se non ulteriormente modificata). L'interfaccia deve essere tradotta completamente (label, menu di navigazione, help, didascalie, ecc.).

Le credenziali digitali devono poter essere emesse in almeno 4 lingue diverse (italiano, inglese, tedesco e spagnolo).

5.15. Accessibilità

L'interfaccia utente di front end deve essere conforme ai requisiti di Accessibilità richiesti dalla Legge 9 gennaio 2004, n. 4, Disposizioni per favorire l'accesso dei soggetti disabili agli strumenti informatici e alle Linee Guida AgID sull'accessibilità degli strumenti informatici.

6. Requisiti di servizio

6.1. Software as a Service (SAAS)

I servizi saranno erogati dall'Appaltatore in modalità SAAS (Software as a Service).

L'Appaltatore dovrà aver qualificato il servizio Software as a Service (SaaS) della PA ai sensi della circolare AgID n. 3 del 9 aprile 2018 «Criteri per la qualificazione di servizi SaaS per il Cloud della PA». In alternativa, l'Appaltatore dovrà dimostrare di aver iniziato il processo di qualificazione, attraverso la piattaforma AgID "Catalogo dei servizi Cloud per la PA qualificati - Cloud Marketplace AgID".

L'esito negativo di qualificazione del servizio SaaS dell'Appaltatore da parte di AgID o la perdita della qualifica nel corso del contratto è condizione di risoluzione dello stesso.

L'Appaltatore si impegna a fornire i servizi di configurazione, disponibilità, correttezza ed evoluzione del sistema rispettando i termini definiti all'interno del presente documento, con particolare riferimento ai paragrafi: *Requisiti di servizio, Sicurezza, Modalità e tempistiche di contratto.*

UniTrento è esente da manutenzioni ordinarie e straordinarie, oltre che dalla gestione dei backup giornalieri.

Sono a carico dell'Appaltatore gli oneri derivanti dall'utilizzo della piattaforma di sviluppo e le licenze di utilizzo della piattaforma Web (sistema host e DBMS compresi), compresi tutti gli oneri eventuali per l'utilizzo delle librerie di terze parti qualora utilizzate.

6.2. Disponibilità del servizio

Il servizio deve essere disponibile 24 ore su 24 e 7 giorni su 7, salvo finestre di manutenzione ordinaria e interventi di manutenzione programmata.

Interruzioni del servizio sono ammesse, se concordate dall'Appaltatore con UniTrento, solo in caso di effettiva necessità.

L'indisponibilità del servizio è da considerarsi come malfunzionamento di gravità bloccante e comporta l'applicazione delle relative penali.

6.3. Formazione

Le attività di formazione saranno rivolte agli operatori, con lo scopo di trasmettere conoscenze tali da consentire loro di procedere in maniera autonoma, in tutte le fasi riguardanti l'utilizzo del

servizio. L'Appaltatore si impegna a fornire per tutta la durata contrattuale formazione alle diverse categorie di utenti sulle funzionalità presenti nel software.

A corredo fornirà anche documentazione sull'uso e manutenzione del sistema predisponendo apposito manuale. Tutta la documentazione deve essere fornita in lingua italiana e in formato elettronico.

In caso di modifiche agli applicativi, l'aggiudicatario si impegna a fornire contestualmente la versione aggiornata della documentazione, sempre in formato elettronico.

6.4. Assistenza Tecnica e service level

L'Appaltatore dovrà mettere a disposizione gli strumenti necessari per la gestione di richieste di intervento e assistenza formulate dagli Amministratori di Sistema di UniTrento. Il supporto verrà svolto da remoto e dovrà essere operativo tutti i giorni lavorativi, per permettere a UniTrento di segnalare malfunzionamenti o guasti del software. È auspicabile la disponibilità di uno strumento di segnalazione, tracciamento e gestione che consenta di effettuare le segnalazioni (sistema di ticketing).

La realizzazione di un intervento di assistenza dovrà essere articolata come segue:

- Richiesta di intervento da parte di UniTrento: effettuata tramite l'Amministratore autorizzato ad interfacciarsi con l'Appaltatore, il quale classifica la richiesta con gravità:
    - Bloccante: Comporta il blocco totale delle funzionalità garantite dal sistema o parti rilevanti dello stesso, oppure un degrado significativo delle performance operative, tale da rendere il sistema inutilizzabile o l'operatività degli utenti fortemente compromessa;
    - Non Bloccante: Non ha un impatto immediato, evidente e generalizzato sull'operatività del sistema. Si intende un malfunzionamento che limita, ma non impedisce l'utilizzo all'operatore o all'utente di una funzionalità, consentendo comunque il raggiungimento del risultato finale con funzionalità alternative.
- Presa in carico da parte dell'Appaltatore e definizione dei tempi di risoluzione: l'Appaltatore valuta la richiesta ricevuta da UniTrento e la prende in carico entro alcune ore. Successivamente informa UniTrento dei tempi di risoluzione previsti per l'anomalia segnalata. Il tempo massimo di risposta, entro il quale l'Appaltatore dà evidenza dei tempi di risoluzione del problema, deve essere pari a mezza giornata lavorativa calcolata a partire dall'orario di invio della comunicazione di UniTrento e considerando lavorativa la fascia oraria dalle 8 alle 17 dal lunedì al venerdì.
- Risoluzione della problematica segnalata dall'utente: Il tempo massimo di risoluzione della problematica segnalata

- non deve essere superiore a 1 giorno lavorativo nel caso di gravità Bloccante;
- non deve superare i 3 giorni lavorativi nel caso di gravità non Bloccante;

Tale livello di servizio deve essere mantenuto per tutta la durata contrattuale.

6.5. Manutenzione

L'Appaltatore garantisce il corretto e continuo funzionamento del software e si impegna ad effettuare tutti i servizi necessari a raggiungere tale obiettivo. Il servizio di manutenzione verrà fornito a seguito dell'emissione del Certificato di Regolare Esecuzione per tutta la durata del contratto.

Durante il periodo di interruzione delle funzionalità del sistema per manutenzione, agli utenti che si collegano dovrà essere esposto un messaggio che li informi della momentanea indisponibilità e che dia indicazioni sull'ora a partire dalla quale il servizio sarà di nuovo funzionante.

6.5.1. Manutenzione correttiva

Scopo della manutenzione correttiva è correggere eventuali malfunzionamenti del sistema applicativo. Questo tipo di intervento non modifica né le funzionalità né la struttura dati dell'applicazione, ma ne ripristina il corretto funzionamento. Rientra in questo servizio l'effettuazione del recupero o ricostruzione al meglio dei dati del sistema persi o invalidati in conseguenza del malfunzionamento stesso. I malfunzionamenti possono essere identificati autonomamente dall'Appaltatore, oppure segnalati dagli Amministratori di Sistema UniTrento tramite il servizio di Assistenza Tecnica. Interventi aventi carattere di urgenza o di continuità di servizio possono essere avviati autonomamente dall'Appaltatore, previa informazione degli Amministratori di Sistema UniTrento. Per malfunzionamenti cui UniTrento non attribuisca carattere di criticità e urgenza (non bloccanti), l'attivazione dell'intervento correttivo verrà concordata su base pianificata.

6.5.2. Manutenzione adattativa

Scopo della manutenzione adattativa sono gli interventi volti a mantenere aggiornato il sistema nel tempo, sia per il variare dell'ambiente tecnologico (ad es. modifiche di piattaforme e/o configurazioni hardware o di rete, dei prodotti di base, di telecomunicazioni e del DataBase), sia per far fronte a nuovi adempimenti di legge/normativi o alla introduzione di nuovi standard di riferimento per le credenziali digitali. Questi interventi verranno sviluppati su base pianificata, fatte salve scadenze e criticità imposte da soggetti Terzi (ad es. nuova normativa con scadenze stringenti).

6.5.3. Manutenzione evolutiva

La manutenzione evolutiva include tutte le attività di analisi, sviluppo e rilascio di implementazioni e/o modifiche migliorative. In particolare gli interventi di manutenzione evolutiva avranno, ad esempio, ad oggetto le seguenti possibili necessità:

- raccolta, analisi, sviluppo e messa in produzione di un nuovo requisito;
- modifica e/o miglioria di una funzionalità esistente;
- modifica e/o miglioria dell'interfaccia utente (nel rispetto dei Requisiti di interfaccia specificati nel paragrafo *Multicanalità e multipiattaforma*).

La realizzazione di un intervento di manutenzione evolutiva dovrà essere articolata come segue:

- Richiesta di un intervento di manutenzione evolutiva straordinaria da parte di UniTrento con specifica della data di fabbisogno;
- Analisi da parte dell'Appaltatore della fattibilità della richiesta;
- Inoltro, entro 7 giorni naturali consecutivi dalla richiesta, di un documento di stima riportante:
    - la stima dell'effort richiesto per la realizzazione dell'intervento in termini di ore/uomo;
    - la redazione del Piano di Lavoro a carico dell'Appaltatore;
    - la data della messa in esecuzione della richiesta.

  Tale documentazione deve essere inviata dall'Appaltatore a UniTrento tramite e-mail.
- Approvazione dell'intervento da parte di UniTrento.
- Sviluppo e realizzazione delle modifiche migliorative nei tempi indicati nel documento.

L'Appaltatore dovrà garantire nel prezzo di offerta un numero di 6 giornate/uomo (indipendenti dalla tipologia di professionalità coinvolte) da usufruire nel corso dei primi 24 mesi di contratto per le attività necessarie alla messa in produzione degli interventi evolutivi straordinari richiesti. Il numero di 6 giornate/uomo (indipendenti dalla tipologia di professionalità coinvolte) dovrà essere garantito per le medesime attività anche nei 24 mesi successivi in caso di attivazione dell'opzione di rinnovo.

6.6. Backup e Restore

L'Appaltatore dovrà eseguire almeno un backup giornaliero notturno, con retention di 10 giorni.

Il ripristino dei dati per eventi straordinari o su richiesta di UniTrento va fatto entro massimo 24 ore dal momento della richiesta.

6.7. Prestazioni - Capacity Plan

Il sistema dovrà supportare, senza modifiche alle prestazioni minime previste, 100 accessi utente contemporanei.

Il sistema dovrà essere in grado di erogare i contenuti, compresi i contenuti multimediali, secondo il criterio della "adeguata esperienza di navigazione" da parte dell'utente: la velocità di risposta dovrà essere paragonabile a quella sperimentabile sugli altri servizi online di Ateneo assimilabili.

Le prestazioni - tempo di risposta / numero di sessioni - saranno misurate, in contraddittorio con l'Appaltatore, all'atto dell'emissione del Certificato di Regolare Esecuzione e nuovi rilievi potranno essere effettuati anche successivamente per verificarne il mantenimento nel tempo.

La mancata erogazione dei servizi richiesti è da considerarsi come malfunzionamento "grave" e comporta l'applicazione di relative penali.

7. Sicurezza

Per sicurezza del sistema si intende la capacità di proteggere funzioni e dati da utenti non autorizzati. In particolare devono essere adottate tutte le misure atte a garantire la riservatezza dei dati applicativi e delle informazioni riguardanti gli utenti dei servizi.

Il sistema garantisce l'aderenza del servizio fornito alle "Misure minime di sicurezza ICT per le pubbliche amministrazioni" (cfr. https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict) e la confidenzialità dei propri documenti (prima e dopo analisi) e la cancellazione del materiale.

In particolare devono essere rispettate le misure minime di sicurezza, almeno di livello minimo e standard, delle classi di seguito elencate:

- ABSC 4 (CSC 4): VALUTAZIONE E CORREZIONE CONTINUA DELLA VULNERABILITÀ che prevede che vengano implementati strumenti automatici che forniscano report con indicazioni delle vulnerabilità più critiche, tali report dovranno essere messi a disposizione del servizio CERT (Computer Emergency Response Team) dell'Ateneo;
- ABSC 5 (CSC 5): USO APPROPRIATO DEI PRIVILEGI DI AMMINISTRATORE

8. Privacy

8.1. Trattamento dei dati personali - Informativa ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679

Ai sensi degli artt. 13 e 14 del Regolamento UE 2016/679 "Regolamento Generale per la Protezione dei Dati Personali" (di seguito anche "GDPR"), si forniscono le seguenti informazioni.

Il Titolare del trattamento dei dati personali è l'Università degli Studi di Trento, via Calepina n. 14, 38122 Trento (TN); email: ateneo@unitn.it.; ateneo@pec.unitn.it.

Il Responsabile della protezione dei dati, al quale rivolgersi per informazioni relative ai propri dati personali, può essere contattato al seguente indirizzo email: rpd@unitn.it.

Finalità e natura del trattamento: I dati personali raccolti verranno trattati dall'Università nell'ambito dell'esecuzione dei propri compiti di interesse pubblico esclusivamente per la finalità di stipulazione ed esecuzione del contratto nonché per l'adempimento dei connessi obblighi di legge (art. 6, 1 par., lett. e), b) e c) e art. 10 del GDPR; art. 2-octies Codice Privacy). Il conferimento dei dati è indispensabile per la stipulazione ed esecuzione del contratto e il mancato conferimento determina l'impossibilità di procedere alla stipula.

Fonte e categorie dei dati: I dati sono raccolti presso l'interessato e presso altri soggetti esterni o provengono da fonti accessibili al pubblico. I dati personali trattati sono dati personali comuni (quali dati anagrafici, dati di contatto, codice fiscale, estremi identificativi del documento di riconoscimento; dati economico/finanziari, dati fiscali, dati bancari) e dati personali relativi a condanne penali e reati (c.d. dati giudiziari).

Modalità di trattamento: il trattamento dei dati personali viene effettuato con modalità cartacea e/o informatizzata da parte di personale autorizzato al trattamento dei dati in relazione ai compiti e alle mansioni assegnate e nel rispetto dei principi di liceità, correttezza, trasparenza, pertinenza, non eccedenza, riservatezza ed in modo da garantire un'adeguata sicurezza.

Destinatari dei dati: I dati personali potranno essere comunicati, oltre che al personale di Ateneo coinvolto nel perseguimento delle finalità sopra indicate, anche ad altri soggetti terzi, pubblici e privati, per il perseguimento delle suddette finalità nonché per l'adempimento di un obbligo di legge e/o di un provvedimento dell'Autorità giudiziaria.

Conservazione: i dati personali saranno conservati per il periodo necessario alla realizzazione delle finalità sopraindicate e comunque per il tempo necessario all'assolvimento degli obblighi di legge. In ogni caso saranno conservati per il tempo stabilito dalla normativa vigente e/o dalla

regolamentazione di Ateneo in tema di gestione e conservazione della documentazione prodotta dall'Università nello svolgimento della propria attività istituzionale.

Diritti degli interessati: in ogni momento potranno essere esercitati nei confronti del Titolare ai contatti sopra indicati i diritti di cui al Capo III del Regolamento UE 2016/679, quali il diritto di accesso, rettifica, integrazione e, nei casi previsti, la cancellazione, la limitazione del trattamento dei dati e il diritto di opposizione. Qualora venga riscontrata una violazione del Regolamento UE 2016/679, è possibile proporre reclamo al Garante per la Protezione dei dati personali ai sensi dell'art. 77 del GDPR.

Per maggiori informazioni consultare l'informativa completa pubblicata sul portale di Ateneo al seguente link: https://www.unitn.it/privacy.

8.2. Nomina dell'Appaltatore a Responsabile del trattamento dati

Ai sensi e per gli effetti dell'art. 28 del Regolamento, l'Università degli Studi di Trento, in qualità di "Titolare del trattamento" nominerà l'Appaltatore come "Responsabile del trattamento ai sensi dell'art 28 del Regolamento UE 679/2016.

Durante l'intera durata del contratto, il Responsabile del trattamento si impegnerà ad osservare e rispettare l'accordo di nomina di cui sopra, che costituirà addendum al contratto stesso nonché ad ottemperare agli obblighi del Regolamento UE 679/2016 specificatamente previsti in capo ai Responsabili del trattamento dei dati personali. Il mancato rispetto delle istruzioni contenute nell'addendum suddetto costituirà grave inadempimento contrattuale con facoltà di UniTrento di risolvere il contratto, di richiedere il risarcimento di tutti i danni che ne dovessero derivare, nonché di provvedere alle segnalazioni alle Autorità competenti.

Il possesso in capo al Responsabile del trattamento dei requisiti di esperienza, conoscenza specialistica, affidabilità e risorse tali da fornire idonea garanzia del pieno rispetto della vigente normativa in materia di protezione dei dati personali, sarà valutato dal Titolare anche nel corso di esecuzione del contratto e in caso di accertata mancanza, a seconda della gravità, potrà essere causa di risoluzione del Contratto.

La nomina a Responsabile del trattamento non comporta alcun compenso aggiuntivo rispetto a quanto previsto per il servizio affidato.

8.3. Definizione ambiti di responsabilità nel trattamento dei dati personali

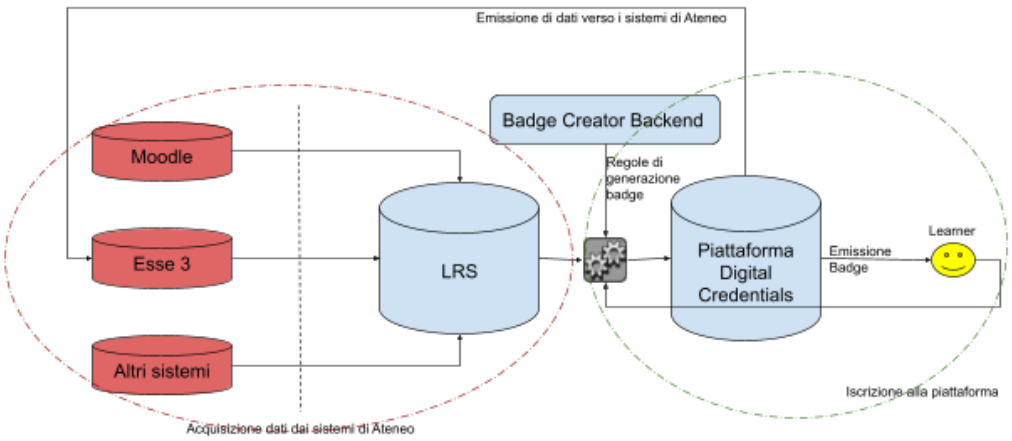

Diagramma di integrazione dei sistemi

Riprendendo il diagramma di integrazione dei sistemi, come esposto al paragrafo *5.11 - Interoperabilità*, si precisa che:

- per quanto riguarda le operazioni di trattamento effettuate sui sistemi ricompresi all'interno del perimetro raffigurato in rosso, il Titolare del trattamento è UniTrento e il Responsabile è l'Appaltatore;
- per quanto riguarda le operazioni di trattamento effettuate sui sistemi ricompresi all'interno del perimetro raffigurato in verde, il Titolare autonomo del trattamento è l'Appaltatore;

9. Modalità e tempistiche di contratto

9.1. Durata del contratto

Il contratto sarà costituito da un'iniziale fase di configurazione della durata di 105 giorni (Fase 1, par. 9.2) che si concluderà con rilascio del Certificato di Regolare Esecuzione relativo alla positiva conclusione della fase di configurazione. Seguirà la fase di erogazione del servizio (Fase 2, par. 9.2) della durata di 24 (ventiquattro) mesi.

É prevista eventuale opzione di rinnovo per ulteriori 24 mesi alle medesime condizioni previste per la fase di erogazione del servizio (Fase 2).

All'aggiudicatario sarà richiesto di costituire la garanzia definitiva secondo quanto previsto dall'art. 103 c. 1 del D. Lgs. 50/2016 e dalla normativa provinciale vigente.

9.2. Fasi del contratto

Il contratto si articola in 2 fasi: una fase iniziale di configurazione (Fase 1) durante la quale verrà configurato e testato l'intero sistema. In caso di esito positivo della Fase 1, si procederà con la fase di erogazione del servizio (Fase 2).

9.2.1. Fase 1 - configurazione

Questa fase ha una durata prevista di 105 giorni naturali e consecutivi a decorrere dalla data di stipula del contratto e prevede le seguenti sotto fasi:

1. Attivazione: avrà la durata di 15 giorni naturali e consecutivi, decorrenti dalla consegna da parte di UniTrento delle necessarie informazioni tecniche. UniTrento invierà i dati necessari alle configurazioni entro 3 giorni lavorativi dalla richiesta dell'Appaltatore. L'attivazione prevede il completamento delle seguenti attività:
    a. Presentazione allo staff UniTrento degli applicativi;
    b. Configurazione dei sistemi di autenticazione federata;
    c. Popolamento dell'ambiente con dati dimostrativi (demo) adeguati ad effettuare i test su diversi casi studio, secondo le indicazioni di UniTrento;
    d. Attivazione delle aree web di lavoro;

    La positiva conclusione della fase di attivazione rappresenta la prima prova di professionalità dell'Appaltatore; essa condiziona il regolare svolgimento del Servizio e pertanto UniTrento, si riserva di contestare l'inadempimento e di esercitare il diritto di risolvere il contratto. La conclusione con esito positivo della fase di attivazione verrà attestata entro 5 giorni tramite invio via PEC all'indirizzo dell'Appaltatore di comunicazione da parte di UniTrento.

2. Test delle funzionalità e delle prestazioni: avrà la durata di 60 giorni naturali e consecutivi a partire dalla positiva conclusione della fase di attivazione. Le attività in questo ambito comprendono i test delle funzionalità e delle prestazioni che dovranno rispondere ai requisiti esposti nel presente capitolato. Eventuali segnalazioni di non corretto funzionamento o richieste di modifica verranno formulate per iscritto e inviate all'Appaltatore via e-mail attraverso indirizzo e-mail dedicato e comunicato durante la fase di stipula del contratto. L'Appaltatore avrà tempo 3 giorni lavorativi per rispondere alla richiesta. La conclusione con esito positivo della fase di test delle funzionalità e delle prestazioni verrà attestata entro 5 giorni tramite invio via PEC all'indirizzo

dell'Appaltatore di comunicazione da parte di UniTrento. In caso di conclusione dei test con esito negativo, UniTrento si riserva di contestare l'inadempimento e di esercitare il diritto di risolvere il contratto.

3. Messa in esercizio: avrà la durata di 15 gg naturali e consecutivi a partire dalla positiva conclusione della fase di test delle funzionalità e delle prestazioni. La messa in esercizio prevede il completamento delle seguenti attività:
    a. Attivazione dell'ambiente di produzione e popolamento del database;
    b. Training degli amministratori di sistema;
    c. Fornitura della documentazione d'uso (manuale);
    d. Collaudo;

    L'esito positivo della fase di messa in esercizio sarà confermato dall'emissione entro 5 giorni da parte di UniTrento di regolare Certificato di Regolare Esecuzione. In caso di conclusione della fase di messa in esercizio con esito negativo, UniTrento, si riserva di contestare l'inadempimento e di esercitare il diritto di risolvere il contratto.

9.2.2. Fase 2 - Erogazione del servizio

La fase di erogazione del servizio ha inizio con la messa in esercizio del software e l'emissione del Certificato di Regolare Esecuzione.

Durante questa fase il sistema dovrà supportare tutte le funzionalità descritte al paragrafo "*Requisiti funzionali e tecnici di sistema*" e dovranno essere erogati tutti i servizi descritti nei precedenti paragrafi del presente documento, in particolare quanto riportato al paragrafo "*Requisiti di servizio*".

9.3. Gestione del progetto

Le attività oggetto del presente Capitolato Prestazionale devono essere effettuate dall'Appaltatore con la responsabilità del raggiungimento di tutti gli obiettivi di progetto sopra specificati.

L'Appaltatore provvederà, a partire dalla data di stipula del contratto, a portare avanti le fasi di cui ai paragrafi *Fase 1: configurazione* e *Fase 2: erogazione del servizio* descritte precedentemente, ponendo l'attenzione ai vincoli temporali imposti.

In sede di stipula del contratto l'Appaltatore dovrà comunicare il referente o i referenti per l'assistenza (specificando a chi rivolgersi per i diversi tipi di assistenza), i canali di contatto (email, telefono, skype, ecc.) e le fasce orarie di reperibilità.

Contestualmente UniTrento comunicherà all'Appaltatore i nominativi ed i riferimenti e-mail del personale autorizzato ad interfacciarsi con l'Appaltatore per portare avanti le fasi di configurazione e di erogazione dei servizi richiesti.

9.4. Conclusione del servizio

Alla conclusione del contratto l'Appaltatore si impegna, senza costi aggiuntivi, a fornire i dati in modo fruibile, in formato concordato e comunque utilizzabile da UniTrento, corredati di adeguata documentazione tecnica relativa alla struttura dati.

L'eventuale inottemperanza a questo punto essenziale verrà considerata interruzione di pubblico servizio. Dovrà inoltre fornire il supporto per la migrazione dei dati di proprietà di UniTrento dal proprio sistema a quello di un eventuale nuovo Fornitore subentrante.

L'Appaltatore è inoltre tenuto, salvo nei casi previsti dalla legge, a cancellare dalla piattaforma tutti i dati di proprietà di UniTrento e gestiti da amministratori, operatori e utenti.