UNIVERSITÀ DEGLI STUDI FIRENZE
SIAF SISTEMA INFORMATICO DELL'ATENEO FIORENTINO

Capitolato Tecnico

Acquisizione servizi di supporto e consulenza per evoluzione sistema di Identity Management Ateneo al fine di supportare SPID

Sommario

Art.1 Introduzione

La trasformazione in atto ha portato alla costituzione di un contesto funzionale (es. applicazioni in SaaS) e operativo (es. accesso wi-fi, BYOD, Storage as a Service) nel quale dati, applicazioni, servizi e dispositivi vengono usati in rete senza più la possibilità di tracciare con precisione i perimetri di protezione e pertanto è notevolmente accresce la necessità di gestire in modo sicuro l'identità digitale degli utenti e le politiche di controllo dell'accesso ai dati e ai servizi.

Il progetto si prefigge l'obiettivo di estendere e trasformare l'attuale sistema di gestione delle identità digitali per consentire l'accesso tramite il Sistema Pubblico di Identità Digitale (SPID) alle applicazioni web e fare evolvere le componenti e le procedure attuali verso un sistema integrato e completo di Identity and Access Management (IAM). Considerata la complessità del contesto di riferimento che include una pluralità di attori (studenti, ricercatori, docenti, collaboratori esterni, soggetti afferenti ad altri enti di ricerca e pubbliche amministrazioni), una molteplicità di servizi e dispositivi utilizzati nei tre diversi ambiti di azione dell'Università (didattica, ricerca, terza missione) e le diverse policy che devono essere applicate alla relativa matrice utenti/servizi garantendo dinamicità e flessibilità, è evidente che il sistema di Identity and Access Management sarà sempre di più un componente fondamentale (core) dell'infrastruttura ICT e che pertanto deve restare sotto il pieno controllo delle strutture dell'Ateneo cui è demandato il governo e la gestione di tale infrastruttura: Area per l'Innovazione e Gestione dei Sistemi Informativi ed Informatici (AIGSII) e Sistema Informatico dell'Ateneo Fiorentino (SIAF). Pertanto, invece di procedere alla selezione all'acquisto di una soluzione IAM di tipo proprietario, si ritiene più opportuno procedere alla realizzazione di un IAM basato su componenti software open source, avvalendosi della consulenza e del supporto di una azienda che abbia già maturato esperienza nella Pubblica Amministrazione, particolarmente in contesti universitari e di ricerca.

Art.2 Oggetto della fornitura

L'oggetto della fornitura è **l'acquisizione di servizi di consulenza e supporto volti al disegno dell'architettura, all'individuazione dei componenti open source, alla implementazione e alla messa in servizio di un sistema di Identity and Access Management** che fin dall'inizio (go live) supporti l'accesso tramite SPID ad alcune applicazioni web e costituisca il sistema di identità digitale sul quale far convergere progressivamente tutte le applicazioni ed i servizi dell'Ateneo.

Art.2.1 Scenario attuale

I servizi web e le piattaforme di e-learning Moodle destinati a studenti, docenti, ricercatori, dottorandi, assegnisti di ricerca, personale tecnico amministrativo ed altre tipologie di soggetti quali collaboratori esterni e borsisti utilizzano credenziali uniche di Ateneo (user e password), mentre altre infrastrutture di Ateneo non sono ancora state centralizzate in termini di autenticazione unica di Ateneo (aule informatiche, accesso alle PDL, fruizione di VDI, posta elettronica del personale tecnico amministrativo e della ricerca e didattica).

Le fonti autoritative per il provisioning delle utenze sono i due principali sistemi gestionali, **Risorse Umane** e **Gestione Carriera Studenti**. Il primo flusso è gestito da procedure che leggono il database, interamente scritte e gestite da SIAF per applicare le policy previste dall'Ateneo. Il secondo flusso è composto da una serie di procedure native di Cineca che aggiornano le proprie strutture dati su Oracle e sincronizzano LDAP tenendo conto della dinamica delle carriere studenti (immatricolazione, iscrizione, conseguimento titolo) ed anche in questo caso applicando le policy definite dall'Ateneo.

I servizi di cambio e reset password per la prima categoria sono stati sviluppati e sono gestiti da SIAF (operano direttamente su LDAP), per la seconda categoria sono quelli nativi del Gestionale Carriera Studenti di Cineca che operano sul DB e sincronizzano in automatico LDAP.

L'integrazione con la Federazione Idem è garantita tramite Shibboleth 3.3 (interfacciato a LDAP) configurato come IdP per supportare i vari SP federati, configurato e gestito in house.

L'infrastruttura tecnologica, oltre che dal DB Oracle, è costituita da due server OpenLDAP in configurazione primario-secondario e un server Shibboleth 3.3. L'accesso federato eduroam è supportato da un server Radius integrato con LDAP.

Per quanto riguarda la posta elettronica gli studenti utilizzano le proprie credenziali uniche di Ateneo per accedere alla casella di posta istituzionale attribuita dall'Ateneo attraverso GMail (dominio @stud.unifi.it). Gli altri soggetti, detentori di una casella di posta del dominio @unifi.it, si autenticano con credenziali riservate al servizio di posta elettronica, gestite attraverso un ulteriore server LDAP dedicato che sono attribuite e seguono un ciclo di vita definito in base a policy diverse. Questi soggetti attraverso tali credenziali dedicate accedono anche ai servizi della GSuite. L'autenticazione ai servizi Google (l'intera GSuite) è implementata mediante SAML attraverso un secondo server Shibboleth 2.2 dedicato.

E' stata allestita un'infrastruttura di tipo Virtual Desktop (VDI) basata su VMware per la gestione delle aule didattiche con dispositivi di tipo thin client che prevede la gestione dell'accesso da parte degli utenti tramite MS Active Directory Domain che al momento ha utenze scorrelate e non sincrone con i sistemi sopra citati. Allo stesso dominio active

directory è possibile effettuare il join di PDL e server, ma l'autenticazione utente rimane per gli stessi motivi legata ad utenze locali alla stazione di lavoro.

Art.2.2 SPID e eIDAS

Il comma 2-quater dell'Art. 64. del Codice per l'Amministrazione digitale (CAD) dispone che *l'accesso ai servizi in rete erogati dalle pubbliche amministrazioni che richiedono identificazione informatica avviene tramite SPID*. Il Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche (eIDAS) stabilisce un framework per assicurare che le interazioni elettroniche tra aziende commerciali, cittadini e pubbliche amministrazioni siano più sicure e efficienti indipendentemente dal paese Europeo in cui avvengono. In tale contesto l'identificazione elettronica (eID) è la modalità attraverso la quale sia le aziende che i clienti/consumatori possono identificarsi (processo di identificazione) e dimostrare di essere chi dicono di essere (processo di autenticazione) al fine di ottenere l'accesso ai servizi o svolgere operazioni in modo più facile.
Dal settembre 2018 è obbligatorio per tutti i paesi europei riconoscere i sistemi di identificazione (eID) notificati da altri paesi alla Commissione Europea. In quest'ottica di mutuo riconoscimento dei mezzi di identificazione elettronica adottati tra gli Stati membri – l'Agenzia per l'Italia Digitale (AgID) ha ultimato il processo che consente ai cittadini italiani di utilizzare la propria identità digitale SPID con credenziali di livello 2 e 3 (è facoltà degli Stati membri accettare il livello 1) per accedere ai servizi in rete delle pubbliche amministrazioni europee. Tale diritto decorre dal 10 settembre 2019 ma può essere anticipato volontariamente dagli altri Stati membri. L'attività svolta in ambito europeo sotto la sigla eIDAS eID (supportata dalla Connecting Europe Facility) prevede di realizzare in modo effettivo e sicuro una "cross-border authentication" (autenticazione transfrontaliera) attraverso il mutuo riconoscimento degli schemi nazionali eID e realizzando una rete di nodi (uno per ogni paese) che effettuano le opportune mappature rispetto ai servizi nazionali offrendo i benefici di interoperabilità, sicurezza e validità delle transazioni transfrontaliere. Nella pagina eID Country Overview https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview è possibile riscontrare lo stato delle notifiche dei paesi europei. In questo scenario l'implementazione di SPID faciliterà anche l'accesso da parte di studenti provenienti da altri paesi europei che potranno usare le proprie identità digitali nazionali per accedere ai servizi dell'Ateneo.
Agid ha pubblicato il 6/11/2019 "Le linee guida per le identità digitali per uso professionale" che consentono il processo di autenticazione con identità digitale uso professionale per la persona giuridica (https://www.agid.gov.it/sites/default/files/repository_files/linee_guida_identita_digitale_per_uso_professionale_v.1.0.pdf).

Art.2.3 Scenario a tendere oggetto dell'implementazione

Si intende procedere alla progressiva implementazione di SPID come modalità di autenticazione ad alcuni servizi offerti, al consolidamento dell'architettura di identity management attraverso la sua graduale evoluzione verso un sistema di tipo Identity and Access management (IAM), implementato tramite componenti open source e pienamente sotto il controllo del personale tecnico informatico dell'Università di Firenze (Area per l'Innovazione e Gestione dei Sistemi informativi ed Informatici e Sistema Informatico dell'Ateneo Fiorentino). L'IAM che si intende implementare deve:

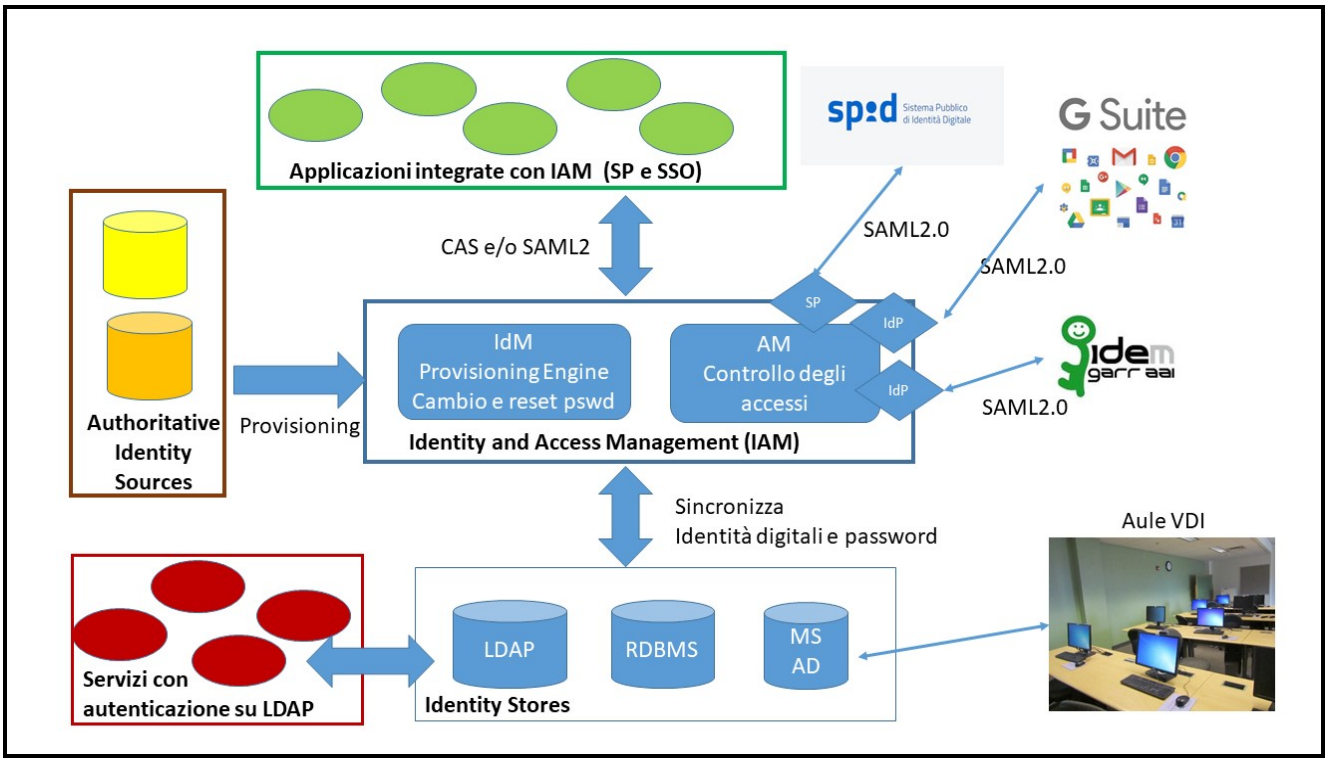
- essere integrato con gli Identity Store (repository utente) esistenti (LDAPv3, Active Directory, RDBMS);
- svolgere il ruolo di Identity Server:
  - per l'autenticazione locale, anche in modalità Single Sign-On (SSO), attraverso i propri Identity Store;
  - di Identity Provider (IdP) SAML 2.0 nell'ambito della *federazione IDEM* del GARR;
  - di server federato della rete *eduroam* (Education Roaming) per l'accesso in mobilità alla rete wireless da parte di utenti di altre organizzazioni di ricerca;
  - di supportare l'accesso tramite SPID ad alcune applicazioni web;
- essere il **punto unico** che eroga i servizi di **cambio e reset della password** e gestire in maniera centralizzata e sincronizzata la **distribuzione delle password su LDAPv3, Active Directory e database SQL**;
- provvedere alla sincronizzazione delle password tenendo conto dei diversi algoritmi di cifratura previsti dagli identity store previsti;
- diventare progressivamente il sistema di governo centralizzato delle politiche di provisioning degli utenti in base alla loro diverse tipologie, alle politiche definite dall'ateneo e alle diverse fonti autoritative
- assumere le funzioni di controllo dell'accesso (access management) ai servizi web, dispositivi, web services esposti dagli applicativi.

Il sistema dovrà garantire:

- l'accesso e la registrazione tramite credenziali SPID per un primo nucleo di servizi sviluppati internamente dall'Ateneo: domande di partecipazione ai concorsi, dichiarazioni fiscali, consultazione cedolini stipendi e CU, domande di laurea;
- l'accesso alla federazione IDEM e a eduroam;
- l'accesso alle postazioni di lavoro operanti nelle aule didattiche in modalità VDI
- la possibilità di accesso alle postazioni client o ai server che siano state inseriti a dominio Active Directory
- l'accesso alle applicazioni web esistenti in modo trasparente garantendo un percorso di evoluzione progressiva verso SSO e SPID a tutte le altre applicazioni JEE e PHP in uso presso l'Università

- la progressiva estensione dell'accesso via SPID anche ad altre applicazioni web, alla piattaforma Moodle e alla posta elettronica.

L'architettura logica di massima è descritta nella seguente figura:



Dove:

- gli Identity Store (RDBMS, LDAP, Active Directory) sono i repository contenenti le identità digitali degli utenti con eventuali metadati (attributi) necessari
- il Motore di Provisioning sincronizza i metadati delle identità digitali (account) degli utenti tra i vari identity stores
- l'Indentity Manger si occupa dell'autenticazione locale e federata (SAML, Eduroam, SPID, OpenID Connect) ed implementa anche funzioni di gestione degli accessi (Access Manager) per il rilascio di autorizzazioni secondo i principi del modello role-base (gruppi, profili, diritti).

Art.3 Requisiti funzionali e operativi

Art.3.1 Requisiti funzionali e operativi obbligatori

La soluzione tecnica proposta e descritta nel Piano di Progetto dovrà soddisfare, a pena di esclusione dell'offerta, i seguenti requisiti funzionali:

- Svolgere le funzioni di Identity and Access Management (punto unico per l'identificazione digitale)
- Erogare il servizio di cambio password
- Erogare il servizio reset/rigenerazione della password sia in modalità autonoma (self service) per l'utente finale (attraverso canali di invio molteplici e configurabili) sia previo intervento di operatori autorizzati
- Implementare la gestione automatica e configurabile della scadenza di validità identità digitale e del cambio password secondo politiche che possono essere differenziate per tipologia di utenza
- Supportare l'autenticazione delegata a SPID consentendo anche l'eventuale riconoscimento di identità digitale uso professionale
- Supportare l'autenticazione federata in ambito e IDEM del GARR e Eduroam
- Gestire l'integrazione con le Group Policy per i sistemi Microsoft tramite integrazione con AD
- Gestire la configurazione e la profilatura dei differenti set di metadati rilasciabili ai diversi Service Provider di tipo SAML
- Supportare molteplici ed eterogenei repository delle identità digitali (LDAPv3, DB Oracle, DB MySQL, Active Directory) assicurando che le operazioni di cambio/reset password avvengano in modo transazionale per mantenere l'allineamento.

Art.3.2 Requisiti funzionali e operativi migliorativi

La soluzione tecnica descritta nel Piano di Progetto potrà fornire indicazioni in merito alle soluzioni proposte dall'operatore economico per soddisfare i seguenti requisiti tecnici funzionali migliorativi che saranno oggetto di valutazione con l'attribuzione del relativo punteggio riportato nel Disciplinare di Gara.

- Flessibilità delle procedure di provisioning dei soggetti cui attribuire e manutenere le identità digitali rispetto alle fonti esistenti (sistema legacy di ateneo, altri db, conferimenti estemporanei tramite file xls, etc.), alla diversa tipologia di tali soggetti, ai differenti metadati associati e alle differenti policy di attivazione/disattivazione previste dall'ateneo.
- Flessibilità per lo sviluppo e la configurazione di procedure di sincronizzazione, inclusi gli algoritmi di encriptazione, tra repository di tipo diverso (es. LDAP, Active Directory, DB) secondo logiche master-slave (primario-secondario).
- Possibilità di integrazione con sistemi di controllo degli accessi (varchi elettronici, tornelli delle biblioteche, accesso a laboratori a rischio) mediante la Tessera dello Studente della Toscana attraverso una o più delle caratteristiche presenti (RFID, banda magnetica, codice a barre). Le card attualmente rilasciate appartengono alla famiglia di smart card che rispettano lo standard ISO 14443A, ovvero che rientrano nell'insieme delle smart card contactless RFID 13.56. In particolare sono state adottate le MIFARE Ultralight C 1kb, che integrano lo standard crittografico 3DES aperto per l'autenticazione dei chip e l'accesso ai dati. Le carte sono utilizzate per l'identificazione degli studenti, per accedere ai tornelli di ingresso presenti nei Plessi universitari di Novoli e Sesto Fiorentino, per usufruire dei servizi di mensa dell'Azienda Regionale per il diritto allo Studio Universitario e dei servizi regionali di trasporto locale e accesso convenzionato a musei e teatri.
- Possibilità di integrazione con sistemi/apparati di tipo valorizzatore (es. pagamento fotocopie) mediante la Tessera dello Studente della Toscana attraverso una o più delle caratteristiche presenti (RFID, banda magnetica, codice a barre).

Art.4 Requisiti tecnici

Art.4.1 Requisiti tecnici

La soluzione tecnica proposta e descritta nel Piano di Progetto dovrà soddisfare, a pena di esclusione dell'offerta, i seguenti requisiti tecnici:

- Utilizzo di componenti software open source quali: Open LDAP, Shibboleth3.3, Apereo CAS, Apache Syncope
- Integrazione con diverse tipologie di repository delle identità digitali (LDAPv3, MS Active Directory, RDBMS)
- Gestione di diversi schemi di cifratura delle password
- Supporto di protocolli SAML 2.0, LDAP v.3
- Deploy dei componenti del sistema su macchine virtuali VMWare.

Art.4.2 Requisiti tecnici migliorativi

I seguenti requisiti tecnici opzionali saranno oggetto di valutazione con l'attribuzione del relativo punteggio migliorativo riportato nella tabella del paragrafo 8.2 della lettera d'invito.

- Supporto di protocolli OAuth, OpenId Connect
- Deploy del sistema in configurazione ridondata in alta affidabilità
- Deploy dei componenti del sistema in cloud tramite servizi IaaS e PaaS pubblico, privato o ibrido

Art.5 Servizi richiesti nella fornitura

La fornitura comprende i seguenti servizi:

a) *Disegno e deploy del sistema*. Definizione dell'architettura e delle sue componenti, installazione e configurazione del sistema IAM conforme ai requisiti funzionali, operativi e tecnici, comprese le azioni necessarie per espletare tutto l'iter di attestazione dell'Università come SP SPID.

b) *Accesso via SPID alle dichiarazioni fiscali, ai cedolini stipendi e ai CU*. Si tratta di due applicazioni web sviluppate in house. La prima, scritta in PHP, permette di compilare on line le dichiarazioni fiscali da parte di soggetti che hanno avuto rapporti di collaborazione con le strutture dell'Ateneo. La seconda, scritta in Java, consente la consultazione dei cedolini stipendi e dei CU. L'integrazione di entrambe con SPID intende semplificare l'autenticazione, visto che spesso i soggetti che devono utilizzare queste applicazioni non hanno credenziali di ateneo valide (per cessazione del rapporto di lavoro) e sono comunque riconoscibili in modo univoco tramite il CF per associarli ai propri dati.

c) *Accesso via SPID al servizio web Domande di Laurea*. Si tratta di un servizio web per studenti, sviluppato in house in Java, da utilizzare come prototipo

nella fase di migrazione dei servizi web per studenti dallo scenario attuale alla soluzione IAM proposta.

d) *Registrazione con SPID degli studenti ancora non immatricolati*. Attualmente questa fase viene gestita esponendo l'apposito servizio di registrazione del Sistema Gestionale Carriere Studenti (ESSE3 di Cineca) attraverso il quale il potenziale studente, oltre ad inserire una serie di dati anagrafici, imposta la password che, insieme al codice fiscale, costituisce la coppia di credenziali per l'accesso ad un insieme ridotto di servizi web erogati in parte dalla stessa piattaforma e in parte dal software Turul sviluppato dall'Ateneo. Fino a quando lo studente non completa l'immatricolazione con il pagamento della tassa, questa coppia resta l'unica modalità di accesso per lo studente, senza alimentazione in LDAP. I futuri studenti sono indirizzati dalle opportune pagine del sito di Ateneo al servizio di registrazione (https://studenti.unifi.it/AddressBook/ABStartProcessoRegAction.do).
L'approccio più semplice consiste nel fare in modo che, una volta effettuato l'accesso con le credenziali SPID, i metadati forniti da SPID siano recuperati e inseriti automaticamente nella form di registrazione, come se fossero stati digitati dall'utente che poi proseguirà la registrazione come in precedenza.

e) *SPID per il reset password*. Si prevede di utilizzare l'autenticazione SPID come modalità self-service per l'accesso alle funzioni di recupero/reset della password di Ateneo dimenticata.

f) *Gestione accessi alle aule didattiche, ai VDI ed alle PDL tecnico amministrative.* Per questo servizio è necessaria l'integrazione del componente di Identity Mangement con MS Active Directory (considerando anche una eventuale estensione ad Azure Active Directory per il provisioning di licenze Microsoft in maniera gestita e controllata) che centralizzerà il servizio di Domain Controller (DC) per le aule didattiche, le PDL tecnico amministrative ed i VDI utilizzabili ad esempio per il telelavoro. Tra le soluzioni possibili si ipotizzano: a) la possibilità di accedere con una fase preliminare di registrazione, tramite una pagina erogata dall'Identity Manager e l'uso delle proprie credenziali, che determini la propagazione dell'utenza su AD completa di password d'accesso; b) la propagazione sul Domain Controller a seguito di una sincronizzazione iniziale tra Identity Manager e AD. In questo secondo caso il profilo utente creato potrebbe richiedere un cambio password obbligatorio al primo accesso, attraverso una pagina del sistema di Identity Management alla quale l'utente accederà per confermare la propria identità. In entrambi i casi il profilo utente su AD sarà configurato per impedire un cambio password dalle macchine client allo scopo di evitare disallineamenti futuri. In entrambe i casi l'attivazione dell'account su AD potrebbe essere soggetta ad approvazione da parte di un utente amministratore delegato.

g) *Gestione accesso piattaforma e-learning*. Oltre a mantenere l'attuale autenticazione via LDAP è previsto di estendere l'accesso attraverso SPID per gli utenti già registrati (già dotati di credenziali di Ateneo).

h) *Accesso alla posta elettronica*. Gli studenti hanno già la casella di posta elettronica su Google. E' in corso un progetto per la migrazione a tale piattaforma anche della posta del dominio @unifi.it. Pertanto un'ulteriore evoluzione dell'IAM e dell'estensione all'uso di SPID riguarderà in una fase successiva anche la posta elettronica.

i) *Eventuale sostituzione di Shibboleth 3.3 con CAS o altro sw equivalente*. Tale ipotesi è inclusa nell'ambito della definizione dell'architettura IAM proposta purché siano garantite il mantenimento trasparente delle stesse funzionalità di Identity Provider SAML 2.0 richieste dalla Federazione IDEM e per la posta elettronica su Google.

j) *Revisione e integrazione delle procedure di provisioning utente*. La soluzione proposta dovrà tener conto dei vincoli imposti dalle procedure esistenti (cfr. Art. 2.1) mantenendo come primario il repository LDAP. Eventuali varianti o alternative dovranno minimizzare l'impatto sui servizi.

k) *Documentazione e formazione*. La fornitura deve comprendere tutta la documentazione dettagliata di progetto, quella sull'architettura definitiva concordata, sui sistemi utilizzati, le configurazioni definite e le procedure implementate.

Art.6 Piano di progetto, fasi e tempi di realizzazione

La sequenza delle attività è quella indicata nel punto precedente "Servizi".

Tempo complessivo previsto: 120 giorni naturali e consecutivi

L'offerta dovrà contenere la strutturazione in work package esplicitando per ciascuno la descrizione, le attività svolte, la relativa documentazione che verrà prodotta, la durata prevista e le risorse impegnate. Tale proposta sarà oggetto di valutazione e potrà essere rinegoziata concordando una diversa priorità dei servizi da implementare tra quelli indicati.

Per la valutazione dei tempi e del Piano di progetto si terrà conto degli elementi riportati nei due paragrafi seguenti.

Art.6.1 Contenuto obbligatorio del Piano di Progetto

Il Piano di progetto dovrà contenere, a pena di esclusione dell'offerta, almeno i seguenti elementi:

- Disegno dell'architettura tecnica e descrizione delle componenti, descrizione funzionale del sistema, della metodologia di lavoro e del deployment
- Impegno all'espletamento dell'iter di attestazione dell'Università come SP SPID secondo quanto previsto da Agid nel sito spid.gov.it
- Impegno a produrre e rilasciare la documentazione e la configurazione di tutti i sistemi e servizi realizzati
- Piano di Formazione, minimo di 3gg
- Schedulazione per la realizzazione e l'avvio operativo dei seguenti servizi:
  - Accesso via SPID alle dichiarazioni fiscali, ai cedolini stipendi e ai CU
  - Accesso via SPID al servizio web Domande di Laurea
  - Uso di SPID per la registrazione al gestionale carriere studenti degli studenti ancora non immatricolati
  - Autenticazione tramite SPID al servizio di reset password
  - Gestione accessi alle aule didattiche, ai VDI ed alle PDL tecnico amministrative
  - Gestione accesso piattaforma e-learning (Moodle).
- Descrizione puntuale dalla quale siano riscontrabili le soluzioni e servizi proposti in relazione agli Art. 3.2 "Requisiti funzionali e operativi migliorativi" e Art. 4.2 "Requisiti tecnici migliorativi" qualora l'operatore economico intenda concorrere all'attribuzione dei relativi punteggi di valutazione.

Art.6.2 Elementi migliorativi per la valutazione del Piano di Progetto

Se esplicitati e opportunamente schedulati i seguenti elementi opzionali saranno oggetto di valutazione con l'attribuzione del relativo punteggio migliorativo riportato nella tabella del paragrafo 8.2 della lettera d'invito.

a. Riduzione dei tempi di realizzazione.
b. Accesso via SPID ad ulteriori servizi web sviluppati in house quali: "Applicativo delle Performances", "Registri della Didattica", "Piattaforma Dialogo per l'orientamento e l'alternanza scuola-lavoro", "Domande Bando dottorati di Ricerca", "Iscrizione ad eventi di Ateneo, laboratori e corsi per la sicurezza su rischi specifici".
c. Ulteriori giornate di formazione rispetto alle 3 previste obbligatoriamente.

Art.7 Esperienze precedenti

La valutazione dell'offerta comprende (vedi tabella del paragrafo 8.2 della lettera d'invito.) le esperienze maturate in precedenza per la realizzazione di soluzioni analoghe presso altri enti pubblici o privati.

Per ciascuna realizzazione dovranno essere indicati nell'offerta: il periodo temporale, le tecnologie utilizzate, la denominazione dell'ente contraente e la sua categoria indicando se trattasi di Università o ente di ricerca o altra tipologia di ente pubblico o azienda privata.

Art.8 Titolarità e riuso del software

La titolarità di tutto il software sviluppato nell'ambito dei servizi oggetto della fornitura, ai sensi dell'Art.69 del Codice dell'Amministrazione Digitale (CAD) è esclusivamente dell'Università di Firenze che si impegna a renderlo disponibile per il "riuso" da parte di altre Pubbliche amministrazioni secondo quanto previsto dagli Art.li 68 e 69 e dalle "Linee Guida AgID sull'acquisizione e il riuso del software nella PA" emanate il 9 maggio 2019.

Art.9 Trattamento dati personali

L'Università degli studi di Firenze in qualità di titolare del trattamento tratta i dati ad essa forniti esclusivamente per la gestione dell'appalto e per la sua esecuzione, per l'adempimento degli obblighi legali ad esso connessi, nonché ai fini di studio, statistici e gestionali. Le parti si impegnano ad improntare il trattamento dei dati ai principi di minimizzazione, correttezza, liceità e trasparenza a nel pieno rispetto di quanto definito dalla normativa europea in materia di protezione dei dati personali di cui al citato l Regolamento UE 2016/679
L'Affidatario è considerato responsabile del trattamento dei dati personali acquisiti e trattati ai fini dell'esecuzione del contratto, ai sensi dell'art. 28 del Regolamento generale sulla protezione dei dati (Regolamento UE 2016/679 – GDPR).
L'Affidatario assume su di sé l'obbligo di trattare i dati personali di cui verrà in possesso, o a conoscenza, in occasione dell'esecuzione del contratto in qualità di "Responsabile", secondo quanto previsto dal Regolamento UE 2016/679 – GDPR.
Maggiori informazioni sono disponibili alla pagina "Protezione dati" del sito istituzionale di Ateneo al seguente indirizzo https://www.unifi.it/vp-11360-protezione-dati.html

Art.10 Penali

L'Università applicherà una penale giornaliera pari all'1/00 (uno per mille) dell'ammontare netto contrattuale (IVA esclusa) per ogni giorno di ritardo nella fornitura rispetto a quanto previsto nell'Articolo 6 con riferimento al tempo complessivo dichiarato nel piano di progetto dell'offerta (cfr. Art. 6.2).

Glossario e riferimenti

AD – Active Directory

AM Access Manager – Sistema per il controllo degli accessi logici

BYOD – Bring Your Own Device

IAM - Identity & Access Management

CAS - Central Authentication Service

IdM - Identity Manager – Sistema per la gestione delle identità digitali

IdP - Identity Provider (generalmente SAML2.0)

LDAP - Lightweight Directory Access Protocol

PIAM - Physical Identity & Access Management

SaaS – Sofware as a Service

SAML Security Assertion Markup Language

SP Service Provider (generalmente SAML2.0)

SPID - Sistema Pubblico di Identità Digitale

Riferimenti

Active Directory Federation Services: https://docs.microsoft.com/it-it/windows-server/identity/active-directory-federation-services;

Active Directory Servizi di dominio: https://docs.microsoft.com/it-it/windows-server/identity/ad-ds/active-directory-domain-services;

Apereo CAS: https://www.apereo.org/projects/cas;

Apache Syncope: https://syncope.apache.org/;

Azure Active Directory: https://azure.microsoft.com/it-it/services/active-directory/;

eiDAS: https://ec.europa.eu/digital-single-market/en/news/cross-border-digital-identification-eu-countries-major-step-trusted-digital-single-market;

e-Identification: https://ec.europa.eu/digital-single-market/en/e-identification;

eID Country overview: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/Country+overview;

LDAP: https://it.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol;

"Linee Guida AgID sull'acquisizione e il riuso del software nella PA": https://www.agid.gov.it/sites/default/files/repository_files/lg-acquisizione-e-riuso-software-per-pa-docs_pubblicata.pdf;

Midpoint: https://evolveum.com/midpoint/;

OAuth2: https://oauth.net/2/;

OpenLDAP: https://www.openldap.org/;

SAML v2: https://wiki.oasis-open.org/security/FrontPage;

SPID: https://helpdesk.spid.gov.it/knowledgebase.php?article=14

SPID "Come diventare fornitore di servizi Pubblici o Privati con SPID" https://www.spid.gov.it/come-diventare-fornitore-di-servizi-pubblici-e-privati-con-spid