UNIVERSITÀ DEGLI STUDI FIRENZE
SIAF SISTEMA INFORMATICO DELL'ATENEO FIORENTINO

AVVISO DI INDAGINE
PER L'ACQUISIZIONE DELLE MANIFESTAZIONI DI INTERESSE
A PARTECIPARE ALLA PROCEDURA EX ART. 36 COMMA 2 LETT. a) D.LGS. 50/2016
SMI FINALIZZATA ALL'AFFIDAMENTO DEI SERVIZI DI SUPPORTO E CONSULENZA PER EVOLUZIONE SISTEMA DI IDENTITY MANAGEMENT DI ATENEO AL FINE DI SUPPORTARE SPID
VERRÀ UTILIZZATA LA PIATTAFORMA START SIA PER LA GESTIONE DELLA FASE DI MANIFESTAZIONE D'INTERESSE, SIA PER LA FASE CONCORRENZIALE

Si informa che il Sistema Informatico dell'Ateneo Fiorentino (SIAF) dell'Università degli Studi di Firenze, con il presente avviso, intende acquisire le manifestazioni di interesse da parte di operatori economici, in possesso dei requisiti di cui al successivo punto 3 ad essere invitati a presentare offerta ai fini dell'affidamento diretto, ai sensi dell'art. 36, comma 2, lettera a) del D.Lgs. n. 50/2016, dei servizi di supporto e consulenza per evoluzione sistema di Identity Management di Ateneo al fine di supportare SPID. I servizi di cui trattasi rientrano nell'ambito della categoria merceologica 72000000-5 "Servizi informatici: consulenza, sviluppo di software, Internet e supporto" presente sul sistema del mercato elettronico.

Il presente avviso è finalizzato a ricevere manifestazioni d'interesse per favorire la partecipazione e la consultazione del maggior numero di Operatori Economici nel rispetto dei principi di non discriminazione, parità di trattamento e trasparenza e non costituisce invito a partecipare alla procedura di affidamento.
Il presente avviso è da intendersi come mero **procedimento preselettivo**, non vincolante per il SIAF, finalizzato alla raccolta di manifestazioni di interesse da parte dei soggetti interessati in possesso dei requisiti di partecipazione *e pertanto non sono previste graduatorie, attribuzioni di punteggi o altre classificazioni in merito.*
Il presente Avviso non costituisce altresì un invito ad offrire né un'offerta al pubblico, ai sensi dell'art. 1336 c.c. né promessa al pubblico, ai sensi dell'art. 1989 c.c.
La manifestazione di interesse ha il solo scopo di comunicare al SIAF la disponibilità ad essere invitati a presentare l'offerta.

Si forniscono di seguito, le informazioni utili per la manifestazione d'interesse, che costituiscono elementi base della documentazione della successiva procedura.

1. *Ente appaltante*

SIAF - Sistema Informatico dell'Ateneo Fiorentino Via delle Gore, 2 - 50141 Firenze
Tel. +39 055 2751100 - Fax +39 055 2751183;
Sito internet e profilo del committente: https://www.siaf.unifi.it/;
PEC: csiaf@pec.unifi.it

2. *Oggetto dell'avviso*

SIAF intende affidare, mediante procedura di affidamento diretto, ai sensi dell'art. 36, comma 2, lettera a) del D.Lgs. n. 50/2016, previa consultazione, da aggiudicare con il criterio dell'offerta economicamente più vantaggiosa i servizi dei servizi di supporto e consulenza per evoluzione sistema di Identity Management di Ateneo al fine di supportare SPID descritti **nell'Allegato B - Capitolato Tecnico.**
Documento allegato costituisce parte integrante della Manifestazione di Interesse.

Importo presunto: €39.000 IVA esclusa (non sono previsti oneri per la sicurezza per le interferenze).

3. *Requisiti di partecipazione*

Possono presentare manifestazione di interesse i soggetti di cui all'art. 45 del Lgs. 50/2016 s.m.i. che, al momento della sua presentazione, siano in possesso:

3.1 Requisiti generali

a. insussistenza delle cause di esclusione di cui all'art. 80 del D.Lgs. n. 50/2016;
b. insussistenza delle cause di divieto, decadenza o di sospensione di cui all'art. 67 del d.lgs. 6 settembre 2011, n. 159.
c. insussistenza delle condizioni di cui all'art. 53, comma 16-ter, del d.lgs. del 2001, n. 165 o di ulteriori divieti a contrarre con la pubblica amministrazione.

3.2 Requisiti speciali

- Idoneità professionale:

a. Iscrizione nel registro tenuto dalla Camera di commercio industria, artigianato e agricoltura oppure nel registro delle commissioni provinciali per l'artigianato o presso i competenti ordini professionali per attività coerenti con quelle oggetto della presente procedura.

- Capacità economica e finanziaria:

Non richiesti.

- Capacità tecniche e professionali:

Esecuzione, negli ultimi 3 anni, di servizi analoghi a quelli oggetto del presente avviso, erogati in favore di Pubbliche Amministrazioni e aziende private in Italia o nel territorio europeo."

4. *Modalità e termine per la presentazione delle candidature*

La manifestazione di interesse dovrà essere redatta sulla base del modello allegato (all. "A") al presente avviso, in formato .pdf, sottoscritta digitalmente dal legale rappresentante o da soggetto munito di idonea procura.
Il termine entro cui inoltrare la manifestazione di interesse è fissato per il giorno: **11 settembre 2019.**

La manifestazione di interesse dovrà pervenire entro la data sopra indicata, in modalità telematica attraverso il Sistema Telematico Acquisti Regione Toscana (START), utilizzando le apposite funzionalità rese disponibili al seguente indirizzo internet: https://start.toscana.it/
Per poter manifestare l'interesse a partecipare, i concorrenti già registrati nell'indirizzario regionale dovranno accedere all'area riservata relativa all'avviso in oggetto e utilizzare l'apposita funzione presente sul Sistema.
I concorrenti non iscritti all'indirizzario dovranno compilare il form telematico presente nella pagina contenente il dettaglio relativo all'avviso in oggetto.
Il concorrente, dopo aver manifestato interesse, riceverà una comunicazione di conferma attraverso il sistema START all'indirizzo di posta elettronica indicato in sede di registrazione.
Ove attivato, l'appalto si svolgerà in modalità telematica attraverso l'utilizzo della piattaforma START; le domande di partecipazione e le offerte dovranno essere formulate dai concorrenti e ricevute dalla Stazione Appaltante esclusivamente per mezzo del Sistema Telematico Acquisti Regionale della Toscana accessibile all'indirizzo: https://start.toscana.it/.

Attenzione: Il sistema telematico di acquisti online della Regione Toscana utilizza la casella denominata noreply@start.toscana.it per inviare tutti i messaggi di posta elettronica.
I concorrenti sono tenuti a controllare che le mail inviate dal sistema non vengano respinte né trattate come Spam dal proprio sistema di posta elettronica e, in ogni caso, a verificare costantemente sul sistema la presenza di comunicazioni."

5. ***Operatori che saranno invitati alla procedura***

Numero minimo previsto: 1
Numero massimo: 10
Criteri obiettivi per la selezione del numero limitato di Operatori:
Nel caso in cui pervenga, da parte degli Operatori Economici, un numero di Manifestazioni di Interesse superiore al numero massimo di 10, SIAF procederà all'individuazione degli operatori economici da invitare a presentare offerta, tramite sorteggio su S.T.A.R.T..

6. ***Pubblicazione dell'avviso***

Il presente avviso viene pubblicato anche sul sito web e sull'Albo Online dell'Università di Firenze.
L'Amministrazione si riserva di interrompere in qualsiasi momento, per ragioni di sua esclusiva competenza, il procedimento avviato, senza che i soggetti richiedenti possano vantare alcuna pretesa.

7. ***Trattamento dei dati personali***

I dati personali saranno raccolti e trattati esclusivamente per le attività previste dalla legge e per le finalità istituzionali dell'Istituto, ai sensi del d.lgs. n. 196/2003 modificato dal d.lgs. 101/2018 di adeguamento della disciplina italiana al regolamento europeo sulla privacy (Reg. UE n. 679/2016, GDPR).

8. ***Informazioni***

Eventuali richieste di informazioni potranno essere rivolte esclusivamente su S.T.A.R.T..

Il Dirigente
Ing. Marius B. Spinu

Firmato digitalmente da
SPINU MARIUS BOGDAN
Data: 2019.08.27 11:57:10
'+02'00

UNIVERSITÀ DEGLI STUDI FIRENZE

Spett. SIAF – Sistema Informatico
dell'Ateneo Fiorentino

Oggetto: **Manifestazione di interesse a partecipare alla procedura ex art. 36 comma 2 lett. a) D.Lgs. 50/2016 finalizzata all'affidamento dei servizi di supporto e consulenza per evoluzione sistema di Identity Management di Ateneo al fine di supportare SPID**

Il sottoscritto_____nato a_____il _____

nella sua qualità di legale rappresentante/titolare _____

dell'impresa _____

con sede in _____

C.F._____P.IVA_____

Telefono _____Email_____

Posta Elettronica Certificata (PEC) _____

MANIFESTA IL PROPRIO INTERESSE

a partecipare alla successiva procedura, ai sensi dell'art. 36 comma 2 lett. a) Codice dei Contratti pubblici, per l'affidamento dei "*Servizi di supporto e consulenza per evoluzione sistema di Identity Management di Ateneo al fine di supportare SPID*".

A tal fine, **DICHIARA che i fatti, stati e qualità riportati nei seguenti punti corrispondono a verità**:

- di non versare in alcuno dei motivi di esclusione dalla partecipazione alle procedure di affidamento delle concessioni e degli appalti di lavori, forniture e servizi previsti dalla legge (art. 80 D.Lgs. 50/2016 smi);

- di essere in possesso dei requisiti di idoneità professionale e tecnici previsti dall'Avviso esplorativo di indagine di mercato pubblicato su S.T.A.R.T. e sul sito istituzionale dell'Università di Firenze.

- **di essere consapevole che la presente istanza non costituisce proposta contrattuale e non vincola in alcun modo il SIAF, che sarà libera di seguire anche altre procedure e che la stessa si riserva di interrompere in qualsiasi momento, per ragioni di sua esclusiva competenza, il procedimento avviato, senza che i soggetti istanti possano vantare alcuna pretesa**;

- di aver preso visione delle informazioni riguardanti il trattamento dei dati personali riportata in https://www.unifi.it/vp-11360-protezione-dati.html e dell'informativa per il trattamento dei dati personali di operatori economici (o loro legali rappresentanti) interessati a partecipare a procedure

- di scelta del contraente, fornitori di beni e servizi https://www.unifi.it/upload/sub/protezionedati/Informativa_TERZI.pdf

Si autorizza l'Università degli Studi di Firenze, ai fini della trasmissione/notifica di ogni comunicazione rilevante del procedimento, ad utilizzare i riferimenti di contatto indicati nella presente istanza ovvero quelli messi a disposizione dalla piattaforma telematica di negoziazione utilizzata per la gestione della procedura concorrenziale

Lì. Firma digitale

_____

UNIVERSITÀ DEGLI STUDI FIRENZE
SIAF SISTEMA INFORMATICO DELL'ATENEO FIORENTINO

ALLEGATO – B Capitolato Tecnico

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

1. Descrizione

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) 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.

2. Obiettivo della fornitura

L'obiettivo 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.

3. 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 (dominio @stud.unifi.it) utilizzano le proprie credenziali uniche di Ateneo per accedere alla casella di posta personale attribuita dall'Ateneo attraverso GMail. L'autenticazione ai servizi Google (l'intera GSuite) è implementata mediante SAML attraverso un secondo server Shibboleth 2.2 dedicato. Gli altri soggetti, detentori di una casella del dominio @unifi.it, invece si autenticano con credenziali riservate al servizio di posta elettronica, gestite attraverso un server LDAP dedicato le cui procedure di provisioning sono diverse da quelle che sincronizzano la coppia di LDAP per le credenziali uniche di Ateneo per ragioni storiche e perché il ciclo di delle caselle di posta segue policy diverse rispetto a quelle delle credenziali uniche di Ateneo. Questi soggetto attraverso tali credenziali dedicate accedono anche ai servizi della GSuite.

E' stata allestita un'infrastruttura di tipo Virtual Desktop (VDI) basata su VMware per la gestione delle aule didattiche tramite 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.

4. 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.

5. 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:

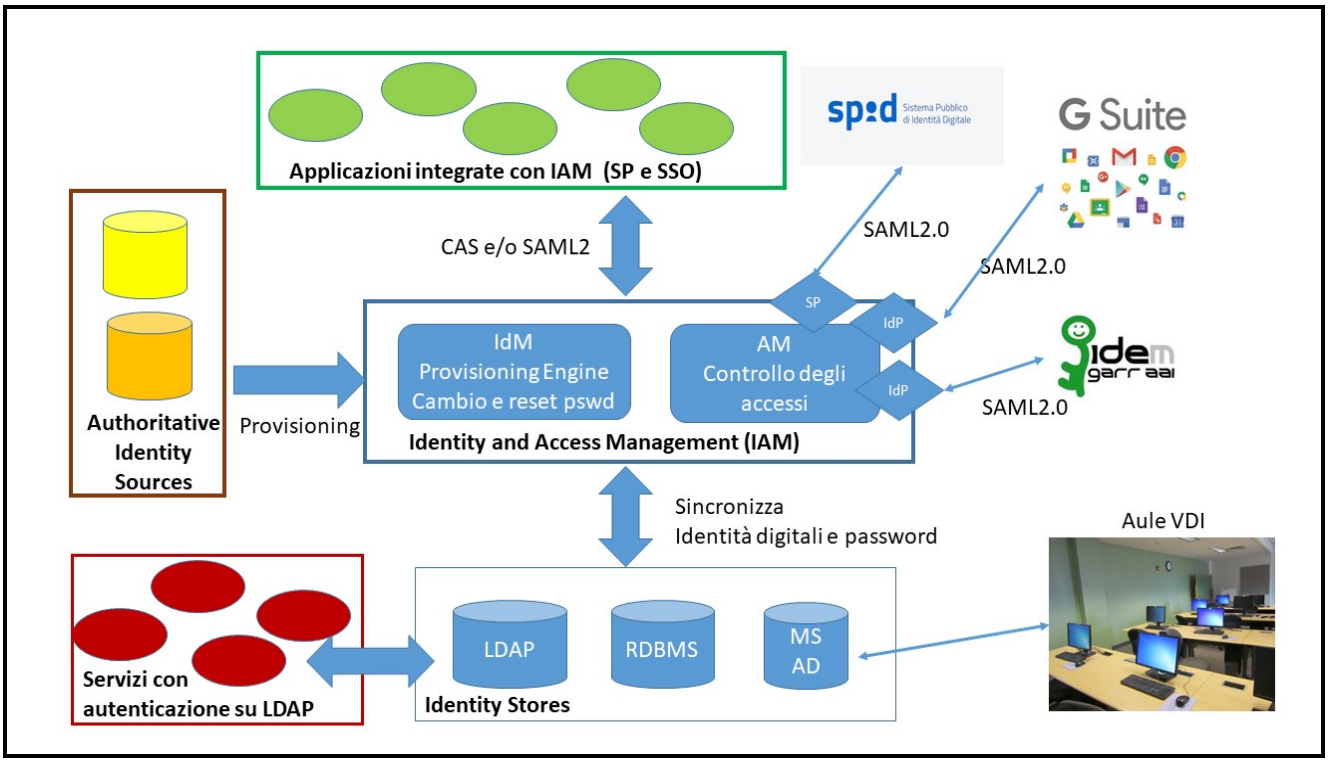
- essere integrato con gli Identity Store (repository utente) esistenti (LDAPv3, Active Directory, RDBMS);
- svolgere il ruolo di Identity Server:
  - per l'autenticazione locale, anche in modalità Single Sign-On (SSO), attraverso i propri Identity Store;
  - di Identity Provider (IdP) SAML 2.0 nell'ambito 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 dai sistemi/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 applicazioni web esistenti in modo trasparente garantendo un percorso evolutivo progressivo verso SSO e SPID a tutte le altre applicazioni JEE e PHP in uso presso l'Università
- 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

- 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).

6. Requisiti funzionali e operativi

- Identity provider (punto unico per l'identificazione digitale)
- Eroga il servizio di cambio password
- Eroga 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
- Gestione automatica e configurabile della scadenza di validità identità digitale e del cambio password secondo politiche che possono essere differenziate per tipologia di utenza
- Supporto dell'autenticazione delegata a SPID
- Supporto dell'autenticazione federata in ambito e IDEM del GARR e Eduroam
- Gestione dei ruoli e dei profili per l'accesso alle risorse e ai servizi
- Supporto ed integrazione con Group Policy per sistemi Microsoft tramite integrazione con AD
- Configurazione e profilatura di differenti set di metadati rilasciabili ai Service Provider di tipo SAML
- Supporto di repository delle identità digitali plurimi ed eterogeni: LDAPv3, DB Oracle, DB MySQL, Active Directory
- Massima flessibilità nella integrazione di procedure di provisioning dei soggetti cui attribuire e manutenere le identità digitali rispetto alle diverse fonti (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
- Massima flessibilità per lo sviluppo e la configurazione di procedure di sincronizzazione tra repository diversi secondo logiche master-slave (primario-secondario.
- Possibilità di integrazione con sistemi di controllo 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)
- 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)

7. Requisiti tecnici

- Utilizzo di componenti software open source quali: Open LDAP, Shibboleth3.3, Apereo CAS, Apache Syncope, Evolveum midpoint
- 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, CAS3, OAuth, OpenId Connect
- Deploy dei componenti del sistema in cloud (pubblico, privato, ibrido) su macchine virtuali (VMWare) e Container Linux in modo clusterizzato
- Deployment in configurazione ridondata in alta affidabilità su rete geografica ottenibile tramite servizi dei PSN/CSP o IaaS, PaaS di provider anche di cloud pubblico.

8. Servizi richiesti nella fornitura

a) *Disegno e deploy del sistema*. Definizione dell'architettura e delle 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) *Registrazione con SPID degli studenti ancora non immatricolati*. Attualmente questa fase viene gestita esponendo l'apposito servizio di registrazione di ESSE3 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 da ESSE3 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
La soluzione 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.

c) *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 semplificherebbe la gestione delle credenziali, visto che spesso i soggetti che devono utilizzare queste applicazioni non hanno credenziali di ateneo o non le hanno più valide e sono comunque riconoscibili in modo univoco dal CF per associarli ai propri dati.

d) *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.

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 da valutare una prevede 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. Una soluzione alternativa prevede 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) *Accesso alla posta Posta elettronica*. In considerazione del fatto che gli studenti hanno già la casella di posta elettronica su Google e che è previsto un progetto per la migrazione a tale piattaforma anche della posta del dominio @unifi.it, un'ulteriore evoluzione dell'IAM e dell'estensione all'uso di SPID riguarderà in una fase successiva anche la posta elettronica.

h) *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).

i) *Eventuale sostituzione di Shibboleth 3.3 con CAS*. Tale ipotesi è volta a garantire la razionalizzazione ed il consolidamento dell'architettura definitiva, purché siano garantite il mantenimento trasparente delle stesse funzionalità per IDEM e per la posta elettronica su Google

j) *Revisione e integrazione delle procedure di provisioning utente*. Questa attività è da ritenersi una delle più delicate e complesse per il consolidamento e l'evoluzione dall'attuale contesto operativo a quello finale basato su IAM.

k) *Documentazione e formazione*. Dovrà essere prodotta la documentazione di progetto, quella sull'architettura definitiva concordata, sui sistemi utilizzati, le configurazioni definite e le procedure implementate.

9. Fasi e tempi di realizzazione

In linea di massima la sequenza delle attività è quella indicata nel pinto precedente "Servizi". L'offerta dovrà contenere la strutturazione in work package esplicitando per ciascuno la descrizione, le attività svolte, i deliverable forniti, 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.

Tempo complessivo previsto: 16 -20 settimane

10. Titolarità e riuso del software

La titolarità di tutto il software sviluppato nell'ambito dei servizi oggetto della fornitura, ail 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.

Glossario

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;

Shibboleth: https://www.shibboleth.net/.