PROPOSTA PER L'AGGIORNAMENTO DELL'INFRASTRUTTURA DI AUTENTICAZIONE E SINGLE SIGN-ON (SSO) E L'ATTIVAZIONE DEL "GATEWAY SPID" PER UNIVERSITÀ DELLA VALLE D'AOSTA

CLASSIFICAZIONE DEL DOCUMENTO

LIVELLO		DATA	RESPONSABILE	DESTINATARI
Riservato				
Ad uso interno	X	17/12/2020	Rossini Angelo	
Di dominio pubblico				

STATO DELLE REVISIONI

Revisioni effettuate			
Rev.:	Data	Paragrafo	Oggetto della revisione
0	17/12/2020		Emissione

Stato del documento	Data	Funzione	Nominativo	Firma
Redatto	17/12/2020		Rossini Angelo	
Rivisto				
Approvato				

Sommario

Riferimenti

[AGID-ATTSPID] AGID – REGOLAMENTO RECANTE LE MODALITÀ ATTUATIVE PER LA REALIZZAZIONE DELLO SPID (articolo 4, comma 2, DPCM 24 ottobre 2014) - (versione 2.0 del 22 luglio 2016)

[AGID-TECSPID] AGID – REGOLAMENTO RECANTE LE REGOLE TECNICHE (articolo 4, comma 2, DPCM 24 ottobre 2014) - (Versione 1)

[AGID-ATTRSPID] AgID – SPID - TABELLA ATTRIBUTI IDENTIFICATIVI - (Versione 1)

[AGID-AVV6] AgID – SPID - NOTE SUL DISPIEGAMENTO DI SPID PRESSO I GESTORI DEI SERVIZI - (Avviso nr 6 del 29/07/2016)

[CINECA-IDPSHIB] CINECA - ALLEGATO TECNICO PER IL SERVIZIO SHIBBOLETH IDP HOSTING CINECA (Rev. 1.0 del 02/08/2016)

[CINECA-GWSPID] CINECA - ALLEGATO TECNICO PER IL SERVIZIO GATEWAY SPID CINECA (Rev. 1.0 del 03/08/2016)

Scopo del documento

L'Università della Valle d'Aosta (di seguito UNIVDA) ha adottato da alcuni anni i prodotti U-GOV, Titulus, U-WEB, U-SIGN e ESSE3 di CINECA in hosting.

Il progetto prevede l'attivazione di una nuova infrastruttura di autenticazione in hosting presso CINECA, per consentire l'accesso in Single sign-on (SSO) ai servizi indicati in precedenza.

Situazione attuale

La situazione attuale è rappresentata nel seguente diagramma di sistema.

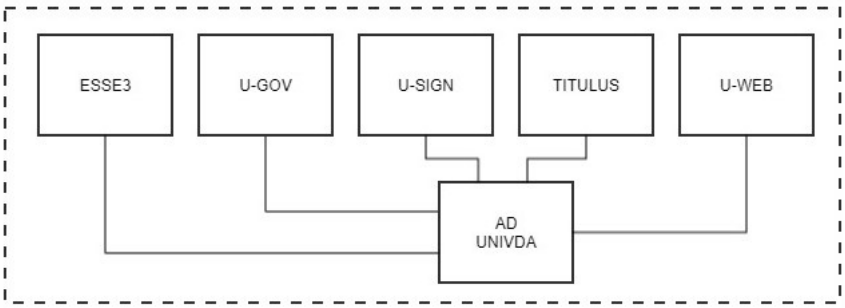

Figura 1– Diagramma di sistema situazione attuale

In dettaglio:

a) AD UNIVDA: è l'Active Directory in house presso UNIVDA; contiene le identità digitali e le credenziali degli utenti dell'Ateneo.

b) ESSE3: autentica localmente registrati o prospect e preimmatricolati, su AD UNIVDA le restanti tipologie di utenti.

c) U-GOV, Titulus, U-WEB e U-SIGN: autenticano su AD UNIVDA gli utenti dell'Ateneo.

Nuova architettura tecnologica

Come richiesto da UNIVDA di seguito viene descritta la fase di attivazione di nuovi componenti infrastrutturali per autenticazione e SSO in hosting presso CINECA, evoluzione necessaria per consentire l'accesso ai servizi con credenziali SPID.

Per il corretto funzionamento di Gateway SPID è di fondamentale importanza che UNIVDA garantisca la corretta attribuzione del codice fiscale alle identità digitali su AD UNIVDA.

Attivazione di nuovi componenti infrastrutturali per autenticazione e SSO in hosting presso CINECA

L'architettura tecnologica in hosting è rappresentata nel seguente diagramma di sistema.

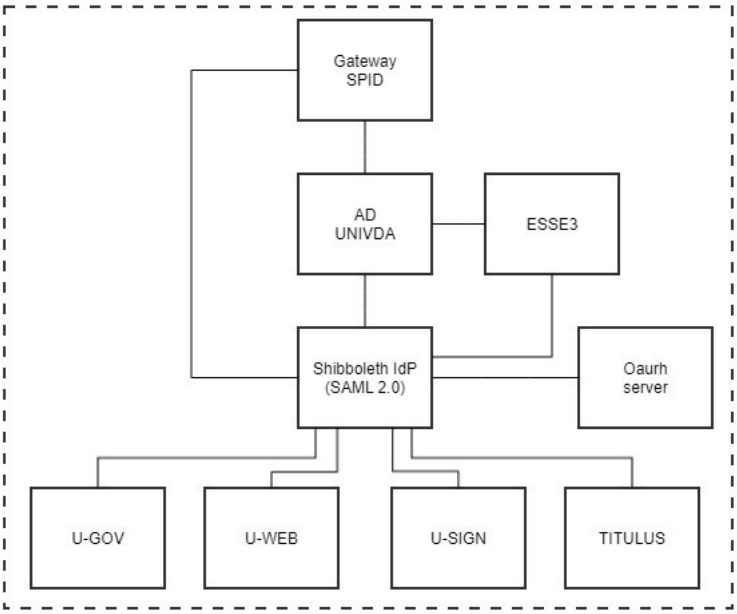

Figura 2– Diagramma si sistema nuova architettura tecnologica in hosting

Le differenze rispetto alla situazione attuale sono le seguenti:

a) ESSE3: è modificato per popolare AD UNIVDA anche con le informazioni relative a registrati o prospect e preimmatricolati, in aggiunta alle informazioni per cui è già attivo il popolamento, e per propagare il valore del campo spidCode valorizzato per gli studenti che si sono registrati con SPID. UNIVDA deve indicare quale attributo di AD UNIVDA utilizzare per il salvataggio del valore di spidCode.

b) Shibboleth [1] IdP: è l'identity provider (IdP) SAML 2.0 in hosting presso CINECA per l'autenticazione, il SSO e il global logout di ESSE3, U-GOV, Titulus, U-WEB e U-SIGN; autentica

[1] Ultima versione stabile rilasciata ufficialmente al momento dell'attivazione.

tutte le tipologie di utenti su AD UNIVDA. Rende inoltre disponibile anche il protocollo OAuth 2.0, utilizzando un'opportuna estensione, ed è configurato per consentire il SSO di Office365 e l'accesso nella federazione GARR-IDEM.

Successivamente l'accesso in SSO potrà essere esteso ad altri servizi (SP); sarà infatti sufficiente censirli su Shibboleth IdP.

Il censimento di nuovi SP associati a servizi CINECA sarà gestito da CINECA, mentre il censimento di nuovi SP non associati a servizi CINECA[2] potrà essere effettuato in autonomia da UNIVDA se renderà disponibile su un web server il file XML dei metadati di tali SP. Shibboleth IdP sarà configurato per "consumare" i metadati e l'eventuale irraggiungibilità del file XML non darà origine a disservizi, poiché si manterrà una copia locale.

L'eventuale estensione del set di attributi rilasciati ai singoli SP richiederà il coinvolgimento di CINECA e le attività necessarie non saranno incluse nel canone di hosting di Shibboleth IdP.

c) Gateway SPID: consente agli utenti già in possesso di credenziali UNIVDA, e quindi censiti su AD UNIVDA, di poter accedere ai servizi in SSO di UNIVDA utilizzando credenziali SPID in alternativa alle credenziali UNIVDA. La riconciliazione tra identità SPID e identità UNIVDA avviene creando una corrispondenza automatica tra il codice fiscale associato all'identità digitale SPID e il codice fiscale associato all'identità digitale UNIVDA.

   Se a un medesimo codice fiscale corrispondono più identità digitali UNIVDA il Gateway SPID richiede all'utente di scegliere quale identità digitale vuole utilizzare per la sessione di SSO che sta attivando; la scelta effettuata viene memorizzata e riproposta come prima opzione al login successivo.

   Se a un codice fiscale non corrisponde nessuna identità digitale UNIVDA il Gateway SPID segnala l'errore utilizzando una pagina di cortesia e interrompe il processo di autenticazione.

   Consente inoltre l'accesso al processo di immatricolazione basato su identità digitali SPID disponibile in ESSE3 che gestisce la registrazione come registrati o prospect e preimmatricolati una volta che l'autenticazione è stata effettuata con credenziali SPID.

d) ESSE3, U-GOV, Titulus, U-WEB e U-SIGN: sono configurati per consentire l'autenticazione e il SSO su Shibboleth IdP.

[2] Come ad esempio Sebina e il wi-fi di Ateneo.

Tavola di sintesi della topologia del sistema

Servizio	Shibboleth IDP	Oauth server	AD UNIVDA	ESSE3	Gateway SPID	U-GOV, Titulus, U-WEB e U-SIGN
Autenticazione utente	X	X	X		X	
Federazione SAML	X			X		X
Provisioning				X		

Note e criticità

L'attivazione di Shibboleth IDP CINECA in hosting, a cui sarà collegato il Gateway SPID, richiede la raggiungibilità di AD UNIVDA dalla rete di CINECA, poiché tale sistema deve essere aggiunto come fonte di autenticazione a Shibboleth IdP e come fonte di riconciliazione al Gateway SPID.

Si presume che tale raggiungibilità sia realizzata con opportune ACL basate sugli indirizzi IP di provenienza, quindi non dovrebbero presentarsi problemi. La sicurezza della connessione è comunque garantita, visto che si utilizza il protocollo cifrato ldaps e le password su AD UNIVDA sono cifrate.

Attività di progetto

Attivazione di nuovi componenti infrastrutturali e configurazione applicativi per autenticazione e SSO in hosting presso CINECA
Autenticazione, Federazione e SSO
Configurazione ESSE3 per alimentazione AD UNIVDA con i dati di registrati o prospect e preimmatricolati [3] e la valorizzazione dell'attributo spidCode
Attivazione Shibboleth IdP in hosting versione 3.x con estensioni CINECA
Attivazione Gateway SPID
Attivazione Oauth server
Riconfigurazione ESSE3, U-GOV, Titulus, U-WEB e U-SIGN per SSO/global logout
Configurazione Shibboleth IdP in hosting per federazione GARR IDEM e eduGAIN
Configurazione Shibboleth IdP in hosting per SSO Office365

Le voci indicate comprendono le necessarie attività di analisi, sviluppo, validazione e test e messa in esercizio del sistema.

L'attività di configurazione per adesione alle federazioni IDEM e eduGAIN comprende unicamente le attività tecniche; resta a carico di UNIVDA la gestione amministrativa necessaria per l'ingresso in federazione.

La predisposizione dell'IdP per il SSO con Office365 non include la configurazione e il provisioning lato Office365 che retano in carico a UNIVDA.

In seguito all'accettazione dell'offerta CINECA, produrrà un cronoprogramma di dettaglio, dove saranno mostrati i tempi di consegna dei deliverable descritti in questa proposta.

[3] Il provisioning è già attivo; deve essere aggiunta una nuova tipologia di utenti.