SPID Gateway: l'interfacciamento dei sistemi di ateneo con il Sistema Pubblico di Identita' Digitale

CINECA 7 Febbraio 2017

SPID – Alcuni numeri (Gennaio 2017)

- **1 Milione** di identità rilasciate
- **3.720** amministrazioni aderenti (3 Università)
- **4.273** servizi abilitati

(*Fonte: AgID https://www.spid.gov.it/infografiche*)

Tra i servizi SPID-compliant:

SPID – La normativa

Il Codice dell'Amministrazione Digitale (CAD) sancisce che **SPID** (*Sistema Pubblico per la gestione dell'Identità Digitale*) sarà **obbligatorio** per l'accesso ai servizi in rete delle PA, in alternativa alla carta d'identità elettronica (CIE) e alla carta nazionale dei servizi (CNS)[1].

Le PA dovranno adeguare i servizi in rete affinché consentano l'autenticazione degli utenti con uno dei metodi previsti dal CAD entro 24 mesi dall'attivazione del primo identity provider SPID[2].

⇨ **Entro il 31/12/2017** (fonte https://www.spid.gov.it/)

1. Decreto legislativo n. 235/2010 - testo vigente dal 21/08/2013, art.64 commi 1 e 2.

2. Decreto del Presidente del Consiglio dei Ministri del 24/10/2014 - Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese.

SPID – Attori coinvolti

- cittadini e imprese, in qualità di utenti dei servizi in rete
- gestori dell'identità digitale (Identity Provider - IdP)
- gestori di attributi qualificati (Attribute Authority - AA)
- pubbliche amministrazioni e imprese, in qualità di erogatori di servizi in rete (Service Provider - SP)
- l'Agenzia per l'Italia digitale (AGID), in qualità di autorità di accreditamento e vigilanza

SPID – Vantaggi

- utilizza il protocollo SAML per il dialogo tra IdP e SP
- garantisce l'identità dell'utente a cui vengono associate le credenziali SPID
- federa identità, quindi l'utente può possedere più identità su differenti IdP SPID riconducibili a lui attraverso il codice fiscale
- i singoli SP possono reperire ulteriori attributi qualificati oltre a quelli di base (identificativi + secondari) utilizzando le AA
- gli IdP SPID prevedono le autenticazioni basate su username+password, OTP o certificato X.509, corrispondenti rispettivamente ai «Level of Assurance» - LoA- 2, 3 e 4 dello standard ISO/IEC 29115; la scelta della modalità di autenticazione da utilizzare avviene sui singoli SP

SPID – Attributi rilasciati

ATTRIBUTI IDENTIFICATIVI

- Codice identificativo SPID → spidCode
- Nome → name
- Cognome → familyName
- Luogo di nascita → placeOfBirth
- Data di nascita → dateOfBirth
- Sesso → gender
- Codice fiscale → fiscalNumber
- Documento d'identità → idCard

ATTRIBUTI SECONDARI

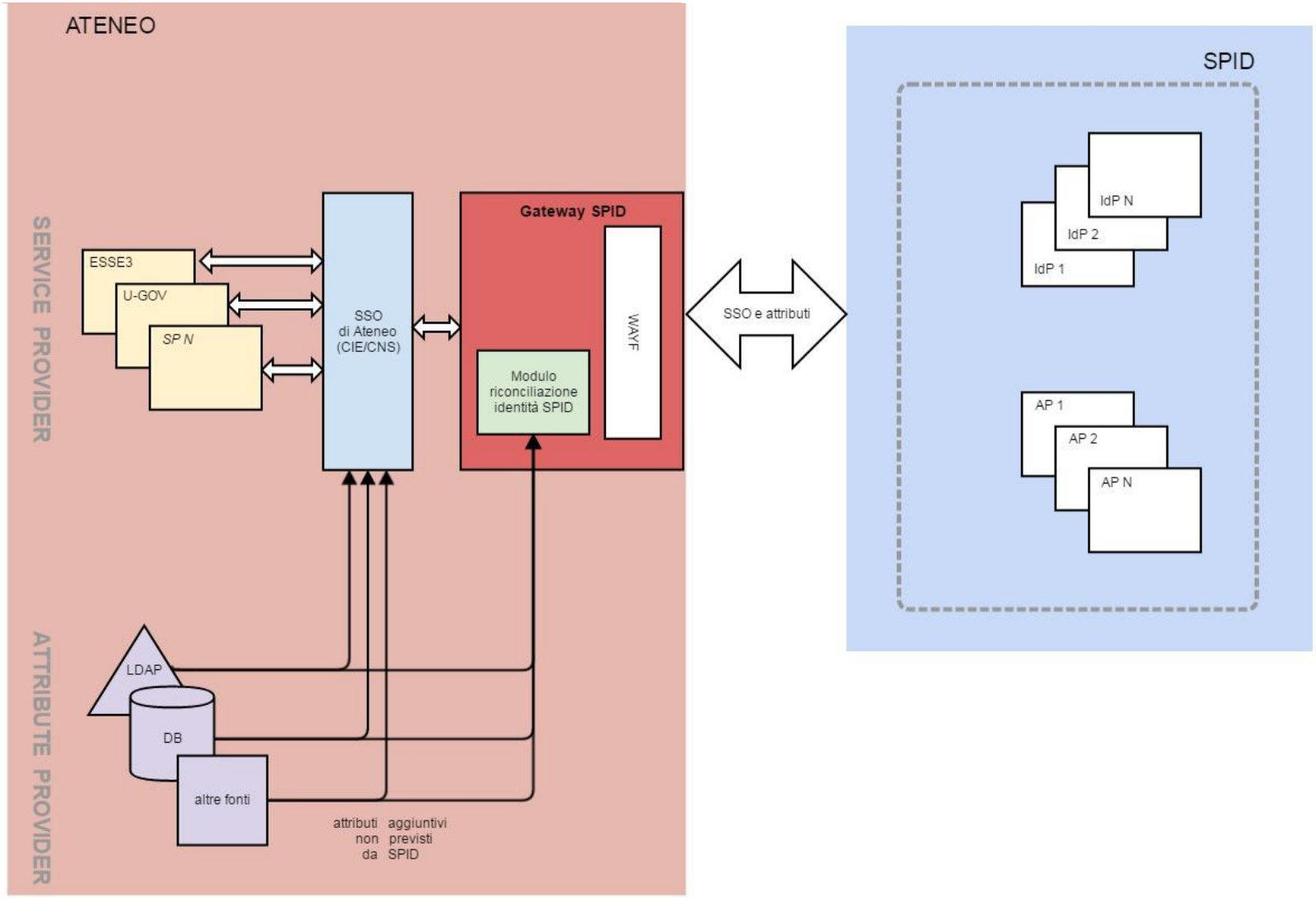
- Numero di telefono mobile → mobilePhone
- Indirizzo di posta elettronica → email
- Domicilio fisico → address
- Domicilio digitale → digitalAddress

SPID - Criticità

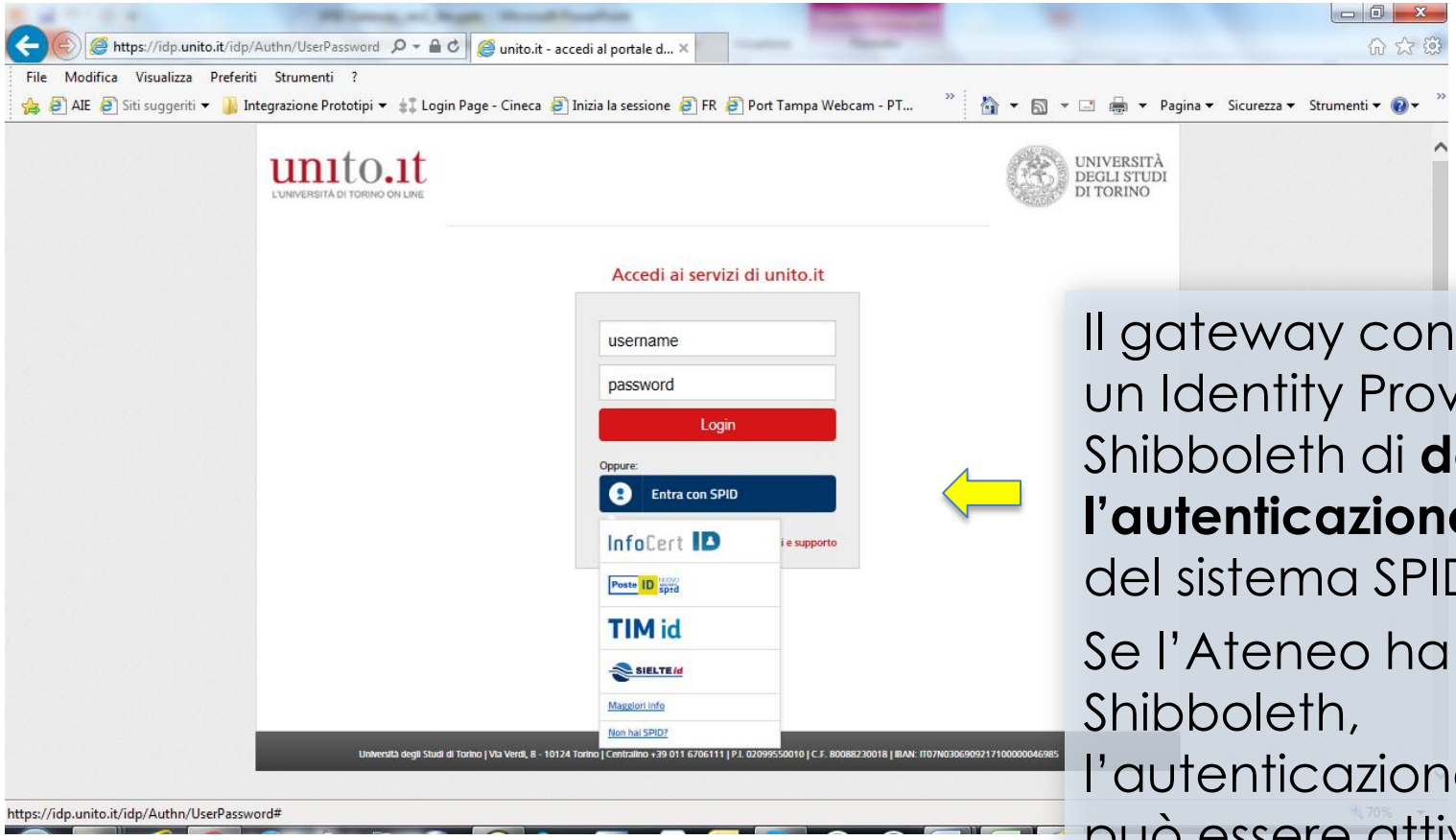
L'introduzione di SPID ha inevitabilmente un impatto sui sistemi esistenti, poiché:

- nasce come federazione di identità digitali non di servizi: mantenere il SSO come attualmente realizzato dagli atenei potrebbe essere complesso
- le identità SPID potrebbero non essere immediatamente riconducibili a quelle esistenti in ateneo
- il censimento diretto di un nuovo SP su SPID prevede un processo che coinvolge AGID e i fornitori dei servizi IdP
- gli IdP SPID rilasciano solo gli attributi previsti dalla normativa (identificativi ed eventualmente secondari)
- se un IdP SPID non è disponibile i relativi utenti non possono accedere ai servizi dell'ateneo
- i servizi dell'ateneo potrebbero richiedere degli adeguamenti per utilizzare gli IdP SPID

Gateway SPID – L'idea



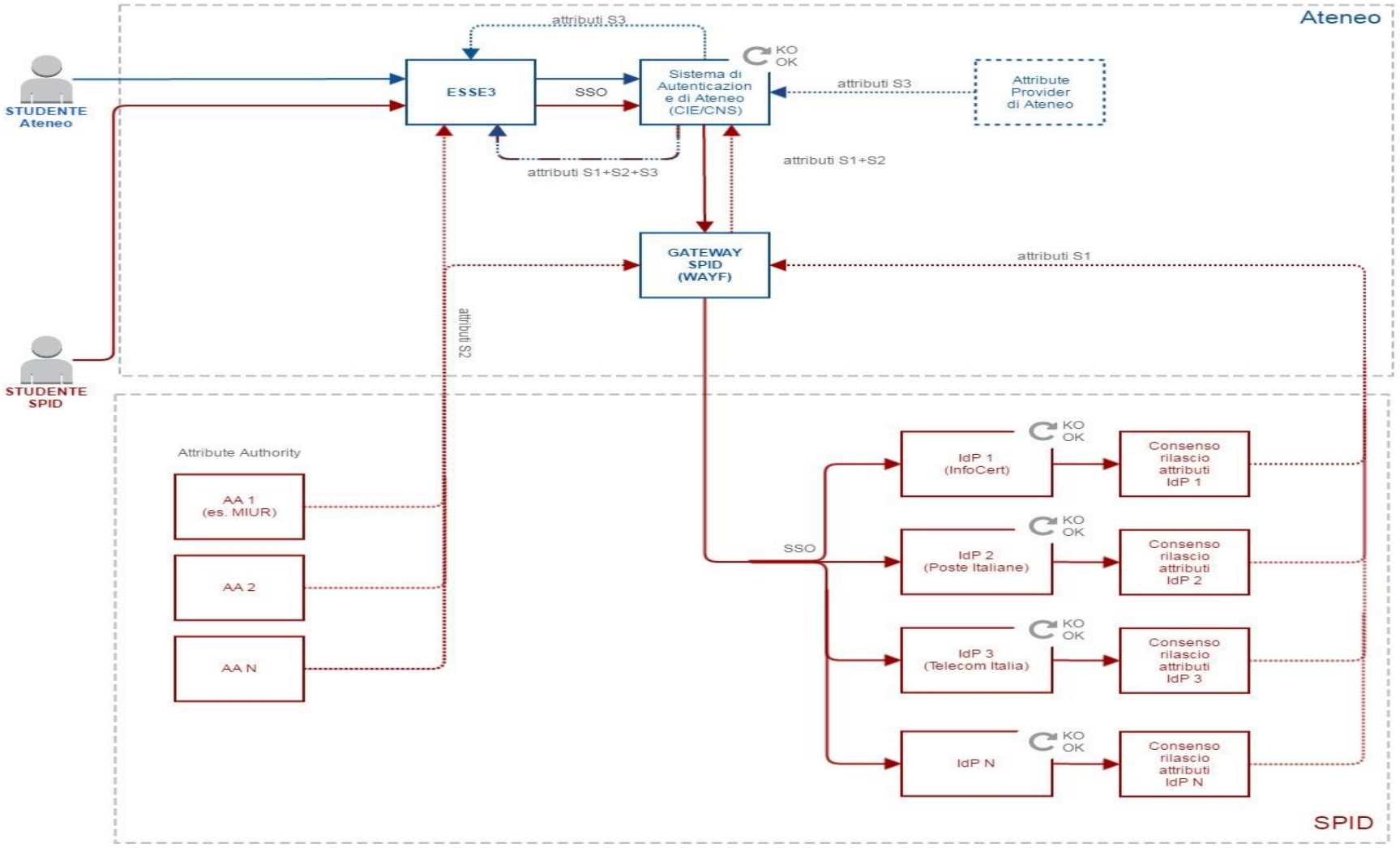
Gateway SPID – Come funziona



Il gateway consente a un Identity Provider (IdP) Shibboleth di **delegare l'autenticazione** agli IdP del sistema SPID.

Se l'Ateneo ha già un IdP Shibboleth, l'autenticazione SPID può essere attivata come alternativa all'autenticazione già presente in Ateneo.

Gateway SPID – Schema di funzionamento



- *In rosso i flussi di autenticazione di un utente con identità SPID*
- *In blu quelli di un utente con identità fornita dall'Ateneo*

Gateway SPID – Benefici

Disaccoppia i servizi dell'ateneo da SPID e permette di:

- far convivere l'**autenticazione di Ateneo** con quella **SPID**
- realizzare politiche di **riconciliazione** per collegare tra loro identità SPID ed identità esistenti
- concentrare in un unico punto l'assolvimento degli **obblighi normativi** previsti da SPID (monitoraggio, compliance e governance)
- accreditare presso AGID **un solo servizio** di Ateneo su SPID (il gateway) guadagnando autonomia nell'aggiunta di nuovi servizi locali con autenticazione SPID e realizzando quello che AGID ha definito "*nodo cluster*"
- aggregare in un solo punto gli **attributi** che verranno rilasciati dalle Attribute Authority SPID, dagli IdP SPID e dalle fonti interne all'Ateneo per distribuirli ai SP

Gateway SPID – Il nodo cluster AGID

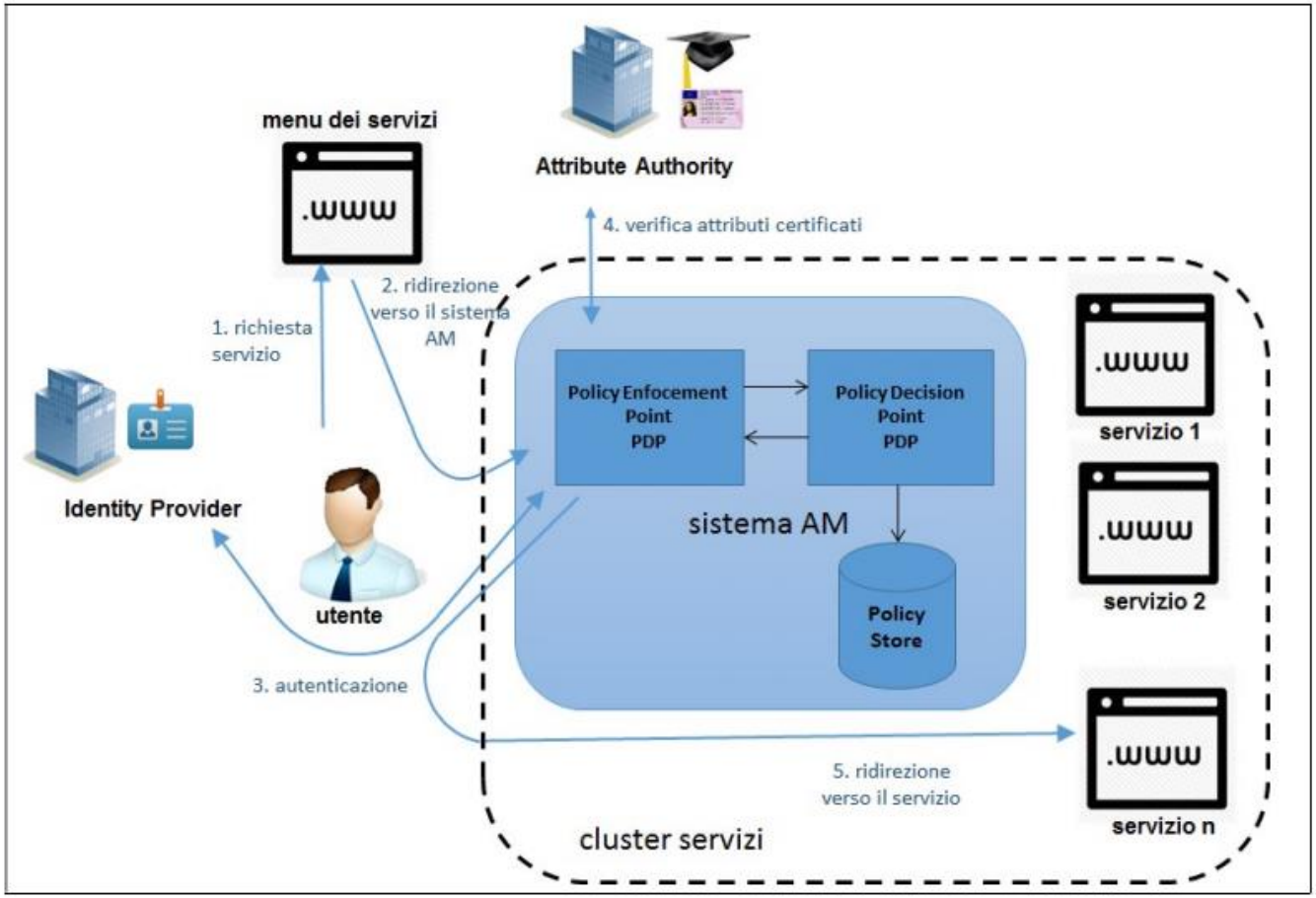


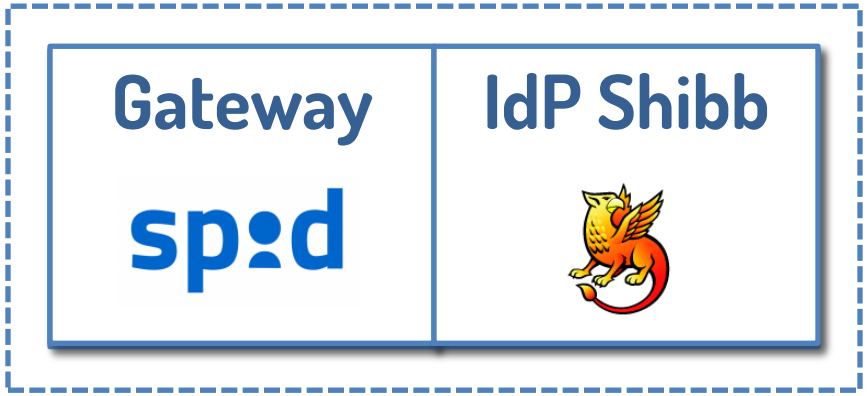
Figura 1 – Nodo cluster di servizi

AGID - Avvisi SPID - Avviso n. 6 - Note sul dispiegamento di SPID presso i gestori dei servizi - Versione v 1.0 del 29/07/2016

Gateway SPID e IdP Shibboleth

Il gateway SPID CINECA richiede un **IdP Shibboleth**:

- se è già presente, il gateway può essere installato come modulo aggiuntivo
- se non è presente, l'IdP deve essere installato ed attivato insieme al gateway



Attualmente il gateway è compatibile con la versione 2.4.5 di Shibboleth.

Gateway SPID – Caso d'uso

Università degli Studi di Torino

- circa 70 servizi collegati in SSO all'IdP Shibboleth di ateneo
- IdP federato IDEM
- Utente con il medesimo codice fiscale associato ai profili STUDENTE e DOCENTE in possesso di più identità digitali SPID

Prossime evoluzioni

- Rilascio di una versione compatibile con **Shibboleth 3** □

- Riconciliazione e gestione multiprofilo ☑

- Predisposizione gateway SPID per utilizzo AA □

Entro **giugno 2017** inoltre ESSE3 sarà opportunamente adeguato e utilizzerà l'autenticazione e le informazioni utente fornite dal gateway SPID per la dematerializzazione del processo di immatricolazione dei futuri studenti.

Grazie per l'attenzione

Angelo Rossini
a.rossini@cineca.it