

# Integrazione di SPID nel sistemi di Identity Management di UniTrento

Maurizio Festi

# Argomenti

1. Obiettivi, casi d’uso
2. Schema della soluzione adottata
3. Problemi affrontati
4. Considerazioni finali

# 1.Obiettivi, requisiti, vincoli

**Revisione** del sistema di **Single Sign On** di UniTrento

1. eseguire l'upgrade alla versione 3 dell'IdP Shibboleth
2. integrare l'autenticazione SPID
3. migliorare il supporto alle federazioni IDEM ed eduGain
4. compatibilità con i servizi UniTrento già in produzione
5. reimplementare alcune funzionalità UniTrento rientrando nello standard
6. rendere responsive (mobile first) la pagina di login e le pagine correlate

# 1.2 Integrare l'autenticazione SPID: requisiti specifici

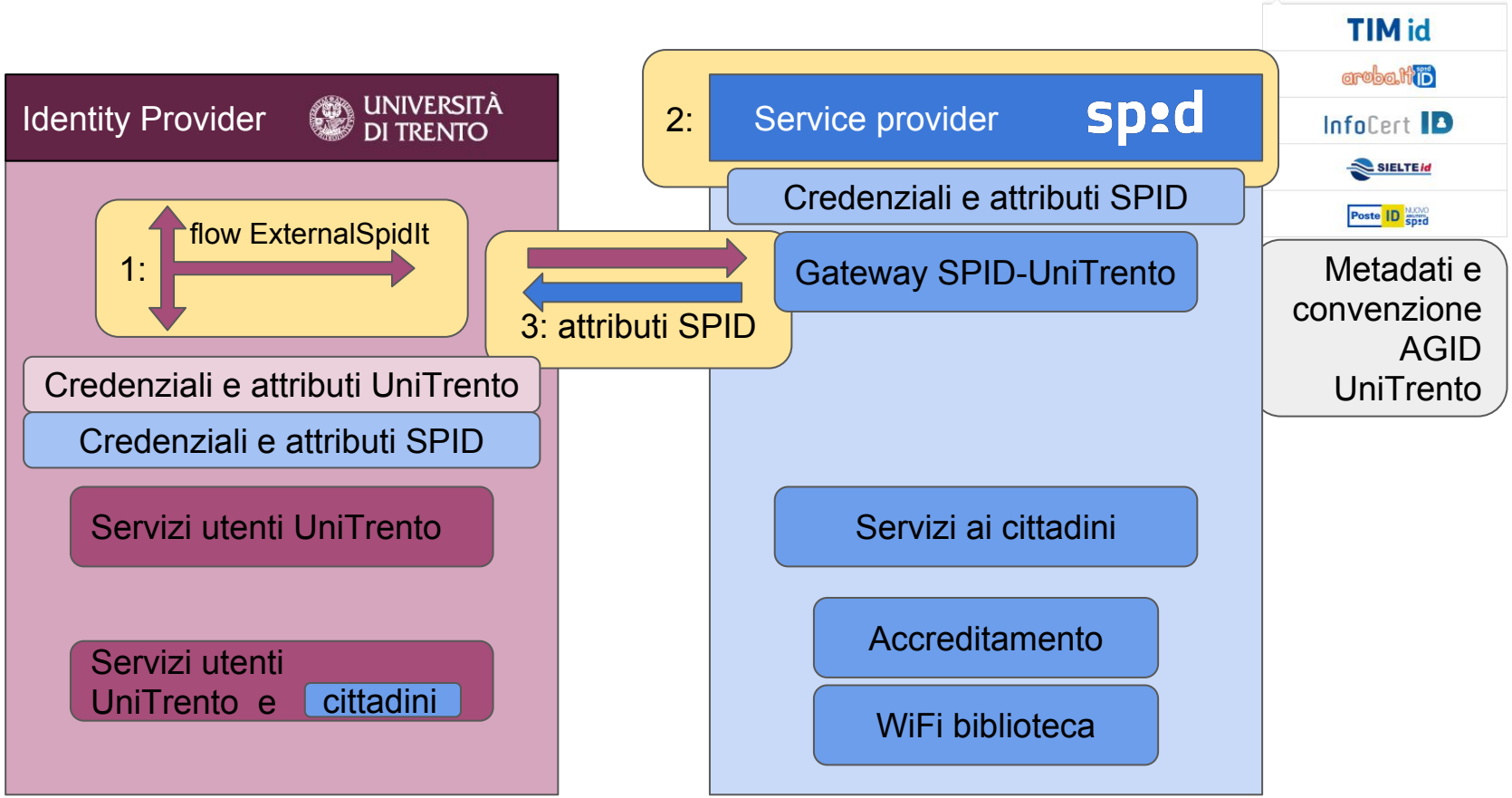
1. **match** dell'**identità SPID** con **l'identità locale**
    a. un **utente UniTrento** autenticato via SPID viene visto dalle applicazioni come un utente UniTrento (set **attributi UniTrento**)
2. **utilizzare** le **identità SPID** anche **in assenza** di un'**identità locale**
3. **gestire la complessità** separando le problematiche
    a. configurazione e manutenzione dell'**IdP UniTrento**
    b. configurazione e manutenzione del **service provider SPID** di UniTrento
    c. registrazione **nuove identità/accreditamento**

# 1.2 Integrare l'autenticazione SPID: alcuni casi d'uso

1. **SPID con identità locali**
   a. **servizi** erogati ai **membri di UniTrento**
   b. accesso ai **servizi web** UniTrento **senza** necessità di ricordare le **credenziali UniTrento**
   c. servizi agli **alumni** e agli ex-membri (non ricordano le credenziali UniTrento)
   d. supporto alle credenziali UniTrento (**reset password**)
   e. potenziale utilizzo di **SpidL2** per servizi critici

2. **SPID senza identità locali**
   a. **servizi erogati ai cittadini**
   b. semplificazione dei **processi di accreditamento** utilizzando gli attributi SPID

# 2. Schema della soluzione adottata

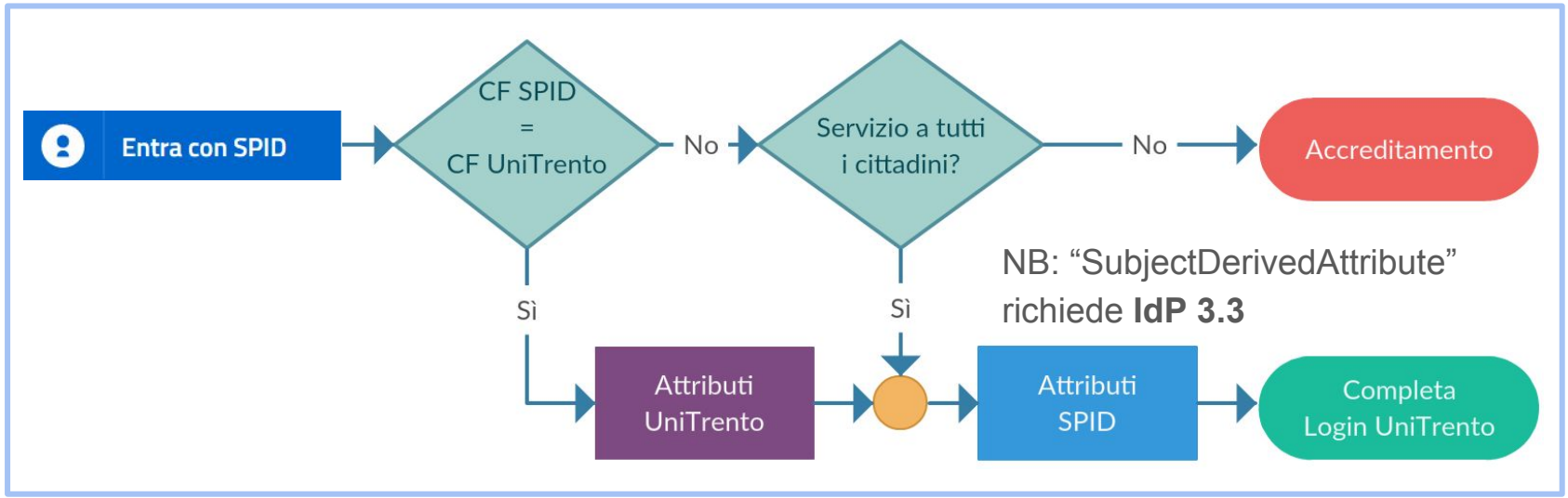



A. Nuovo authn flow authn/ExternalSpidIt basato su ExternalAuthentication
B. Match con le identità locali (quando serve)
C. Osservazioni


A. Nuovo authn flow authn/ExternalSpidIt basato su ExternalAuthentication
B. Match con le identità locali (quando serve) e attributi SPID
C. Osservazioni

a. modificati e aggiunti **file di configurazione** Shibboleth
b. implementazione **codice java** (classi e interfacce)
c. definito un **contesto di autenticazione** specifico per il flow: ExternalSpidItAuthContext

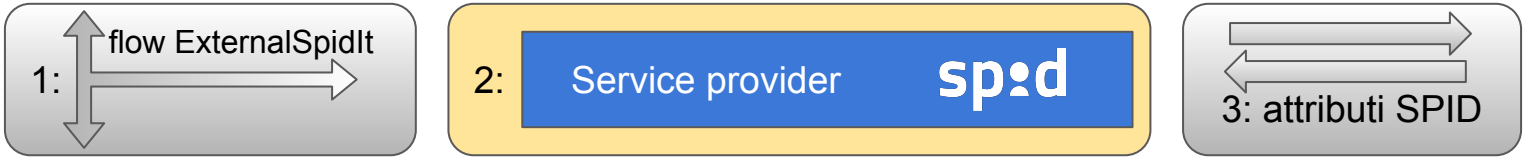

A. Nuovo authn flow authn/ExternalSpidIt basato su ExternalAuthentication
B. Match con le identità locali (quando serve) e attributi SPID
C. Osservazioni



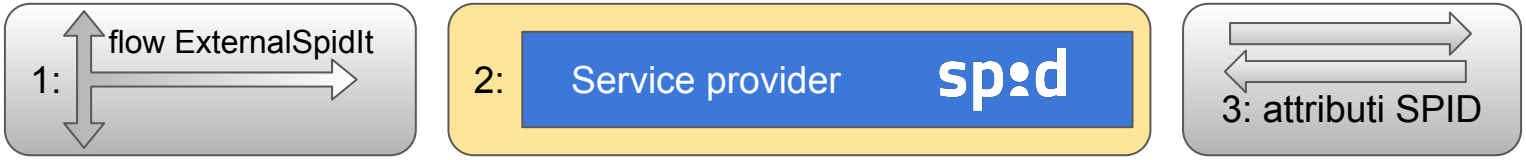

A. Nuovo authn flow authn/ExternalSpidIt basato su ExternalAuthentication
B. Match con le identità locali (quando serve) e attributi SPID
C. Osservazioni

E' un'attività relativamente complessa in quanto richiede:

1. conoscenza della struttura interna di **Shibboleth**
2. conoscenza di **Spring WebFlow** con cui sono implementati i flow dell'IdP
3. la scrittura e la modifica di file di **configurazione non elementari**
4. l'implementazione di **codice Java** dedicato
5. il **rischio** di introdurre **errori** e problemi di **sicurezza** anche banali

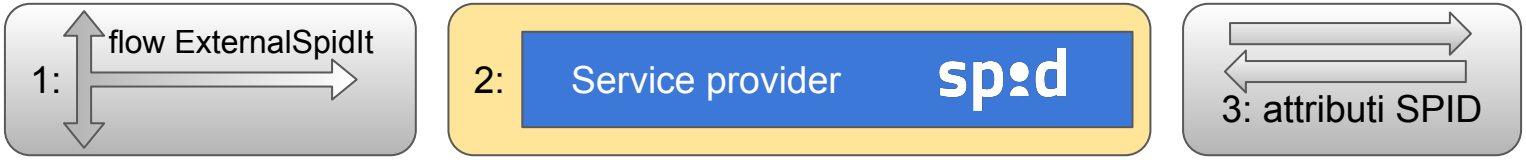



A. Procedura tecnica
B. Procedura amministrativa
C. Osservazioni



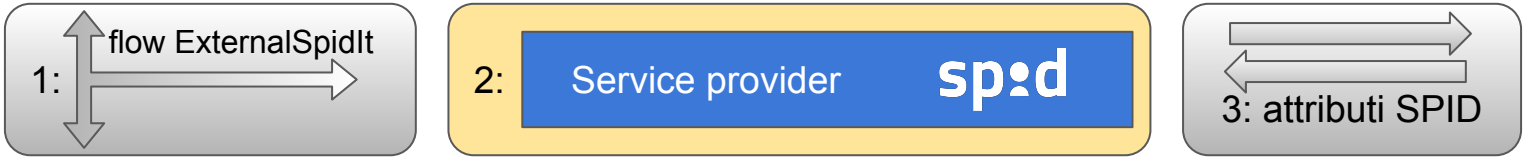

A. Procedura tecnica
B. Procedura amministrativa
C. Osservazioni

a. costruzione dei **metadati del service provider** da inviare ad AGID
b. configurare l'**AuthnRequest** da inviare agli IdP SPID
c. implementare la **form di selezione dell'IdP** dalla lista degli IdP **SPID** (su specifiche AGID e Embedded Discovery Service di Shibboleth)
d. test con tutti i **5 IdP SPID:** sono implementazioni differenti con **comportamenti leggermente differenti**




A. Procedura tecnica
B. Procedura amministrativa
C. Osservazioni

a. Descrizione dei **servizi**
b. Elenco degli **attributi** richiesti
c. **Ragionevolezza** tra attributi richiesti e servizi erogati
d. Rispetto delle **clausole della convenzione**
e. Elenco servizi e attributi in **documento allegato**




A. Procedura tecnica
B. Procedura amministrativa
C. Osservazioni

a. Relativamente complicato in quanto richiede:
   i. il rispetto delle **specifiche AGID** (**Metadati** e **AuthnRequest)**
   ii. il rispetto dei termini della **convenzione** con **AGID**
   iii. l'**interazione con AGID** per procedure tecniche e amministrative
b. C'è **molto supporto** da parte di **AGID** e dai referenti degli **IdP**
c. Procedure e strumenti in **evoluzione costante**
d. **Consultare:** https://www.spid.gov.it/sei-una-pubblica-amministrazione

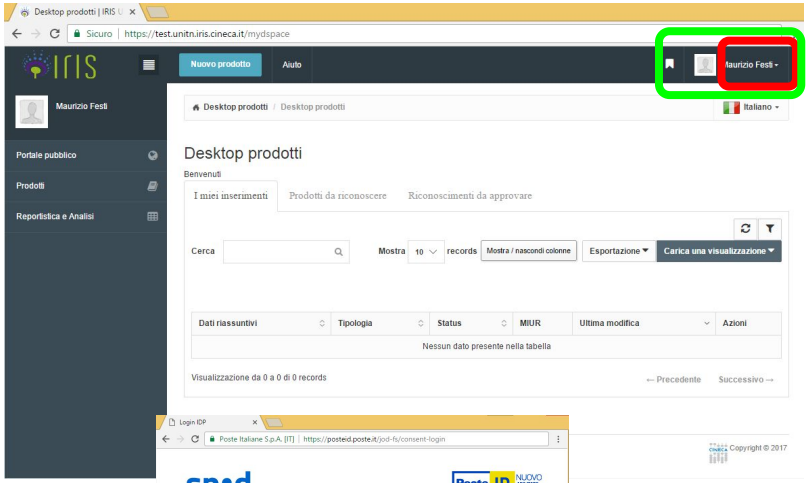

A. Da flow IdP UniTrento a gateway SPID e ritorno degli attributi
B. Osservazioni

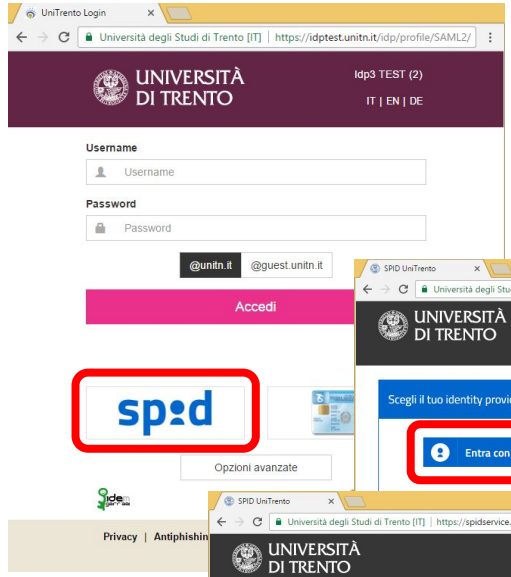

A. Da flow IdP UniTrento a gateway SPID e ritorno degli attributi
B. Osservazioni

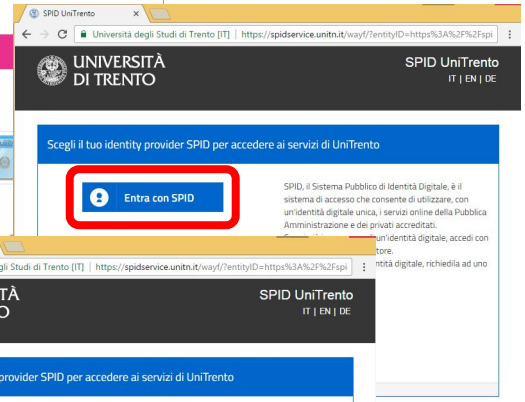
a. **Gateway SPID-UniTrento** è una **normale applicazione** protetta dal service provider SPID
b. attiva l'autenticazione SPID e **riceve gli attributi** dall'IdP **SPID**
c. riceve il **riferimento al flow di autenticazione** in corso sull'IdP UniTrento
d. **ritorna** gli attributi/riferimento flow all'**IdP UniTrento** che **prosegue il flow** di autenticazione in corso

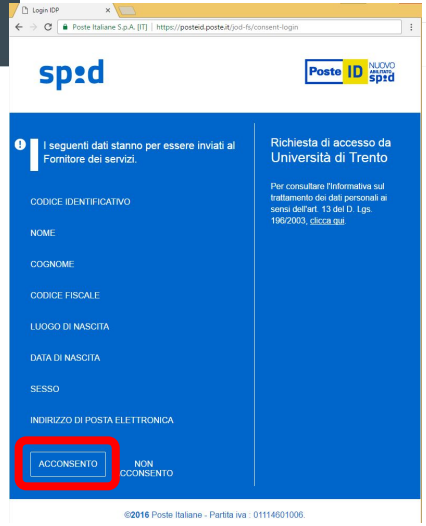

A. Da flow IdP UniTrento a gateway SPID e ritorno degli attributi
B. Osservazioni

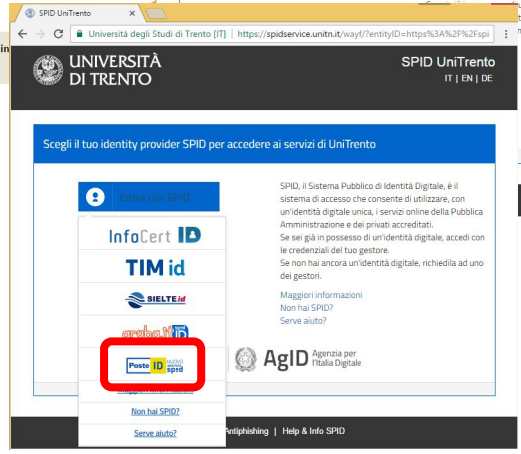
a. **Non** è un'attività particolarmente **complessa**
b. Dipende solo da scelte e **valutazioni** tecniche **locali**
c. Va solo gestito un buon **livello di sicurezza**
    i. utilizzo di 2 **certificati self signed dedicati** (per IdP e SPIDSPGW)

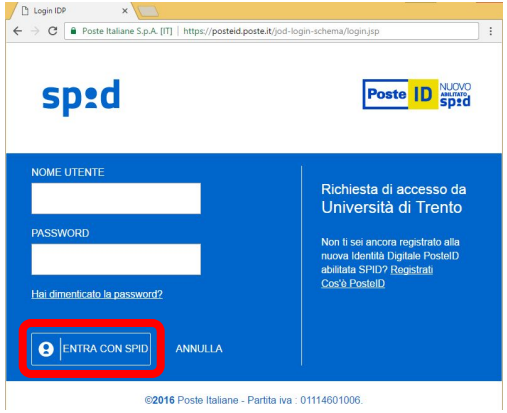

Desktop prodotti | IRIS
Sicuro | https://test.unitn.iris.cineca.it/mydspace
IRIS
Nuovo prodotto
Aiuto
Maurizio Festi
Maurizio Festi
Portale pubblico
Prodotti
Reportistica e Analisi
Desktop prodotti / Desktop prodotti
Italiano
Desktop prodotti
Benvenuti
I miei inserimenti
Prodotti da riconoscere
Riconoscimenti da approvare
Cerca
Mostra 10 records
Mostra / nascondi colonne
Esportazione
Carica una visualizzazione
Dati riassuntivi
Tipologia
Status
MIUR
Ultima modifica
Azioni
Nessun dato presente nella tabella
Visualizzazione da 0 a 0 di 0 records
← Precedente
Successivo →
Copyright © 2017


UniTrento Login
Università degli Studi di Trento [IT] | https://idptest.unitn.it/idp/profile/SAML2/
UNIVERSITÀ DI TRENTO
Idp3 TEST (2)
IT | EN | DE
Username
Username
Password
Password
@unitn.it
@guest.unitn.it
Accedi
spid
Opzioni avanzate
Privacy | Antiphishin


SPID UniTrento
Università degli Studi di Trento [IT] | https://spidservice.unitn.it/wayf/?entityID=https%3A%2F%2Fspi
UNIVERSITÀ DI TRENTO
SPID UniTrento
IT | EN | DE
Scegli il tuo identity provider SPID per accedere ai servizi di UniTrento
Entra con SPID
SPID, il Sistema Pubblico di Identità Digitale, è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati.


Login IDP
Poste Italiane S.p.A. [IT] | https://posteid.poste.it/jod-fs/consent-login
spid
Poste ID NUOVO spid
I seguenti dati stanno per essere inviati al Fornitore dei servizi.
CODICE IDENTIFICATIVO
NOME
COGNOME
CODICE FISCALE
LUOGO DI NASCITA
DATA DI NASCITA
SESSO
INDIRIZZO DI POSTA ELETTRONICA
ACCONSENTO
NON CONSENTO
Richiesta di accesso da Università di Trento
Per consultare l'informativa sul trattamento dei dati personali ai sensi dell'art. 13 del D. Lgs. 196/2003, clicca qui.
©2016 Poste Italiane - Partita iva : 01114601006


SPID UniTrento
Università degli Studi di Trento [IT] | https://spidservice.unitn.it/wayf/?entityID=https%3A%2F%2Fspi
UNIVERSITÀ DI TRENTO
SPID UniTrento
IT | EN | DE
Scegli il tuo identity provider SPID per accedere ai servizi di UniTrento
Entra con SPID
InfoCert ID
TIM id
SIELTE id
Poste ID NUOVO spid
Non hai SPID?
Serve aiuto?
SPID, il Sistema Pubblico di Identità Digitale, è il sistema di accesso che consente di utilizzare, con un'identità digitale unica, i servizi online della Pubblica Amministrazione e dei privati accreditati.
Se sei già in possesso di un'identità digitale, accedi con le credenziali del tuo gestore.
Se non hai ancora un'identità digitale, richiedila ad uno dei gestori.
Maggiori informazioni
Non hai SPID?
Serve aiuto?
AgID Agenzia per l'Italia Digitale
Antiphishing | Help & Info SPID


Login IDP
Poste Italiane S.p.A. [IT] | https://posteid.poste.it/jod-login-schema/login.jsp
spid
Poste ID NUOVO spid
NOME UTENTE
PASSWORD
Hai dimenticato la password?
ENTRA CON SPID
ANNULLA
Richiesta di accesso da Università di Trento
Non ti sei ancora registrato alla nuova Identità Digitale PosteID abilitata SPID? Registrati
Cos'è PosteID
©2016 Poste Italiane - Partita iva : 01114601006.

# Considerazioni finali

1. Non è un'attività banale, né tecnicamente (IdP locale) né proceduralmente (AGID-SPID)
2. C'è il rischio di introdurre errori e problemi di sicurezza
3. L'implementazione presso UniTrento è rilasciata in pre-produzione
4. Abbiamo alcuni aspetti da rifinire
    a. log AuthnRequest/Response per 24 mesi
    b. logout
    c. test
    d. documentazione utente e HelpDesk
5. Se c'è interesse, l'idea è quella di **rendere pubblico il codice** tramite IDEM contando su revisioni e contributi

# Grazie dell’attenzione.