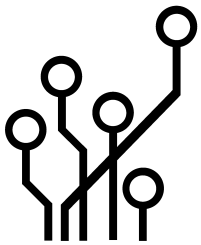

PROJECT ORIGIN

*projectorigin2023@gmail.com*

# *Ricerca Requisiti SPID*

| | |
|---|---|
| **Versione** | 0.2.0 |
| **Responsabile** | Beschin Michele |
| **Redattori** | Bobirica Andrei Cristian |
| **Verificatori** | Bobirica Andrei Cristian<br>Corbu Teodor Mihail |
| **Uso** | Interno |
| **Destinatari** | *Project Origin*<br>Prof. Vardanega Tullio<br>Prof. Cardin Riccardo |

**Descrizione**

*Documento* in cui vengono approfonditi il funzionamento e i requisiti di utilizzo dello SPID

# Registro delle modifiche

| Vers. | Data | Autore | Ruolo | Descrizione |
|---|---|---|---|---|
| 0.2.0 | 2023-05-08 | Corbu Teodor | Verificatore | Verifica documento |
| 0.1.0 | 2023-05-07 | Bobirica Andrei | Verificatore | Aggiornamento template Latex e Verifica documento |
| 0.0.1 | 2023-05-02 | Bobirica Andrei | Analista | Redazione documento |

# Indice

# 1 Informazioni generali

## 1.1 Descrizione

SPID, il Sistema Pubblico di Identità Digitale, è la soluzione che permette di accedere a tutti i servizi online della Pubblica Amministrazione con un'unica Identità Digitale (username e password) utilizzabile da computer, tablet e smartphone.

## 1.2 Riferimenti Normativi

Sono state seguite le REGOLE TECNICHE (articolo 4, comma 2, DPCM 24 ottobre 2014).
Sono state seguite anche le regole del sistema previste da SAML v2 per il profilo "Web Browser SSO".

## 1.3 Funzionamento in breve

La richiesta di autenticazione SAML può essere inoltrata da un Service Provider all'Identity Provider usando il binding HTTP Redirect o il binding HTTP POST.
La relativa risposta SAML può invece essere inviata dall'Identity Provider al Service Provider solo tramite il binding HTTP POST.

# 2 Interfacce Logiche

Esaminando le interfacce logiche si può capire il funzionamento.

## 2.1 Interfacce dell' Identity Provider

- **IIDPUserInterface**: permette agli utenti l'interazione via web in fase di autenticazione.
- **IAuthnRequest**: permette la ricezione di richieste di autenticazione SAML.
- **IMetadataRetrieve**: permette il reperimento dei SAML metadata dell'Identity Provider.

## 2.2 Interfacce del Service Provider

- **IAuthnResponse**: permette la ricezione delle risposte di autenticazione SAML.
- **IMetadataRetrieve**: permette il reperimento dei SAML metadata del Service Provider.
- **IDSResponse**: permette la ricezione delle risposte da parte del Discovery Service.

# 3 Schema Funzionamento

## 3.1 Scenario di Interazione in Modalità SSO

Di seguito è rappresentato il passaggio di autentificazione nel momento in cui si preme sul pulsante SSO e si viene reindirizzati al Service Provider.

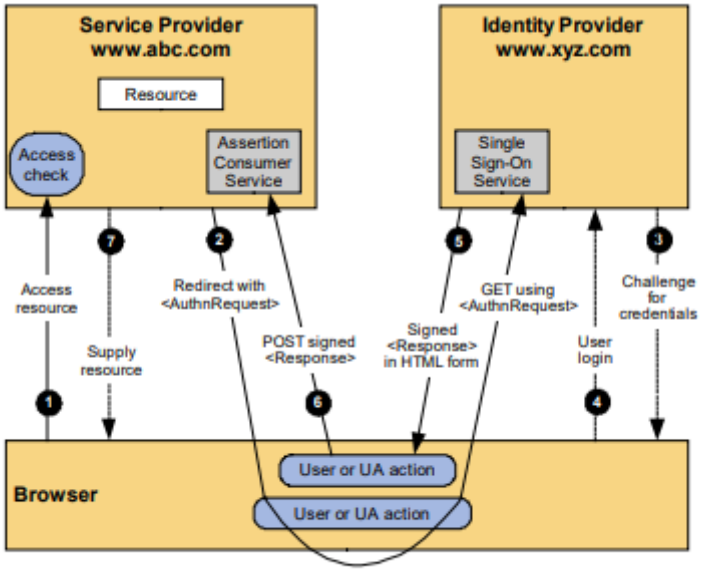


**Figura 1 - SSO SP-Initiated Redirect/POST binding**

# 4 Scenario Di Utilizzo

| | Descrizione | Interfaccia | SAML | Binding |
|---|---|---|---|---|
| 1 | Il fruitore utilizzando il browser (User Agent) richiede l'accesso alla risorsa | | | |
| 2a | Il Service Provider (SP) invia allo User Agent (UA) una richiesta di autenticazione da far pervenire all'Identity Provider (IdP). | IAuthnRequest | AuthnRequest | HTTP Redirect<br>HTTP POST |
| 2b | Lo User Agent inoltra la richiesta di autenticazione contattando L'Identity Provider. | - | AuthnRequest | HTTP Redirect<br>HTTP POST |
| 3 | L'Identity Provider esamina la richiesta ricevuta e se necessario esegue una challenge di autenticazione con l'utente. | - | - | HTTP |
| 4 | L'Identity Provider portata a buon fine l'autenticazione effettua lo user login e prepara l'asserzione contenente lo statement di autenticazione dell'utente destinato al Service Provider (più eventuali statement di attributo emessi dall'Identity Provider stesso). | - | - | - |
| 5 | L'Identity Provider restituisce allo User Agent la <Response> SAML contenente l'asserzione preparata al punto precedente. | - | Response | HTTP POST |
| 6 | Lo User Agent inoltra al Service Provider (SP) la <Response> SAML emessa dall'Identity Provider. | IAuthnResponse | Response | HTTP POST |

# 5 Binding

## 5.1 Breve descrizione

Il termine "Binding" si riferisce al momento in cui l'User Agent viene reindirizzato da un portale all'altro durante l'autenticazione. In particolare, questo avviene quando il Service Provider reindirizza l'utente all'Identity Provider e, una volta che l'Identity Provider ha verificato l'identità dell'utente, lo reindirizza nuovamente al Service Provider per completare il processo$_g$di autenticazione.

## 5.2 Binding HTTP Redirect

Il Service Provider invia allo User Agent un messaggio HTTP di redirezione, cioè avente uno Status Code con valore 302 ("Found") o 303 ("See Other");
Il Location Header del messaggio HTTP contiene l'URI$_g$di destinazione del servizio di Single Sign-On esposto dall' Identity Provider.
Il Pacchetto HTTP trasporta i parametri tutti URL-encoded codificato in formato Base64 e compresso con algoritmo DEFLATE.
Il messaggio all'interno è la risorsa richiesta originaria a cui trasferire il controllo una volta terminata l'autenticazione, algoritmo e firma per la codifica delle informazioni.
Una volta avute queste informazioni il User Agent fa una richiesta GET all' Identity Provider con tutte le informazioni sopracitate sotto forma di URLENCODED.

## 5.3 Binding HTTP POST

Il Service Provider invia allo User Agent un messaggio HTTP con uno status code avente valore 200 ("OK"). Questo messaggio HTTP contiene un form HTML codificato come valore di un elemento nascosto del form. L'utilizzo di questa metodologia consente di superare i limiti di dimensione della query string.
L'intero messaggio SAML in formato XML può essere firmato tramite la XML Digital Signature e il risultato viene codificato in formato Base64. La risorsa richiesta originariamente è inclusa nel messaggio e viene utilizzata per trasferire il controllo a termine dell'autenticazione. Inoltre, è possibile utilizzare un form autopostante attraverso uno script Javascript.
Infine, il browser dell'utente elabora la risposta HTTP e invia una richiesta HTTP POST verso il componente Single Sign-On dell'Identity Provider.

# 6 Invio del Responso

## 6.1 Breve descrizione

Per Response si intende la risposta che l'Identiry Provider invia al Service Provider con l'esito dell'autentificazione e con le informazioni richieste dal Service Provider appartenente all' Utente.

## 6.2 Response

Dopo che l'utente ha completato l'autenticazione, l'Identity Provider crea una Response che contiene la firma digitale e la invia direttamente al Service Provider.
La Response viene inclusa in un form HTML come campo nascosto denominato "SAMLResponse".
L'Identity Provider invia il form HTML al browser dell'utente tramite una risposta HTTP.
Il browser dell'utente elabora quindi la risposta HTTP e invia una richiesta HTTP POST contenente la Response firmata verso il Service Provider.

# 7 Sicurezza

## 7.1 Accorgimenti Attuati

Per quanto riguarda la gestione della sicurezza nel canale di trasmissione si utilizza SSLv.3.0 o TLS 1.0.

# 8 Metadata

## 8.1 Scopo

Ciascuna entità fornisce dei metadati per dichiarare in modo trasparente le proprie caratteristiche, nonché i servizi e le informazioni offerti o richiesti.

## 8.2 Identity Provider METADATA

I metadata sono conformi allo standard SAMLv2.0:

- **entityID**: indicante l'identificativo ($URI_g$) dell'entità univoco in ambito SPID.
- **Protocollo**: identificatore dei protocolli supportati dall'entità.
- **SingleSignOnService**: endpoint URL del servizio per ricevere le richieste e il tipo di binding da utilizzare con il Service Provider (HTTP-Redirect" oppure HTTP-POST).
- **Organizzazione**: Organizzazione a cui afferisce l'Identity Provider.
- **Signature**: firma proprietaria.
- **Attributi**: uno o più elementi "attribute" ad indicare nome e formato degli attributi certificabili dell'Identity Provider. Molto importante, poiché potremmo utilizzare anche noi un sistema simile.

I metadata Identity Provider saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia IMetadataRetrive all'URL "dominioGestoreIdentita/metadata".

## 8.3 Service Provider METADATA

- **IMetadataRetrieve**: permette il reperimento dei SAML metadata del Service Provider da parte dell'Identity Provider.
- **IdentityID**: ID indicante l'identificativo univoco (un $URI_g$) dell'entità.
- **Chiave**: chiave pubblica dell'entità per Signature.
- **Signature**: firma proprietaria.
- **AssertionConsumerService**: si riferisce all'indicazione di come il Service Provider deve essere contattato per ricevere la Response, specificando il tipo di binding e l'$URI_g$di destinazione.
- **Organizzazione**: organizzazione a cui afferisce il Service Provider.
- **Attributi**: sono una lista di informazioni che il Service Provider richiede all'Identity Provider di fornire, come ad esempio nome, cognome, data di nascita e indirizzo. La lista degli attributi richiesti può variare a seconda del service name desiderato, e possono essere molteplici.

# 9 Attribute Authority

## 9.1 Descrizione

Durante la ricerca del sistema SPID non sono state fornite informazioni dettagliate sulle funzioni di questo attore. Tuttavia, è stato chiarito che il suo ruolo è quello di verificare gli altri due tipi di enti coinvolti nel sistema.
Esso deve essere in grado di certificare un determinato set di attributi relativi ad un soggetto titolare di un'identità digitale.
A fronte di una richiesta di uno o più attributi l'Attribute Authority deve essere in grado di:

- **1**. ricevere ed interpretare la richiesta di attributo pervenuta da un Service Provider;
- **2**. elaborare la richiesta;
- **3**. costruire la risposta inerente la richiesta pervenuta ed inoltrarla al Service Provider.

## 9.2 Interfacce

Il componente Attribute Authority deve esporre le seguenti interfacce:

- **IAttributeQuery**: interfaccia applicativa che supporta le operazioni di richiesta di attributo SAML;
- **IMetadataRetrive**: permette il reperimento dei SAML metadata da parte del Service Provider.

# 10 Tracciatura Attività

Le tracce delle attività svolte devono essere conservate nel rispetto delle norme sulla privacy, sotto la responsabilità del titolare del trattamento dell'Identity Provider. L'accesso ai dati di tracciatura deve essere consentito solo al personale autorizzato. Per tenere traccia delle attività, si utilizza un sistema di gestione di database (DBMS) in cui vengono registrate, per un periodo di 24 mesi, le informazioni relative alla richiesta di autenticazione (AuthnRequest) e alla corrispondente risposta (Response).

# 11 Design e Grafica

La standardizzazione delle interfacce, della comunicazione e dell'utilizzo del logo SPID è necessaria per gestire l'accesso ai servizi pubblici e privati che utilizzano il sistema SPID. Ciò è importante non solo per migliorare l'esperienza dell'utente, ma anche per preservare l'immagine del sistema.

# 12 SPID Button

Lo SPID Button consente all'utente la scelta del proprio Identity Provider per l'autenticazione. Con l'utilizzo di spid-smart-button si intende:

- facilitare l'integrazione del bottone "Entra con SPID";
- fornire un bottone ospitato via CDN (implementabile tramite javascript e CDN);
- migliorare l'esperienza utente.

```
1    //Codice HTML5
2    <script type="text/javascript" src="https://XXXXXXXXXXX/spid-button.min.js">
         </script>
3    <div id="spid-button">
4        <noscript>
5            Il login tramite SPID richiede che JavaScript sia abilitato nel browser.
```

```
6           </noscript>
7       </div>
8       //Da inizializzare con una chiamata JavaScript
9       //Codice Javascript
```

# 13 Linguaggi di Programmazione e Framework

E' possibile utilizzare diverse librerie per implementare lo SPID in quasi ogni framework, rendendo l'implementazione del sistema indipendente dalla piattaforma. Tra le varie opzioni disponibili, la libreria in PHP sembra essere quella più semplice ed utile.
Qui di seguito è disponibile una demo che mostra l'implementazione dell'SPID utilizzando questa libreria.

# 14 Demo Example

Di seguito è presente il riferimento a una demo che include due container utilizzabili con Docker: uno per il Service Provider e uno per l'Identity Provider.
https://github.com/simevo/spid-php-lib-example
Sfortunamente Questa Demo pare obsoleta e non completamente compatibile con tutte le architettture.

# 15 Riferimenti

Lista delle repo ufficiali per lo SPID:
https://github.com/italia
Regole Tecniche (articolo 4, comma 2, DPCM 24 ottobre 2014):
https://github.com/italia/spid-regole-tecniche
https://www.agid.gov.it/sites/default/files/repository_files/circolari/spid-regole_tecniche_v1.pdf
Riferimenti agli standard grafici e ai layout:
https://github.com/italia/spid-graphics
Esempio di Service Provider e Identity Provider con Docker:
https://github.com/simevo/spid-php-lib-example
Smart button SPID per autenticazione (in progress, ma attualmente da seguire come riferimento):
https://github.com/italia/spid-smart-button