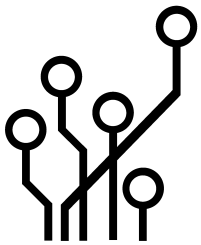

PROJECT ORIGIN

projectorigin2023@gmail.com

Ricerca Requisiti SPID

Versione	0.1.0
Responsabile	
Redattori	Andrei Bobirica
Verificatori	Andrei Bobirica
Uso	Interno
Destinatari	*Project Origin* Prof. Vardanega Tullio Prof. Cardin Riccardo

Descrizione

Documento in cui si approfondisce il funzionamento e i requisiti di funzionamento dello SPID

Registro delle modifiche

Vers.	Data	Autore	Ruolo	Descrizione
0.1.0	07-05-23	Andrei Bobirica	Verificatore	Aggiornamento template Latex e Verica documento
0.0.1	02-05-23	Andrei Bobirica	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 del Identity Provider

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

2.2 Interfacce del Service Provider

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

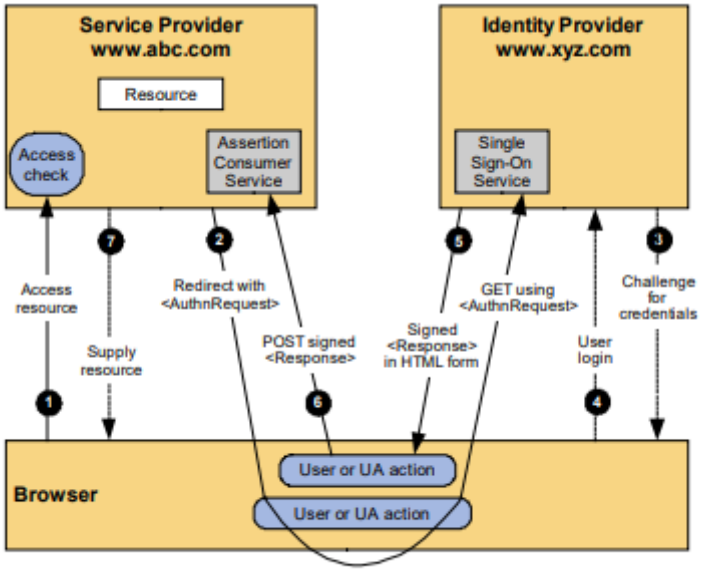

Figura 1 - SSO SP-Initiated Redirect/POST binding

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 HTTP POST
2b	Lo User Agent inoltra la richiesta di autenticazione contattando L'Identity Provider.	-	AuthnRequest	HTTP Redirect 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

Per Binding si intende il momento in cui l'User Agent viene reindirizzato verso un'altro portale durante l'autentificazion; in particolare dal Service Provider al Identity Provider e in fine per ritornare al primo.

5.2 BINDING HTTP Redirect

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 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 al Identity Provider con tutte le informazioni sopracitate sotto forma di URLENCODED.

5.3 BINDING HTTP POST

Service Provider invia allo User Agent un messaggio HTTP con status code avente valore 200 ("OK").
Il messaggio HTTP contiene una form HTML codificato come valore di un hidden form Utilizzando questa metodologia questo permette di superare i limiti di dimensione della query string.
L'intero messaggio SAML in formato XML può essere firmato (XML Digital Signature)
Il risultato codificato in formato Base64;
Il messaggio all'interno e' la risorsa originaria richiesta a cui trasferire il controllo a termine della autentificazione, Form autopostante attraverso uno script javascript.
In fine Il browser dell'utente elabora quindi 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 della autentificazione e con le informazioni richieste dal Service Provider appartenente al Utente.

6.2 Response

Conclusa la fase di autenticazione, l'Identity Provider costruisce una Response firmata diretta al Service Provider.
La Response viene inserita in una form HTML come campo nascosto di nome "SAMLResponse".
L'Identity Provider invia la form HTML al browser dell'utente in 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

Ogni entità fornisce dei Metadata per dichiarare con trasparenza le proprie carateristiche e i servizi ed informazioni offerte o richieste.

8.2 Identity Provider METADATA

metadata conformi allo standard SAMLv2.0.

- **entityID**: indicante l'identificativo (URI) dell'entità univoco in ambito SPID.
- **Protocollo**: Identificatore dei protocolli supportati dalla entità.
- **SingleSignOnService**: Location url endpoint del servizio per la ricezione delle richieste ed il tipo di binding da fare con il service Provider (HTTP-Redirect" oppure HTTP-POST)
- **Organizzazione**: Organizzazione a cui afferisce il identity Provider.
- **Signature**: Segnatura propietaria.
- **Attributi**: Uno o più elementi ¡attribute¿ ad indicare nome e formato degli attributi certificabili dell'Identity provider. Molto Importante in quanto un sistema simile potremmo utilizzare anche noi.

I metadata Identity Provider saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia IMetadataRetrive alla 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) dell'entità.
- **Chiave**: Chiave pubblica della entità per Signature.
- **Signature**: Segnatura propietaria.
- **AssertionConsumerService**: Il come contattare il service provider con il response, specificando il tipo di binding e il location URI.
- **Organizzazione**: Organizzazione a cui afferisce il Service Provider.
- **Attributi**: Lista attributi che il Service Provider richiede che gli vengano rilasciati dal identity provider (nome, cognome, data nascita, residenza, etc...), Possono essere diversi in base al service name desiderato, i quali possono essere molteplici.

9 Attribute Authority

9.1 Descrizione

Durante il processo di ricerca per il suddetto sistema SPID non si è evidenziato con dettaglio le funzioni di questo attore, si è però visto che ha come ruolo la repsonsabilità di verificare le altre due tipologie di enti.
Esso deve essere in grado di certificare un determinato set di attributi relativi ad un soggetto titolare di una 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 una Service Provider;
- **2**. elaborare la richiesta;
- **3**. costruire la risposta inerente la richiesta pervenuta ed inoltrarla alla 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 delle Service Provider;

10 Tracciatura Attività

Le tracciature devono essere mantenute nel rispetto del codice della privacy sotto la responsabilità titolare del trattamento dell'Identity Provider e l'accesso ai dati di tracciatura deve essere riservato a personale incaricato.
Si utilizza un (DBMS) in cui viene tenuto traccia per 24 mesi del a coppia dalla ¡AuthnRequest¿ e della relativa ¡ Response¿.

11 Design e Grafica

Per gestire l'accesso ai servizi pubblici e privati che utilizzano il sistema SPID, si rende necessario, sia per una questione di user experience che di immagine del sistema, la standardizzazione delle interfacce, della comunicazione e dell'utilizzo del logo SPID.

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.

//Codice HTML ¡script type="text/javascript" src="https://XXXXXXXXXXXX/spid-button.min.js"¿¡/script¿ ¡div id="spid-button"¿ ¡noscript¿ Il login tramite SPID richiede che JavaScript sia abilitato nel browser. ¡/noscript¿ ¡/div¿ //Da inizializzare con una chiamata JavaScript //Codice Javascript SPID.init(...);

13 Linguaggi Di Programmazione e Framework

Per quanto riguarda lo SPID sono state fornite diverse librerie quasi per ogni framework, è indifferente la piattaforma infatti esiste una libreria che permette la sua implementazione ovunque.
Il più semplice e di utilità e' sembrato quello in PHP. Di seguito ho trovato una demo proprio di questa sua implementazione

14 Demo Example

Di seguito è presente il riferimento a una Demo in cui sono contenuti due Container utilizzabili con Docker, uno per il service provider ed uno per il identity provider.
https://github.com/simevo/spid-php-lib-example
Sfortunamente Questa Demo pare obsoleta e non completamente compatibile con tutte le archttetture.

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 allo standard grafici e 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