Python

Nov 05, 2018

Contents

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. Maggiori informazioni sono riportate nel sito www.spid.gov.it

Le Regole Tecniche definiscono le specifiche per l'integrazione di Identity Provider, Service Provider ed Attribute Authority mediante il protocollo SAML.

Warning: Questo documento è la versione consolidata delle Regole Tecniche emanate dall'Agenzia per l'Italia Digitale, con applicati i successivi Avvisi che le emendano, per una facile consultazione da parte degli sviluppatori. I contenuti sono aderenti ai documenti ufficiali, disponibili nel sito AgID, ma sono presentati secondo una differente struttura dei capitoli e sono arricchiti da informazioni utili indicate con le diciture "Nota" e "Questo paragrafo ha scopo informativo e non normativo".

CHAPTER 1

Indice dei contenuti

1.1 Introduzione

SPID è basato sul framework SAML (Security Assertion Markup Language), sviluppato e manutenuto dal Security Services Technical Committee di OASIS, che permette la realizzazione di un sistema sicuro di Single Sign-On (SSO) federato. Grazie a SAML, un utente può accedere ad una moltitudine di servizi appartenenti a domini differenti effettuando un solo accesso.

Il sistema è composto da 3 entità:

- **Gestore delle identità (Identity Provider o IdP)** che gestisce gli utenti e la procedura di autenticazione;
- **Fornitore di servizi (Service Provider o SP)** che, dopo aver richiesto l'autenticazione dell'utente all'Identity Provider, ne gestisce l'autorizzazione sulla base degli attributi restituiti dal Gestore dell'identità, ed eroga il servizio richiesto;
- **Gestore di attributi qualificati (Attribute Authority o AA)** che fornisce attributi qualificati sulla base dell'utente autenticato.

Le modalità di funzionamento di SPID sono quelle previste da SAML v2 per il profilo "Web Browser SSO" - SAML V2.0 Technical Overview - Oasis par4.3.

1.2 Metadata

Ciascuna entità presente nella federazione SPID è descritta da un file di metadati, che ne riporta il certificato X509, gli endpoint e le altre informazioni necessarie alla comunicazione con le altre entità.

Note: La distribuzione dei metadati a tutti i soggetti è operata dall'Agenzia per l'Italia Digitale attraverso il Registro.

1.2.1 Identity Provider

Le caratteristiche dell'Identity provider sono definite attraverso metadata conformi allo standard SAML v2.0 (SAML-Metadata) e rispettano le condizioni di seguito indicate:

SI DEVE

- Nell'elemento `<EntityDescriptor>` deve essere presente il seguente attributo:
  - `entityID` indicante l'identificativo (URI) dell'entità univoco in ambito SPID
- L'elemento `<IDPSSODescriptor>` specifico che contraddistingue l'entità di tipo Identity Provider deve riportare i seguenti attributi:
  - `protocolSupportEnumeration`: che enumera gli URI indicanti i protocolli supportati dall'entità (poiché si tratta di un'entità SAML 2.0, deve indicare almeno il valore del relativo protocollo: `urn:oasis:names:tc:SAML:2.0:protocol`)
  - `WantAuthnRequestSigned`: attributo con valore booleano che impone ai Service Provider che fanno uso di questo Identity provider l'obbligo della firma delle richieste di autenticazione;

  all'interno di `<IDPSSODescriptor>` devono essere presenti:
  - l'elemento `<KeyDescriptor>` che contiene l'elenco dei certificati e delle corrispondenti chiavi pubbliche dell'entità, utili per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (SAMLMetadata, par. 2.4.1.1)
  - l'elemento `<KeyDescriptor>` che contiene il certificato della corrispondente chiave pubblica dell'entità, utile per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (SAML-Metadata, par. 2.4.1.1)
  - l'elemento `<NameIDFormat>` riportante l'attributo:
    - `format`, indicante il formato `urn:oasis:names:tc:SAML:2.0:nameidformat:transient` come quello supportato per l'elemento di `<NameID>` utilizzato nelle richieste e risposte SAML per identificare il *subject* cui si riferisce un'asserzione
  - uno o più elementi `<SingleSignOnService>` che specificano l'indirizzo del Single Sign-On Service riportanti i seguenti attributi:
    - `Location` URL endpoint del servizio per la ricezione delle richieste
    - `Binding` che può assumere uno dei valori
      - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`
      - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`
  - uno o più elementi `<SingleLogoutService>` che specificano l'indirizzo del Single Logout Service riportanti i seguenti attributi:
    - `Location` URL endpoint del servizio per la ricezione delle richieste di Single Logout;
    - `Binding` che può assumere uno dei valori
      - `urn:oasis:names:tc:SAML:2.0:bindings:SOAP`
      - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`
      - `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`

> **Note:** Ad oggi, nessun Identity Provider espone un SingleLogoutService basato su SOAP.

* `ResponseLocation` (opzionale): URL endpoint del servizio per la ricezione delle risposte alle richieste di Single Logout.

opzionalmente possono essere presenti:

- uno o più elementi `<Attribute>` ad indicare nome e formato degli attributi SPID certificabili dell'Identity Provider (cfr. Tabella attributi SPID), riportanti gli attributi:
  * `Name`: nome dell'attributo SPID (colonna *identificatore* della Tabella attributi SPID)
  * `xsi:type`: tipo dell'attributo (colonna *tipo* della Tabella attributi SPID)

- Deve essere presente l'elemento `<Signature>` riportante la firma sui metadata. La firma deve essere prodotta secondo il profilo specificato per SAML (SAML-Metadata, cap. 3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;

SI PUÒ

- È consigliata la presenza di un elemento `<Organization>` a indicare l'organizzazione a cui afferisce l'entità specificata, riportante gli elementi:
  - `<OrganizationName>` indicante un identificatore language-qualified dell'organizzazione a cui l'entità afferisce
  - `<OrganizationURL>` riportante in modalità language-qualified la URL istituzionale dell'organizzazione.

1.2.1.1 Esempio: metadata IdP

```
<md:EntityDescriptor xmlns:md = "urn:oasis:names:tc:SAML:2.0:metadata"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance"
    entityID="http://spid.identityprovider.it"
    ID="_2ini49248n98dn984n...">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        [...]
    </ds:Signature>
    <md:IDPSSODescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
        WantAuthnRequestsSigned="true">
        <md:KeyDescriptor use="signing">...</md:KeyDescriptor>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
↪POST"
            Location="https://spid.identityprovider.it/Post-Post-saml2slo"
            ResponseLocation="https://spid.identityprovider.it/Post-Post-saml2slo"/>
        <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-
↪Redirect"
            Location="https://spid.identityprovider.it/redirect-Post-saml2slo"
            ResponseLocation="https://spid.identityprovider.it/redirect-Post-saml2slo
↪"/>
        <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</
↪md:NameIDFormat>
```

(continues on next page)

(continued from previous page)

```
        <md:SingleSignOnService
            Location="https://spid.identityprovider.it/redirect-Post-saml2sso"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
        <md:SingleSignOnService
            Location="https://spid.identityprovider.it/Post-Post-saml2sso"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        <saml:Attribute xsi:type="xsi:string" Name="familyName"/>
        <saml:Attribute xsi:type="xsi:string" Name="name"/>
        <saml:Attribute xsi:type="xsi:string" Name="spidCode"/>
        <saml:Attribute xsi:type="xsi:string" Name="fiscalNumber"/>
        <saml:Attribute xsi:type="xsi:string" Name="gender"/>
        <saml:Attribute xsi:type="xsi:string" Name="dateOfBirth"/>
        <saml:Attribute xsi:type="xsi:string" Name="placeOfBirth"/>
        <saml:Attribute xsi:type="xsi:string" Name="companyName"/>
        <saml:Attribute xsi:type="xsi:string" Name="registeredOffice"/>
        <saml:Attribute xsi:type="xsi:string" Name="ivaCode"/>
        <saml:Attribute xsi:type="xsi:string" Name="idCard"/>
        <saml:Attribute xsi:type="xsi:string" Name="mobilePhone"/>
        <saml:Attribute xsi:type="xsi:string" Name="email"/>
        <saml:Attribute xsi:type="xsi:string" Name="address"/>
        <saml:Attribute xsi:type="xsi:string" Name="digitalAddress"/>
    </md:IDPSSODescriptor>
</md:EntityDescriptor>
```

1.2.1.2 Disponibilità dei metadata

I metadata Identity Provider saranno disponibili per tutte le entità SPID federate attraverso la URL *https://<dominioGestoreIdentita>/metadata*, ove non diversamente specificato nel **Registro SPID**, e saranno firmate in modalita detached dall'Agenzia per l'Italia Digitale. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.

1.2.2 Service Provider

Le caratteristiche del Service Provider devono essere definite attraverso metadata conformi allo standard SAML v2.0 (SAML-Metadata) e rispettare le condizioni di seguito indicate:

SI DEVE

- Nell'elemento `<EntityDescriptor>` deve essere presente il seguente attributo:
  - `entityID`: indicante l'identificativo univoco (un URI) dell'entità;
- Deve essere presente l'elemento `<KeyDescriptor>` contenenete il certificato della corrispondente chiave pubblica dell'entità, utile per la verifica della firma dei messaggi prodotti da tale entità nelle sue interazioni con le altre (SAML-Metadata, par. 2.4.1.1);
- Deve essere presente l'elemento `<Signature>` riportante la firma sui metadata. La firma deve essere prodotta secondo il profilo specificato per SAML (SAML-Metadata, cap. 3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- Deve essere presente l'elemento `<SPSSODescriptor>` riportante i seguenti attributi:
  - `protocolSupportEnumeration`: che enumera, separati da uno spazio, gli URI associati ai protocolli supportati dall'entita (poiche si tratta di un'entita SAML 2.0, deve indicare almeno il valore del relativo protocollo: `urn:oasis:names:tc:SAML:2.0:protocol`);

  - `AuthnRequestSigned`: valorizzato `true` attributo con valore booleano che esprime il requisito che le richieste di autenticazione inviate dal Service Provider siano firmate;

- Deve essere presente almeno un elemento `<AssertionConsumerService>` indicante il servizio (in termini di URL e relativo binding HTTP-POST) a cui contattare il Service Provider per l'invio di risposte SAML, riportante i seguenti attributi:
  - `index` che puo assumere valori unsigned;
  - `Binding` posto al valore `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`;
  - `Location` URL endpoint del servizio per la ricezione delle risposte;

  In particolare il primo di questi elementi (o l'unico elemento riportato) deve obbligatoriamente riportare:
  - l'attributo `index` posto al valore `0`;
  - l'attributo `isDefault` posto al valore `true`;
- Deve essere presente almeno un elemento `<SingleLogoutService>` indicante l'indirizzo del SingleLogoutService e riportante i seguenti attributi:
  - `Location` URL endpoint del servizio per la ricezione delle richieste di Single Logout;
  - `Binding` che può assumere uno dei valori
    * `urn:oasis:names:tc:SAML:2.0:bindings:SOAP`
    * `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`
    * `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`

  ed opzionalmente l'attributo:
  - `ResponseLocation`, URL endpoint del servizio per la ricezione delle risposte alle richieste di Single Logout.
- Deve essere presente uno o piu elementi `<AttributeConsumingService>` a descrizione dei set di attributi richiesti dal Service Provider, riportante:
  - l'attributo `index`, indice posizionale dell'elemento relativo all'i-esimo servizio richiamato dalla AuthnRequest mediante l'attributo `AttributeConsumingServiceIndex`;
  - l'elemento `<ServiceName>`, riportante l'identificatore dell'i-esimo set minimo di attributi necessari per l'autorizzazione all'accesso (per la massima tutela della privacy dell'utente il Service Provider deve rendere minima la visibilità dei servizi effettivamente invocati; in questa logica occorre rendere ove possibile indifferenziate le richieste relative a servizi che condividono lo stesso set minimo di attributi necessari per l'autorizzazione);

SI PUÒ

- È consigliata la presenza di un elemento `<Organization>` a indicare l'organizzazione a cui afferisce l'entita specificata, riportante gli elementi:
  - `<OrganizationName>` indicante un identificatore language-qualified dell'organizzazione a cui l'entita afferisce;
  - `<OrganizationURL>` riportante in modalita language-qualified la URL istituzionale dell'organizzazione.

1.2.2.1 Esempio: metadata SP

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https://spid.serviceprovider.it"
    ID="_0j40cj0848d8e3jncjdjss...">
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        [...]
    </ds:Signature>
    <md:SPSSODescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
        AuthnRequestsSigned="true"
        WantAssertionsSigned="true">
        <md:KeyDescriptor use="signing">
            [...]
        </md:KeyDescriptor>
        <SingleLogoutService
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
            Location="https://spid.serviceprovider.it/slo-location"
            ResponseLocation="https://spid.serviceprovider.it/slo-location"/>
        <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</
↪NameIDFormat>
        <md:AssertionConsumerService
            index="0" isDefault="true"
            Location="https://spid.serviceprovider.it/sso-location"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        <md:AssertionConsumerService
            index="1"
            Location="https://spidSP.serviceProvider.it/sso-location"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
        <md:AttributeConsumingService index="0">
            <md:ServiceName xml:lang="it">Set 0</md:ServiceName>
            <md:RequestedAttribute Name="name"/>
            <md:RequestedAttribute Name="familyName"/>
            <md:RequestedAttribute Name="fiscalNumber"/>
            <md:RequestedAttribute Name="email"/>
        </md:AttributeConsumingService>
            <md:AttributeConsumingService index="1">
            <md:ServiceName xml:lang="it">Set 1</md:ServiceName>
            <md:RequestedAttribute Name="spidCode"/>
            <md:RequestedAttribute Name="fiscalNumber"/>
        </md:AttributeConsumingService>
    </md:SPSSODescriptor>
    <md:Organization>
        <OrganizationName xml:lang="it">Service provider</OrganizationName>
        <OrganizationDisplayName xml:lang="it">Nome service provider</
↪OrganizationDisplayName>
        <OrganizationURL xml:lang="it">http://spid.serviceprovider.it</
↪OrganizationURL>
    </md:Organization>
</md:EntityDescriptor>
```

1.2.2.2 Disponibilità dei metadata

I metadata dei Service Provider saranno disponibili per tutte le entità SPID federate attraverso la URL **https://<dominioServiceProvider>/metadata** e saranno firmate dall'Agenzia per l'Italia Digitale. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.

Note: Nonostante sia richiesta la pubblicazione dei metadata nel dominio del Service Provider, la distribuzione dei metadati agli Identity Provider è operata centralmente dall'Agenzia per l'Italia Digitale. Gli Identity Provider di conseguenza non ottengono i metadati direttamente dai Service Provider.

1.3 Trasmissione dei messaggi (binding)

La trasmissione dei messaggi tra le entità della federazione SPID può avvenire secondo le due modalità previste da SAML:

- HTTP-Redirect
- HTTP-POST

1.3.1 Binding HTTP-Redirect

Nel caso del binding HTTP-Redirect la richiesta viene veicolata con le seguenti modalità:

1. L'entità mittente invia allo User Agent un messaggio HTTP di redirezione, cioè avente uno status code con valore 302 ("Found") o 303 ("See Other").
2. Il Location Header del messaggio HTTP contiene l'URI di destinazione del servizio esposto dall'entità destinataria.
3. Il browser dell'utente elabora quindi tale messaggio HTTP-Redirect indirizzando una richiesta HTTP con metodo GET al servizio dell'entità destinataria sotto forma di URL con tutti i sopraindicati parametri contenuti nella query string.

Il messaggio HTTP trasporta i seguenti parametri (tutti URL-encoded):

`SAMLRequest` Un costrutto SAML codificato in formato Base64 e compresso con algoritmo DEFLATE. Come da specifica, il messaggio SAML **non contiene la firma** in formato XML Digital Signature esteso (come avviene in generale nel caso di binding HTTP-POST). Ciò a causa delle dimensioni eccessive che esso raggiungerebbe per essere veicolato in una query string. La specifica indica come modalità alternativa quella di specificare con parametri aggiuntivi l'algoritmo utilizzato per firmare (`SigAlg`) e la stringa con la codifica Base64 URL-encoded dei byte del messaggio SAML (`Signature`).

`RelayState` Identifica la risorsa (servizio) originariamente richiesta dall'utente e a cui trasferire il controllo alla fine del processo di autenticazione. Il Service Provider a tutela della privacy dell'utente nell'utilizzare questo parametro deve mettere in atto accorgimenti tali da rendere minima l'evidenza possibile sulla natura o tipologia della risorsa (servizio) richiesta

`SigAlg` Identifica l'algoritmo usato per la firma prodotta secondo il profilo specificato per SAML (SAML-Core, cap. 5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore; il valore esteso di questo parametro è contestualizzato da un namespace appartenente allo standard XML Digital Signature. Come indicato al punto 1, tuttavia, la firma prodotta non fa uso della struttura XML definita in tale standard

`Signature` Contiene la firma digitale della query string, così come prodotta prima di aggiungere questo parametro, utilizzando l'algoritmo indicato al parametro precedente;

Un esempio di tale URL è il seguente, nel quale sono evidenziati in grassetto i parametri citati (i valori di alcuni parametri sono stati ridotti per brevità, inoltre il valore del parametro `RelayState` è stato reso non immediatamente intellegibile, come suggerito dalla specifica, sostituendo la stringa in chiaro con l'ID della richiesta: l'entità mittente tiene traccia della corrispondenza)

```
SAMLRequest=nVPLbtswELz3KwTeZb0M2SYsBa6NoAbSRrGUHnqjqFVDQCJVLuU4f19KlhEDb
VygR5K7O7Mzw%2FXdqW2cI2gUSiYkmPnEAclVJeTPhDwX%2B6S3KWf1sjapqOb3rzIA%2FzqAY2zQQRtbNtWSe
[...]
ZwPAU88aUQvQ%2F8oe8S68piBDNabB5s3AyThb1XZMCxxEhhPj5qLZddW2sZIcoP4fBW
↪%2BWccqH0fZ6iNir0tU
QGeCWZaGZxE5pM4n8Nz7p%2Be2D3S6L51x1N1jO%2BCO2qh8zO%2Bji%2FfnN098%3D&
↪RelayState=s29f6c7d
6bbf9e62968d27309e2e4beb6133663a2e&SigAlg=http%3A%2F%2Fwww.w3.org%2F2000%2F09
↪%2Fxmldsig
%23rsa-sha1&Signature=LtNj%2BbMc8j%2FhglWzHPMmo0ESQzBaWlmQbZxas%2B%2FIfNO4F
↪%2F7WNoMKDZ4
VVYeBtCEQKWp12pU7vPB5WVVMRMrGB8ZRAdHmmPp0hJ9opO3NdafRc04Z%2BbfnkSuQCN9NcGV%2BajT
[...]
ra169jhaGRReRQ9KkgSB3aTpQGaffAYUPVo2XZiWy6f9Z7zsmV%2FFoT8dg%3D%3D
```

1.3.2 Binding HTTP-POST

Nel caso del binding HTTP-POST, l'entità mittente invia allo User Agent (il browser dell'utente) un messaggio HTTP con status code avente valore 200 ("OK"):

1. Il messaggio HTTP contiene una form HTML all'interno della quale è trasportato un costrutto SAML codificato come valore di un hidden form control di nome `SAMLRequest` oppure `SAMLResponse`. Rispetto al binding HTTP-Redirect, l'utilizzo di una form HTML permette di superare i limiti di dimensione della query string. Pertanto, l'intero messaggio SAML in formato XML può essere firmato in accordo alla specifica XML Digital Signature. Il risultato a valle della firma è quindi codificato in formato Base64
    - Il parametro deve essere denominato `SAMLRequest` nel trasporto dei messaggi `<AuthnRequest>` e `LogoutRequest`, mentre deve essere denominato `SAMLResponse` nel trasporto dei messaggi `<Response>` e `<LogoutResponse>`.
2. La form HTML contiene un secondo *hidden form control* di nome `RelayState` che contiene il corrispondente valore del Relay State, cioè della risorsa originariamente richiesta dall'utente e alla quale dovrà essere trasferito il controllo al termine della fase di autenticazione
3. La form HTML è corredata da uno script che la rende auto-postante all'indirizzo indicato nell'attributo `action`
4. Il browser dell'utente elabora quindi la risposta HTTP e invia una richiesta HTTP POST verso il servizio dell'entità destinataria.

Un esempio di form HTML per trasferire in HTTP-POST la richiesta di autenticazione è descritto nell'esempio successivo. Osservando attentamente il codice riportato in figura si può notare il valore del parametro `SAMLRequest` (ridotto per brevità); il valore del parametro `RelayState` reso non immediatamente intellegibile (cfr. sez. precedente); l'elemento `<input type="submit" value="Invia"/>`, che ha lo scopo di visualizzare all'interno del web browser il pulsante di invio della form utilizzabile dall'utente, non strettamente necessario in quanto la form è resa autopostante.

```
<html>
    <head>
        [...]
    </head>
    <body onload="javascript:document.forms[0].submit()">
        <form method="post" action="https://spid.identityprovider.it/SSOServiceProxy">
            <input type="hidden" name="SAMLRequest"
                value=
↪"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZVRGLTgiPz4KPHNhbWxwOkF1dGhuUmVxdWVzdCBB
                ␣
↪c3NlcnRpb25Db25zdW1lclNlcnZpY2VVUkw9Imh0dHA6Ly9zcC5pY2FyLml0OjgwODAvaWNhc
```

(continues on next page)

(continued from previous page)

```
                [...]
                ␣
↪N0ZWRUcmFuc3BvcnQ8L3NhbWw6QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1scDpSZXF1ZXN0ZWRBdXRobkNvb
                ␣
↪nRleHQ+PHNhbWxwOlNjb3BpbmcgUHJveHlDb3VudD0iMiIgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1lczp0
                 YzpTQU1MOjIuMDpwcm90b2NvbCIvPjwvc2FtbG5SZXF1ZXN0Pg==">
            <input type="hidden" name="RelayState" value="s2645f48777bd62ec83eddc62...
↪">
            <input type="submit" value="Invia"/>
        </form>
    </body>
</html>
```

Un esempio di form HTML per trasferire in HTTP-POST la risposta ad una richiesta di autenticazione è descritto nell'esempio successivo.

```
<html>
    <head>
        [...]
    </head>
    <body onload="javascript:document.forms[0].submit()">
        <form method="post" action="https://spid.serviceprovider.it/
↪AssertionConsumerService">
            <input type="hidden" name="SAMLResponse"
                value=
↪"PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwOlJlc3BvbnNlIERlc3Rp
                ␣
↪bmF0aW9uPSJodHRwOi8vc3AuaWNhci5pdDo4MDgwL2ljYXItc3AvQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWNlIiB
                ␣
↪JRD0iczJhNTdmN2RhYTUyMTc2NWZmOTQ2ODM0ZmY2NjIzNTA3ZTcwNGI1MDQ3IiBJblJlc3BvbnNlVG89InMyOG
                ␣
↪Q5MWEyNmJkNGQ2MGY0N2E0OTkxMzMwMGZhZjc2MzFiZjMxNDBlOSIgSXNzdWVJbnN0YW50PSIyMDA4LTAzLTA0V
                 DIyOjEzOjQ4LjUwMFoiIFZlcnNpb249IjIuMCIgeG1sbnM6c2Ftb
                 [...]
                ␣
↪2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFjOmNsYXNzZXM6UGFzc3dvcmRQcm90ZWN0ZWRUcmFuc3BvcnQ8L3NhbWw6
                ␣
↪QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1sOkF1dGhuQ29udGV4dD48L3NhbWw6QXV0aG5TdGF0ZW1lbnQ+PC9
                 zYW1sOkFzc2VydGlvbj48L3NhbWxwOlJlc3BvbnNlPg==">
            <input type="hidden" name="RelayState" value=
↪"s28d91a26bd4d60f47a49913300f...">
            <input type="submit" value="Invia"/>
        </form>
    </body>
</html>
```

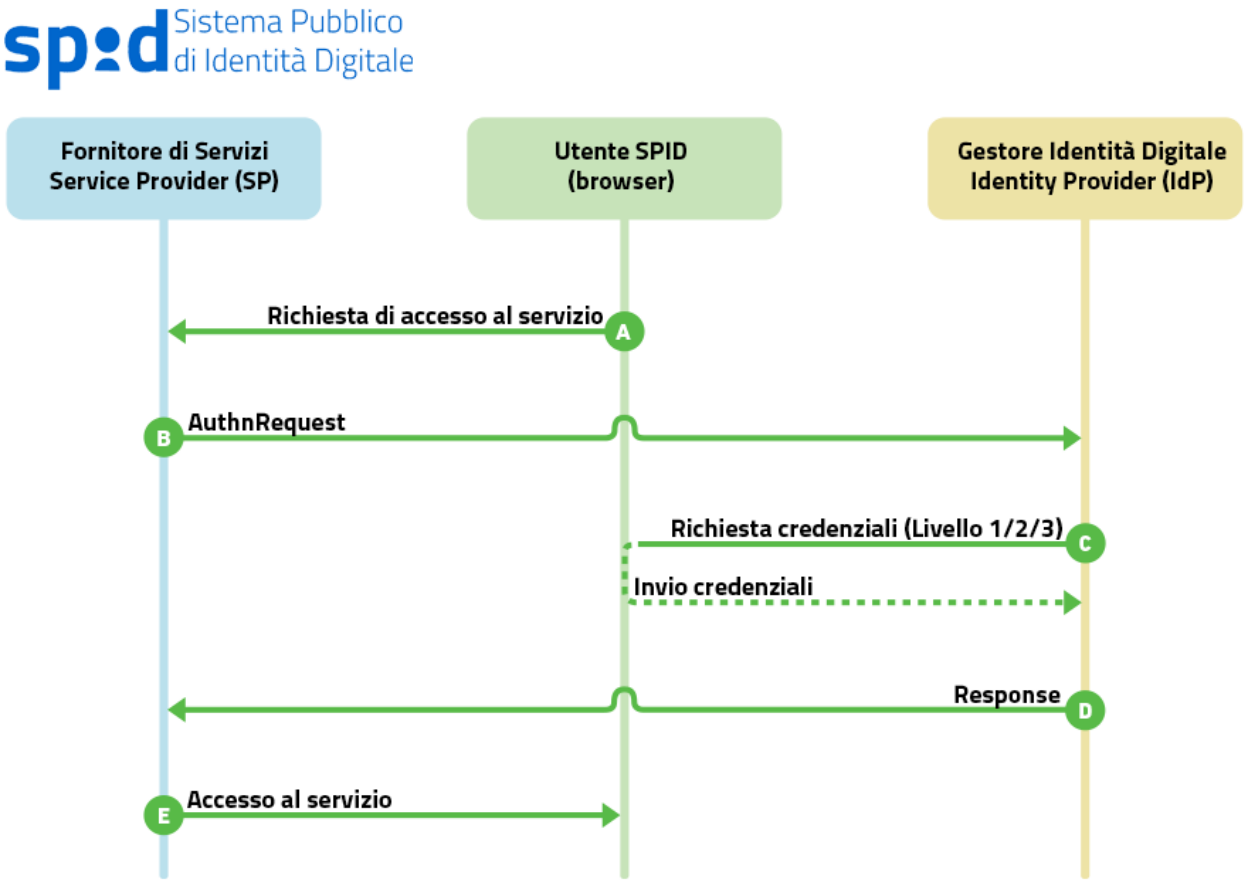
1.3.3 Gestione della sicurezza sul canale di trasmissione

Important: Il profilo SAML SSO raccomanda l'uso di **TLS 1.2** nei colloqui tra Asserting party (Identity Provider e Attribute Authority), le Relaying Party (Service Provider) e lo user agent. In ambito SPID si rende obbligatorio l'impiego di TLS 1.2. In casi particolari e temporanei, può essere adottata la versione 1.1, fermo restando che la versione 1.2 deve essere adottata lato server. Conseguentemente, le versioni più obsolete dei browser, che non supportano le versioni del protocollo indicate, non devono essere utilizzate e, i livelli minimi accettati per l'accesso ai servizi

SPID, devono essere documentati nei confronti degli utenti.

1.4 Single Sign-On

Il meccanismo di autenticazione è innescato dalla selezione, da parte dell'utente, del Gestore delle Identità con cui intende effettuare l'accesso; tale selezione avviene all'interno del sito del Fornitore di Servizi mediante un bottone ufficiale "Entra con SPID" da integrarsi nel servizio. Il Fornitore di Servizi prepara di conseguenza una `<AuthnRequest>` da inoltrarsi al Gestore delle Identità, dove l'utente viene reindirizzato per effettuare l'autenticazione. Eseguita l'autenticazione, l'utente torna presso il sito del Fornitore di Servizi con un'asserzione firmata dal Gestore delle Identity contenente gli attributi richiesti (ad es. nome, cognome, codice fiscale) che il Fornitore di Servizi può usare per autorizzare l'utente in base alle proprie policy ed erogare il servizio richiesto.



	Descrizione	SAML	Binding
A	L'utente richiede l'accesso ad un servizio		
B1	Il Service Provider (SP) invia allo User Agent (UA) una richiesta di autenticazione da far pervenire all'Identity Provider (IdP)	`AuthnRequest`	HTTP POST/REDIRECT
B2	Lo User Agent inoltra la richiesta di autenticazione contattando L'Identity Provider	`AuthnRequest`	HTTP POST/REDIRECT
C1	L'Identity Provider esamina la richiesta ricevuta e, se necessario, esegue una challenge di autenticazione con l'utente		
C2	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)		
D	L'Identity Provider restituisce allo User Agent la `<Response>` SAML contenente l'asserzione preparata al punto precedente	`Response`	HTTP POST
E	Lo User Agent inoltra al Service Provider (SP) la `<Response>` SAML emessa dall'Identity Provider	`Response`	HTTP POST

1.4.1 AuthnRequest

Il messaggio `AuthnRequest` è inviato dal Service Provider, per tramite dello User Agent, al SingleSignOnService dell'Identity Provider ed ha la funzione di avviare il flusso di autenticazione. Può essere inoltrato da un Service Provider all'Identity Provider usando il binding HTTP-Redirect o il binding HTTP-POST. Il messaggio deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

SI DEVE

- nell'elemento `<AuthnRequest>` devono essere presenti i seguenti attributi:
  - l'attributo `ID` univoco, per esempio basato su un *Universally Unique Identifier* (UUID) o su una combinazione *origine* + *timestamp* (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità)
  - l'attributo `Version`, che deve valere sempre `2.0`, coerentemente con la versione della specifica SAML adottata;
  - l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC (esempio: `2017-03-05T18:03:10.531Z`)
  - l'attributo `Destination`, a indicare l'indirizzo (URI reference) dell'Identity Provider a cui è inviata la richiesta, come risultante nell'attributo entityID presente nel metadata IdP dell'Identity Provider a cui viene inviata la richiesta

    Il valore richiesto per l'attributo `Destination` differisce da quanto previsto dalle specifiche SAML.
  - l'attributo `ForceAuthn` nel caso in cui si richieda livelli di autenticazione superiori a SpidL1 (SpidL2 o SpidL3)
  - l'attributo `AssertionConsumerServiceIndex`, riportante un indice posizionale facente riferimento ad uno degli elementi `<AssertionConsumerService>` presenti nei metadata del Service Provider, atto ad indicare, mediante l'attributo `Location`, l'URL a cui inviare il messaggio di risposta alla richiesta di autenticazione, e mediante l'attributo `Binding`, il binding da utilizzare, quest'ultimo valorizzato obbligatoriamente con `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`. In alternativa all'attributo `AssertionConsumerServiceIndex` (scelta sconsigliata) possono essere presenti:

    * l'attributo `AssertionConsumerServiceURL` ad indicare l'URL a cui inviare il messaggio di risposta alla richiesta di autenticazione (l'indirizzo deve coincidere con quello del servizio riportato dall'elemento `<AssertionConsumingService>` presente nei metadata del Service Provider);
    * l'attributo `ProtocolBinding`, identificante il binding da utilizzare per inoltrare il messaggio di risposta, valorizzato con `urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`;

- nell'elemento `<AuthnRequest>` non deve essere presente l'attributo `IsPassive` (ad indicare `false` come valore di default)
- deve essere presente l'elemento `<Issuer>` attualizzato come l'attributo `entityID` riportato nel corrispondente SP metadata, a indicare l'identificatore univoco del Service Provider emittente. L'elemento deve riportare gli attributi:
  - `Format` fissato al valore `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`
  - `NameQualifier` che qualifica il dominio a cui afferisce tale valore (URI riconducibile al Service Provider stesso)
- deve essere presente l'elemento `<NameIDPolicy>` avente l'attributo:
  - `Format` valorizzato come `urn:oasis:names:tc:SAML:2.0:nameid-format:transient`
- deve essere presente l'elemento `<RequestedAuthnContext>` (SAMLCore, sez. 3.3.2.2.1) ad indicare il contesto di autenticazione atteso, ossia la "robustezza" delle credenziali richieste. Allo scopo sono definite le seguenti *"authentication context class"* estese (SAMLAuthContext, sez. 3) in riferimento SPID:
  - `https://www.spid.gov.it/SpidL1`
  - `https://www.spid.gov.it/SpidL2`
  - `https://www.spid.gov.it/SpidL3`

  referenziate dagli elementi `<AuthnContextClassRef>`

  Ciascuna di queste classi indica in ordine di preferenza il contesto di autenticazione (atteso o effettivo) secondo alcune dimensioni di riferimento, quali per esempio i meccanismi di autenticazione con cui l'Identity Provider può identificare l'utente. L'elemento `<RequestedAuthnContext>` prevede un attributo `Comparison` con il quale indicare il metodo per stabilire il rispetto del vincolo sul contesto di abilitazione: i valori ammessi per questo attributo sono:
  - `exact`
  - `minimum`
  - `better`
  - `maximum`

  Nel caso dell'elemento `<RequestedAuthnContext>`, questa informazione si riflette sulle tipologie di meccanismi utilizzabili dall'Identity Provider ai fini dell'autenticazione dell'utente. L'esempio seguente di `<RequestedAuthnContext>` fa riferimento a una *"authentication context class"* di tipo *SpidL2* o superiore.

```
<samlp:RequestedAuthnContext Comparison="minimum">
    <saml:AuthnContextClassRef>
        https://www.spid.gov.it/SpidL2
    </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

  N.B. L'Identity Provider ha facoltà di utilizzare per l'autenticazione un livello SPID più alto rispetto a quelli risultanti dall'indicazione del richiedente mediante l'attributo Comparison. Tale scelta non deve comportare un esito negativo della richiesta.

- nel caso del binding **HTTP POST** deve essere presente l'elemento `<Signature>` contenente la firma sulla richiesta apposta dal Service Provider. La firma deve essere prodotta secondo il profilo specificato per SAML (SAML-Core, cap. 5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

SI PUÒ

- nell'elemento `<AuthnRequest>` può essere opzionalmente presente l'attributo:
  - `AttributeConsumingServiceIndex` riportante un indice posizionale in riferimento alla struttura `<AttributeConsumingService>` presente nei metadata del Service Provider, atta a specificare gli attributi che devono essere presenti nell'asserzione prodotta. Nel caso l'attributo fosse assente l'asserzione prodotta non riporterà alcuna attestazione di attributo
- può essere presente l'elemento `<Subject>` a indicare il soggetto per cui si chiede l'autenticazione in cui deve comparire:
  - l'elemento `<NameID>` atto a qualificare il soggetto in cui sono presenti i seguenti attributi:
    * `Format` che deve assumere il valore `urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified` (cfr. SAMLCore, sez. 8.3)
    * `NameQualifier` che qualifica il dominio a cui afferisce tale valore (URI)

    Warning: L'obbligatorietà dell'attributo `NameQualifier` differisce da quanto previsto dalle specifiche SAML.

- l'elemento `<Conditions>`, se presente, deve indicare i limiti di validità attesi dell'asserzione ricevuta in risposta, per esempio specificando gli attributi `NotBefore` e `NotOnOrAfter` opportunamente valorizzati in formato UTC.

  N.B. L'Identity Provider non è obbligato a tener conto dell'indicazione nel caso che questa non sia confacente con i criteri di sicurezza da esso adottati.

- se presente l'elemento `<Scoping>` il relativo attributo `ProxyCount` deve assumere valore `0` per indicare che l'Identity Provider invocato non può delegare il processo di autenticazione ad altra *Asserting Party*.
- eventuali elementi `<RequesterID>` contenuti devono indicare l'URL del servizio di reperimento metadati di ciascuna delle entità che hanno emesso originariamente la richiesta di autenticazione e di quelle che in seguito la hanno propagata, mantenendo l'ordine che indichi la sequenza di propagazione (il primo elemento `<RequesterID>` dell'elemento `<Scoping>` è relativo all'ultima entità che ha propagato la richiesta).

  Gli elementi `<Scoping>` `<RequesterID>` sono previsti per futuri usi ed **al momento non devono essere utilizzati.** Nel caso di presenza di tali parametri nella richiesta questi dovranno essere al momento ignorati all'atto dell'elaborazione della risposta da parte dell'Identity Provider.

1.4.1.1 Esempio di AuthnRequest

```
<samlp:AuthnRequest xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_4d38c302617b5bf98951e65b4cf304711e2166df20"
    Version="2.0"
    IssueInstant="2015-01-29T10:00:31Z"
    Destination="https://spid.identityprovider.it"
    AssertionConsumerServiceURL="http://spid.serviceprovider.it"
```

(continues on next page)

(continued from previous page)

```
    ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="1">
    <saml:Issuer
        NameQualifier="http://spid.serviceprovider.it"
        Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
        http://spid.serviceprovider.it
    </saml:Issuer>
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        [...]
    </ds:Signature>
    <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" /
↪>
    <samlp:RequestedAuthnContext Comparison="exact">
        <saml:AuthnContextClassRef>
            https://www.spid.gov.it/SpidL2
        </saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

1.4.2 Response

La risposta inviata dall'Identity Provider al Service Provider puo essere trasmessa solo tramite il binding HTTP-POST e deve avere le seguenti caratteristiche:

SI DEVE

- Nell'elemento `<Response>` devono essere presenti i seguenti attributi:
  - l'attributo `ID` univoco basato, per esempio, su un Universally Unique Identifier (UUID) (cfr. UUID) o su una combinazione *origine* + *timestamp* (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
  - deve essere presente l'attributo `Version`, che deve valere sempre `2.0`, coerentemente con la versione della specifica SAML adottata;
  - deve essere presente l'attributo `IssueInstant` a indicare l'istante di emissione della risposta, in formato UTC;
  - deve essere presente l'attributo `InResponseTo`, il cui valore deve fare riferimento all'ID della richiesta a cui si risponde;
  - deve essere presente l'attributo `Destination`, a indicare l'indirizzo (`URI` reference) del Service Provider a cui è inviata la risposta;
- Deve essere presente l'elemento `<Status>` a indicare l'esito della AuthnRequest secondo quanto definito nelle specifiche SAML (SAML-Core, par. 3.2.2.1 e successivi) comprendente il sotto-elemento
  - `<StatusCode>`

  ed opzionalmente i sotto-elementi
  - `<StatusMessage>`
  - `<StatusDetail>`

  (Messaggi di errore SPID)

- Deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'entità emittente, cioè l'Identity Provider stesso. L'attributo `Format` deve essere omesso o fissato al valore `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`.
- Deve essere presente un elemento `<Assertion>` ad attestare l'avvenuta autenticazione, contenente almeno un elemento `<AuthnStatement>`; nel caso l'Identity Provider abbia riscontrato un errore nella gestione della richiesta di autenticazione l'elemento `<Assertion>` non deve essere presente.

SI PUÒ

- Può essere presente l'elemento `<Signature>` contenente la firma sulla risposta apposta dall'Identity Provider. La firma deve essere prodotta secondo il profilo specificato per SAML (SAML-Core, cap. 5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

1.4.2.1 Assertion

SI DEVE

- Nell'elemento `<Assertion>` devono essere presenti i seguenti attributi:
  - l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) o su una combinazione origine + timestamp (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocità);
  - l'attributo `Version`, che deve valere sempre `2.0`, coerentemente con la versione della specifica SAML adottata;
  - l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC (esempio: `2017-03-01T15:05:10.531Z`);
- Deve essere presente l'elemento `<Subject>` a referenziare il soggetto che si è autenticato in cui devono comparire gli elementi:
  - `<NameID>` atto a qualificare il soggetto dell'asserzione, in cui sono presenti i seguenti attributi:
  - `Format` che deve assumere il valore `urn:oasis:names:tc:SAML:2.0:nameidformat:transient` (SAML Core, par8.3)
  - `NameQualifier` che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'Identity Provider stesso)
  - `<SubjectConfirmation>` contenente l'attributo
    - `Method` riportante il valore `urn:oasis:names:tc:SAML:2.0:cm:bearer`
  - `<SubjectConfirmationData>` riportante gli attributi:
    - `Recipient` riportante l'`AssertionConsumerServiceURL` relativa al servizio per cui è stata emessa l'asserzione e l'attributo
    - `NotOnOrAfter` che limita la finestra di tempo durante la quale l'asserzione può essere propagata.
    - `InResponseTo`, il cui valore deve fare riferimento all'ID della richiesta.
- Deve essere presente l'elemento `<Issuer>` a indicare l'entityID dell'Identity Provider emittente (attualizzato come l'attributo `entityID` presente nei corrispondenti IdP metadata) con l'attributo `Format` riportante il valore `urn:oasis:names:tc:SAML:2.0:nameidformat:entity`;
- Deve essere presente l'elemento `<Conditions>` in cui devono essere presenti:

  - gli attributi `NotBefore` `NotOnOrAfter`;
  - l'elemento `<AudienceRestriction>` riportante a sua volta l'elemento `<Audience>` attualizzato con l'entityID del Service Provider per il quale l'asserzione è emessa.
- Deve essere presente l'elemento `<AuthStatement>` a sua volta contenente l'elemento:
  - `<AuthnContext>` riportante nel sotto elemento `<AuthnContextClassRef>` la classe relativa all'effettivo contesto di autenticazione (es. `https://www.spid.gov.it/SpidL2`);

  Nel caso di asserzioni emesse a seguito di richieste di autenticazione per il livello SPID 1 l'elemento `<AuthStatement>` deve avere l'attributo `SessionIndex` specificante l'indice della sessione di autenticazione instaurata per l'utente presso il gestore dell'identita; tale elemento non dovra essere presente nel caso di asserzioni emesse a seguito di richieste di autenticazione per i livelli SPID 2 e SPID 3.
- Deve essere presente l'elemento `<Signature>` riportante la firma sull'asserzione apposta dall'Identity Provider emittente. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

SI PUÒ

- Può essere presente l'elemento `<AttributeStatement>` riportante gli attributi identificativi certificati dall'Identity Provider. Tale elemento se presente dovrà comprendere:
  - uno o più elementi di tipo `<Attribute>` relativi ad attributi che l'Identity Provider può rilasciare (cfr. Tabella attributi SPID) su richiesta del Service Provider espressa attraverso l'attributo `AttributeConsumingServiceIndex` quando presente nella AuthnRequest;
  - per gli elementi `<AttributeValue>` si raccomanda l'uso dell'attributo `xsi:type` attualizzato come specificato nella Tabella attributi SPID;
- Può essere presente un elemento `<Advice>`, contenente a sua volta altri elementi `<Assertion>`. La possibile presenza dell'elemento, prevista per futuri usi, consente, nei casi in cui gli statement emessi dall'Identity Provider si basino su altre asserzioni SAML ottenute da altre authority, di fornire evidenza delle stesse in forma originale unitamente alla risposta alla richiesta di autenticazione.

L'elemento `<Advice>` è previsto per futuri usi ed al momento non deve essere utilizzato.

1.4.2.2 Esempio di Response con Assertion

```
<samlp:Response xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
    xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_66bc42b27638a8641536e534ec09727a8aaa"
    Version="2.0"
    InResponseTo="_4d38c302617b5bf98951e65b4cf304711e2166df20"
    IssueInstant="2015-01-29T10:01:03Z"
    Destination="http://spid-sp.it">
        <saml:Issuer NameQualifier=""https://spidIdp.spidIdpProvider.it"
            Format=" urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
                spididp.it
        </saml:Issuer>
        <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                ............
        </ds:Signature>
```

(continues on next page)

(continued from previous page)

```
        <samlp:Status>
                <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success" /
↪>
        </samlp:Status>
        <saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
            ID="_27e00421b56a5aa5b73329240ce3bb832caa"
            IssueInstant="2015-01-29T10:01:03Z" Version="2.0">
                <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity
↪">
                        spididp.it
                </saml:Issuer>
                <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
                        ......
                </ds:Signature>
                <saml:Subject>
                        <saml:NameID Format="urn:oasis:names:tc:SAML:2.0:nameid-
↪format:transient"
                            NameQualifier="http://spidIdp.spididpProvider.it">
                                _06e983facd7cd554cfe067e
                        </saml:NameID>
                        <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.
↪0:cm:bearer">
                                <saml:SubjectConfirmationData Recipient="https://
↪spidSP.serviceProvider.it/"
                                NotOnOrAfter="2001-12-31T12:00:00"
                                InResponseTo="_
↪4d38c302617b5bf98951e65b4cf304711e2166df20">
                                </saml:SubjectConfirmationData>
                        </saml:SubjectConfirmation>
                </saml:Subject>
                <saml:Conditions NotBefore="2015-01-29T10:00:33Z"
                    NotOnOrAfter="2015-01-29T10:02:33Z">
                        <saml:AudienceRestriction>
                                <saml:Audience>
                                        https://spidSP.serviceProvider.it
                                </saml:Audience>
                        </saml:AudienceRestriction>
                </saml:Conditions>
                <saml:AuthnStatement AuthnInstant="2015-01-29T10:01:02Z">
                        <saml:AuthnContext>
                                <saml:AuthnContextClassRef>
                                        https://www.spid.gov.it/SpidL1
                                </saml:AuthnContextClassRef>
                        </saml:AuthnContext>
                </saml:AuthnStatement>
                <saml:AttributeStatement xmlns:xsi="http://www.w3.org/2001/
↪XMLSchemainstance">
                        <saml:Attribute Name="familyName">
                                <saml:AttributeValue xsi:type="xsi:string">
                                        Rossi
                                </saml:AttributeValue>
                        </saml:Attribute>
                        <saml:Attribute Name="spidCode">
                                <saml:AttributeValue xsi:type="xsi:string">
                                        ABCDEFGHILMNOPQ
                                </saml:AttributeValue>
                        </saml:Attribute>
```

(continues on next page)

(continued from previous page)

```
                </saml:AttributeStatement>
        </saml:Assertion>
</samlp:Response>
```

1.4.2.3 Processamento della Response

Alla ricezione della `<Response>` qualunque sia il binding utilizzato il Service Provider prima di utilizzare l'asserzione deve operare almeno le seguenti verifiche:

- controllo delle firme presenti nella `<Assertion>` e nella `<Response>`;
- nell'elemento `<SubjectConfirmationData>` verificare che:
  - l'attributo `Recipient` coincida con la AssertionConsumerServiceURL a cui la `<Response>` è pervenuta
  - l'attributo `NotOnOrAfter` non sia scaduto;
  - l'attributo `InResponseTo` si riferisca correttamente all'ID della `<AuthnRequest>` di richiesta

Il fornitore di servizi deve garantire che le asserzioni non vengano ripresentate, mantenendo il set di identificatori di richiesta (`ID`) usati come per le `<AuthnRequest>` per tutta la durata di tempo per cui l'asserzione risulta essere valida in base dell'attributo `NotOnOrAfter` dell'elemento `<SubjectConfirmationData>` presente nell'asserzione stessa.

1.5 Single Logout

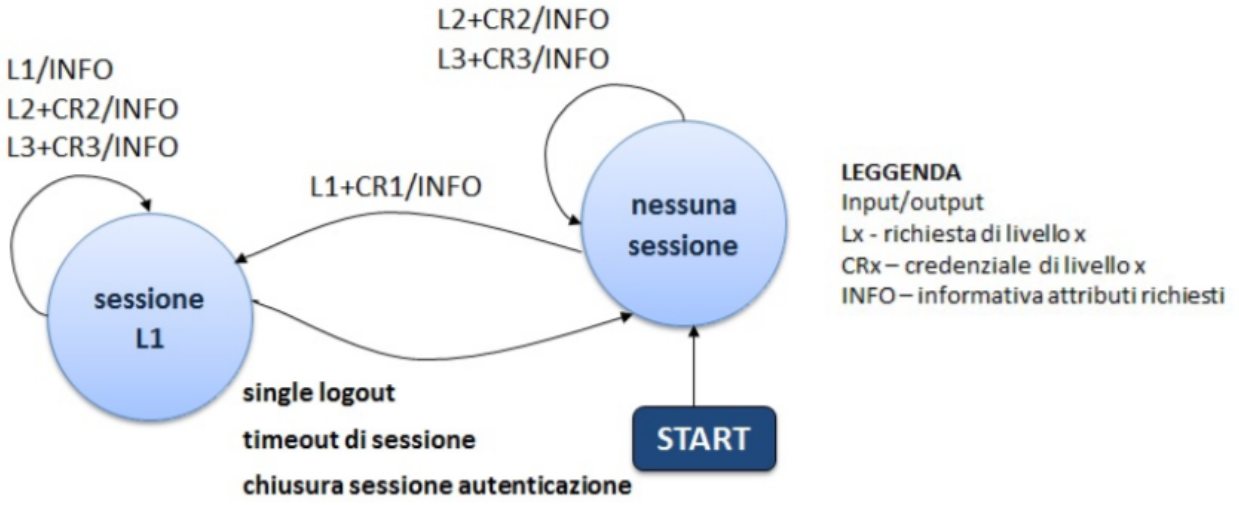
1.5.1 Gestione delle sessioni

Ai sensi dell'art 28 del regolamento *Modalita attuative per la realizzazione dello SPID* un gestore delle identita a completamento con esito positivo dell'autenticazione relativa al livello SPID 1 di un utente stabilisce per lo stesso utente una sessione finalizzata al processo di autenticazione. Nel corso di validita della sessione instaurata, il gestore delle identita puo rilasciare ai fornitori di servizi, che fanno richiesta di autenticazione di livello SPID 1 per l'utente con il quale e stata stabilita la sessione, asserzioni di autenticazione basate sull'evento di autenticazione che ha dato origine alla sessione stessa. Ancora a i sensi dell'art 28 del regolamento *Modalita attuative per la realizzazione dello SPID*, per le richieste di autenticazione di livello SPID 2 e 3 non e prevista l'instaurazione di alcuna sessione, pertanto per ogni richiesta di questo tipo deve essere ripetuto l'evento di autenticazione. La sessione stabilita a seguito di un evento di autenticazione relativo al livello SPID 1 e denominata, per chiarezza di esposizione, **sessione di autenticazione** per distinguerla dalla sessione che un fornitore di servizi puo instaurare con l'utente al fine dell'erogazione di un particolare servizio richiesto, denominata a sua volta **sessione individuale**.

La relazione esistente tra la *sessione di autenticazione*, mantenuta dal gestore dell'identita per un dato utente, e le *sessioni individuali* gestite per lo stesso utente dai fornitori di servizi stabilite sullo stesso evento di autenticazione che ha dato origine alla *sessione di autenticazione*, costituisce, in senso logico, una sessione distribuita che denominiamo **sessione globale**. Il diagramma di stato riportato in figura 1 specifica il comportamento che deve assumere il gestore delle identita per la gestione della *sessione di autenticazione* relativa ad un dato utente a fronte delle diverse richieste che possono essere presentate dai fornitori di servizi relativamente allo stesso utente.

L'evoluzione dello stato associato alla *sessione di autenticazione* deve rispettare le seguenti regole:

1. l'instaurazione di una *sessione di autenticazione* per un determinato utente avviene al completamento con esito positivo di una richiesta di autenticazione di livello SPID 1 da parte di un fornitore di servizi - evento di autenticazione andato a buon fine con contestuale assenso al trasferimento delle informazioni richieste -. Il fornitore di servizi che ha effettuato la richiesta entra a far parte della *sessione globale*;



2. le richieste di autenticazione per i livelli SPID 2 e SPID3 per un dato utente, non devono influenzare il regime di sessione per esso vigente. In particolare, se le richieste dovessero pervenire in presenza di una *sessione di autenticazione* relativa all'utente questa non deve essere in nessun caso chiusa; viceversa, se le richieste dovessero giungere in assenza di una *sessione di autenticazione* relativa all'utente questa non deve essere in nessun caso creata. Il fornitore di servizi che ha effettuato la richiesta non entra a far parte della *sessione globale* relativa all'utente qualora questa esistesse;

3. le richieste di autenticazione di livello SPID1 per un dato utente successive all'instaurazione di una *sessione di autenticazione* per lo stesso utente, qualunque sia il loro esito, non devono incidere sul perdurare della sessione stessa. Il mancato assenso da parte dell'utente al trasferimento delle informazioni richieste dal fornitore di servizi determina il fallimento della richiesta ma non deve produrre conseguenze sulla vigente *sessione di autenticazione* ne sulla *sessione globale*; ovvero, in merito a quest'ultima, il mancato assenso non deve comportare:

    - l'esclusione dalla *sessione globale* del fornitore di servizi che opera la richiesta se questo fosse gia coinvolto nella stessa *sessione globale* per una precedente richiesta andata a buon fine;
    - l'inclusione nella *sessione globale* del fornitore di servizi nel caso questo non fosse ancora coinvolto nella stessa *sessione globale* per una precedente richiesta andata a buon fine.

    L'assenso da parte dell'utente al trasferimento delle informazioni determina il successo della richiesta ed il coinvolgimento del fornitore di servizi nella *sessione globale* relativa all'utente, se lo stesso fornitore di servizi non ne facesse gia parte per via di una precedente richiesta da esso effettuata ed andata a buon fine.

4. L'evento di Single Logout consiste nella chiusura della *sessione di autenticazione* e di tutte le *sessioni individuali* messe tra loro in relazione dalla *sessione globale*. Tale chiusura avviene su espressa richiesta dell'utente presso il gestore dell'identita o presso uno dei fornitori di servizi. La modalita prevista in SPID per il processo di Single Logout e quella definita dal SAML Single Logout Profile (cfr.[SAML-profiles] sez. 4.4). L'insieme dei fornitori di servizi che entrano a far parte della *sessione globale*, necessario alla corretta gestione del Single Logout Profile e popolato dinamicamente dal gestore delle identita, applicando i criteri espressi nei precedenti punti a), b, c). Il processo di Single Logout necessita per andare a buon fine del corretto comportamento di tutti i fornitori di servizio coinvolti nella *sessione globale* secondo quanto previsto dal suddetto Single Logout Profile. Se qualcuno di questi fornitori di servizi non rispetta il comportamento previsto dal Single Logout Profile, il processo non potra essere concluso con successo e il Single Logout sara percio degradato a partial logout. Il partial logout, pur non dando garanzia che tutte le *sessioni individuali* vigenti presso i fornitori di

servizio coinvolti nella *sessione globale* siano effettivamente chiuse, deve comunque assicurare la chiusura della *sessione di autenticazione* e, qualora la richiesta di Single Logout venga fatta presso un fornitore dei servizi, della *sessione individuale* mantenuta dallo stesso fornitore dei servizi presso cui viene operata la richiesta.

5. La *sessione di autenticazione* puo essere chiusa ad opera del gestore dell'identita allo scadere del timeout associato alla sessione stessa o su richiesta operata dall'utente presso lo stesso gestore dell'identita. Con la chiusura della *sessione di autenticazione* viene meno la relazione che lega la *sessione di autenticazione* stessa con le *sessioni individuali* stabilite sulla base di quest'ultima e di conseguenza la *sessione globale* decade. Una eventuale richiesta di Single Logout relativa ad una *sessione globale* in precedenza venuta meno a seguito di una chiusura della *sessione di autenticazione* si risolve in una immediata notifica di partial logout, presentata dal gestore dell'identita al fornitore di servizi presso cui ne e stata fatta richiesta.

I gestori delle identita dovranno mettere a disposizioni dell'utente funzionalita per la richiesta di Single Logout o per la chiusura della *sessione di autenticazione*.

1.5.1.1 Sessioni individuali

E' lasciata ai fornitori di servizi la scelta delle modalita da adottare per la gestione del ciclo di vita delle *sessioni individuali*. In particolare le *sessioni individuali* possono:

1. non essere affatto instaurate (il fornitore di servizi eroga il servizio richiesto dall'utente senza, per quanto possibile, stabilire con esso alcuna sessione);
2. essere chiuse anche nel corso di validita della *sessione di autenticazione* che le ha originate (ovvero prima di una eventuale richiesta di Single Logout o della scadenza del timeout associato alla *sessione di autenticazione*).

In entrambi i casi i fornitori di servizio devono essere comunque in condizione di supportare il processo di Single Logout notificando, a fronte della prevista richiesta da parte del gestore delle identita, l'avvenuta chiusura delle sessioni mai instaurate o gia in precedenza chiuse. I fornitori di servizio che instaurano *sessioni individuali* dovranno mettere a disposizioni dell'utente funzionalita per la richiesta della chiusura della *sessione individuale* o della *sessione globale*.

1.5.1.2 Meccanismi di Single Logout

Per la realizzazione del processo di Single Logout secondo quanto previsto dal SAML Single Logout Profile le entita coinvolte (gestore dell'identita e fornitori di servizi) dovranno mettere a disposizione una apposita interfaccia per la notifica dei messaggi:

- **SingleLogoutService**: ricezione di richieste e notifiche per il Single Logout SAML.

Le tabelle seguenti specificano i passi previsti ed il flusso di messaggi che intercorrono tra il gestore delle identita, l'utente ed i fornitori di servizi nel corso del processo di Single Logout, nei due casi distinti in cui l'inizio avviene presso il gestore dell'identita oppure presso uno dei fornitori di servizi.

Table 1: Single Logout iniziato presso un Fornitore di Servizi

	Descrizione	SAML	Binding
1	L'utente utilizzando il browser (User Agent) richiede il Single Logout presso un fornitore di servizi		
2	Il fornitore di servizi procede con la chiusura della propria sessione individuale ed invia una richiesta	LogoutRequest	HTTP-Redirect, HTTP-POST
3	Il gestore dell'identita ricevuta la richiesta chiude la sessione di autenticazione associata alla sessione globale. Successivamente per ciascun fornitore di servizi facente parte della sessione globale, a partire da quelli in grado di supportare il bindind SOAP, procede alla chiusura delle sessioni individuali. In particolare:		
3.1	invia una richiesta di logout all'i- esimo fornitore di servizi riportando l'identificatore associato alla sessione globale che si vuole chiudere	LogoutRequest	SOAP, HTTP-Redirect, HTTP-POST
3.2	l'i-esimo fornitore di serviziricevuta la richiesta chiude la sessione identificata (se la stessa non fosse stata gia chiusa in precedenza o mai instaurata) ed invia una notifica di avvenuta chiusura al gestore dell'identita	LogoutResponse	SOAP, HTTP-Redirect, HTTP-POST
3.3	Se l'i-esimo fornitore di servizi non e raggiungibile il processo degrada a partial logout		
4	Il gestore dell'identita completata la notifica a ciascun fornitore di servizi facente parte della sessione globale trasmette l'esito (success/partial logout) del global logout al fornitore di servizi che aveva dato inizio al processo.	LogoutResponse	SOAP, HTTP-Redirect, HTTP-POST

Table 2: Single Logout avente origine presso il gestore dell'identità

	Descrizione	SAML	Binding
1	L'utente utilizzando il browser (User Agent) richiede il Single Logout presso il gestore dell'identita		
2	Il gestore dell'identita ricevuta la richiesta chiude la sessione di autenticazione associata alla sessione globale. Successivamente per ciascun fornitore di servizi facente parte della sessione globale, a partire da quelli in grado di supportare il bindind SOAP, procede alla chiusura delle sessioni individuali. In particolare:		
2.1	invia una richiesta di logout all'i-esimo fornitore di servizi riportando l'identificatore associato alla sessione globale che si vuole chiudere	LogoutRequest	SOAP, HTTP-Redirect
2.2	L'iesimo fornitore di servizi ricevuta la richiesta chiude la sessione identificata (se la stessa non fosse stata gia chiusa in precedenza o mai instaurata) ed invia una notifica di avvenuta chiusura al gestore dell'identita	LogoutResponse	SOAP, HTTP-Redirect, HTTP-POST
2.3	Se l'i-esimo fornitore di servizi non e raggiungibile il processo degrada a partial logout		

Il risultato della sequenza di scambio e la chiusura della *sessione globale*.

In condizioni di anomalia derivate da una mancata, intempestiva o non corretta risposta da parte di uno o piu fornitori di servizi coinvolti nella sessione, il processo di Single Logout degrada ad un **partial logout**. In questo caso alla fine del processo risulteranno chiuse la *sessione di autenticazione* e la *sessione individuale* presso il fornitore dei servizi

presso cui viene operata la richiesta di Single Logout ma non si potra avere garanzia sulla effettiva chiusura delle altre *sessioni individuali* facenti parte della *sessione globale*. Nel caso di richiesta di Single Logout operata presso un fornitore di servizi (Tabella 1) il gestore dell'identita nel caso di operazione conclusa con successo dovra notificare tale situazione al fornitore di servizi richiedente, riportando nella response il seguente status code:

- StatusCode: `urn:oasis:names:tc:SAML:2.0:status:Success`

Viceversa nel caso in cui si verificasse una condizione di partial logout il gestore dell'identita, se in condizione di poterlo fare, dovra notificare tale esito al fornitore di servizi richiedente, riportando nella response i seguenti status code:

- StatusCode: `urn:oasis:names:tc:SAML:2.0:status:Requester`
- sub-StatusCode: `urn:oasis:names:tc:SAML:2.0:status:PartialLogout`

Quest'ultimo comportamento deve essere assunto dal gestore dell'identita anche nel caso di una richiesta di Single Logout operata presso un fornitore di servizi e presentata dopo la scadenza della *sessione globale*, a seguito del timeout della relativa sessione di autenticazione o della esplicita chiusura della stessa da parte dell'utente.

1.5.2 LogoutRequest

Note: Come sopra descritto, **il messaggio di LogoutRequest può essere inviato dal Service Provider all'Identity Provider o viceversa**, a seconda dell'entità presso la quale l'utente ha richiesto il Single Logout.

Il messaggio di LogoutRequest deve seguire le specifiche SAML (cfr.[SAML-Core] sez. 3.7) e avere le seguenti caratteristiche:

SI DEVE

- Nell'elemento `<LogoutRequest>` devono essere presenti i seguenti attributi:
  - l'attributo `ID` univoco, per esempio basato su un Universally Unique Identifier (UUID) o su una combinazione origine + timestamp (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocita);
  - l'attributo `Version`, che deve valere sempre `2.0`, coerentemente con la versione della specifica SAML adottata;
  - l'attributo `IssueInstant` a indicare l'istante di emissione della richiesta, in formato UTC (esempio: `2008-03-13T18:04:15.531Z`);
  - l'attributo `Destination`, a indicare l'indirizzo (URI reference) dell'entita (gestore delle identita o fornitori di servizi) a cui e inviata la richiesta.
- Nell'elemento `<LogoutRequest>` devono essere presenti i seguenti elementi:
  - l'elemento `<Issuer>` attualizzato come l'attributo `entityID` riportato nel corrispondente metadata, a indicare l'identificatore univoco dell'entita (gestore delle identita o fornitori di servizi) emittente. L'elemento deve riportare gli attributi:
    - `Format` fissato al valore `urn:oasis:names:tc:SAML:2.0:nameid-format:entity`;
    - `NameQualifier` che qualifica il dominio a cui afferisce tale valore (URI riconducibile alla stessa entita emittente);
  - l'elemento `<NameID>` atto a qualificare il soggetto a cui si riferisce l'evento di autenticazione che ha dato origine alla sessione, in cui sono presenti i seguenti attributi:

    * Format che deve assumere il valore urn:oasis:names:tc:SAML:2.0:nameid-format:transient (cfr. SAMLCore, sez. 8.3);
    * NameQualifier che qualifica il dominio a cui afferisce tale valore (URI riconducibile al gestore dell'identita che ha emesso l'asserzione);
  - l'elemento <SessionIndex> atto ad identificare la sessione a cui la richiesta di chiusura si riferisce;
- Nel caso del binding SOAP e HTTP POST deve essere presente l'elemento <Signature> contenente la firma sulla richiesta apposta dal Service Provider. La firma deve essere prodotta secondo il profilo specificato per SAML (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

1.5.3 LogoutResponse

Note: Come sopra descritto, **il messaggio di LogoutResponse può essere inviato dal Service Provider all'Identity Provider o viceversa**, a seconda dell'entità presso la quale l'utente ha richiesto il Single Logout.

Il messaggio di LogoutResponse deve seguire le specifiche SAML (cfr.[SAML-Core] sez. 3.7) e avere le seguenti caratteristiche:

SI DEVE

- Nell'elemento <LogoutResponse> devono essere presenti i seguenti elementi:
  - l'attributo ID univoco, per esempio basato su un Universally Unique Identifier (UUID) (cfr. UUID) o su una combinazione origine + timestamp (quest'ultimo generato con una precisione di almeno un millesimo di secondo per garantire l'univocita);
  - deve essere presente l'attributo Version, che deve valere sempre 2.0, coerentemente con la versione della specifica SAML adottata;
  - deve essere presente l'attributo IssueInstant a indicare l'istante di emissione della risposta, in formato UTC;
  - deve essere presente l'attributo InResponseTo, il cui valore deve fare riferimento all'ID della richiesta a cui si risponde;
  - deve essere presente l'attributo Destination, a indicare l'indirizzo (URI reference) dell'entita (gestore delle identita o fornitori di servizi) a cui e inviata la risposta;
- Nell'elemento <LogoutResponse> devono essere presenti i seguenti elementi:
  - deve essere presente l'elemento <Issuer> a indicare l'entityID dell'entita emittente; l'elemento deve riportare gli attributi:
    * Format fissato al valore urn:oasis:names:tc:SAML:2.0:nameid-format:entity;
    * NameQualifier che qualifica il dominio a cui afferisce tale valore (URI riconducibile alla stessa entita emittente);
  - deve essere presente l'elemento <Status> a indicare l'esito della LogoutRequest secondo quanto definito nelle specifiche SAML (cfr. [SAML-Core] par. 3.2.2.1 e ss.) comprendente il sotto-elemento <StatusCode> ed opzionalmente i sotto-elementi <StatusMessage> e <StatusDetail> (cfr [SPID-TabErr]);

1.5.4 Binding

Per il trasporto dei messaggi di LogoutRequest e del relativo LogoutResponse. possono essere utilizzati binding di tipo sincrono (SOAP) o di tipo asincrono (http-redirect o http-POST). Nel caso di uso di binding http-redirect o http-POST, si faccia riferimento a quanto gia specificato nel documento SPID Regole tecniche rispettivamente ai paragrafi al paragrafo 1.2.2.1 e 1.2.2.2 per le richieste di autenticazione (SSO Profile), tenendo presente che i messaggi di LogoutRequest e LogoutResponse devono essere veicolati rispettivamente nei previsti parametri/hidden form control denominati SAMLRequest e SAMLResponse. Per il binding SOAP si faccia riferimento a quanto gia specificato sempre nel documento SPID Regole tecniche al paragrafo 2.2.3. Gli scambi dovranno avvenire su canale sicuro realizzato mediante l'impiego di TLS nella versione piu recente disponibile.

1.5.4.1 Impiego del binding SOAP

Per conferire maggior robustezza al processo di Single Logout, si raccomanda ai fornitori di servizi la messa a disposizione del binding SOAP attraverso apposite interfacce, e ai gestori dell'identita di privilegiarne l'impiego quando disponibile presso gli stessi fornitori di servizi, dando priorita, nel processo di Single Logout, ai fornitori di servizi in grado di supportarlo. La richiesta di Single Logout, quando operata dall'utente presso un fornitore di servizi, deve comunque essere iniziata utilizzando uno dei binding asincroni resi disponibili dai gestori dell'identita, per dar modo ai gestori dell'identita di completare il processo anche presso i fornitori di servizi sprovvisti di interfacce SOAP. Per rafforzare tale prescrizione i gestori dell'identita, pur dovendo essere in grado di supportare il binding SOAP, non dovranno pubblicare interfacce richiesta di Single Logout secondo tale modalita.

1.6 Gestori di attributi qualificati (Attribute Authority)

Warning: Questa sezione non è stata ancora trascritta nel presente documento consolidato. Si rimanda al documento originale delle Regole Tecniche SPID.

Note: È in corso, presso l'Agenzia per l'Italia Digitale, un Gruppo di Lavoro per la ridefinizione delle regole tecniche per i gestori di attributi qualificati. È possibile che le regole ad oggi vigenti subiscano modifiche.

1.7 Registro

Il Registro SPID e il repository di tutte le informazioni relative alla entita aderenti a SPID e costituisce l'evidenza del cosiddetto circle of trust in esso stabilito. La relazione di fiducia su cui si basa la federazione stabilita in SPID si realizza per il tramite dell'intermediazione dell'Agenzia, terza parte garante, attraverso il processo di accreditamento dei gestori dell'identita digitale, dei gestori degli attributi qualificati e dei fornitori di servizi. L'adesione a SPID costituisce l'instaurazione di una relazione di fiducia con tutti i soggetti gia aderenti, accreditati dall'Agenzia, sulla base della condivisione dei livelli standard di sicurezza dichiarati e garantiti da SPID. L'adesione al patto di fiducia tra le entita aderenti (gestori dell'identita digitale, gestori degli attributi qualificati e fornitori di servizi) si evidenzia nella presenza di tali entita nel Registro SPID gestito dall'Agenzia.

1.7.1 Contenuti del Registro

Il federation registry contiene la lista delle entita che hanno superato il processo di accreditamento e quindi facenti parte della federazione SPID. Le informazioni contenute nel registro per ciascuna delle suddette entita sono le seguenti:

- `AuthorityInfo`: entry del Registro relativa ad una entita, a sua volta costituita da:
  - `EntityId`: identificatore SAML dell'entita;
  - `Soggetto`: denominazione del soggetto a cui afferisce l'entita della federazione;
  - `EntityType`: tipo di entità (Identity Provider, Attribute Authority, Service Provider);
  - `MetadataProviderURL`: l'URL del servizio di reperimento metadati;
  - `AttributeList`: elenco di attributi qualificati certificabili da una entita di tipo Attribute Authority.

Il federation registry viene popolato dall'Agenzia per l'Italia Digitale a seguito del processo di stipula delle convenzioni e aggiornata dalla stessa Agenzia nel corso delle attivita legate alla gestione delle convenzioni e della vigilanza sui soggetti del circuito SPID. Il contenuto informativo della federation registry e in fruizione a tutte le entita appartenenti al circuito SPID ai fini della verifica della sussistenza di relazioni di trust nei confronti di entita terze (IdP, AA, SP) e del reperimento delle informazioni associate alla alle stesse. Il Discovery Service puo anch'esso accedere al federation registry per utilizzarne i contenuti ai fini dell'attivita di discovering.

Note: Non è al momento attivo un Discovery Service.

1.7.2 Accesso al Registro

Warning: Questa sezione non è stata ancora trascritta nel presente documento consolidato. Si rimanda al documento originale delle Regole Tecniche SPID.

Note: Il Registro è disponibile alla URL https://registry.spid.gov.it/

1.7.3 Accesso al Registro in modalità LDAP

Warning: Questa sezione non è stata ancora trascritta nel presente documento consolidato. Si rimanda al documento originale delle Regole Tecniche SPID.

Note: L'accesso via LDAP non è al momento attivo.

1.8 Log

1.8.1 Identity Provider

Ai fini della tracciatura l'Identity Provider dovra mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unita di memorizzazione di tale registro dovra rendere persistente per ogni transazione la tripla composta dell'identificativo dell'identita digitale (`spidCode`) interessata dalla transazione, dalla `<AuthnRequest>` e della relativa `<Response>`.

Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi in formato SAML. A titolo esemplificativo e non esaustivo le informazioni presenti in un record del registro potrebbero essere le seguenti:

- SpidCode
- <AuthnRequest>
- <Response>
- AuthnReq_ID
- AuthnReq_ IssueInstant
- AuthnReq_ Issuer
- Resp_ID
- Resp_IssueInstant
- Resp_Issuer
- Assertion_ID
- Assertion_subject
- Assertion_subject_NameQualifier

1.8.2 Service Provider

Il comma 2 dell'articolo 13 del DPCM obbliga i fornitori di servizi (Service Provider) alla conservazione per ventiquattro mesi delle informazioni necessarie a imputare alle singole identita digitali le operazioni effettuate sui propri sistemi.

A tal fine **un Service provider dovra mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi.** L'unita di memorizzazione di tale registro dovra rendere persistente per ogni transazione la coppia dalla <AuthnRequest> e della relativa <Response>.

Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi in formato SAML. A titolo esemplificativo e non esaustivo le informazioni presenti in un record del registro potrebbero essere le seguenti:

- <AuthnRequest>
- <Response>
- AuthnReq_ID
- AuthnReq_IssueInstant
- Resp_ID
- Resp_IssueInstant
- Resp_Issuer
- Assertion_ID
- Assertion_subject
- Assertion_subject_NameQualifier

1.9 Tabella attributi

L'identificatore sotto indicato è il valore dell'attributo `Name` dell'elemento `<saml:Attribute>`. Il valore dell'attributo `NameFormat` dello stesso elemento e, come da specifica SAML-core, `urn:oasis:names:tc:SAML:2.0:attrname-format:basic`.

Il tipo sotto indicato è il valore dell'attributo `xsi:type` dell'elemento `<saml:AttributeValue>`.

Table 3: Tabella attributi identificativi

Attributo	Identificatore	Tipo	Note
Codice identificativo	`spidCode`	xs:string	Il codice identificativo e assegnato dal gestore dell'identita digitale, deve essere univoco in ambito SPID. Il formato e il seguente: `<cod_IdP><nr. univoco>` dove: • `<cod_IdP>` e un codice composto da 4 lettere univocamente assegnato al gestore delle identita; • `<nr.univoco>` e una stringa alfanumerica composta da 10 caratteri che il gestore delle identita genera in maniera univoca nell'ambito del proprio dominio. (Es. `ABCD123456789A`)
Nome	`name`	xs:string	Stringa composta da una sequenza di una o piu sottostringhe non vuote con carattere iniziale in maiuscolo intervallate da uno (solo) spazio (Es. `Francesca` , `Giovanni Mario`)
Cognome	`familyName`	xs:string	Stringa composta da una sequenza di una o piu sottostringhe non vuote con carattere iniziale in maiuscolo intervallate da uno (solo) spazio (Es. `Rossi`, `Bianchi Verdi`)
Luogo di nascita	`placeOfBirth`	xs:string	Stringa corrispondente al codice catastale (Codice Belfiore) del Comune o della nazione estera di nascita. (Es. `F205` per la città di Milano)
Provincia di nascita	`countyOfBirth`	xs:string	Stringa corrispondente alla sigla della provincia di nascita. (Es. `MI` per provincia di Milano)
Data di nascita	`dateOfBirth`	xs:date	Secondo specifica xs:date nel formato *YYYY-MM-DD* dove:

Table 4: Tabella attributi secondari

Attributo	Identificatore	Tipo	Note
Numero di telefono mobile	`mobilePhone`	xs:string	Stringa numerica senza spazi intermedi (Es. `34912345678`)
Indirizzo di posta elettronica	`email`	xs:string	Formato standard indirizzo di posta elettronica
Domicilio fisico	`address`	xs:string	Stringa composta da una sequenza di sottostringhe non vuote intervallate da uno (solo) spazio rappresentanti: • Tipologia (via, viale, piazza...); • Indirizzo; • Nr. civico; • CAP; • Luogo; • Provincia.
Data di scadenza identita	`expirationDate`	xs:date	Secondo specifica xs:date
Domicilio digitale	`digitalAddress`	xs:string	Indirizzo casella PEC

1.10 Messaggi di errore

1.10.1 Autenticazione corretta

Error code:	1 (Autenticazione corretta)
Binding:	HTTP-POST, HTTP-Redirect
HTTP status code:	200
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Success`
Destinatario notifica:	Fornitore del servizio (SP)

1.10.2 Anomalie del sistema

Error code:	2 (Indisponibilita sistema)
Binding:	HTTP-POST
Destinatario notifica:	Utente
Schermata IdP:	Messaggio di errore generico
Troubleshooting utente:	Ripetere l'accesso al servizio piu tardi

Error code:	3 (Errore di sistema)
Binding:	HTTP-Redirect
HTTP status code:	500
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio “Sistema di autenticazione non disponibile - Riprovare piu tardi”
Troubleshooting utente:	Ripetere l’accesso al servizio piu tardi
Note:	Tutti i casi di errore di sistema in cui e possibile mostrare un messaggio informativo all’utente

1.10.3 Anomalie delle richieste

Error code:	4 (Formato binding non corretto)
Binding:	HTTP-Redirect, HTTP-POST
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *“Formato richiesta non corretto - Contatare il gestore del servzio”*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare la conformita con le regole tecniche SPID del formato del messaggio di richiesta
Parametri obbligatori:	• `SAMLRequest` • `SigAlg` (solo per HTTP-Redirect) • `Signature` (solo per HTTP-Redirect)
Parametri non obbligatori:	• `RelayState`

Error code:	5 (Verifica della firma fallita)
Binding:	HTTP-Redirect
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *“Impossibile stabilire l’autenticita della richiesta di autenticazione - Contattare il gestore del servizio”*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare certificato o modalita di apposizione firma
Note:	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati

Error code:	6 (Binding su metodo HTTP errato)
Binding:	HTTP-Redirect, HTTP-POST
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non ricevibile - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare metadata Gestore dell'identita (IdP)
Note:	Invio richiesta in HTTP-Redirect su entrypoint HTTP-POST dell'identity, oppure invio richiesta in HTTP-POST su entrypoint HTTP-Redirect dell'identity

Error code:	7 (Errore sulla verifica della firma della richiesta)
Binding:	HTTP-POST
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non corretto - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare certificato o modalita di apposizione firma
Note:	Firma sulla richiesta non presente, corrotta, non conforme in uno dei parametri, con certificato scaduto o con certificato non associato al corretto EntityID nei metadati registrati

Error code:	8 (Formato della richiesta non conforme alle specifiche SAML)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML StatusMessage:	ErrorCode nr08
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente
Note:	Non conforme alle specifiche SAML - Il controllo deve essere operato successivamente alla verifica positiva della firma

Error code:	9 (Parametro version non presente, malformato o diverso da `2.0`)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:VersionMismatch`
SAML StatusMessage:	ErrorCode nr09
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare la richiesta secondo le regole tecniche SPID - Fornire pagina di cortesia all'utente

Error code:	10 (Issuer non presente, malformato o non corrispondete all'entita che sottoscrive la richiesta)
Binding:	HTTP-Redirect, HTTP-POST
HTTP status code:	403
Destinatario notifica:	Utente
Schermata IdP:	Pagina di cortesia con messaggio *"Formato richiesta non corretto - Contattare il gestore del servizio"*
Troubleshooting utente:	Contattare il gestore del servizio
Troubleshooting SP:	Verificare formato delle richieste prodotte

Error code:	11 (ID non presente, malformato o non conforme)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML StatusMessage:	ErrorCode nr11
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente
Note:	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata solo a seguito di una positiva verifica della firma.

Error code:	12 (`RequestAuthnContext` non presente, malformato o non previsto da SPID)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML subStatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:NoAuthnContext`
SAML StatusMessage:	ErrorCode nr12
Destinatario notifica:	Fornitore del servizio (SP)
Schermata IdP:	Pagina temporanea con messaggio di errore: *"Autenticazione SPID non conforme o non specificata"*
Troubleshooting SP:	Informare l'utente
Note:	Identificatore necessario per la correlazione con la risposta. L'eventuale presenza dell'anomalia va verificata e segnalata solo a seguito di una positiva verifica della firma.

Error code:	13 (`IssueInstant` non presente, malformato o non coerente con l'orario di arrivo della richiesta)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestDenied`
SAML StatusMessage:	ErrorCode nr13
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente

Error code:	14 (`Destination` non presente, malformata o non coincidente con il Gestore delle identita ricevente la richiesta)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported`
SAML StatusMessage:	ErrorCode nr14
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente

Error code:	15 (Attributo `IsPassive` presente e attualizzato al valore true)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Requester`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:NoPassive`
SAML StatusMessage:	ErrorCode nr15
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente

Error code:	16 (AssertionConsumerService non correttamente valorizzato)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	urn:oasis:names:tc:SAML:2.0:status:Requester
SAML sub-StatusCode:	urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported
SAML StatusMessage:	ErrorCode nr16
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente
Note:	• AssertionConsumerServiceIndex presente e attualizzato con valore non riportato nei metadata • AssertionConsumerServiceIndex riportato in presenza di uno od entrambi gli attributi AssertionConsumerServiceURL e ProtocolBinding • AssertionConsumerServiceIndex non presente in assenza di almeno uno attributi AssertionConsumerServiceURL e ProtocolBinding • La response deve essere inoltrata presso AssertionConsumerService di default riportato nei metadata

Error code:	17 (Attributo Format dell'elemento NameIDPolicy assente o non valorizzato secondo specifica)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	urn:oasis:names:tc:SAML:2.0:status:Requester
SAML sub-StatusCode:	urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported
SAML StatusMessage:	ErrorCode nr17
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Formulare correttamente la richiesta - Fornire pagina di cortesia all'utente
Note:	Nel caso di valori diversi dalla specifica del parametro opzionale AllowCreate si procede con l'autenticazione senza riportare errori

Error code:	18 (AttributeConsumerServiceIndex malformato o che riferisce a un valore non registrato nei metadati di SP)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	urn:oasis:names:tc:SAML:2.0:status:Requester
SAML sub-StatusCode:	urn:oasis:names:tc:SAML:2.0:statuss:RequestUnsupported
SAML StatusMessage:	ErrorCode nr18
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Riformulare la richiesta con un valore dell'indice presente nei metadati

1.10.4 Anomalie derivanti dall'utente

Error code:	19 (Autenticazione fallita per ripetuta sottomissione di credenziali errate - superato numero tentativi secondo le policy adottate)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr19
Destinatario notifica:	HTTP POST/HTTP Redirect
Schermata IdP:	Messaggio di errore specifico ad ogni interazione prevista
Troubleshooting utente:	Inserire credenziali corrette
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
Note:	Si danno indicazioni specifiche e puntuali all'utente per risolvere l'anomalia, rimanendo nelle pagine dello IdP. Solo al verificarsi di determinate condizioni legate alle policy di sicurezza aziendali, ad esempio dopo 3 tentativi falliti, si risponde al SP.

Error code:	20 (Utente privo di credenziali compatibili con il livello HTTP richiesto dal fornitore del servizio)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr20
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting utente:	Acquisire credenziali di livello idoneo all'accesso al servizio richiesto
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

Error code:	21 (Timeout durante l'autenticazione utente)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr21
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting utente:	Si ricorda che l'operazione di autenticazione deve essere completata entro un determinato periodo di tempo
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

Error code:	22 (Utente nega il consenso all'invio di dati al SP in caso di sessione vigente)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr22
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting utente:	Dare consenso
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto
Note:	Sia per autenticazione da fare, sia per sessione attiva di classe SpidL1.

Error code:	23 (Utente con identita sospesa/revocata o con credenziali bloccate)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr23
Destinatario notifica:	Fornitore del servizio (SP)
Schermata IdP:	Pagina temporanea con messaggio di errore: "Credenziali sospese o revocate"
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto

Error code:	24 (Riservato)

Error code:	25 (Processo di autenticazione annullato dall'utente)
Binding:	HTTP-Redirect, HTTP-POST
SAML StatusCode:	`urn:oasis:names:tc:SAML:2.0:status:Responder`
SAML sub-StatusCode:	`urn:oasis:names:tc:SAML:2.0:statuss:AuthnFailed`
SAML StatusMessage:	ErrorCode nr25
Destinatario notifica:	Fornitore del servizio (SP)
Troubleshooting SP:	Fornire una pagina di cortesia notificando all'utente le ragioni che hanno determinato il mancato accesso al servizio richiesto