Agenzia per l'Italia Digitale

Presidenza del Consiglio dei Ministri

SPID

REGOLE TECNICHE

PAGINA BIANCA

INDICE

MODIFICHE AL DOCUMENTO

Descrizione Modifica	Edizione	Data
Prima emissione versione bozza	V 0.1	12/01/14

PREFAZIONE

Il presente documento è emesso ai sensi dell'art.4 comma 2 del DPCM 24 ottobre 2014 "*Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID)*

1 REGOLE TECNICHE PER IL GESTORE DELL'IDENTITÀ DIGITALE

Le modalità di funzionamento del *Gestore dell'identità digitali,* nel seguito indicato anche con il termine tecnico *Identity provider*, dovranno essere quelle previste da SAML v2 per il profilo "*Web Browser SSO*" (cfr. [SAML-TechOv] sez. 4.1)

Devono essere previste le due versioni "*SP-Initiated*": "*Redirect/POST binding*" e "*POST/POST binding*". in cui il meccanismo di autenticazione è innescato dalla richiesta inoltrata dall'utente (tramite il suo User Agent) ad un *fornitore di servizi*, nel seguito indicato anche con il termine tecnico *Service Provider*, il quale a sua volta si rivolge opportunamente all'autorità di certificazione d'identità in modalità "pull".

La richiesta di autenticazione SAML (basata sul costrutto <AuthnRequest>) può essere inoltrata da un *Service Provider* all'*Identity Provider* usando il binding HTTP Redirect o il binding HTTP POST.

La relativa risposta SAML (basata sul costrutto <Response>) può invece essere inviata dall'*Identity Provider* al *Service Provider* solo tramite il binding HTTP POST.

Interfacce logiche dell'*Identity Provider* coinvolte:

- **IIDPUserInterface :** permette agli utenti l'interazione via web con il componente tramite User Agent in fase di challenge di autenticazione;
- **IAuthnRequest**: ricezione di richieste di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei SAML metadata dell'*Identity Provider* da parte delle *Service Provider*.

Interfacce logiche del *Service Provider* coinvolte:

- **IMetadataRetrieve**: permette il reperimento dei SAML metadata del *Service Provider* da parte dell'*Identity Provider*.
- **IAuthnResponse**: ricezione delle risposte di autenticazione SAML.

1.1. SCENARIO DI INTERAZIONE IN MODALITÀ SSO

Lo scenario completo è quello illustrato in figura1.1 nel caso di SP-Initiated - Redirect/POST binding e descritto dalla tabella 1.1

	Descrizione	Interfaccia	SAML	Binding
1	Il fruitore utilizzando il browser (User Agent) richiede l'accesso alla risors			
2	La Service Provider (SP) invia allo User Agent una richiesta di autenticazione da far pervenire all'Identity Provider.	IAuthnRequest	AuthnRequest	HTTP Redirect HTTP POST
3	Lo User Agent inoltra la richiesta di autenticazione contattando L'Identity Provider secondo la modalità adottata al passo 1.	-	AuthnRequest	HTTP Redirect HTTP POST
4	L'Identity Provider esamina la richiesta ricevuta e se necessario esegue una challenge di autenticazione con l'utente.	-	-	HTTP
5	L'Identity Provider effettuata l'autenticazione prepara l'asserzione contenente lo statement di autenticazione dell'utente destinato al Service Provider (più eventuali statement di attributo emessi dall'Identity Provider stesso).	-	-	-
6	L'Identity Provider restituisce allo User Agent la <Response> SAML contenente l'asserzione preparata al punto precedente.	-	Response	HTTP POST
7	Lo User Agent inoltra al Service Provider (SP) la <Response> SAML emessa dall'Identity Provider.	IAuthnResponse	Response	HTTP POST

Tabella 1.1 SSO SP-Initiated Redirect/POST binding

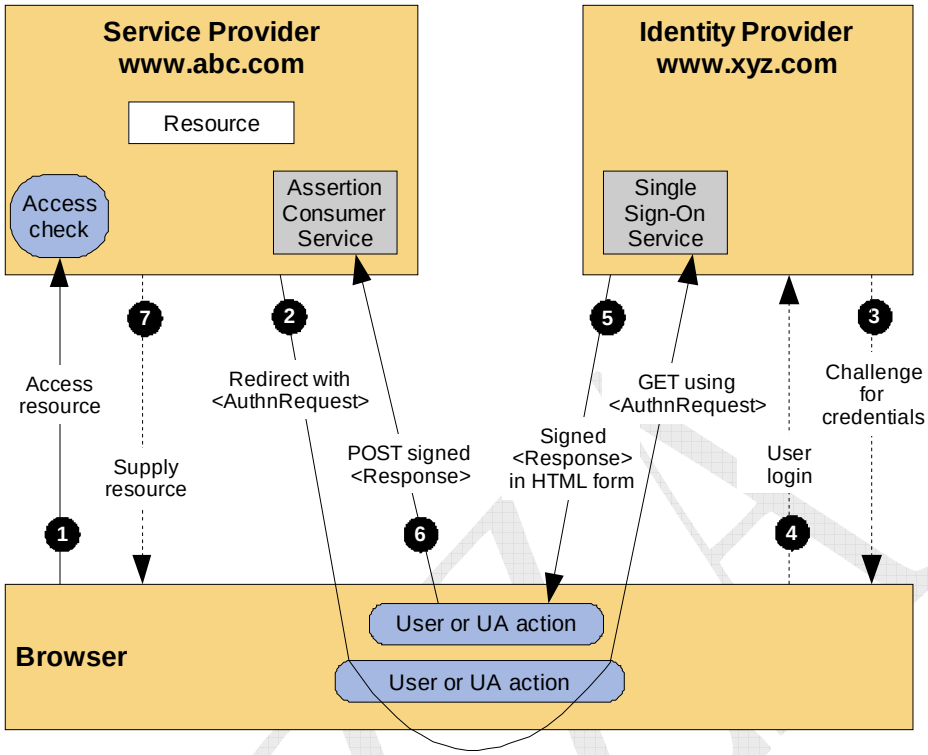

Figura 1.1 SSO SP-Initiated Redirect/POST binding

1.2. SPECIFICHE DELLE INTERFACCE

Di seguito vengono esposte le specifiche delle interfacce del *Identity Provider* riportanti

- Le caratteristiche delle asserzioni prodotte
- Le caratteristiche delle AuthnRequest e della AuthnResponse
- Le caratteristiche del binding
- I metadati

1.2.1. CARATTERISTICHE DELLE ASSERZIONI

Le asserzioni prodotte dall'*Identity Provider* devono essere conformi allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le seguenti condizioni

- nella **<Assertion>** di autenticazione deve essere presente l'elemento **<Subject>** a indicare il soggetto che si è autenticato;
- nell'elemento <**Subject**> deve essere presente l'elemento <**NameID**> atto a qualificare meglio il subject dell'asserzione: in particolare deve essere presente l'attributo ***Format*** avente valore "urn:oasis:names:tc:SAML:2.0:nameid-format:transient" (cfr. SAMLCore, sez. 8.3), e l'attributo ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (per esempio un URI riconducibile all'*Identity Provider* stesso);

- nell'elemento <**Subject**> dell'asserzione di autenticazione deve essere presente almeno un elemento <**SubjectConfirmation**> con attributo ***Method*** avente valore "*urn:oasis:names:tc:SAML:2.0:cm:bearer*";
- nella <**Assertion**> di autenticazione deve essere presente l'elemento <**Issuer**> a indicare l'entityID dell'authority emittente, cioè l'*Identity Provider* stesso;
- nella <**Assertion**> di autenticazione, nell'elemento <**Conditions**> devono essere presenti almeno i vincoli di validità temporale dell'asserzione (per esempio *NotBefore, NotOnOrAfter*);
- nella <**Assertion**> di autenticazione, nell'elemento <**AuthnContext**> deve essere presente la descrizione del contesto di autenticazione effettivo;
- all'interno dell'asserzione deve essere necessariamente presente un elemento <**AttributeStatement**> relativo all' asserzione di attributo *codice Identificativo SPID* dell'utente autenticato. . L'elemento <**Attribute**> deve essere identificato tramite l'attributo ***Name*** pari a "*CodiceIdentificativoSPID*".
- all'interno dell'asserzione possono essere presenti altri elementi <**AttributeStatement**>, relativi ad asserzioni di ulteriori attributi che l'*Identity Provider* può rilasciare contestualmente a quello del *codice identificativo SPID*

  Di seguito si riporta un esempio di *attribute statement* con all'interno l'attributo *spidCode* relativo al *codice identificativo SPID*.

```
<saml:AttributeStatement xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
<saml:Attribute Name=" spidCode " xmlns:saml="urn….">
<saml:AttributeValue xmlns:xs=..xsi:type="xs:string">
YYRRTT1234556789
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
```

Listato 1.1 – attribute statement

- nella <**Assertion**> di autenticazione può essere presente l'elemento <**Advice**>, contenente altri elementi <**Assertion**>: questo meccanismo è utilizzabile nei casi in cui gli statement emessi dall'*Identity Provider* si basino su altre asserzioni SAML, ottenute per esempio da altre authority, delle quali è necessario fornire evidenza in forma originale unitamente alla risposta alla richiesta di autenticazione;
- deve essere presente l'elemento <**Signature**> apposto dall'*Identity Provider*.

1.2.2. CARATTERISTICHE DELLE AUTHNREQUEST E DELLA RESPONSE

Il protocollo AuthnRequest previsto per l'*Identity Provider* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le seguenti condizioni

1.2.2.1. AUTHNREQUEST

L'authnrequest che deve confermare le seguenti caratteristiche:

- deve essere presente l'attributo ***ID*** univoco, per esempio basato su un Universally Unique Identifier (UUID) o su una combinazione origine + timestamp.(Esempio ID = Assertion-uuidae7136e4-0118-18d8-999d-cff934ae63db);
- 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 richiesta, in formato UTC (esempio: "2008-03-13T18:04:15.531Z");
- deve essere presente l'attributo ***ProtocolBinding***, una URI reference che identifica il binding da utilizzare per inoltrare il messaggio di risposta (<**Response**>): deve valere "*urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST*";
- deve essere presente l'attributo ***Destination***, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta,;
- deve essere presente l'attributo ***IsPassive*** con valore "*false*", poiché non si vuole prevenire l'interazione esplicita tra certificatore di identità e utente;
- deve essere presente l'attributo ***AssertionConsumerServiceURL*** ad indicare l'URL a cui inviare il messaggio di risposta alla richiesta di autenticazione (in questo caso l'indirizzo del servizio ***AssertionConsumingService*** del *Service Provider*);
- deve essere presente l'elemento <**Issuer**> a indicare l'entityID del *Service Provider* emittente (N.B. la specifica SAML considera opzionale questo elemento; tuttavia esso è necessario ai fini del reperimento dei metadati o per la verifica della firma da parte dell'entità destinataria);
- può non essere presente l'elemento <**Subject**> (per esempio nel caso in cui esso non sia ancora noto al *Service Provider*);
- l'elemento <**NameIDPolicy**> avente il relativo attributo ***AllowCreate*** valorizzato a "*false*" segnala all'*Identity Provider* che non è ammesso che l'identificativo dell'utente venga creato

contestualmente alla fase di autenticazione (in altre parole, si richiede che il subject sia già registrato presso il certificatore d'identità). All'interno dell'elemento <**NameIDPolicy**> deve essere presente l'attributo Format valorizzato con l'URI "*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*";

- l'attributo ***ProxyCount*** dell'elemento <**Scoping**> deve assumere valore "0";
- opzionalmente può essere presente l'attributo ***AttributeConsumingServiceIndex***. Se presente deve essere posto pari all'indice posizionale della struttura ***AttributeConsumingService*** presente nei metadati del *Service Provider* atta a descrivere i requisiti in termini di attributi necessari per l'accesso al servizio richiesto dall'utente;
- opzionalmente possono essere presenti zero o più elementi <**RequesterID**> dell'elemento <**Scoping**>. Se presente deve 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, possibilmente mantenendo un ordine che indichi la sequenza di propagazione (per esempio, il primo elemento <**RequesterID**> dell'elemento <**Scoping**> è relativo all'ultima entità che ha propagato la richiesta);
- 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;
- deve essere presente l'elemento <**RequestedAuthnContext**> (cfr. [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 (cfr.[SAMLAuthContext] sez. 3) in riferimento SPID:
    - urn:oasis:names:tc:SAML:2.0:ac:classes: SpidL1
    - urn:oasis:names:tc:SAML:2.0:ac:classes: SpidL2
    - urn:oasis:names:tc:SAML:2.0:ac:classes: 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 presente documento si adotta sempre il valore "*exact*", che richiede l'esatta corrispondenza con uno dei contesti descritti). 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 "*SpidL3*" o in subordine a una di tipo "*SpidL2*" .

```
<samlp:RequestedAuthnContext Comparison="exact">
      <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL3
      </saml:AuthnContextClassRef>
      <saml:AuthnContextClassRef>
            urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL2
      </saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
```

Listato 1.2 – RequestedAuthnContext

- nel caso del binding HTTP POST, deve essere presente l'elemento <**Signature**> apposto dal *Service Provider*.

1.2.2.2. RESPONSE

Le caratteristiche che deve avere la <Response> inviata dall'*Identity Provider* al *Service Provider* in risposta alla richiesta di autenticazione sono le seguenti:

- deve essere presente 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)
- 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 *Relying*; *Party* a cui è inviata la risposta;
- deve essere presente l'elemento <**Status**> a indicare l'esito (sotto-elemento <**StatusCode**>) della richiesta a cui si risponde;
- deve essere presente l'elemento <**Issuer**> a indicare l'*entityID* dell'entità emittente, cioè l'*Identity Provider* stesso;
- deve essere presente un elemento <**Assertion**> ad attestare l'avvenuta autenticazione, contenente un elemento <**AuthnStatement**>;

Per l'asserzione veicolata resta valido quanto già specificato nel paragrafo 1.2.1.

1.2.3. CARATTERISTICHE DEL BINDING

1.2.3.1. BINDING HTTP REDIRECT

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

- come risposta alla richiesta di accesso dell'*end user* ad un servizio o risorsa, il *Service Provider* invia allo *User Agent* un messaggio HTTP di redirezione, cioè avente uno status code con valore 302 ("*Found*") o 303 ("*See Other*");
- il *Location Header* del messaggio HTTP contiene l'URI di destinazione del servizio di Single Sign-On esposto dall' *Identity Provider*. L'interfaccia è sempre la *IAuthnRequest*);
- il messaggio HTTP trasporta i seguenti parametri (tutti URL-encoded):
    1. "*SAMLRequest*": un costrutto SAML <**AuthnRequest**> 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 e la stringa con la codifica *Base64 URL-encoded* dei byte del messaggio SAML;
    2. "*RelayState*": identifica la risorsa (servizio) originariamente richiesta dall'utente e a cui trasferire il controllo alla fine del processo di autenticazione;
    3. "*SigAlg*": identifica l'algoritmo usato per la firma che può essere *DSAwithSHA256* oppure *RSAwithSHA256*; 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;
    4. "*Signature*": contiene la firma digitale della *query string*, così come prodotta prima di aggiungere questo parametro, utilizzando l'algoritmo indicato al parametro precedente.
    5. Il browser dell'utente elabora quindi tale messaggio *HTTP Redirect* indirizzando una richiesta HTTP con metodo GET al servizio di Single Sign-On dell' *Identity Provider* (interfaccia *IAuthnRequest*) sotto forma di URL con tutti i sopraindicati parametri contenuti nella *query string*.

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 "*RelyState*" è stato reso non immediatamente intellegibile, come suggerito dalla specifica, sostituendo la stringa in chiaro con l'Id della richiesta: il *Service Provider* tiene traccia della corrispondenza):

```
https://idp.cnipa.gov.it:6443/idp/SSOServiceProxy?
SAMLRequest=nVPLbtswELz3KwTeZb0M2SYsBa6NoAbSRrGUHnqjqFVDQCJVLuU4f19KlhEDbVygR5K7O7Mzw%2
FXdqW2cI2gUSiYkmPnEAclVJeTPhDwX9%2B6S3KWf1sjapqOb3rzIA%2FzqAY2zQQRtbNtWSe

[…]

ZwPAU88aUQvQ%2F8oe8S68piBDNabB5s3AyThb1XZMCxxEhhPj5qLZddW2sZIcoP4fBW%2BWccqH0fZ6iNir0tU
QGeCWZaGZxE5pM4n8Nz7p%2Be2D3S6L51x1NljO%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
```

Listato 1.3 – http redirect query string

1.2.3.2. BINDING HTTP POST

Nel caso del *binding* HTTP POST, come risposta alla richiesta di accesso dell'utente ad un servizio o risorsa, il SP invia allo *User Agent* (il browser dell'utente) un messaggio HTTP con status code avente valore 200 ("OK");

- il messaggio HTTP contiene una *form* HTML all'interno della quale è trasportato un costrutto SAML <**AuthnRequest**> codificato come valore di un *hidden form* control di nome "*SAMLRequest*". 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*;
- 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;
- la *form* HTML è corredata da uno script che la rende auto-postante all'indirizzo indicato nell'attributo "*action*".
- Il browser dell'utente elabora quindi la risposta HTTP e invia una richiesta HTTP POST verso il componente *Single Sign-On* dell'*Identity Provider* (interfaccia *IAuthnRequest*).

Un esempio di *form* HTML per trasferire in HTTP POST la richiesta di autenticazione è descritto nel listato 1.4. Osservando attentamente il codice riportato in figura si può notare il valore del parametro "*SAMLRequest*" (ridotto per brevità); il valore del parametro *RelyState* reso non immediatamente intellegibile (cfr. sez. precedente); l'elemento <**input** type="*submit*" value="*Go*"/>, 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 auto-postante.

```
<html>
  <body onload="javascript:document.forms[0].submit()">
        <form method="post" action="https://lp.cnipa.gov.it:6443/lp/SSOServiceProxy">
            <input type="hidden" name="RelayState"
                                value="s2645f48777bd62ec83eddc62c066da5cb987c1eb3">
            <input type="hidden" name="SAMLRequest"
value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwOkF1dGhuUmVxdWVzdCBB
c3NlcnRpb25Db25zdW1lclNlcnZpY2VVUkw9Imh0dHA6Ly9zcC5pY2FyLml0OjgwODAvaWNhc
[…]
N0ZWRUcmFuc3BvcnQ8L3NhbWw6QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1scDpSZXF1ZXN0ZWRBdXRobkNvb
nRleHQ+PHNhbWxwOlNjb3BpbmcgUHJveHlDb3VudD0iMiIgeG1sbnM6c2FtbHA9InVybjpvYXNpczpuYW1lczp0
YzpTQU1MOjIuMDpwcm90b2NvbCIvPjwvc2FtbHA6QXV0aG5SZXF1ZXN0Pg==">
            <input type="submit" value="Go"/>
        </form>
  </body>
</html>
```

Listato 1.4 – Richiesta http POST bindig

Conclusa la fase di autenticazione, l'*Identity Provider* costruisce una <**Response**> firmata diretta al *Service Provider*, e in particolare al relativo servizio *AssertionConsumerService*. 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*.

Un esempio di tale *form* è riportato nel listato 1.5 (anche in questo caso, il valore del parametro "*SAMLResponse*" è stato ridotto per brevità).

```
<html>
  <body onload="javascript:document.forms[0].submit()">
    <form method="post"
                action="http://rp.cnipa.gov.it:8080/cniparp/AssertionConsumerService">
      <input type="hidden" name="SAMLResponse"
value="PD94bWwgdmVyc2lvbj0iMS4wIiBlbmNvZGluZz0iVVRGLTgiPz4KPHNhbWxwOlJlc3BvbnNlIERlc3Rp
bmF0aW9uPSJodHRwOi8vc3AuaWNhci5pdDo4MDgwL2ljYXItc3AvQXNzZXJ0aW9uQ29uc3VtZXJTZXJ2aWNlIiB
JRD0iczJhNTdmN2RhYTUyMTc2NWZmOTQ2ODM0ZmY2NjIzNTA3ZTcwNGI1MDQ3IiBJblJlc3BvbnNlVG89InMyOG
Q5MWEyNmJkNGQ2MGY0N2E0OTkxMzMwMGZhZjc2MzFiZjMxNDBlOSIgSXNzdWVJbnN0YW50PSIyMDA4LTAzLTA0V
DIyOjEzOjQ4LjUwMFoiIFZlcnNpb249IjIuMCIgeG1sbnM6c2Ftb
[…]
2lzOm5hbWVzOnRjOlNBTUw6Mi4wOmFjOmNsYXNzZXM6UGFzc3dvcmRQcm90ZWN0ZWRUcmFuc3BvcnQ8L3NhbWw6
QXV0aG5Db250ZXh0Q2xhc3NSZWY+PC9zYW1sOkF1dGhuQ29udGV4dD48L3NhbWw6QXV0aG5TdGF0ZW1lbnQ+PC9
zYW1sOkFzc2VydGlvbj48L3NhbWxwOlJlc3BvbnNlPg==">
      <input type="hidden" name="RelayState"
                        value="s28d91a26bd4d60f47a49913300faf7631bf3140e9">
      <input type="submit" value="Go"/>
   </form>
 </body>
</html>
```

Listato 1.5 – Risposta http POST bindig

1.2.3.3. GESTIONE DELLA SICUREZZA SUL CANALE DI TRASMISSIONE

Il profilo SAML SSO raccomanda l'uso di SSLv.3.0 o TLS 1.0 nei colloqui tra Asserting party e

le Service Provider. In ambito SPID si rende obbligatorio l'impiego di TLS preferibilmente nella versione più recente.

1.2.3.4. IDP METADATA

Il funzionamento dell'*Identity provider* deve essere definito attraverso *metadata* conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]) secondo le seguenti caratteristiche:

- **`<EntityDescriptor>`** deve riportare i seguenti attributi:
  - **entityID**: indicante l'identificativo univoco (un URI) dell'entità;
  - **cacheDuration**: indicante la durata (in millisecondi) della cache di un file di metadati; un documento di metadati letto e memorizzato localmente ha validità fino alla scadenza di tale periodo di tempo; successivamente è necessario richiedere nuovamente il file alla relativa entità.
- **`<IDPSSODescriptor>`** 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 esprime il requisito che le richieste di autenticazione ricevute siano firmate;
- **`<KeyDescriptor>`:** elemento 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 (cfr.[SAML-Metadata], sez. 2.4.1.1);
- **`<NameIDFormat>`:** elemento che indica i formati di **NameID** supportati (NameID è l'elemento utilizzato nelle richieste e risposte SAML per identificare il *subject* cui si riferisce un'asserzione): può adottare il formato di un indirizzo e-mail, di un *entity* identifier *SAML* o altri formati ancora, oppure rimanere non specificato ("*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*") (cfr.[SAML-Core], sez. 8.3).
- **`<SingleSignOnService>`**: uno o più elementi (analogamente all'AssertionConsumerService del *Service Provider*) che specificano l'indirizzo del Single Sign-On Service (attributo **Location**) e il binding (attributo **Binding**, che può valere "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-REDIRECT" oppure "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST") utilizzato per comunicare mediante costrutti SAML con tale servizio.

I *metadata Identity Provider* saranno disponibili per tutte le entità SPID federate, ove non diversamente specificato nel registro SPID, attraverso l'interfaccia **IMetadataRetrive** alla URL <*dominioGestoreIdentita*>/*metadata* e saranno firmate dell'*Agenzia per l'Italia Digitale*.

1.3. FORNITORE DEI SERVIZI

Il *fornitore di servizi* denominato anche con il termine tecnico di *Service Provider* per la realizzazione dei profili SSO previsti, *SP-Initiated* Redirect/POST binding e POST/POST binding, deve mettere a disposizione le seguenti interfacce:

- **IAuthnResponse**: ricezione delle risposte di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei SAML metadata del *Service Provider* da parte dell'*Identity Provider*

1.3.1. SP METADATA

Le caratteristiche del *Service Provider* devono essere anch'esse definite attraverso metadati conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]), nei quali, in aggiunta quanto vale in generale, devono presenti le seguenti informazioni:

- **`<EntityDescriptor>` deve riportare i seguenti attributi:**
  - **entityID**: indicante l'identificativo univoco (un URI) dell'entità;
  - **cacheDuration**: indicante la durata (in millisecondi) della cache di un file di metadati; un documento di metadati letto e memorizzato localmente ha validità fino alla scedenza di tale periodo di tempo; successivamente è necessario richiedere nuovamente il file alla relativa entità.
- **`<SPSSODescriptor>`** 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");
  - **AuthnRequestSigned**: attributo con valore booleano che esprime il requisito che le richieste di autenticazione ricevute siano firmate;
- **`<AssertionConsumerService>`:** elemento indicante il servizio (in termini di URL e relativo binding "HTTP POST") a cui contattare il *Service Provider* per l'invio di risposte SAML;
- **`<AttributeConsumingService>`**: elemento che descrive i servizi esposti dal *Service Provider*, in termini di indice posizionale, nome e attributi richiesti per l'accesso.

I *metadata Services Provider* saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL < *dominioServiceProvider* >/*metadata* e saranno firmate dell' *Agenzia per l'Italia Digitale.*

2 REGOLE TECNICHE PER IL GESTORE DI ATTRIBUTI QUALIFICATI

2.1. INTRODUZIONE

Un *Gestore di attributi qualificati,* nel seguito indicato anche con il termine tecnico *Attribute Authority* , 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*.

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.

2.2. SCENARIO DI INTERAZIONE

	Descrizione	Interfaccia	SAML	Binding
1	**La Service Provider invia all'Attribute Authority una richiesta di attributi. Ciò avviene utilizzando il costrutto <AttributeQuery> della specifica SAML e interagendo mediante "SAML SOAP binding".**	**IAttributeQuery**	**<AttributeQuery>**	**SOAP Over HTTP**
2	**L'Authority Registry elabora la richiesta ricevuta.**	**-**	**-**	**-**

3	**La Attribute Authority risponde alla richiesta di attributi del Service Provider con una <Response> SAML contenente l'asserzione contenente a sua volta gli statement di attributo e interagendo mediante "SAML SOAP binding".**	**IAttributeQuery**	**<Response>**	**SOAP Over HTTP**

Tabella 2.1 AttributeRequest

2.3. SPECIFICHE DELLE INTERFACCE

Di seguito vengono esposte le specifiche delle interfacce dell'*Attribute Authority* riportanti

- Le caratteristiche delle asserzioni prodotte
- Le caratteristiche delle *AttributeQuery* e della *Response*
- Le caratteristiche del *binding*
- I metadati

2.3.1. CARATTERISTICHE DELLE ASSERZIONI

Le asserzioni prodotte dall'Autorità di attributo devono essere conformi allo standard SAML v2.0 (cfr. [SAML-Core])e rispettare le seguenti condizioni

- l'elemento <**Assertion**> deve avere attributi ***ID***, ***Version*** e ***IssueInstant*** oltre agli elementi <**Issuer**> e <**Subject**>;
- nell'elemento <**Subject**> deve essere presente l'elemento <**NameID**> atto a qualificare meglio il *subject* dell'asserzione: in particolare deve essere presente l'attributo ***Format*** avente valore "*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*", e l'attributo ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (per esempio un URI riconducibile all'*Attribute Authority* stessa);
- l'elemento <**Assertion**> deve contenere un elemento <**Conditions**> che ne determina i vincoli di validità temporale che deve essere limitata ad una durata di ore 24;
- l' elemento <**AttributeStatement**> deve contenere elementi di tipo <**Attribute**> (con attributo ***Name*** e i relativi elementi <**AttributeValue**>) in corrispondenza degli attributi richiesti, eventualmente codificati in formato *Base64* per permettere la trasmissione di valori strutturati;
- l'elemento <**AttributeStatement**> deve contenere un elemento <**Attribute**> relativo al codice fiscale del soggetto per cui si attestano i rimanenti attributi, avente <**Name**> attualizzato con l'identificatore "*CodiceFiscale*".
- l'elemento <**Assertion**> può eventualmente presentare l'elemento <**Advice**>, contenente altri elementi <**Assertion**> di cui è necessario fornire evidenza in forma originale in sede di risposta alla richiesta di attributo;

- l'elemento <**Assertion**> deve essere firmato dall'authority emittente; per cui deve essere presente l'elemento <**Signature**> apposto dall'entità emittente.

2.3.2. CARATTERISTICHE DELLE ATTRIBUTEQUERY E DELLA RESPONSE

2.3.2.1. ATTRIBUTEQUERY

Le caratteristiche che deve avere la <**AttributeQuery**> sono le seguenti:

- deve essere presente l'attributo ***ID*** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) o su una combinazione *origine* + *timestamp*;
- 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 richiesta, in formato UTC;
- deve essere presente l'attributo ***Destination***, a indicare l'indirizzo (URI reference) a cui è inviata la richiesta, cioè l'AttributeService della *Attribute Authority*;
- deve essere presente l'elemento <**Issuer**> a indicare l'***entityID*** dell'entità emittente (il *Service Provider*); qualora fosse necessario specificare insieme alla richiesta di attributi altre informazioni (per esempio il servizio richiesto in origine dall'utente al *Service Provider*), data la mancanza di opportune strutture all'interno della <**AttributeQuery**> e volendo evitare di estendere la specifica, il valore dell'elemento <**Issuer**> può essere ottenuto concatenando al valore dell'*issuer* vero e proprio tali informazioni in formato stringa separate dal carattere *"#";*
- deve essere presente l'elemento <**Subject**> a indicare il soggetto a cui si riferisce la richiesta di attributi, contenente l'elemento <**NameID**> e i relativi attributi ***Format*** e ***NameQualifier***;
- possono essere presenti uno o più elementi <**Attribute**>, il cui attributo ***Name*** indica lo specifico attributo di cui si vuole conoscere il valore;
- in ciascun elemento <**Attribute**> possono essere presenti uno o più elementi <**AttributeValue**> per richiedere la verifica che l'attributo abbia i valori specificati;
- deve essere presente l'elemento <**Signature**> apposto dall'entità emittente.

2.3.2.2. RESPONSE

- Le caratteristiche che deve avere la <**Response**> di risposta ad una richiesta di attributi sono le seguenti:
- deve essere presente l'attributo ***ID*** univoco, per esempio basato su un *Universally Unique Identifier* (UUID) (cfr. UUID) o su una combinazione origine + timestamp;
- 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) a cui è inviata la richiesta, cioè l'AttributeService del Service Provider;
- deve essere presente l'elemento <**Status**> a indicare l'esito (sotto-elemento <**StatusCode**>) della richiesta a cui si risponde;
- deve essere presente l'elemento <**`Issuer`**> a indicare l'*entityID* dell'entità emittente, cioè la *Attribute Authority* stessa;
- devono essere presenti uno o più elementi <**`Assertion`**> contenenti elementi <**`AttributeStatement`**>;

Per le asserzioni veicolate resta valido quanto già specificato nel paragrafo 2.3.1.

2.3.3. CARATTERISTICHE DEL BINDING

Il binding previsto per il trasporto di messaggi è il SAML SOAPbinding su http.

2.3.4. ATTRIBUTE AUTHORITY METADATA

Le caratteristiche dell'*Attribute Authority* devono essere definite attraverso metadati conformi allo standard SAMLv2.0 (cfr [SAML-Metadata) nei quali devono presenti le seguenti informazioni:

- **`<EntityDescriptor>`** deve riportare i seguenti attributi:
  - **entityID**: indicante l'identificativo univoco (un URI) dell'entità;
  - **cacheDuration**: indicante la durata (in millisecondi) della cache di un file di metadati; un documento di metadati letto e memorizzato localmente ha validità fino alla scedenza di tale periodo di tempo; successivamente è necessario richiedere nuovamente il file alla relativa entità.
- **`<AttributeAuthorityDescriptor>`** è l'elemento specifico che contraddistingue l'entità *Attribute Authority*; deve riportare il seguente attributo:
  - **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");
- <**`AttributeService`**>: uno o più elementi che specificano l'indirizzo dell'AttributeService (attributo Location) ed il binding utilizzato per comunicare con tale servizio (attributo Binding). A differenza di IdP e SP, in questo caso il binding utilizzato è SOAP (indicato dal valore "urn:oasis:names:tc:SAML:2.0:bindings:SOAP").

- <**AttributeProfile**>: enumerazione dei profili di rappresentazione di attributi supportati dall'entità (cfr.[SAML-Profile], sez. 8); nel caso specifico solo "basic" (cfr. [SAML-Profile], sez. 8.1).
- <**Attribute**>: gli attributi (nome e "friendly name") certificati dall'authority: "*job*", "*role*", "*dept*", "*salary*".

I *metadata Attribute Authority* saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL, ove non diversamente specificato nel registro SPID, <*dominioAttributiQualificati*>/*metadata* e saranno firmate dell'*Agenzia per l'Italia Digitale*

3 REGISTRO SPID

Il *Registro SPID,* nel seguito indicato anche con il termine *federation registry*, è il repository di tutte le informazioni relative alla entità certificatrici *(assertion party*) della federazione e costituisce il cardine del circolo di fiducia associata a SPID.

Tale circolo di fiducia si realizza per il tramite dell'intermediazione dell'*Agenzia per l'Italia Digitale*, terza parte garante, che, attraverso un processo di accreditamento dei *Gestori dell'identità digitali* (*Identity provider*) e dei *Gestori di attributi qualificati (Attribute authority)* che entreranno a far parte della federazione, garantisce i livelli standard di sicurezza previsti da SPID e preventivamente accettati da tutti i soggetti che intendono ad esso aderire.

L'evidenza di tale garanzia e dell'accettazione dei livelli di sicurezza stabiliti in SPID da parte delle entità certificatrici *(Identity Provider*, *Attribute Authority*) si sostanzia nella presenza delle stesse nel *Federation registry* gestito dell'*Agenzia per l'Italia Digitale*

Questo realizza una relazione di *trust* n-n tra tutti i soggetti partecipanti a SPID come definiti all'art.3 del DPCM 24 ottobre 2014..

3.1. CONTENUTI DEL REGISTRO

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

- **<AuthorityInfo>** entry del registro relativa ad una entità; a sua volta costituita da:
  - **<EntityId> :** identificatore SAML dell'entità;
  - **<Soggetto>:** denominazione del soggetto a cui afferisce l'entità della federazione;
  - **<AuthorityType>:** tipo di entità *(Identity Provider, Attribute Authority)*;
  - **<MetadataProviderURL>:** l'URL del servizio di reperimento metadati;
  - <**AttributeList>:** elenco di attributi certificabili dall'entità.

Lo schema XML relativo e quello riportato nel listato 3.1.

3.1.1. ACCESSO AL REGISTRO

L'accesso ai contenuti del registro avviene attraverso l'interfaccia **IRegistryAccess** in modalità http GET specificando una *query string* con i seguenti parametri:

1. "*entityId*": per selezionare la entry relativa ad una determinata *entityId*; si usi * come wildcard;
2. "*soggetto:* per selezionare la entry relativa ad un determinato soggetto; si usi * come wildcard;
3. "authorityT*ype*": per selezionare le entry relative ad una determinata categoria di entità (IdP, AA); si usi * come wildcard,

4. "*attributeType*": per selezionare le entry relative ad entità in grado di certificare un determinato attributo qualificato; si usi * come wildcard,

```
<?xml version="1.0" encoding="UTF-8"?>
- <schema elementFormDefault="qualified" xmlns:tns="http://www.agid.gov.it/spid"
targetNamespace="http://www.agid.gov.it/spid"
xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns="http://www.w3.org/2001/XMLSchema">
    <element type="tns:FederationRegistryType" name="FederationRegistry"/>
  - <complexType name="FederationRegistryType">
    - <sequence>
        <element type="tns:AuthorityInfoType" name="AuthorityInfo"
          maxOccurs="unbounded" minOccurs="0"/>
      </sequence>
    </complexType>
  - <complexType name="AuthorityInfoType">
    - <sequence>
        <element type="anyURI" name="EntityID" maxOccurs="1"
          minOccurs="1"/>
        <element type="string" name="IdSoggetto" maxOccurs="1"
          minOccurs="1"/>
        <element type="tns:entityType" name="Type" maxOccurs="1"
          minOccurs="1"/>
        <element type="anyURI" name="MetadataProviderURL" maxOccurs="1"
          minOccurs="1"/>
        <element type="tns:attributeListType" name="AttributeList"
          maxOccurs="1" minOccurs="1"/>
      </sequence>
    </complexType>
  - <complexType name="attributeListType">
    - <sequence>
        <element type="tns:attributeType" name="Attribute"
          maxOccurs="unbounded" minOccurs="1"/>
      </sequence>
    </complexType>
  - <simpleType name="entityType">
    - <restriction base="xs:string">
        <enumeration value="IdP"/>
        <enumeration value="AA"/>
      </restriction>
    </simpleType>
  - <simpleType name="attributeType">
    - <restriction base="xs:string">
        <enumeration value="Ad1"/>
        <enumeration value="Ad2"/>
        <enumeration value="Ad3"/>
      </restriction>
    </simpleType>
</schema>
```

Listato 3.1 – federationRegistry.xsd

Il risultato sarà un file xml estrattoRegistro.xlm, firmato dall'*Agenzia per l'Italia Digitale*, costruito sullo schema definito al listato 3.1.

ACRONIMI

IdP	Identity Provider
AA	Attribute Authority
SP	Service Provider

GLOSSARIO

Identity Provider	gestore delle Identità
Attribute Authority	gestore degli attributi qualificati
Service Provider	gesture dei servizi
End user	Utente del servizio
User Agent	Sistema utilizzato dall'utente per l'accesso ai servizi. Di solito il browser per la navigazione in rete

RIFERIMENTI

OASIS	OASIS	https://www.oasis-open.org/
SAML	SAML Specifications	http://saml.xml.org/saml-specifications
SAML-Core	Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0	http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
SAMLAuthContext	Authentication Context for the OASIS Security Assertion Markup Language (SAML) V2.0	http://docs.oasis-open.org/security/saml/v2.0/saml-authn-context-2.0-os.pdf
SAML-Metadata	Metadata for the OASIS Security Assertion Markup Language (SAML) V2.0	http://docs.oasis-open.org/security/saml/v2.0/saml-metadata-2.0-os.pdf
SAML-TechOv	SAML Technical Overview	http://www.oasis-open.org/committees/download.php/20645/sstc-saml-tech-overview-2%200-draft-10.pdf