Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

REGOLAMENTO

RECANTE LE REGOLE TECNICHE (articolo 4, comma 2, DPCM 24 ottobre 2014)

Visto il decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il Codice dell'amministrazione digitale, e, in particolare, l'articolo 64 che prevede l'istituzione del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese" (di seguito: SPID);

Visto il decreto del Presidente del Consiglio dei Ministri 24 ottobre 2014, pubblicato sulla Gazzetta Ufficiale n. 285 del 9 dicembre 2014 che definisce le caratteristiche di SPID, nonché i tempi e le modalità di adozione dello stesso da parte delle pubbliche amministrazioni e delle imprese, e, in particolare, l'articolo 4, comma 2;

Visto il decreto legislativo 30 giugno 2003, n. 196 e successive modificazioni, recante il Codice in materia di protezione dei dati personali;

Visto il Regolamento (UE) N. 910/2014 del Parlamento europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE, pubblicato nella Gazzetta ufficiale dell'Unione europea serie L 257 del 28 agosto 2014;

Sentito il Garante per la protezione dei dati personali;

l'Agenzia per l'Italia Digitale emana il seguente Regolamento.

1 REGOLE TECNICHE PER IL GESTORE DELL'IDENTITÀ DIGITALE

Le modalità di funzionamento del *Gestore dell'identità digitale,* 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 all'*Identity provider* opportuno 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** *(singleSignOnService)*: ricezione di richieste di autenticazione SAML;
- **IMetadataRetrieve**: permette il reperimento dei SAML *metadata* dell'*Identity Provider*

Interfacce logiche del *Service Provider* coinvolte:

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

1.1. SCENARIO DI INTERAZIONE IN MODALITÀ SSO

Lo scenario completo è quello illustrato in Figura 1 - SSO SP-Initiated Redirect/POST binding nel caso di *SP-Initiated - Redirect/POST binding* e descritto dalla Tabella 1 - SSO SP-Initiated Redirect/POST binding.

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

Tabella 1 - SSO SP-Initiated Redirect/POST binding

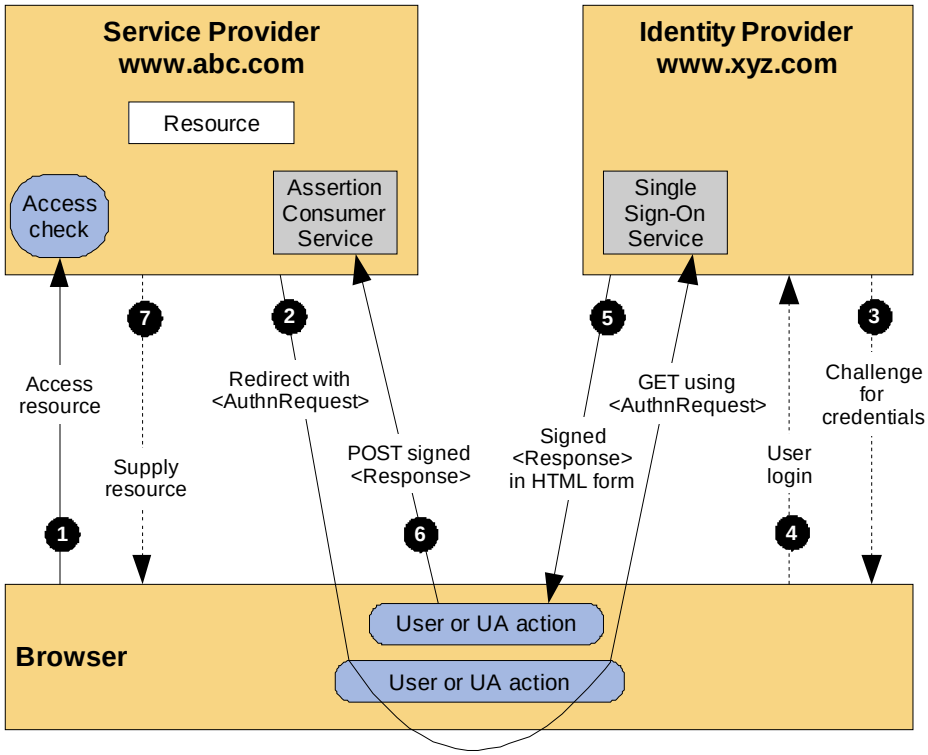

Figura 1 - SSO SP-Initiated Redirect/POST binding

1.2. SPECIFICHE DELLE INTERFACCE

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

- le caratteristiche dell'*asserzione* prodotta;
- le caratteristiche delle *AuthnRequest* e della relativa *Response*;
- le caratteristiche del *binding*;
- i *metadati*.

1.2.1. CARATTERISTICHE DELLE ASSERZIONI

L'*asserzione* prodotta dall'*Identity Provider* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

L'*asserzione* deve avere le seguenti caratteristiche:

- 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: "2008-03-13T18:04:15.531Z");
- deve essere presente l'elemento **<Subject>** a referenziare il soggetto che si è autenticato in cui devono comparire:
  - l'elemento <**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:nameid-format:transient*" (cfr. SAMLCore, sez. 8.3);
    - ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Identity Provider* stesso);
  - l'elemento <**SubjectConfirmation**> contenente l'attributo
    - ***Method*** riportante il valore "*urn:oasis:names:tc:SAML:2.0:cm:bearer*"

    e l'elemento:
    - <**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:nameid-format:entity*";
- deve essere presente l'elemento <**Conditions**> in cui devono essere presenti gli attributi:
  - ***NotBefore***,
  - ***NotOnOrAfter***);

  e l'elemento:

- <**AudienceRestriction**> riportante a sua volta l'elemento <**Audience**> attualizzato con l'*entityID* del *ServiceProvider* 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. *urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1*);
- 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;
- 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;
- 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.

```
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
    ID="_27e00421b56a5aa5b73329240ce3bb832caa"
    IssueInstant="2015-01-29T10:01:03Z"
    Version="2.0" >
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ……</ds:Signature>
    <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">spididp.it</saml:Issuer>
      <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/ Location_0"
          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>
                    urn:oasis:names:tc:SAML:2.0:ac:classes: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>
      </saml:AttributeStatement>
</saml:Assertion>
```

Listato 1 - Asserzione di autenticazione

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

1.2.2.1. AUTHNREQUEST

L'*authnrequest* deve avere le seguenti caratteristiche:

- 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: "2008-03-13T18:04:15.531Z");
  - 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;
  - 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 <**AttributeConsumingService** > 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 al precedente attributo (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**> può essere opzionalmente 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:1.1:nameid-format:unspecified*" (cfr. SAMLCore, sez. 8.3);
    - ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (URI);
- 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 il relativo attributo ***AllowCreate***, se presente, valorizzato a "*true*" e l'attributo ***Format*** valorizzato come "*urn:oasis:names:tc:SAML:2.0:nameid-format:transient*";
- 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.
- 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 caso dell'elemento <**RequestedAuthnContext**>, questa informazione si riflette sulle tipologie di meccanismi utilizzabili dall'*Identity Provider* ai fini dell'autenticazione dell'utente. L'esempio di <**RequestedAuthnContext**> riportato nel Listato 2 - RequestedAuthnContext fa riferimento a una "*authentication context* class" di tipo "*SpidL2*" o superiore.

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

Listato 2 - 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 (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- 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.

```
<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:// spidIdp.spidIdpProvider.it "
  AssertionConsumerServiceURL="http://spidSp.spidSpProvider.it"
  ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    AttributeConsumingServiceIndex="1">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
    <saml:Issuer
          NameQualifier=" http://spid-sp.it"
          Format=" urn:oasis:names:tc:SAML:2.0:nameid-format:entity " >
            SPID-sp-test
      </saml:Issuer>
    <samlp:NameIDPolicy
          Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient" />
      <samlp:RequestedAuthnContext
          Comparison="exact">
          <saml:AuthnContextClassRef>
              urn:oasis:names:tc:SAML:2.0:ac:classes:SpidL1
            </saml:AuthnContextClassRef>
    </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Listato 3 - AuthnRequest

1.2.2.2. RESPONSE

Le caratteristiche che deve avere la risposta inviata dall'*Identity Provider* al *Service Provider* a seguito di una richiesta di autenticazione sono le seguenti:

- nell' elemento <**Response**> devono essere presenti i seguenti attributi:
  - 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'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 (cfr. [SAML-Core] par. 3.2.2.1 e ss.) comprendente il sotto-elemento <**StatusCode**> ed opzionalmente i sotto-elementi <**StatusMessage**> <**StatusDetail**> (cfr [SPID-TabErr]);
- 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 assumere 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;
- 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 (cfr [SAML-Core] cap5) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore.

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

```
<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">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ……</ds:Signature>
    <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>
    <samlp:Status>
      < samlp:StatusCode
            Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
     <saml:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
            ……..
      </saml:Assertion>
</samlp:Response>
```

Listato 4 - Response (AuthnRequest)

1.2.2. CARATTERISTICHE DEL BINDING

1.2.2.1. 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. 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;
3. "***SigAlg***": identifica l'algoritmo usato per la firma 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; 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 5 - http redirect query string

1.2.2.2. 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 6 - 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 1.8 (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
zYW1sOkFzc2VydGlvbj48L3NhbWxPg==">
 <input type="hidden" name="RelayState"″
 value="s28d91a26bd4d60f47a49913300faf7631bf3140e9">
 <input type="submit" value="Go"/>
 </form>
 </body>
</html>
```

Listato 7 - Risposta http POST binding

1.2.2.3. 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* (*Identity Provider* e *Attribute Authority*), le *Relying Party* (*Service Provider*) e lo *user agent*. In ambito SPID si rende obbligatorio l'impiego di TLS nella versione più recente disponibile.

1.2.2.4. IDP METADATA

Le caratteristiche dell'*Identity provider* devono essere definite attraverso *metadata* conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]), e rispettare le condizioni di seguito indicate:

- nell'elemento **<EntityDescriptor>** devono essere presenti i seguenti attributi:
  - ***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;

al suo interno 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 (cfr.[SAML-Metadata], sez. 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 (cfr.[SAML-Metadata], sez. 2.4.1.1);
- l'elemento **<NameIDFormat>** riportante l'attributo:
  - ***format***, indicante il formato "*urn:oasis:names:tc:SAML:2.0:nameid-format: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";

opzionalmente possono essere presenti:

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

- deve essere l'elemento <**Signature**> riportante la firma sui *metadata* . La firma deve essere prodotta secondo il profilo specificato per SAML (cfr. [SAML-Metadata] cap3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- 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.

```
<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://spidIdp.idpProvider.it">
      <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:NameIDFormat>
                urn:oasis:names:tc:SAML:2.0:nameid-format:transient
          </md:NameIDFormat>
          <md:SingleSignOnService
              Location="https://spidIdp.idpProvider.it/redirect-Post-saml2sso"
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
          <md:SingleSignOnService
              Location="https://spidIdp.idpProvider.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>
```

Listato 8 - Metadata IdP

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

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. REGOLE DI PROCESSAMENTO DELLA <RESPONSE>

Alla ricezione <**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 assertion consuming service URL a cui la <**Response**> è pervenuta;
  - l'attributo ***NotOnOrAfter*** non sia scaduto;
  - l'attributo ***InResponseTo*** riferisca correttamente all'ID della <**AuthnRequest**> di 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 esser valida in base dell'attributo ***NotOnOrAfter*** dell'elemento <**SubjectConfirmationData**> presente nell'asserzione stessa.

1.3.2. SP METADATA

Le caratteristiche del *Service Provider* devono essere definite attraverso metadata conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]), e rispettare le condizioni di seguito indicate:

- nell'elemento **<EntityDescriptor>** devono essere presenti i seguenti attributi**:**
  - **entityID**: indicante l'identificativo univoco (un URI) dell'entità;
- deve 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 (cfr.[SAML-Metadata], sez. 2.4.1.1);
- deve essere l'elemento <**Signature**> riportante la firma sui *metadata* . La firma deve essere prodotta secondo il profilo specificato per SAML (cfr. [SAML-Metadata] cap3) 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'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:*** 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, riportanti i seguenti attributi:
  - ***index*** che può 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'atrtibuto ***isDefault*** posto al valore true**;**

- deve essere presente uno o più 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 authReq mediante l'attributo **AttributeConsumingServiceIndex** dell'elemento <**AuthnRequest**>;
  - l'elemento <**ServiceName**>, riportante l'identificatore dell'i-esimo set minimo di attributi necessari[1] per l'autorizzazione all'acceso;
  - uno o più elementi di tipo <**RequestedAttribute**>, ciascuno di essi costituente la lista degli attributi associati all'i-esimo servizio;

- 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] 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.

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*. L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.

1.4. ELENCO DEGLI ATTRIBUTI E MESSAGGI DI ERRORE

L'elenco degli attributi certificabili ed i messaggi di anomalia relativi agli scambi SAML sono descritti nelle relative tabelle pubblicate presso il sito dell' *Agenzia per l'Italia Digitale*.

```
<md:EntityDescriptor xmlns:md = "urn:oasis:names:tc:SAML:2.0:metadata"
    entityID="https:// spidSP.serviceProvider.it">
      <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">
      <md:KeyDescriptor use="signing"> ….. </md:KeyDescriptor>
      <md:AssertionConsumerService
        index="0"
        Location="https:// spidSP.serviceProvider.it /Location_0"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AssertionConsumerService
        index="1"
        Location="https:// spidSP.serviceProvider.it /Location_1"
        Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
      <md:AttributeConsumingService index="0">
          <md:ServiceName xml:lang="it">set0</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" >set1</md:ServiceName>
          <md:RequestedAttribute Name="name"/>
          <md:RequestedAttribute Name="familyName"/>
          <md:RequestedAttribute Name="fiscalNumber"/>
          <md:RequestedAttribute Name="email"/>
      </md:AttributeConsumingService>
    </md:SPSSODescriptor>
</md:EntityDescriptor>
```

Listato 9 - Metadata SP

2 REGOLE TECNICHE PER IL GESTORE DI ATTRIBUTI QUALIFICATI

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.

2.1. 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, interagendo mediante "SAML SOAP binding".	IAttributeQuery	<Response>	SOAP Over HTTP

Tabella 2 - AttributeRequest

2.2. 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.

2.2.1. CARATTERISTICHE DELLE ASSERZIONI

Le asserzioni prodotte dall' *Attribute Authority* devono essere conformi allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

L'*Asserzione* deve avere le seguenti caratteristiche:

- 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: "2008-03-13T18:04:15.531Z");
- deve essere presente l'elemento **<Subject>** a indicare il soggetto a cui si riferiscono gli attributi in cui deve comparire:
  - l'elemento <**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:1.1:nameid-format:unspecified*" (cfr. SAMLCore, sez. 8.3);
    - ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Attribute Authority*);
- l'elemento <**Issuer**> a indicare l'*entityID* dell'*Attribute Authority* emittente (attualizzato come l'attributo ***entityID*** presente nei corrispondenti AAA *metadata*.) con l'attributo ***Format*** riportante il valore "*urn:oasis:names:tc:SAML:2.0:nameid-format:entity*";
- deve essere presente l'elemento <**Conditions**> in cui devono essere presenti gli attributi:
  - ***NotBefore***,
  - ***NotOnOrAfter***;

e l'elemento:

- <**AudienceRestriction**> riportante a sua volta l'elemento <**Audience**> attualizzato con l'*entityID* del *ServiceProvider* per il quale l'asserzione è emessa;

- deve essere presente l'elemento <**AttributeStatement**> riportante gli attributi certificati dall'*Attribute Authority*. Tale elemento dovrà comprendere uno o più elementi di tipo <**Attribute**>;
- un elemento di tipo <**Attribute**> relativo ad un attributo certificato dovrà comprendere:
  - l'attributo ***Name*** attualizzato con identificativi di attributo definiti nella tabella attributi SPID (cfr. SPID - Tabella attributi);
  - uno o più elementi <**AttributeValue**> ciascuno riportante l'attributo ***Type*** (cfr. SPID - Tabella attributi) e attualizzato con il valore assunto dall'attributo;
- 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 <**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.

```
<ns2:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion"
  ID="_27e00421b56a5aa5b73329240ce3bb832caa"
  IssueInstant="2015-01-29T10:01:03Z"
  Version="2.0" >
    <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> .....</ds:Signature>
      <ns2:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
          spidIAA.spidiAADomain.it
      </ns2:Issuer>
    <ns2:Subject>
        <ns2:NameID
          Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"
          NameQualifier= "http://spidIAA.spidiAADomain.it">
            TINIT-BNLFNC68E28F205T
        </ns2:NameID>
    </ns2: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>
    <ns2:AttributeStatement xmlns:xsi="http://www.w3.org/2001/XMLSchemainstance" >
      <ns2:Attribute Name="NomeAttributo">
        <ns2:AttributeValue xsi:type="xsi:string" >ValoreAttributo</ns2:AttributeValue>
      </ns2:Attribute>
    </ns2:AttributeStatement>
</ns2:Assertion>
```

Listato 10- Asserzione di attributo

2.2.2. CARATTERISTICHE DELLE ATTRIBUTEQUERY E DELLA RESPONSE

Il protocollo *attributeQuery* previsto per l'*Attribute Authority* deve essere conforme allo standard SAML v2.0 (cfr. [SAML-Core]) e rispettare le condizioni di seguito indicate.

2.2.2.1. ATTRIBUTEQUERY

L' *attributeQuery* deve avere le seguenti caratteristiche:

- nell' elemento <**`AttributeQuery`**> 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*;
  - 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;
- 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'identificatore univoco del *Service Provider* emittente attualizzato come l'attributo ***entityID*** riportato nel corrispondente *SP metadata*.. L'elemento deve riportare l'attributo ***Format*** attualizzato con il valore "urn:oasis:names:tc:SAML:2.0:nameid-format:entity";
- deve essere presente l'elemento **<Subject>** a referenziare il soggetto a cui si riferisce la richiesta di attributo, in cui deve comparire:
  - l'elemento <**NameID**> attualizzato con il codice fiscale del soggetto (cfr. Tabella attributi SPID), in cui dee essere presente l'attributo:
    - ***Format*** che deve assumere il "*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*" (cfr. SAMLCore, sez. 8.3);
    - ***NameQualifier*** che qualifica il dominio a cui afferisce tale valore (URI riconducibile all'*Attribute Authority*);
- deve essere presente uno o più elementi <**Attribute**>, il cui attributo ***Name*** indica lo specifico attributo di cui si vuole conoscere il valore (cfr. SPID - Tabella attributi);
- 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**> 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.

```
<samlp:AttributeQuery 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=" spidIAA.spidiAADomain.it ">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </ds:Signature>
   <saml:Issuer
        Format=" urn:oasis:names:tc:SAML:2.0:nameid-format:entity " >
          https:// spidSP.spidSPDomain.it
      </saml:Issuer>
   <saml:Subject>
        <saml:NameID
          NameQualifier= "http://spidIAA.spidAADomain.it"
          Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">
            TINIT-BNLFNC68E28F205T
        </saml:NameID>
   </saml:Subject>
      <saml:Attribute
          Name="NomeAttributo"/>
</samlp:AttributeQuery >
```

Listato 11 - AttributeQuery

2.2.2.2. RESPONSE

Le caratteristiche che deve avere la risposta inviata dall' *Attribute Authority* al *Service Provider* a seguito di una richiesta di attributi sono le seguenti:

- nell' elemento <**Response**> devono essere presenti i seguenti attributi:
  - 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 <**Issuer**> a indicare l'identificatore univoco dall' *Attribute Authority* emittente attualizzato come l'attributo ***entityID*** riportato nel corrispondente *AA metadata*.,. L'elemento deve riportare l'attributo ***Format*** attualizzato

con il valore "urn:oasis:names:tc:SAML:2.0:nameid-format:entity";

- deve essere presente l'elemento <**Status**> a indicare l'esito della *attributeQuery* 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**> <**StatusDetail**> (cfr [SPID-TabErr]);
- deve essere presente l'elemento <**Assertion**> come specificato al paragrafo 2.3.1, contenenti elementi <**AttributeStatement**> relativi agli attributi richiesti;
- può 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.

```
<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://spidIAA.spidiAADomain.it">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ……</ds:Signature>
    <saml:Issuer
  Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
            https:// spidAA.spidAADomain.it
      </saml:Issuer>
    <samlp:Status>
      <samlp:StatusCode
            Value="urn:oasis:names:tc:SAML:2.0:status:Success" />
    </samlp:Status>
     <saml:Assertion xmlns:ns2="urn:oasis:names:tc:SAML:2.0:assertion">
            ……
      </saml:Assertion>
</samlp:Response>
```

Listato 12 - Response (AuthnRequest)

2.2.3. CARATTERISTICHE DEL BINDING

Il binding previsto per il trasporto di messaggi è il SAML SOAPbinding su http(cfr. [SAML-Bin] par. 3.2.).

2.2.4. ATTRIBUTE AUTHORITY METADATA

Le caratteristiche dell'*Attribute Authority* devono essere definite attraverso *metadata* conformi allo standard SAMLv2.0.(cfr. [SAML-Metadata]), e rispettare specificatamente le condizioni di seguito indicate:

- nell'elemento **<EntityDescriptor>** devono essere presenti i seguenti attributi:
  - ***entityID***: indicante l'identificativo univoco (un URI) dell'entità;
- l'elemento **<AttributeAuthorityDescriptor>** specifico che contraddistingue l'entità di tipo *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");

inoltre al suo interno 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 (cfr.[SAML-Metadata], sez. 2.4.1.1);
- uno o più elementi <**AttributeService**> indicante il servizio a cui contattare l'*Attribute Authority* riportante i seguenti attributi:
  - ***Binding*** posto al valore "*urn:oasis:names:tc:SAML:2.0:bindings:SOAP*";
  - ***Location*** url endpoint del servizio per la ricezione delle richieste;
- l'elemento **<NameIDFormat>** riportante l'attributo:
  - ***format***, indicante il formato "*urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified*" come quello supportato per l'elemento di <**NameID>** utilizzato nelle richieste e risposte SAML per identificare il *subject* cui si riferisce un'asserzione;
- <**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);
- uno o più elementi <**Attribute**> riportanti gli attributi:
  - ***Name*** riportante l'identificativo dell'attributo;
  - ***NameFormat*** riportante il format dell'attributo;

- deve essere l'elemento <**Signature**> riportante la firma sui *metadata* . La firma deve essere prodotta secondo il profilo specificato per SAML (cfr. [SAML-Metadata] cap3) utilizzando chiavi RSA almeno a 1024 bit e algoritmo di digest SHA-256 o superiore;
- 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*

- `<OrganizationURL>` dell'organizzazione a cui l'entità afferisce; riportante in modalità language-qualified la url istituzionale dell'organizzazione.

I *metadata Attribute Authority* saranno disponibili per tutte le entità SPID federate attraverso l'interfaccia **IMetadataRetrive** alla URL *<dominioAttributiQualificati>/metadata,* ove non diversamente specificato *nel Registro SPID,* e saranno firmate dell'*Agenzia per l'Italia Digitale.* L'accesso deve essere effettuato utilizzando il protocollo TLS nella versione più recente disponibile.

```
<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=" https:// spidAA.spidAAProvider.it">
      <ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#"> ..... </ds:Signature>
      <md:AttributeAuthorityDescriptor
        protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <md:KeyDescriptor use="signing"> .....</md:KeyDescriptor>
          <md:AttributeService
            Location=" https:// spidAA.spidAAProvider.it/AAService"
            Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"/>
          <md:NameIDFormat>
              urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
          </md:NameIDFormat>
          <md:AttributeProfile>
              urn:oasis:names:tc:SAML:2.0:attrname-format:basic
          </md:AttributeProfile>
          <saml:Attribute Name="IdentificativoAttributo1"/>
          <saml:Attribute Name="IdentificativoAttributo2"/>
          <saml:Attribute Name=" IdentificativoAttributo3"/>
      </md:AttributeAuthorityDescriptor>
</md:EntityDescriptor>
```

Listato 13 - Metadata AA

2.3. ELENCO DEGLI ATTRIBUTI E MESSAGGI DI ERRORE

L'elenco degli attributi certificabili ed i messaggi di anomalia relativi agli scambi SAML sono descritti nelle relative tabelle pubblicate presso il sito dell' *Agenzia per l'Italia Digitale.*

3 REGISTRO SPID

Il *Registro SPID* è il repository di tutte le informazioni relative alla entità 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'identità 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 già 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 entità aderenti (gestori dell'identità digitale, gestori degli attributi qualificati e fornitori di servizi) si evidenzia nella presenza di tali entità nel *Registro SPID* gestito dall'Agenzia.

3.1. CONTENUTI DEL REGISTRO

Il *federation registry* 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;
  - **`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 entità 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 attività legate alla gestione delle convenzioni e della vigilanza sui soggetti del circuito SPID.

Il contenuto informativo della *federation registry* è in fruizione a tutte le entità appartenenti al circuito SPID ai fini della verifica della sussistenza di relazioni di trust nei confronti di entità terze (IdP, AA, SP) e del reperimento delle informazioni associate alla alle stesse. Il *Discovery Service* può anch'esso accedere al *federation registry* per utilizzarne i contenuti ai fini de attività di discovering.

3.1.1. ACCESSO AL REGISTRO

L'accesso ai contenuti del *federation registry* avviene in modalità REST attraverso l'interfaccia (risorsa) **IRegistry.** In particolare:

- l'accesso in consultazione ai contenuti del directory avviene attraverso il metodo ***http GET***

request

parametri *query string*:

- *entityId:*string per selezionare la entry relativa ad una determinata entityId; si usi * come wildcard;
- *soggetto:*string per selezionare la entry relativa ad un determinato soggetto; si usi * come wildcard;
- *authorityType:*string per selezionare le entry relative ad una determinata categoria di entità (IdP, AA); si usi * come wildcard,
- *attributeType:*string per selezionare le entry relative ad entità in grado di certificare un determinato attributo qualificato; si usi * come wildcard,

response

status: 200- OK

representation	application/xml
formato risposta	secondo lo schema riportato nel Listato 14 - federationRegistry.xsd firmata *xml signature* [XMLSig].

status: 400 - Bad request

status: 403 - Forbidden – User does not have privilege to read the resource

status 404 - Not Found

Per l'accesso al registro si rende obbligatorio l'impiego di TLS nella versione più recente disponibile.

3.1.1.1. ACCESSO AL REGISTRO IN MODALITA' LDAP

Insieme o in alternativa alla modalità di accesso al *federation registry* precedentemente descritta potrà essere fornita una interfaccia di accesso interrogabile secondo il protocollo LDAP. Questa seconda modalità di accesso sarà relativa allo stesso contenuto informativo e funzionante secondo le stesse logiche di accesso descritti per l'interfaccia REST. Le specifiche di tale interfaccia saranno rese note in un separato documento pubblicato sul sito dell'Agenzia per l'Italia Digitale.

```
<SCHEMA xmlns="http://www.w3.org/2001/XMLSchema"

    xmlns:xs="http://www.w3.org/2001/XMLSchema" targetNamespace="http://www.agid.gov.it/spid"
    xmlns:tns="http://www.agid.gov.it/spid" elementFormDefault="qualified">
        <import namespace="http://www.w3.org/2000/09/xmldsig#" schemaLocation="… "/>
        <import namespace="http://www.w3.org/2001/04/xmlenc#" schemaLocation="… "/>
        <element name="FederationRegistry" type="tns:FederationRegistryType"/>
        <complexType name="FederationRegistryType">
            <sequence>
                <element name="AuthorityInfo" type="tns:AuthorityInfoType"
                    minOccurs="0" maxOccurs="unbounded"/>
                </sequence>
        </complexType>
        <complexType name="AuthorityInfoType">
            <sequence>
                <element name="EntityID" type="anyURI" maxOccurs="1" minOccurs="1"/>
                <element name="IdSoggetto" type="string" maxOccurs="1" minOccurs="1"/>
                <element name="EntityType" type="tns:entity" maxOccurs="1" minOccurs="1"/>
                <element name="MetadataProviderURL" type="anyURI" maxOccurs="1" minOccurs="1"/>
                <element name="AttributeList" type="tns:attributeListType" maxOccurs="1" minOccurs="0"/>
            </sequence>
        </complexType>
        <complexType name="attributeListType">
            <sequence>
                <element name="Attribute" type="tns: qualifiedAttributeType "
                        minOccurs="1" maxOccurs="unbounded"/>
            </sequence>
        </complexType>
        <simpleType name="entity">
            <restriction base="xs:string">
            <enumeration value="IdP"/>
            <enumeration value="AA"/>
             <enumeration value="SP"/>
            </restriction>
        </simpleType>
        <simpleType name="qualifiedAttributeType">
            <restriction base="xs:string">
            <enumeration value="Ad1"/>
            <enumeration value="Ad2"/>
            <enumeration value="Ad3"/>
            </restriction>
        </simpleType>
 </schema>
```

Listato 14 - federationRegistry.xsd

4 TRACCIATURE

4.1. TRACCIATURE IDENTITY PROVIDER

Ai fini della tracciatura l'*Identity Provider* dovrà mantenere un *Registro delle transazioni* contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà rendere persistente per ogni transazione la tripla composta dell'identificativo dell'identità 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;**

4.2. TRACCIATURE 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 identità digitali le operazioni effettuate sui propri sistemi. A tal fine un *service provider* dovrà mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà 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;**

4.3. MANTENIMENTO TRACCIATURE

Le tracciature devono essere mantenute nel rispetto del codice della privacy sotto la responsabilità titolare del trattamento dell'Identity Provider. e l'accesso ai dati di tracciatura deve essere riservato a personale incaricato.

Al fine di garantire la confidenzialità potrebbero essere adottai meccanismi di cifratura dei dati o impiegati sistemi di basi di dati (DBMS) che realizzano la persistenza cifrata delle informazioni.

Per il mantenimento devono essere messi in atto meccanismi che garantiscono l'integrità e il non ripudio.

5 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
SAML-Bin	Bindings for the OASIS Security Assertion Markup Language (SAML) V2.0	http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-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
XMLSig	W3C XML Signature WG	http://www.w3.org/Signature/