AGID
Agenzia per l'Italia Digitale

spid

COME DIVENTARE SOGGETTI AGGREGATORI DI SERVIZI PUBBLICI

I Soggetti Aggregatori di servizi pubblici (nel seguito "Aggregatori") sono soggetti che offrono, tramite apposito servizio, a soggetti pubblici (nel seguito "Aggregati") la possibilità di rendere accessibili tramite credenziali SPID servizi online, individuando le attività necessarie a tale scopo.

L'Aggregatore, a seguito dell'iscrizione nel Registro SPID, può gestire in totale autonomia i rapporti con i soggetti Aggregati, nel rispetto della convenzione sottoscritta con AGID.

L'Aggregatore può gestire il sistema di autenticazione in modalità "*light*" e/o in modalità "*full*".

La modalità "*light*" è quella per la quale il Soggetto Aggregatore di servizi pubblici o privati garantisce l'attività di autenticazione tramite l'infrastruttura del Soggetto Aggregato, su cui è stata installata la soluzione fornita dall'Aggregatore. In questo caso, AgID rilascia un certificato di CA intermedia (*sub-CA*) che l'Aggregatore utilizza per generare certificati di sigillo elettronico per ciascun Aggregato.

La modalità "*full*" è quella per la quale il Soggetto Aggregatore di servizi pubblici o privati esegue l'attività di autenticazione tramite la propria infrastruttura. In questo caso, AgID rilascia direttamente un certificato di sigillo elettronico.

Il rilascio dei certificati elettronici è regolato dall'Avviso SPID №23.

Uno stesso Soggetto Aggregatore può operare sia in modalità "*full*" sia in modalità "*light*".

Le procedure da completare per l'adesione sono due, una tecnica e una amministrativa.

Procedura tecnica

Il sistema SPID si basa sul protocollo SAML2:

1. Consulta le regole tecniche, gli avvisi SPID e la tabella anomalie, con le indicazioni necessarie a guidarti durante l'implementazione di SPID e le linee guida interfacce e informazioni. Queste ultime hanno l'obiettivo di guidarti nell'utilizzo delle componenti grafiche necessarie a garantire la riconoscibilità di SPID tra gli utenti.

2. Implementa l'autenticazione con SPID sui tuoi servizi. Sul repository https://developers.italia.it/it/spid sono disponibili librerie per i diversi linguaggi di programmazione e risorse utili per l'integrazione ai quali puoi fare riferimento.

3. Elabora un metadata relativo ad un aggregato fittizio, per effettuare il collaudo finale, seguendo le indicazioni riportate nelle regole tecniche, nell'Avviso SPID №6 e nell'Avviso SPID №22.

4. **Accertati del corretto funzionamento della tua implementazione prima di richiedere ad AgID la verifica tecnica.** Verifica autonomamente la correttezza del metadata di cui al punto 3, usando lo *SPID Validator*, e la conformità della tua implementazione[1] ai requisiti tecnici, utilizzando in locale sia lo *SPID Validator* che lo ambiente di test (l'ambiente di test è anche disponibile online all'indirizzo https://idp.spid.gov.it). In particolare, occorre verificare il corretto funzionamento in relazione ad ognuno dei test indicati nel seguente documento SPID Quality Assessment Document. Per utilizzare l'ambiente di test online, occorre registrare il proprio metadata all'indirizzo https://idp.spid.gov.it/admin/databasesprecord/ Essendo l'ambiente di test online pubblico, i metadati registrati sono pubblicamente visibili. Per maggiori informazioni circa l'utilizzo dell'ambiente di test o per segnalare eventuali problemi fare riferimento al repository ufficiale GitHub.

5. Rendi disponibile il metadata di cui al punto 3 su una URL 'https' del tuo dominio e inserisci tra gli IdP del bottone "Entra con SPID" un ulteriore IdP del tool *SPID Validator*, il cui metadata è disponibile alla seguente URL: https://validator.spid.gov.it/metadata.xml.

   Compila e firma digitalmente in formato PAdES il modulo per l'Adesione a SPID e invialo a protocollo@pec.agid.gov.it e p.c. a spid.tech@agid.gov.it .

[1] SPID Validator non verifica che il metadata contenga quanto previsto specificatamente per i soggetti aggregatori nell'Avviso 19 e nel documento Struttura del metadata di test per soggetto aggregato.

6. AgID provvederà a verificare il metadata ricevuto e la correttezza dell'implementazione. Se necessario, saranno segnalate le modifiche necessarie a garantire il rispetto delle regole tecniche.

   Se AgID richiede delle modifiche dovrai ripetere la procedura a partire dal punto 3.

Procedura amministrativa

Completata la procedura tecnica, AgID invierà al referente amministrativo, indicato nel modulo di cui al punto 5 della procedura tecnica, la copia della convenzione e il modulo per la richiesta di emissione di certificato elettronico (CSR), in conformità con l'Avviso SPID №23.

La convenzione, il modulo e il CSR devono essere restituite, compilate e sottoscritte con firma elettronica qualificata, via PEC a protocollo@pec.agid.gov.it.

Entro pochi giorni la convenzione ti tornerà controfirmata dal Direttore Generale di AgID insieme al suddetto certificato elettronico.

Se non provvederai a restituire la convenzione firmata entro 30 giorni solari prendi immediati contatti con AgID per concordare altro termine, altrimenti i tuoi servizi saranno tolti dalla federazione e non saranno più accessibili con SPID.

Comunicazione dei metadata per gli Enti aggregati

A seguito della sottoscrizione della Convenzione da parte del Direttore Generale dell'AgID e della conseguente iscrizione nel Registro SPID il Soggetto Aggregatore può gestire in totale autonomia i rapporti con gli Aggregati, inviando ad AgID un solo metadata per ogni Aggregato secondo le seguenti modalità.

Verifica se hai già prodotto ed inviato ad AgID un metadata per un soggetto aggregato. In caso affermativo modifica[2] il metadata già presentato per

[2] Attenzione, se invii un nuovo metadata anziché modificare il precedente, andrai a sostituire l'ultimo al precedente con il risultato che i servizi precedenti non funzioneranno più! Modificando il metadata fai anche attenzione a non modificare l'entityID, non corrisponderebbe più a quanto contenuto nel certificato di firma delle asserzioni e vi sarebbero disservizi.

includere i nuovi servizi, altrimenti elabora un metadata come indicato nelle regole tecniche, nell'Avviso SPID №6 e nell'Avviso SPID №19.

Sigilla il metadata con la chiave privata afferente al certificato di sigillo elettronico rilasciato da AgID, se sei un Aggregatore "full" o se sei sia "full" che "light".

Se, invece, sei solo "light" genera, con la chiave privata afferente al certificato di CA intermedia (*sub-CA*) rilasciato da AgID, un certificato di sigillo elettronico a te intestato e utilizza la relativa chiave privata *esclusivamente* per sigillare i metadata da inviare ad AgID.

La comunicazione del metadata può essere effettuata esclusivamente i giorni lunedì, mercoledì e venerdì (se feriali) entro e non oltre le ore 15 con un'unica mail giornaliera da inviare a spid.techaggr@agid.gov.it, con oggetto "[Metadata Aggregatori]", contenente, *in un unico file ZIP in allegato:*

- un file XML per ogni metadata nuovo o aggiornato;
- un file JSON riepilogativo dei dati degli Aggregati interessati.

Un modello di esempio per il file JSON da compilare e allegare nel file ZIP è scaricabile da qui (file compresso); lo schema da seguire nel compilarlo è riportato in questa pagina.

Il nome dei file contenenti i metadata utilizza la seguente *naming convention*: il codice IPA (se SP pubblico) ovvero dalla P.IVA o, in alternativa, del codice fiscale (se SP privato) dell'**Aggregato**, seguito da *doppio underscore* "__", seguito dal codice IPA ovvero dal numero di partita IVA dell'**Aggregatore**, seguito dal suffisso "`.xml`".

Esempio di invio da Aggregatore con P.IVA 57575757575 del metadata:

- di un Aggregato privato con P.IVA 12345678901:

  `12345678901__57575757575.xml`

- di un Aggregato pubblico con codice IPA "`agid`":

```
agid__57575757575.xml
```

I nomi del file ZIP e del file JSON in esso contenuto utilizzano la seguente *naming convention*: "`md-aggr-`" seguito dal codice IPA ovvero dal numero di partita IVA dell'Aggregatore, seguito da "`_`", seguito dalla data in formato statunitense *AAAAMMGG*, seguito dal suffisso "`.zip`" e, rispettivamente, "`.json`".

Esempio di file ZIP inviato il 26 marzo 2020 da Aggregatore con numero di partita IVA 57575757575:

```
md-aggr-57575757575-20200326.zip
```

AgID provvederà a comunicare il metadata agli Identity Provider (IdP), dandone informazione all'Aggregatore e, tramite PEC, all'Aggregato.

Di norma, entro un giorno lavorativo[3], gli IdP provvedono al loro caricamento ed il tuo servizio sarà accessibile tramite SPID.

Supporto tecnico e amministrativo

Se hai bisogno di supporto nella fase tecnica e per i metadata puoi rivolgerti a spid.tech@agid.gov.it.

Se hai bisogno di supporto nella fase amministrativa e per la convenzione puoi rivolgerti a convenzioni.spid@agid.gov.it.

Riepilogo

I principali interventi tecnici che ti verranno chiesti

1. Interventi di implementazione del sistema SPID, utilizzando SAML2, nei propri applicativi web;

[3] Al massimo entro due giorni lavorativi.

2. Consegna di un metadata, come da regole tecniche e successivi avvisi, per la configurazione dei propri servizi presso gli IDP.

Le figure di riferimento necessarie per concludere il processo di adesione a SPID

1. Referente tecnico del Soggetto Aggregatore per tutte le attività di implementazione del sistema di autenticazione SPID;
2. Rappresentante legale per la firma della convenzione;
3. Referente amministrativo del Soggetto Aggregatore;
4. Referente amministrativo del Soggetto Aggregato.

Riferimenti

DPCM 24 ottobre 2014

Documentazione e regole tecniche

Avvisi

Linee guida interfacce e informazioni SPID per IdP e Sp

Repository Github Italia

Convenzione per soggetti aggregatori

Allegato alla Determinazione AGID №80/2018.

AGID
Agenzia per l'Italia Digitale

spid

Schema JSON per le comunicazioni tecniche tra AgID e altri soggetti in merito ai metadata degli SP SPID

Schema per la comunicazione agli IdP dei metadata di tutti gli SP da parte di AgID

Il file JSON con il quale l'Agenzia per l'Italia Digitale comunica agli IdP, con cadenza giornaliera, l'elenco dei metadata SAML per i SP oggetto di cambiamenti tecnici è un oggetto contenente i seguenti elementi, tutti *obbligatori*:

i. `dateTime` (string) — La data e l'ora (in fuso orario italiano) in cui il file JSON è preparato per l'invio da parte di AgID, secondo la sintassi "*YYYY-MM-DD*T*hh:mm:ss*".
ii. `metadata` (array) — Una lista non vuota di object, ciascuno relativo a un SP di cui comunicare l'azione.

Schema per la comunicazione ad AGID dei metadata degli SP aggregati da parte di un Soggetto Aggregatore

Con riferimento agli Avvisi SPID №19, №22, №23 e alla procedura per gli Aggregatori pubblicata sul sito dell'Agenzia per l'Italia Digitale, il file JSON con il quale gli Aggregatori comunicano ad AgID l'elenco dei metadata SAML per i propri Aggregati oggetto di cambiamenti tecnici è un oggetto contenente i seguenti elementi, tutti *obbligatori*:

iii. `aggregatorCode` (string) — Il numero di partita IVA (se ente di diritto privato) ovvero con il codice IPA (se Ente pubblico) del soggetto Aggregatore.
iv. `aggregatorName` (string) — La denominazione o ragione sociale completa dell'Aggregatore.
v. `entityID` (string) — L'`entityID` dell'Aggregatore, conforme all'Avviso SPID №19.
vi. `dateTime` (string) — La data e l'ora (in fuso orario italiano) in cui il file ZIP è preparato per l'invio ad AgID, secondo la sintassi "*YYYY-MM-DD*T*hh:mm:ss*".
vii. `metadata` (array) — Una lista non vuota di object, ciascuno relativo al soggetto Aggregato di cui comunicare l'azione.

Gli `entityID` di ciascun Aggregato, valorizzati dagli omonimi sotto-elementi all'interno dell'array `metadata`, sono anch'essi conformi all'Avviso SPID №19.

Componenti comuni dello schema

Gli oggetti JSON presenti nell'array `metadata` per ciascuno dei due tipi di file JSON sopra introdotti sono in numero di uno per ciascun SP e sono costituiti dai sotto-elementi elencati qui sotto. Tali sotto-elementi sono tutti *obbligatori*, salvo ove espressamente specificato:

1. `action` (string) — Verbo RESTful che consente di stabilire l'azione da intraprendere sul metadata corrispondente; è valorizzato dalle seguenti stringhe alternative:
   - `POST` — aggiunta di un metadata (subentro di un nuovo SP);
   - `PUT` — modifica di un metadata esistente (cambiamento dei servizi di un SP);
   - `DELETE` — rimozione di un metadata (esclusione del SP dalla federazione, ovvero interruzione della gestione di un Aggregato da parte di un Aggregatore); solo nel caso di tale valorizzazione, va omesso l'elemento, comunque facoltativo, `metadataUrl` (vedi sotto).

Si precisa che, nonostante la differenza semantica tra i due verbi `POST` e `PUT`, un scambio fra i due non deve risultare in un rifiuto nell'accettazione del JSON. In particolar modo, un metadata elencato con verbo `POST` a fronte di una pre-esistente versione dello stesso, risulta nell'aggiornamento del metadata esistente (come per effetto di un verbo `PUT`) e viceversa.

2. `entityCode` (string) — Il numero di partita IVA o, in alternativa, il codice fiscale, qualora il SP sia ente di diritto privato; il codice IPA, qualora il SP sia un Ente pubblico.
3. `entityID` (string) — L'`entityID` del SP.
4. `isPrivate` (boolean) — Booleano **vero**, qualora il SP sia un ente di diritto privato; **falso**, qualora il SP sia un Ente pubblico.
5. `metadataFilename` (string) — Il nome del file XML del metadata del SP (*senza* alcun percorso di filesystem né URL), e la cui *naming convention* rispetta la procedura indicata sul sito di AgID per tali file.
6. `metadataUrl` (string, *facoltativo*) — URL con schema HTTPS afferente al mittente del JSON, ove questo rende disponibile online il metadata del SP al destinatario.

Infine, anche se non necessario per la conformità del JSON allo schema del W3C, si consiglia di rispettare le seguenti indicazioni sintattiche aggiuntive:

- un elemento per riga di testo (incluse le parentesi di chiusura e apertura), ad eccezione di quelli di tipo `object` e `array`, per i quali i loro sotto-elementi saranno anch'essi in righe separate;
- adottare carattere di *newline* compatibile con sistemi Windows (cioè carattere "`\r\n`", cioè `0x0D0A` esadecimale);
- rispettare l'ordinamento degli elementi come elencati nel presente schema.

Segue un esempio di metadata json che un Aggregatore identificato da un numero di partita IVA `57575757575` invia ad AgID le informazioni circa:

- l'aggiunta di un Comune aggregato, identificato dal codice IPA `c_X000`;
- la modifica dei servizi di un Aggregato privato identificato tramite la P.IVA `12345678901`;
- l'interruzione della gestione di un'Unione di Comuni, identificato dal codice IPA `ucYYY`.

```
{
 "aggregatorCode": "57575757575",
 "aggregatorName": "Ragione sociale dell'Aggregatore",
 "entityID": "https://id.aggregatore/",
 "dateTime": "2020-03-27T17:24:16",
 "metadata":[
       {
             "action": "POST",
             "entityCode": "c_X000",
             "entityName": "Comune di XXXXXXXX",
             "entityID": "https://id.aggregatore/id.aggr/1",
             "isPrivate": false,
             "metadataFilename": "c_X000_57575757575.xml",
             "metadataUrl": "https://sito-
aggregatore/percorso/al/metadata/c_X000__57575757575.xml"
       },
       {
             "action": "PUT",
             "entityCode": "12345678901",
             "entityName": "Ragione sociale dell'Azienda",
```

```
            "entityID": "https://id.aggregatore/id.aggr/2",
            "isPrivate": true,
            "metadataFilename": "12345678901_57575757575.xml",
            "metadataUrl": "https://sito-
aggregatore/percorso/al/metadata/12345678901__57575757575.xml"
      },
      {
            "action": "DELETE",
            "entityCode": "ucYYY",
            "entityName": "Unione dei Comuni di YYYYYYYY",
            "entityID": "https://id.aggregatore/id.aggr/3",
            "isPrivate": false,
            "metadataFilename": "ucYYY__57575757575.xml"
      }
 ]
}
```

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

ATTENZIONE

gli Avvisi pubblicati alla pagina:
https://www.agid.gov.it/index.php/it/piattaforme/spid/avvisi-spid
contengono integrazioni alle presenti regole tecniche, si raccomanda di prenderne visione e applicarle.

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

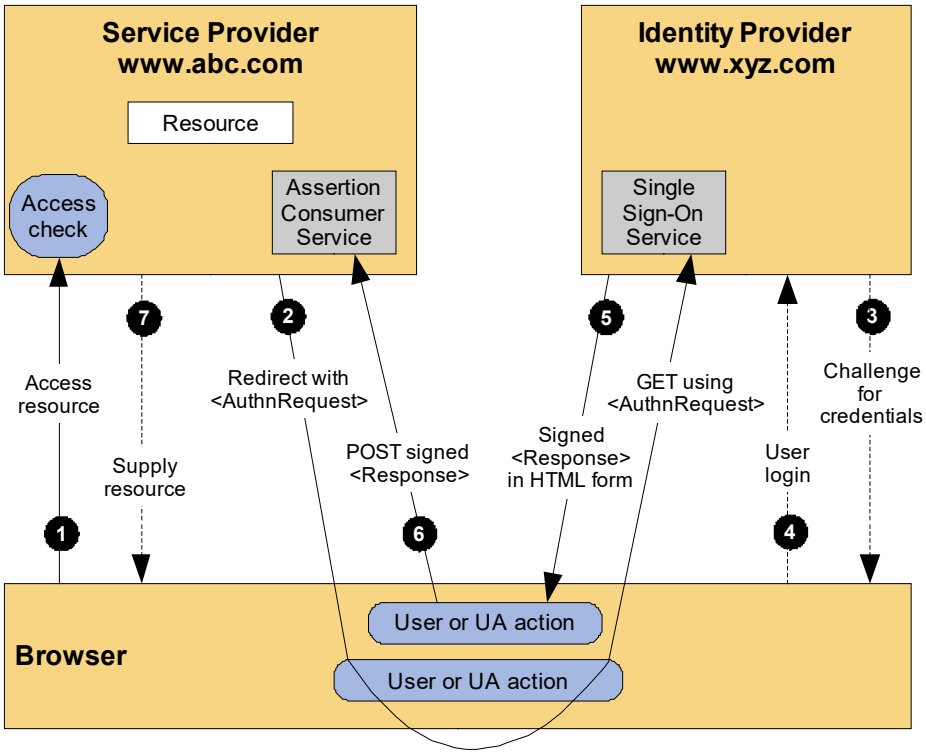

Figura 1 - SSO SP-Initiated Redirect/POST binding

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'*AssertionConsumerService*URL 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
zYW1sOkFzc2VydGlvbj48L3NhbWxwOlJlc3BvbnNlPg==">
 <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.

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

[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.

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/

Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri

spid

SPID – SISTEMA PUBBLICO PER L'IDENTITA' DIGITALE

Avviso nr 6
Data 29/07/2016

NOTE SUL DISPIEGAMENTO DI SPID PRESSO I GESTORI DEI SERVIZI

SOMMARIO

1 INTRODUZIONE

Il presente avviso ha lo scopo di fornire, attraverso un esempio rappresentativo, un riferimento per la configurazione dei sistemi afferenti ai gestori di servizi in ambito SPID, nel caso generale in cui questi siano enti il cui dispiegamento può essere distribuito geograficamente su vari siti di erogazione.

I formati previsti da SAML consentono di definire, nel file di configurazione (*metadata*) di un gestore di servizi (*service provider*), diversi punti di erogazione dei servizi (*assertionConsumerServer*). Questa flessibilità consentita dal SAML standard, recepita dal profilo di interoperabilità SPID, costituisce un elemento di strutturazione del file di configurazione che consente di evitare frammentazione nelle informazioni afferenti la stessa entità, con conseguente eliminazioni di ridondanze, semplificazione della manutenzione dei dati di configurazione e facilità nel dispiegamento dei sistemi.

2 ESEMPIO DI DISPIEGAMENTO DI UN GESTORE DI SERVIZI.

I siti di erogazione dei gestori dei servizi possono essere costituiti da nodi ospitanti singoli servizi oppure nodi dai quali vengono erogati una pluralità di servizi.

Un *nodo singolo* è un sistema finalizzato all'erogazione di un singolo servizio che integra al proprio interno componenti per la gestione dei profili utente e per la gestione degli accessi. Un esempio di nodo singolo potrebbe essere quello di un portale istituzionale o tematico.

Un *nodo cluster* è un sistema che mette a disposizione un insieme di servizi diversi. Il criterio di aggregazione di questi servizi può ad esempio essere basato sulla strutturazione interna dell'ente, esempio servizi erogati dallo stesso dipartimento oppure sulla responsabilità della gestione operativa dei servizi, esempio - nel caso di enti che si avvalgono di diversi fornitori – servizi erogati da uno stesso fornitore. La caratteristica di un *nodo cluster* è quella di avere un'infrastruttura condivisa per la gestione dei profili utente e per la gestione degli accessi, che operi come gateway unico verso i sistemi di autenticazione e di certificazione esterni.

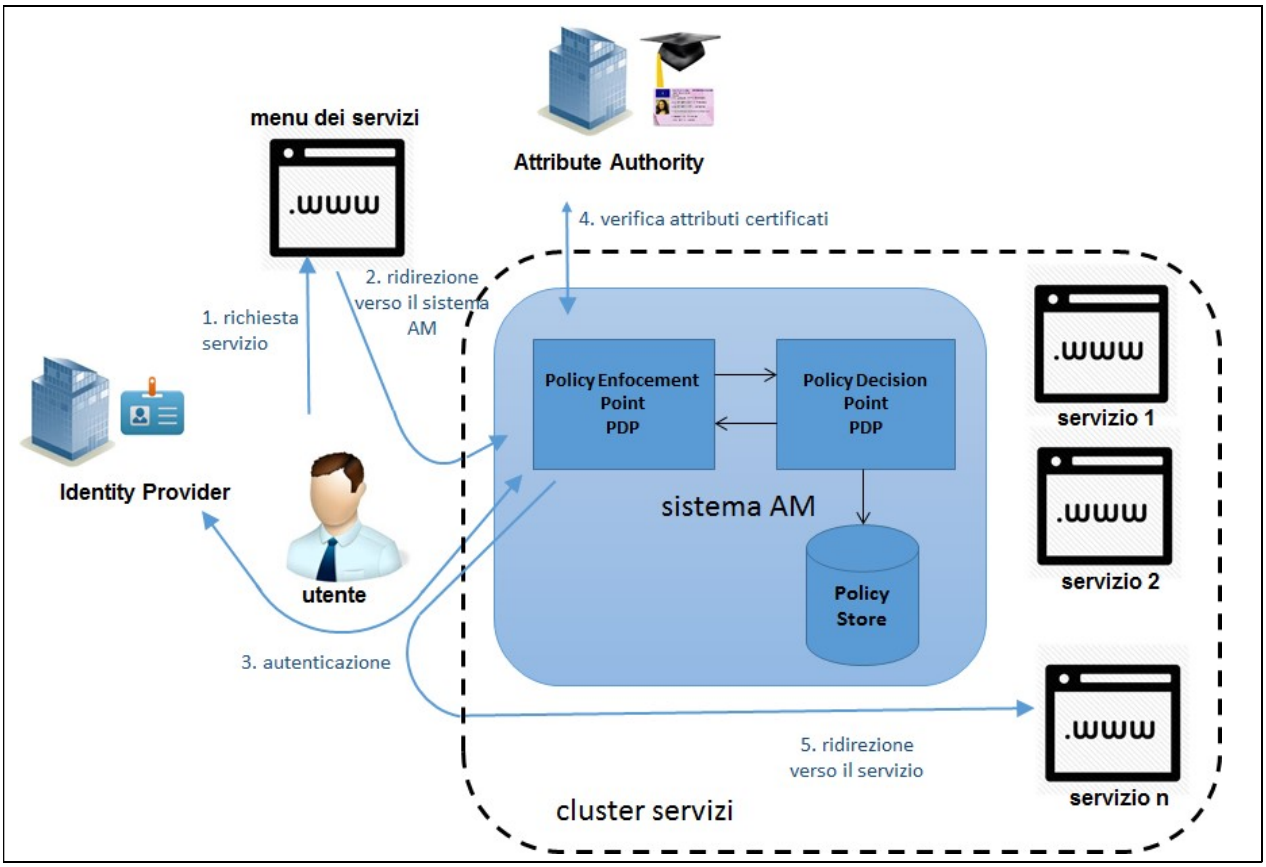

Figura 1 – Nodo cluster di servizi

In figura 1 è riportato una rappresentazione schematica auto esplicativa delle componenti di un nodo cluster, in cui sono riportati i passi relativi all'eccesso degli utenti ai servizi resi disponibili e le architetture classiche di riferimento relative ai sistemi di gestione degli accessi (access management)[1].

[1] la correlazione tra le risposte ed i relativi servizi di pertinenza potrà essere realizzata ad esempio mediante l'uso di identificatori univoci veicolati attraverso il parametro di *binding relaystate* oppure attraverso gli identificativi univoci dei messaggi SAML e dell'attributo inResposeTo.

In questo avviso si farà riferimento ad un ipotetico gestore dei servizi (*service provider*) il cui dispiegamento abbia le seguenti caratteristiche:

- presenza di tre diversi nodi di erogazione distribuiti geograficamente (siano essi nodi semplici o nodi cluster);
- servizi, orientati al cittadino, aggregati in due classi in base al set di attributi per i quali si chiede la certificazione contestualmente all'autenticazione dell'utente[2].

Classe di servizio	Elenco dei servizi	Attributi richiesti
Classe 1	servizio a, servizio b, …. servizio n	**family name;** **name;** **gender;** **dateOfBirth**
Classe 2	servizio k, servizio w, …. servizio z	**FiscalNumber;**

Tabella 1 – Ipotesi di dispiegamento

Per questo caso d'uso descriveremo contenuti e struttura dei file di configurazione (metadata).

La scelta di utilizzare un raggruppamento dei servizi per classi individuate dall'insieme di attributi richiesti, dando evidenza nel file di configurazione delle classi di servizi piuttosto che dei servizi stessi, consente di minimizzare la necessità di aggiornamento dei file di configurazione. Infatti, adottando questa modalità, la messa in produzione di un nuovo servizio afferente ad una classe e ad un nodo già specificati, non richiede alcun aggiornamento del file di configurazione.

2.1. METADATA INFOSET

Allo scopo di fornire autoconsistenza all'esposizione ed agevolare una rapida lettura del documento si riassumono in questo paragrafo i diversi parametri, previsti dallo standard SAML e recepiti dalle regole tecniche SPID, per la definizione dei file di configurazione delle entità operanti come *gestori di servizi*, quest'ultimi riferiti nella nomenclatura SAML con il termine *service provider*.

I file di configurazione sono indicati nella nomenclatura SAML con il termine *metadata*; ogni *service provider* secondo le regole tecniche SPID deve mettere a disposizione un solo *metadata*.

[2] con il criterio di classificazione adottato tutti i servizi appartenente ad una classe sono equivalenti ai fini della certificazione degli attributi operata dai gestori dell'identità a seguito dell'autenticazione dell'utente.

Il *metadata* dal punto di vista formale è un documento XML e nei contenuti riporta tutte le informazioni necessarie per l'interfacciamento dei sistemi di un *service provider* con quelli delle entità con essi interagenti (i gestori delle identità, nella nomenclatura SAML *Identity provider* e le autorità di attributo, nella nomenclatura SAML *attribute authority*). Si tratta dunque di un file di configurazione espresso in un linguaggio formale. Le informazioni necessarie per la configurazione dei sistemi sono contenute in determinati elementi e attributi previsti allo scopo dallo standard SAML. Si riportano di seguito, sinteticamente, tali elementi/attributi SAML con una breve illustrazione dei contenuti per essi previsti.

entityId — attributo SAML atto a definire una *uri* rappresentante l'identificatore univoco del *service provider*;

KeyDescriptor
Cardinalità: uno o più — elemento atto ad ospitare, nel sotto-elemento <*X509Certificate*>, il certificato da utilizzarsi per la verifica della firma del messaggio di richiesta di autenticazione; all'interno del *metadata* possono essere riportati uno o più elementi di questo tipo;

SingleLogoutService
Cardinalità: uno o più — elemento atto a riportare, attraverso gli attributi per esso previsti, le informazioni relative al servizio di *single logout* messo a disposizione dal *service provider*.

Attributi SAML previsti per l'elemento *SingleLogoutService*:

- *binding* — protocollo di trasporto da utilizzare;
- *location* — indirizzo *(url)* del servizio;

all'interno del *metadata* possono essere riportati uno o più elementi di questo tipo;

AssertionConsumerService
Cardinalità: uno o più — elemento atto a riportare, attraverso gli attributi per esso previsti, i riferimenti ad un nodo di erogazione dei servizi nel dominio dell'amministrazione, a cui i gestori delle identità (*identity provider*) devono far pervenire le risposte relative agli esisti dell'autenticazione (*SAMLResponse*). All'interno del *metadata* possono essere riportati uno o più elementi di questo tipo ad indicare l'unico o i diversi punti di erogazione dei servizi all'interno del dominio del gestore dei servizi (*service provider*). Ogni elemento presente è individuato da un indice che lo distingue dagli altri presenti; tale indice deve essere riportato nella richiesta di autenticazione (SAMLReq), mediante un attributo SAML (*AttributeConsumerServiceIndex*) appositamente previsto, al fine di selezionare l'indirizzo di risposta richiesto tra quelli elencati nel *metadata*.

attributi SAML previsti per l'elemento *AssertionConsumerService*:

index	indice associato all'i-esimo indirizzo di risposta;
isDefault	presente in un solo elemento atto ad evidenziare l'indirizzo di risposta nel caso non sia presente nella richiesta (*SAMLReq*) l' attributo SAML (*AssertionConsumerServiceIndex*) previsto per selezionarlo;
binding	protocollo di trasporto (*binding*) da utilizzare per il colloquio;
location	indirizzo *(url)* del punto di erogazione;

AttributeConsumingService
Cardinalità: uno o più

elemento atto a indicare, attraverso gli attributi per esso previsti, un set di attributi SPID di cui può essere richiesta la certificazione a seguito dell'avvenuta autenticazione. All'interno del *metadata* possono essere riportati uno o più elementi di questo tipo ad indicare l'unico o i diversi set di attributi SPID di cui si può chiedere la certificazione. Ogni elemento è caratterizzato da un indice che lo distingue dagli altri presenti; tale indice deve essere riportato nella richiesta di autenticazione (SAMLReq), mediante un attributo SAML (*AttributeConsumingServiceIndex*) appositamente previsto, al fine di selezionare tra quelli elencati nel metadata il set di attributi SPID richiesto; nel caso in cui il predetto attributo SAML fosse assente, a seguito della autenticazione non sarà certificato nessun attributo SPID

attributi/sottoelementi SAML previsti per l'elemento *AttributeConsumingService*:

index	indice associato all'i-esimo set di attributi SPID di cui si può fare richiesta;
ServiceName	elemento riportante l'identificatore associato al servizio che richiede lo specifico set di attributi SPID. Tale identificatore potrebbe, piuttosto che riferirsi ad un singolo servizio, corrispondente ad una categoria di servizi che richiedono tutti lo stesso set di attributi SPID;
RequestedAttribute *Cardinalità: uno o più*	elemento atto a indicare un attributo SPID appartenente al set. Possono essere riportati uno o più elementi di questo tipo uno per ogni attributo SPID appartenete all'insieme;

attributi SAML previsti per l'elemento *RequestedAttribute*:

Name identificatore dell'i-esimo attributo SPID richiesto (secondo la nomenclatura riportata nella tabella di attributi SPID pubblicata sul sito AgID);

Organization
Cardinalità: opzionale
Elemento opzionale riportante i riferimenti all'ente gestore dei servizi;

OrganizationName
Cardinalità: uno o più
denominazione ufficiale del gestore dei servizi;

OrganizationDisplayName
Cardinalità: uno o più
denominazione pubblica sul web del gestore dei servizi;

OrganizationURL
Cardinalità: uno o più
uri specificante una posizione in cui indirizzare un utente per ulteriori informazioni sul gestore dei servizi. Comunemente il sito istituzionale;

2.2. PARAMETRI DI CONFIGURAZIONE

Nella seguente tabella sono raccolte le informazioni necessarie per la configurazione del sistema in esame da riportare nel *metadata*.

Parametro di configurazione	Metadata infoset	Valore di attualizzazione element/attributi	Note
Identificatore ente	*entityId*	`https://denominazione.ente.it/sp`	Per garantire l'univocità si consiglia di usare il nome di dominio registrato dall'ente od un suo sottodominio
Denominazione	*OrganizationName*	`denominazione ente`	Denominazione dell'ente a che opera come gestore del servizio

Denominazione visibile sul web	*OrganizationDisplayName*	**denominazione ente**	Denominazione che l'ente che opera come gestore del servizio vuole rendere visibile in rete.
Indirizzo sito internet	*OrganizationURL*	**https://denominazione.ente.it**	
Indirizzo nodo di erogazione dei servizi nr1	*AssertionConsumerService* *index* *isDefault* *binding* *location*	*protocollo* **http-POST** *indirizzo* **https://denominazione.ente.it/nodo1/assertionConsumerService/POST** *protocollo* **http-redirect** *indirizzo* **https://denominazione.ente.it/nodo1/assertionConsumerService/redirect**	Ogni singolo nodo di servizi può supportare diversi binding (SAML). Nel caso di diversi tipi di binding supportati dallo stesso nodo saranno presenti nel *metadata* più elementi *AssertionConsumerService* ad esso corrispondenti (uno per ogni diverso tipo di binding)
Certificato verifica firma relativo al nodo 1	*KeyDescriptor* *KeyInfo* *X509Data* *X509Certificate*	**0kgUGll….. VBAs**	certificato X509 (codificato base64)
Indirizzo nodo di erogazione dei servizi nr2	*AssertionConsumerService* *index* *isDefault* *binding* *location*	*protocollo* **http-POST** *indirizzo* **https://denominazione.ente.it/nodo2/assertionConsumerService**	
Certificato verifica firma relativo al nodo 2	*KeyDescriptor* *KeyInfo* *X509Data* *X509Certificate*	**0kgUGll….. VBAs**	certificato X509 (codificato base64) nel caso specifico stesso del nodo 1

Indirizzo nodo di erogazione dei servizi nr3	*AssertionConsumerService* *index* *isDefault* *binding* *location*	*protocollo* **http-redirect** *indirizzo* **https://denominazione.ente.it/nodo3/assertionConsumerService**	
Certificato verifica firma relativo al nodo 3	*KeyDescriptor* *KeyInfo* *X509Data* *X509Certificate*	FZaz…….Mw8T	certificato X509 (codificato base64)
servizio di singleLogout		*protocollo* **SOAP** *indirizzo* **https://denominazione.ente.it/logoutService**	
Set di attributi classe 1	*AttributeConsumingService* *ServiceName* *RequestedAttribute*	**family name;** **name;** **gender;** **dateOfBirth;**	Corrispondenti a n servizi effettivi richiedenti lo stesso set di attributi, comunque dislocati nei nodi: servizio 1 servizio 2 ……. servizio n
Set di attributi classe 2	*AttributeConsumingService* *ServiceName* *RequestedAttribute*	**FiscalNumber;**	Corrispondenti a m servizi effettivi richiedenti lo stesso set di attributi, comunque dislocati nei nodi: servizio 1 servizio 2 ……. servizio m

Tabella 2 – Elenco dei parametri di configurazione

2.3. METADATA ESEMPIO

Il *metadata* corrispondente ai dati di configurazione esposti nella tabella 2 è quello riportato nel seguente listato.

```
<md:EntityDescriptor entityID="https://denominazione.ente.it/sp"
ID="_c75b48d19e23e90be40c4ab5eb331e7c4f04f73fb5" xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" xmlns:xsi="http://www.w3.org/2001/XMLSchema-
instance">
        <ds:Signature>…… </ds:Signature>
        <md:SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
WantAssertionsSigned="true">
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo>
                                <ds:X509Data>
                                <ds:X509Certificate> 0kgUGll….. VBAs</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:KeyDescriptor use="signing">
                        <ds:KeyInfo>
                                <ds:X509Data>
                                        <ds:X509Certificate> FZaz…….Mw8T</ds:X509Certificate>
                                </ds:X509Data>
                        </ds:KeyInfo>
                </md:KeyDescriptor>
                <md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
Location="https://denominazione.ente.it/diparttimento1/singleLogoutService"/>
                <md:NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-
format:transient</md:NameIDFormat>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://denominazione.ente.it/nodo1/assertionConsumerService/POST" index="0"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"
Location="https://denominazione.ente.it/nodo1/assertionConsumerService/redirect" index="1"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
Location="https://denominazione.ente.it/nodo2/assertionConsumerService " index="2"/>
        <md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings: HTTP-Redirect"
Location="https://denominazione.ente.it/nodo3/assertionConsumerService " index="3"/>
                <md:AttributeConsumingService index="0">
                        <md:ServiceName xml:lang="it">serviziClasse1</md:ServiceName>
                        <md:RequestedAttribute Name="familyName"/>
                        <md:RequestedAttribute Name="name"/>
                        <md:RequestedAttribute Name="gender"/>
                        <md:RequestedAttribute Name="dateOfBirth"/>
                </md:AttributeConsumingService>
                <md:AttributeConsumingService index="1">
                        <md:ServiceName xml:lang="it"> serviziClasse2</md:ServiceName>
                        <md:RequestedAttribute Name="fiscalNumber"/>
                </md:AttributeConsumingService>
```

```
        </md:SPSSODescriptor>
        <md:Organization>
                <md:OrganizationName xml:lang="it"> denominazione ente
                </md:OrganizationName>
                <md:OrganizationDisplayName xml:lang="it"> denominazione ente
                </md:OrganizationDisplayName>
                <md:OrganizationURL xml:lang="it"> https://nome.ente.it</md:OrganizationURL>
        </md:Organization>
</md:EntityDescriptor>
```

Listato 1 – metadata associato ai parametri di configurazione riportati in tabella 1

2.4. FORMATO RICHIESTE

La presenza presso il *service provider* di più nodi di erogazione del servizio comporta la necessità di riportare nella richiesta di autenticazione (*SAMLReq*) l'indicazione del nodo a cui afferisce il servizio per il quale si chiede l'autenticazione dell'utente. Questo può essere fatto utilizzando l'attributo *AssertionConsumerServiceIndex* (scelta consigliata), come riportato nell'esempio di richiesta seguente:

```
<samlp:AuthnRequest ID="_69aa0f5e9025aa57ac57fce83554e75c50b1a67230" Version="2.0"
IssueInstant="2016-07-05T10:03:17Z" Destination="https://identity.provider.it/idp/SSOService"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AssertionConsumerServiceIndex="2"
AttributeConsumingServiceIndex="1">
        <ds:Signature> …</ds:Signature>
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
        <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
        <samlp:RequestedAuthnContext Comparison="minimum">
                <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL1</saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Listato 2 – Formato richiesta – prima variante

In alternative è possibile utilizzare la coppia di attributi *AssertionConsumerServiceURL* e *ProtocolBinding* riportanti rispettivamente l'indirizzo (url) ed il binding (protocollo di trasporto tra quelli definiti dal SAML v2.0) da utilizzare per la trasmissione delle risposte. In questo caso, si ricorda, la coppia dei valori riportati nella richiesta deve necessariamente corrispondere ad una coppia già prevista nel *metadata* (in un elemento di tipo *AssertionConsumerService*).

```
<samlp:AuthnRequest ID="_69aa0f5e9025aa57ac57fce83554e75c50b1a67230" Version="2.0"
IssueInstant="2016-07-05T10:03:17Z" Destination="https://identity.provider.it/idp/SSOService"
xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" xmlns:samlp="urn:oasis:names:tc:SAML:2.0:protocol"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" AssertionConsumerServiceURL="
https://denominazione.ente.it/nodo2/assertionConsumerService"
ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
AttributeConsumingServiceIndex="1">
        <ds:Signature> …</ds:Signature>
        <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"/>
        <samlp:NameIDPolicy Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"/>
        <samlp:RequestedAuthnContext Comparison="maximum">
                <saml:AuthnContextClassRef>https://www.spid.gov.it/SpidL1</saml:AuthnContextClassRef>
        </samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

Listato 3 – Formato richiesta – seconda variante

Si noti in entrambe le richieste la presenza dell'attributo *AttributeConsumingServiceIndex* ad indicare la classe a cui appartiene il servizio, associata all'insieme di attributi per i quali viene richiesta la certificazione nell'ambito dell'asserzione prodotta a seguito del buon esito dell'autenticazione.

SPID – SISTEMA PUBBLICO PER L'IDENTITÀ DIGITALE
Avviso nr. 19 – Versione 4
02/11/2020

SPECIFICHE TECNICHE PER I CERTIFICATI ELETTRONICI E I METADATA DEI SOGGETTI AGGREGATORI DI SERVIZI PUBBLICI E PRIVATI

Definizione di Soggetti Aggregatori e loro funzione

Il presente Avviso si applica, esclusivamente, alla "funzione di autenticazione con SPID" (come di seguito definita) gestita dai soggetti aggregatori di servizi pubblici e privati per i propri aggregati e dai gestori di pubblico servizio che operano in qualità di soggetti aggregatori di servizi pubblici.

Ai fini del presente Avviso, quando si fa riferimento ai **soggetti pubblici** o agli **Aggregati *pubblici***, ci si riferisce alle Pubbliche Amministrazioni (PP.AA.), così come individuate nell'Avviso SPID №28/2020, ed ai Gestori, così come in seguito definiti; quando si fa riferimento ai **soggetti privati** o agli **Aggregati *privati*** ci ri riferisce a tutti gli altri soggetti privati.

I soggetti aggregatori (cd. **Aggregatori**) sono i fornitori di servizi, ai sensi dell'articolo 1 comma 1 lettera *i)* del DPCM 24 ottobre 2014, mediante i quali gli Aggregati pubblici e gli Aggregati privati consentono l'autenticazione informatica degli utenti attraverso l'uso dello SPID, per l'accesso ai propri servizi in rete (cd. servizi aggregati).

I gestori di pubblico servizio (c.d. **Gestori**) sono tutti i soggetti, diversi dalle PP.AA., che hanno l'esigenza di erogare direttamente servizi di PP.AA. on-line.

Gli Aggregatori provvedono all'invio delle richieste di autenticazione informatica dell'utente ai gestori dell'identità digitale (**IDP**) e alla gestione dei relativi esiti (cd. "funzione di autenticazione con SPID").

Gli Aggregatori, nell'accettare l'identità digitale, non discriminano gli utenti in base all'IDP che l'ha fornita.

Gli Aggregatori si distinguono inoltre in "Aggregatori di servizi pubblici" e "Aggregatori di servizi privati." Gli Aggregatori di servizi pubblici usufruiscono gratuitamente delle verifiche rese disponibili dagli IDP e dai gestori di attributi qualificati (**AA**).

Gli Aggregatori di servizi pubblici aggregano *esclusivamente* gli Aggregati pubblici; gli Aggregatori di servizi privati aggregano *esclusivamente* gli Aggregati privati.

I Gestori – limitatamente per l'esercizio dei servizi pubblici – entrano nella federazione SPID in qualità di:

- Aggregatori di servizi pubblici, aggregando la Pubblica Amministrazione (P.A.) o le PP.AA. per le quali erogano direttamente i servizi on-line, seguendo le specifiche previste dal presente Avviso; *ovvero*
- Aggregati pubblici (cd. **Gestori Aggregati**).

Il medesimo soggetto può svolgere sia l'attività di fornitore di servizi (**SP**), sia di Aggregatore di servizi pubblici, sia di Aggregatore di servizi privati, stipulando le rispettive convenzioni.

Le convenzioni per l'adesione a SPID in qualità di Aggregatori di servizi pubblici o privati consentono agli Aggregatori di erogare, in qualità di fornitori di servizi, ai sensi dell'articolo 1 comma 1 lettera *i)* del DPCM 24 ottobre 2014, la sola funzione di autenticazione con SPID per i propri Aggregati.

Gli Aggregatori oltre a svolgere per l'Aggregato la funzione di autenticazione con SPID – garantendone *sempre* la manutenzione evolutiva e correttiva – possono ospitare l'intero servizio dell'Aggregato.

Gli Aggregatori possono operare, nei confronti di ciascun Aggregato,[1] in modalità *"light"* ovvero in modalità *"full"*:

- la modalità *light* è quella in cui l'Aggregatore di servizi pubblici o privati provvede alla funzione di autenticazione con SPID tramite l'infrastruttura in uso all'Aggregato, su cui è stata installata la soluzione fornita dall'Aggregatore;
- la modalità *full* è quella in cui l'Aggregatore di servizi pubblici o privati provvede alla funzione di autenticazione con SPID per conto dell'Aggregato, tramite propria infrastruttura.

Gli Aggregatori di servizi privati, sia *light* che *full*, riconoscono agli IDP i corrispettivi previsti per ogni utente unico in relazione ad ogni Aggregato (cfr. Allegato 4, 'Tabella corrispettivi', alla Determinazione AgID №166/2019).

Infrastruttura a chiave pubblica per i Soggetti Aggregatori

Su ogni metadata presentato ad AgID l'Aggregatore appone un sigillo elettronico avanzato creato dallo stesso Aggregatore mediante il **certificato di federazione** proveniente dall'infrastruttura a chiave pubblica (**PKI**) che AgID ha istituito appositamente per la gestione fiduciaria della federazione SPID. AgID fornisce un unico certificato elettronico di federazione:

1. Agli **Aggregatori *light***, un certificato di CA intermedia ("*sub*-CA") con cui l'Aggregatore genera:
    a. uno o più certificati[2] associati al sigillo elettronico creato sui metadata dei propri Aggregati, afferenti a chiavi private che DEVONO rimanere sotto il controllo esclusivo dell'Aggregatore;
    b. un certificato[3] di sigillo elettronico per ciascun Aggregato *light*, associato al sigillo elettronico creato sulle richieste di autenticazione (*request*) di ogni Aggregato. La chiave privata afferente a questo certificato NON DEVE essere condivisa tra più Aggregati.
2. Agli **Aggregatori *full***, un certificato afferente al sigillo elettronico apposto su tutti i metadata e richieste di autenticazione. La chiave privata afferente a questo certificato DEVE essere usata esclusivamente dall'Aggregatore e DEVE rimanere sotto il suo controllo esclusivo.

Gli Aggregatori operanti sia in modalità *light* che in modalità *full* ricevono da AgID entrambe i certificati di cui ai punti 1 e 2.

Al fine di ottenere detti certificati si deve far riferimento all'Avviso SPID №23/2016 e s.m.i. e compilare il previsto modulo di richiesta.

Struttura dei certificati elettronici di Aggregatori e Aggregati

Al fine dell'interoperabilità del Sistema Pubblico delle Identità Digitali (SPID), i certificati di sigillo elettronico di cui al presente Avviso sono conformi alla RFC-5280 e a quanto qui ulteriormente regolato.

I certificati utilizzati dagli Aggregatori contengono informazioni relative al soggetto aggregatore.

I certificati emessi dagli Aggregatori in favore degli Aggregati *light* contengono informazioni relative sia all'Aggregato (in qualità di soggetto del certificato) che dell'Aggregatore (in qualità di emettitore del certificato).

---

[1] Si può pertanto parlare anche di "Aggregato *light*" ovvero di "Aggregato *full*."
[2] Nel caso l'Aggregatore generi più di un certificato, ogni certificato deve afferire a una differente chiave privata.
[3] Per particolari esigenze, sono ammessi più certificati per servizi del medesimo Aggregato *light*.

I certificati in questione DEVONO contenere le seguenti estensioni, tutte valorizzate con il corretto uso di minuscole, maiuscole, lettere accentate e altri segni diacritici:

1. Nel campo **`SubjectDN`**:
    a. `organizationName` (OID 2.5.4.10) — Denominazione *completa e per esteso* del soggetto del certificato, così come indicato nei pubblici registri; cioè, per i certificati:
        - di cui ai precedenti punti 1.a e 2, con la denominazione dell'Aggregatore (per esempio, "`Aggregatore S.p.A.`" e *non* "`AGGREGATORE`"; anche "`Agenzia per l'Italia Digitale`" e *non* "`Agenzia per l'italia digitale`");
        - di cui al precedente punto 1.b, con la denominazione dell'Aggregato (per esempio "`Comune di XYZ`"), così come riportata nel tag XML `<OrganizationName>` del metadata dell'Aggregato;

    b. `commonName` (OID 2.5.4.3) — La denominazione che valorizza l'estensione `organizationName`, eventualmente senza esplicitazione degli acronimi, così come riportata nel tag XML `<OrganizationDisplayName>` del metadata dell'Aggregato (ad esempio, "`AgID`").

    c. `uri` (OID 2.5.4.83) — Visto il capitolo 'Definizione di EntityID':
        - per i certificati emessi da AgID, è valorizzato con l'*EntityID dell'Aggregatore*;
        - per i certificati emessi dall'Aggregatore agli Aggregati, per le attività di cui ai punti 2, 4 e 6 del paragrafo 'Attività degli Aggregatori', è valorizzato con l'*EntityID dell'Aggregato*.

    d. `organizationIdentifier` (OID 2.5.4.97) — Un codice identificativo del soggetto, unico nella federazione SPID, conforme alla sintassi prevista dalla norma ETSI EN 319-412-1, §5.1.4:
        i. per i soggetti pubblici, così come individuati nell'Avviso SPID №28/2020 — il **codice IPA** del soggetto preceduto, in base al §5.1.4 punto 3 della suddetta norma, dal prefisso '`PA:IT-`' — ad esempio, per una Regione con codice IPA '`r_xyz`' tale estensione sarebbe valorizzata come "`PA:IT-r_xyz`";
        ii. per tutti gli altri soggetti, ivi compresi gli Aggregatori che svolgono l'attività di Gestori di cui ai punti 5 e 6 del paragrafo 'Attività degli Aggregatori' — il **numero di partita IVA** del soggetto preceduto, in base al §5.1.4 punto 1 della suddetta norma, dal prefisso '`VAT`' seguito dal codice ISO 3166-1 α-2 del Paese, seguito dal carattere '`-`' (`0x2D`), (ad esempio, "`VATIT-12345678901`") o – nel caso in cui il soggetto *non* sia dotato di partita IVA – il **codice fiscale** della persona giuridica valorizzato, in base al §5.1.4 punto 2 della suddetta norma, con il prefisso '`CF:IT-`' (esempio; "`CF:IT-XYZABCAAMGGJ000W`").
        iii. altro codice alternativo, fornito da AgID in casi particolari.

    e. `countryName` (OID 2.5.4.6) — Il codice ISO 3166-1 α-2 del Paese ove è situata la sede legale del soggetto del certificato (esempio: "`IT`");

    f. `localityName` (OID 2.5.4.7) — Il nome completo della città ove è situata la sede legale del soggetto del certificato (esempio: "`Roma`").

2. Il campo **`Issuer`**, *per i certificati di cui ai punti 1.a e 1.b* del capitolo "Infrastruttura a chiave pubblica per i Soggetti Aggregatori," è valorizzato con quanto presente nel campo `SubjectDN` del relativo certificato di CA intermedia, di cui al punto 1 del suddetto capitolo.

3. Nel campo **`CertificatePolicies`**:
    a. `policyIdentifier` — contenente quantomeno una e una sola tra le seguenti estensioni:
        i. `spid-publicsector-fullaggregator` (OID 1.3.76.16.**4.2.2**) — nei certificati di Aggregatore *full* di servizi pubblici (emessi da AgID, come da precedente punto 2);
        ii. `spid-publicsector-lightaggregator` (OID 1.3.76.16.**4.2.5**) — nei certificati di *sub*-CA di Aggregatore *light* di servizi pubblici (emessi da AgID, come da punto 1);
        iii. `spid-publicsector-lightaggregator-metadataseal` (OID 1.3.76.16.**4.2.5.1**) — nei certificati di Aggregatore *light* di servizi pubblici (emessi dall'Aggregatore stesso, come da punto 1.a);
        iv. `spid-publicsector-lightaggregator-aggregatedseal` (OID 1.3.76.16.**4.2.5.2**) — nei certificati di Aggregati pubblici (emessi dall'Aggregatore *light*, come da punto 1.b);
        v. `spid-privatesector-fullaggregator` (OID 1.3.76.16.**4.3.2**) — nei certificati di Aggregatore *full* di servizi privati (emessi da AgID, come da precedente punto 2);
        vi. `spid-privatesector-lightaggregator` (OID 1.3.76.16.**4.3.5**) — nei certificati di *sub*-CA di Aggregatore *light* di servizi privati (emessi da AgID, come da punto 1);
        vii. `spid-privatesector-lightaggregator-metadataseal` (OID 1.3.76.16.**4.3.5.1**) — nei certificati di Aggregatore *light* di servizi privati (emessi dall'Aggregatore stesso, come da punto 1.a);
        viii. `spid-privatesector-lightaggregator-aggregatedseal` (OID 1.3.76.16.**4.3.5.2**) — nei certificati di Aggregati privati (emessi dall'Aggregatore *light*, come da punto 1.b).

    I certificati di sigillo elettronico conformi con la Determinazione AgID №121/2019 s.m.i.[4] – anche se non qualificati[5] – contengono inoltre l'estensione `agIDcert` (OID 1.3.76.16.**6**).

Trattandosi di certificati di *sigillo elettronico* e non di certificati di firma elettronica, gli attributi `name` (OID 2.5.4.41), `surname` (OID 2.5.4.4), `givenName` (OID 2.5.4.42), `initials` (OID 2.5.4.43) e `pseudonym` (OID 2.5.4.65) NON DEVONO essere utilizzati. Altre estensioni, come ad esempio `emailAddress` (OID 1.2.840.113549.1.9.1), se presenti, NON SONO valorizzate con dati personali afferenti a persone fisiche.

Ulteriori estensioni stabilite dagli standard e dalle normative sono liberamente utilizzabili, purché non vadano in contrasto con le predisposizioni di cui al presente Avviso.

Algoritmi crittografici, di *hash* e tipologia delle chiavi

Per la generazione delle chiavi crittografiche di cui al presente Avviso, gli Aggregatori e gli Aggregati utilizzano l'algoritmo **RSA** (Rivest-Shamir-Adleman) con lunghezza delle chiavi non inferiore a 2048 bit. L'algoritmo impiegato per le impronte crittografiche è il *dedicated hash-function 4* definito nella norma ISO/IEC 10118-3, corrispondente alla funzione **SHA-256**. È consentito l'uso della funzione **SHA-512**.

Definizione di EntityID

[4] Linee Guida contenenti le *Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*.
[5] Ai sensi del Regolamento (UE) №910/2014 s.m.i..

L'EntityID è l'attributo che identifica univocamente l'Aggregato, nell'ambito dell'attività dell'Aggregatore, o il Gestore *full*.

L'Aggregatore è identificato univocamente, all'interno della federazione SPID, mediante l'*EntityID dell'Aggregatore*, unico per tutte le attività sotto indicate, che soddisfa le seguenti regole sintattiche:

- corrisponde a un URI che comprende lo *schema* HTTPS ma non è terminato da un carattere *slash* (ad es.: `https://agid.gov.it`);
- può includere o meno un *percorso* ma, se presente, il percorso deve poter essere estendibile con dei percorsi relativi aggiunti in calce (ad es. `https://registry.spid.gov.it/metadata/sp` è valido; `https://agid.gov.it/datapolicy.pdf#retention` *non* è valido);
- *non* contiene, in alcuna sua parte, *query string* o ulteriori frammenti (quali, ad es., `?id=1234567#data`).

Attività degli Aggregatori

I soggetti Aggregatori usano uno o più metadata a seconda dell'attività svolta (nel seguito solo "attività"), ogni attività essendo individuata da un codice (*codice attività*):

1. l'Aggregatore *full* di servizi pubblici (codice attività: `pub-ag-full`) descrive i servizi di ogni Aggregato in un metadata dedicato (uno per ciascun Aggregato);
2. l'Aggregatore *light* di servizi pubblici (codice attività: `pub-ag-lite`) descrive i servizi di ogni Aggregato in un metadata dedicato (uno per ciascun Aggregato);
3. l'Aggregatore *full* di servizi privati (codice attività: `pri-ag-full`) descrive i servizi di ogni Aggregato in un metadata dedicato (uno per ciascun Aggregato);
4. l'Aggregatore *light* di servizi privati (codice attività: `pri-ag-lite`) descrive i servizi di ogni Aggregato in un metadata dedicato (uno per ciascun Aggregato);
5. il Gestore *full* di servizi pubblici (codice attività: `pub-op-full`) descrive tutti i servizi erogati direttamente per una o più PP.AA. in un metadata dedicato (unico per tutte le PP.AA.);
6. il Gestore *light* di servizi pubblici (codice attività: `pub-op-lite`) descrive i servizi di ogni Aggregato in un metadata dedicato (uno per ciascun Aggregato).

I soggetti che svolgono più attività, producono metadata diversi per ciascuna attività.

Le stringhe dei codici attività definite nei punti dall'1 al 6 SONO indicate nell'EntityID una sola volta per distinguere l'Aggregatore dall'Aggregato.

Composizione dell'EntityID

I metadata sono identificati univocamente da un EntityID; pertanto, non possono esistere in produzione metadata diversi con il medesimo EntityID.

L'EntityID è composto:

- per le attività di cui ai punti 1, 2, 3, 4 e 6, da una concatenazione, mediante caratteri '/' (*slash*, `0x2F`) dell'EntityID dell'Aggregatore, del codice attività, e di un percorso URI *relativo* (privo di *query string* o ulteriori frammenti). L'EntityID è unico per l'Aggregato (ad esempio il Gestore Aggregato), nell'ambito dell'attività dell'Aggregatore; è dunque chiamato *EntityID dell'Aggregato*;

- per l'attività di Gestore *full*, di cui al punto 5, da una concatenazione, mediante il carattere '/' (*slash*) del solo EntityID dell'Aggregatore e del codice attività.

Ad esempio:

- per le attività di cui al precedente punto 1, l'EntityID dell'Aggregato da un Aggregatore *full* di servizi pubblici, il cui EntityID dell'Aggregatore è `https://aggregatorEntityID`, può risultare in una stringa del tipo `https://aggregatorEntityID/pub-ag-full/estensione.unica.Aggregato`;
- per le attività di cui al precedente punto 5, l'EntityID relativo al medesimo Aggregatore, che opera questa volta come Gestore *full*, corrisponde alla stringa `https://aggregatorEntityID/pub-op-full`;
- l'EntityID relativo a un Gestore Aggregato (dall'Aggregatore *full* del primo esempio) è una stringa del tipo `https://aggregatorEntityID/pub-ag-full/estensione.unica.GestoreAggregato`.

Struttura dei Metadata degli Aggregati

Ogni soggetto che entra nella federazione SPID per mezzo di Aggregatori è dotato di un metadata da Aggregato relativo al proprio Aggregatore.

Per l'attività di Gestore *full*, di cui al punto 5, gli Aggregatori usano un unico metadata per tutti i servizi.

I metadata contengono particolari estensioni SAML che permettono agli altri soggetti della federazione SPID di individuare l'Aggregatore e l'Aggregato. Tali estensioni contengono informazioni utili a contattare l'Aggregatore nei rapporti B2B: sia per finalità tecnico-operative che, se del caso, di fatturazione elettronica.

L'Aggregatore rende disponibili i metadata nella federazione SPID con le modalità definite dall'Agenzia.

Ove occorrano estensioni proprie di SPID, è adeguatamente definito il *namespace* XML associato: `https://spid.gov.it/saml-extensions`.

I metadata così introdotti presentano caratteristiche tecniche realizzate mediante la presenza dei seguenti tag figli (tutti con *namespace* `md`), ovvero dei seguenti attributi, del tag `EntityDescriptor`.

- `entityID` — Attributo che identifica univocamente l'Aggregato nell'ambito dell'attività dell'Aggregatore o del Gestore *full*, valorizzato con l'EntityID di cui al capitolo "Definizione di EntityID."
- `SPSSODescriptor` (1 occorrenza) — Contiene vari tag figli, tra i quali:
  - `KeyDescriptor` (1 o più occorrenze) — Ciascuna occorrenza con attributo `use` valorizzato con `signing` si riferisce ad una chiave privata utilizzata per apporre sigilli elettronici sulle *request*, identificata tramite i seguenti tag figli (tutti con *namespace* `ds`), secondo la normativa *XML Signature Syntax and Processing* del W3C, nella revisione prevista dalle specifiche SAML in uso:
    - `KeyName` (0 o più occorrenze) — contiene un'indicazione *human-readable* dell'ambito d'uso della chiave privata, ovvero l'URI dell'`AssertionConsumerService` cui questa si riferisce;
    - `KeyInfo` (1 occorrenza) — contiene all'interno un tag `X509Data` con uno o più figli:
      - `X509SubjectName` (0 o più occorrenze) — contiene un riferimento ad un `AssertionConsumerService`, codificato in base allo standard RFC-4514;
      - `X509Certificate` (1 occorrenza, *obbligatorio*) — contiene la codifica *Base64*

del certificato di sigillo elettronico afferente alla suddetta chiave privata.

Qualora siano presenti più certificati elettronici, allo scopo di distinguerne l'uso a livello del metadata SAML, si *consiglia* di valorizzare (consistentemente su tutti gli elementi del `KeyDescritor`), almeno uno[6] dei tag figli facoltativi sopra definiti.

- `Organization` (1 occorrenza) — Contiene le informazioni di base circa il soggetto del metadata, specificate mediante i seguenti tag, ciascuno dei quali ripetuto almeno una volta valorizzato in lingua italiana (e con il corretto uso di minuscole, maiuscole, lettere accentate e altri segni diacritici) e occorrenze facoltative localizzanti il medesimo nome in ulteriori lingue (*tutte* identificate mediante l'attributo `xml:lang`, obbligatoriamente presente nei tag sotto indicati):
  - `OrganizationName` (1 o più occorrenze nel caso multilingua) —
    - per le attività di Aggregatore (punti da 1 a 4 del paragrafo 'Attività degli Aggregatori'), contiene il nome *completo e per esteso* dell'**Aggregato** (p.es. "`Società Aggregata Nazionale S.p.A.`" e *non* "`SOCIETA' AGGREGATA nazionale`"; anche "`Regione Emilia-Romagna`" e *non* "`regione emilia romagna`"; anche, per il Gestore Aggregato, "`Gestore S.p.A.`" e *non* "`GESTORE`");
    - per le attività di Gestore (punti 5 e 6 del suddetto paragrafo), contiene il nome *completo e per esteso* del **Gestore** (p.es. "`Gestore S.p.A.`" e *non* "`GESTORE`").
  - `OrganizationDisplayName` (1 o più occorrenze nel caso multilingua) — Contiene la denominazione del soggetto riportato nel tag `OrganizationName`, eventualmente abbreviata e senza esplicitazione di acronimi (dal primo esempio soprastante, per la Società Nazionale S.p.A., "`SAN`").

    Durante la fase di autenticazione, gli IDP avvisano l'utente dell'invio degli attributi al soggetto indicato nel tag `OrganizationDisplayName`.
  - `OrganizationURL` (1 o più occorrenze) — Contiene l'URL di una pagina web relativa al servizio di autenticazione o ai servizi accessibili tramite essa, i cui contenuti sono localizzati nella lingua specificata dal proprio attributo `xml:lang`.
- `ContactPerson` (da 1 a 3 occorrenze) — È sempre presente un'occorrenza contenente le informazioni di contatto obbligatorie dell'Aggregatore. Per tutte le attività diverse da Gestore *full* (punto 5 del paragrafo 'Attività degli Aggregatori'), è presente anche un'occorrenza contenente le informazioni di contatto obbligatorie dell'Aggregato. Ove previsto nel paragrafo 'Informazioni obbligatorie per la fatturazione', è presente un'ulteriore occorrenza contenente informazioni per la fatturazione elettronica. Le occorrenze `ContactPerson` utilizzano i seguenti attributi:
  - `contactType` (*obbligatorio*) — Per le occorrenze contenti le informazioni di contatto obbligatorie dell'Aggregatore o dell'Aggregato, è presente e valorizzato con `other`. Per l'occorrenza contenente le informazioni per la fatturazione elettronica, è valorizzato con `billing`, di cui al paragrafo 'Informazioni obbligatorie per la fatturazione'.
  - `spid:entityType` — Presente solo quando il `contactType` è valorizzato con `other`. Per le

[6] Possono essere adottati più tag dello stesso tipo qualora nel metadata vi siano più ambiti d'uso per la medesima chiave o certificato elettronico (afferenti, ad esempio, a più `AssertionConsumerService`).

attività di Aggregatore, è valorizzato come `spid:aggregator`; nelle occorrenze relative al contatto dell'Aggregato, invece, è valorizzato come `spid:aggregated`.

Sono *obbligatorie* le occorrenze di `ContactPerson`, corredate dall'attributo `contactType` valorizzato con `other`, contenenti le informazioni minime sia per l'Aggregatore che per l'Aggregato.

Tutte le occorrenze del tag `ContactPerson` con il `contactType` valorizzato con `other` contengono i seguenti tag minimi (tutti con *namespace* `md`):

- `Extensions` (1 occorrenza, *obbligatorio*) — Valorizzata come da paragrafo 'Estensioni SPID nel metadata'
- `Company` (1 occorrenza, *obbligatorio*) — La denominazione dell'Aggregatore (p.es. `Sogetto Aggregatore s.r.l.`) ovvero dell'Aggregato (p.es. `Società Aggregata S.p.A.`, in quest'ultimo caso valorizzato *esattamente* come l'antenato indiretto `OrganizationName`), in ogni caso riportante il nome completo e per esteso di una persona giuridica, con il corretto uso di minuscole, maiuscole e segni diacritici.
- `EmailAddress` (1 occorrenza, *obbligatorio* per l'Aggregatore) — Contiene l'indirizzo di posta elettronica per contattare il soggetto cui il genitore `ContactPerson` si riferisce. NON DEVE trattarsi di un indirizzo riferibile direttamente ad una persona fisica.
- `TelephoneNumber` (0 o 1 occorrenze) — Contiene il numero di telefono, per contattare il soggetto cui il genitore `ContactPerson` si riferisce; *senza spazi* e comprensivo del prefisso internazionale (esempio: "`+39`" per l'Italia).

Estensioni SPID nel metadata

Il tag `Extensions` presente in ciascun tag `ContactPerson` il cui attributo `contactType` è valorizzato con `other` contiene *almeno una* delle seguenti estensioni, dedicate a SPID per gli Aggregatori e gli Aggregati, tutte afferenti al *namespace* `spid`, salvo ove diversamente indicato.

1. `IPACode` — Relativamente al soggetto (Aggregatore o Aggregato) cui l'antenato `ContactPerson` si riferisce, è *obbligatorio* qualora questo sia una P.A. o un Gestore ed è valorizzato con il suo codice IPA.
2. `VATNumber` — Relativamente al soggetto cui l'antenato `ContactPerson` si riferisce, è *obbligatorio* qualora questo sia un soggetto privato o un Gestore (e facoltativo altrimenti) ed è valorizzato con il numero della sua partita IVA (comprensivo del codice ISO 3166-1 α-2 del Paese, senza spazi).
3. `FiscalCode` — Relativamente al soggetto cui l'antenato `ContactPerson` si riferisce, è *obbligatorio* qualora questo sia un soggetto privato o un Gestore (e facoltativo altrimenti) ed è valorizzato con il suo codice fiscale.

Qualora il numero di partita IVA e il codice fiscale coincidano, è comunque necessario valorizzare sia `VATNumber` che `FiscalCode`.

Il tag `Extensions` il cui tag antenato `ContactPerson` possiede l'attributo `spid:entityType` valorizzato con `spid:aggregator` contiene uno (e solo uno) dei seguenti tag "vuoti," da utilizzarsi alternativamente a seconda delle sei attività svolte dall'Aggregatore in relazione al metadata in oggetto, elencate nel paragrafo 'Attività degli Aggregatori':

1. `PublicServicesFullAggregator` — Aggregatore *full* di servizi pubblici;

2. `PublicServicesLightAggregator` — Aggregatore *light* di servizi pubblici;
3. `PrivateServicesFullAggregator` — Aggregatore *full* di servizi privati;
4. `PrivateServicesLightAggregator` — Aggregatore *light* di servizi privati;
5. `PublicServicesFullOperator` — Gestore *full* di servizi pubblici;
6. `PublicServicesLightOperator` — Gestore *light* di servizi pubblici.

Il tag scelto tra i precedenti sei deve corrispondere al *codice attività* utilizzato per formare l'EntityID del metadata, di cui al paragrafo 'Definizione di EntityID'.

Per i SOLI metadata afferenti ad Aggregati *light*, il tag `Extensions` il cui tag antenato `ContactPerson` possiede l'attributo `spid:entityType` valorizzato con `spid:aggregator` DEVE inoltre contenere:

- `KeyDescriptor` (*namespace* `spid` e *non* `md`) — Dotato di attributo `use` valorizzato come `spid:validation`, contiene le informazioni necessarie a individuare il *trust anchor* dell'Aggregatore *light* presso la PKI di AgID, cioè il certificato di CA intermedia di cui al punto 1 del capitolo "Infrastruttura a chiave pubblica per i Soggetti Aggregatori." È perciò valorizzato con un tag `KeyInfo` (*namespace* `ds`), secondo quanto previsto dalla normativa *XML Signature Syntax and Processing* del W3C, nella revisione prevista dalle specifiche SAML in uso.

Nei metadata di cui al presente Avviso i certificati di certificazione (inclusi quelli intermedi) NON DEVONO essere contenuti all'interno di tag `KeyDescriptor` con attributo `use` valorizzato con `signing`.

Il tag `Extensions` il cui tag antenato `ContactPerson` possiede l'attributo `spid:entityType` valorizzato con `spid:aggregated` contiene uno (e solo uno) dei seguenti tag "vuoti," da utilizzarsi alternativamente a seconda della tipologia dell'Aggregato:

1. `Public` — P.A., così come individuata nell'Avviso SPID №28/2020;
2. `PublicOperator` — Gestore, così come definito dal presente Avviso;
3. `Private` — soggetto privato, così come definito dal presente Avviso;

Ad esempio[7] nelle estensioni del `ContactPerson` con le informazioni di un Aggregatore di servizi *privati* operante in modalità *light*, è presente il numero di partita IVA e il codice fiscale dell'Aggregatore, oltre al tag `PrivateServicesLightAggregator` e al certificato di CA intermedia dell'Aggregatore tramite tag `KeyDescriptor`; nell'occorrenza afferente al suo Aggregato (soggetto privato) sono presenti il numero di partita IVA, il codice fiscale e il tag `Private`.

Nel caso di attività di Gestore *full*[8] sono presenti il codice IPA, il numero di partita IVA, il codice fiscale e il tag `PublicServicesFullOperator` del Gestore (coerentemente con la valorizzazione dell'estensione `organizationIdentifier` di cui al capitolo "Struttura dei certificati elettronici di Aggregatori e Aggregati").

Invece[9] nelle estensioni del `ContactPerson` con le informazioni di un Aggregatore di servizi *pubblici* operante in modalità *full*, deve essere presente il codice IPA se l'Aggregatore è una P.A. (e, opzionalmente, anche il numero di partita IVA e/o il codice fiscale), oppure sia il numero di partita IVA che il codice fiscale se

[7] Cfr. paragrafo 'Esempio di metadata di una società Aggregata in modalità *light* (codice attività: `pri-ag-lite`)'.
[8] Cfr. paragrafo 'Esempio di metadata di un Gestore *full* (codice attività: `pub-op-full`)'.
[9] Cfr. paragrafi 'Esempio di metadata di una P.A. Aggregata in modalità *full* (codice attività: `pub-ag-full`)' e 'Esempio di metadata di un Gestore Aggregato in modalità *full* (codice attività: `pub-ag-full`)'.

l'Aggregatore è un soggetto privato, oltre al tag `PublicServicesFullAggregator` in entrambe i casi; nell'occorrenza afferente al suo Aggregato è presente *almeno* il codice IPA, mentre il numero di partita IVA e il codice fiscale sono *facoltativi* qualora l'Aggregato sia una P.A. (seguiti dal tag obbligatorio `Public`), *obbligatori* qualora sia un Gestore Aggregato (seguiti, in questo caso, dal tag obbligatorio `PublicOperator`).

Informazioni obbligatorie per la fatturazione

Per le attività di Aggregatori di servizi privati, di cui ai numeri 3 e 4, l'occorrenza di `ContactPerson` con l'attributo `contactType` valorizzato con `billing` è *obbligatoria* e contiene le informazioni fiscali *minime* per l'individuazione del soggetto che sarà il destinatario di fatturazione elettronica, in qualità di **committente**, da parte degli IDP. Al suo interno sono presenti i seguenti tag:

- `Extensions` (1 occorrenza *obbligatorio*) — Tramite estensione con opportuno *namespace* `https://spid.gov.it/invoicing-extensions`, ispirato dallo standard[10] **FatturaPA** dell'Agenzia delle Entrate, contiene i tag minimi necessari alla suddetta individuazione fiscale. Sono dunque presenti il tag figlio `CessionarioCommittente` e, qualora necessario, il tag figlio `TerzoIntermediarioSoggettoEmittente`, valorizzati come previsto dallo standard:
  - **`CessionarioCommittente`** (1 occorrenza) — con figli:
    - `DatiAnagrafici` (1 occorrenza) — con figli: `IdFiscaleIVA` (figli: `IdPaese` e `IdCodice`) e/o `CodiceFiscale`; `Anagrafica` (figli: `Denominazione`, *ovvero* `Nome` e `Cognome`; opzionalmente `Titolo`; opzionalmente `CodiceEORI`);
    - `Sede` (1 occorrenza) — con figli: `Indirizzo`, `NumeroCivivo` (opzionale), `CAP`, `Comune`, `Provincia` (opzionale), `Nazione`.
  - **`TerzoIntermediarioSoggettoEmittente`** (0 o 1 occorrenze) — valorizzato, se necessario e *solo relativamente al committente*.
- `Company` (1 occorrenza, *obbligatorio*) — Valorizzata con il nome del soggetto cui emettere le fatture elettroniche.
- `EmailAddress` (1 occorrenza, *obbligatorio*) — Contiene l'indirizzo di posta elettronica, *aziendale o istituzionale*, per contattare l'Aggregatore per questioni di fatturazione elettronica. PUÒ trattarsi di un indirizzo di posta elettronica certificata (PEC) aziendale, ma NON DEVE trattarsi di una casella e-mail personale.
- `TelephoneNumber` (1 occorrenza, *facoltativo*) — Contiene un numero di telefono, *aziendale o istituzionale*, per contattare l'Aggregatore per questioni di fatturazione elettronica. NON DEVE trattarsi di una casella e-mail personale.

Esempio di metadata di una società Aggregata in modalità *light* (codice attività: `pri-ag-lite`)

Il seguente esempio di metadata è relativo a un soggetto privato, `Società Aggregata Nazionale S.p.A.`, aggregato da un Aggregatore privato, `Soggetto Aggregatore s.r.l.`, operante quale Aggregatore di

[10] Cioè lo standard **FatturaPA** adottato a livello nazionale per le fatture elettroniche in formato XML, corrispondente al *namespace* originale `http://ivaservizi.agenziaentrate.gov.it/docs/xsd/fatture/v1.2`.

servizi privati in modalità *light*, nel quale sono specificati, nell'ordine, i dati identificativi dell'Aggregatore (incluso il certificato di *sub*-CA rilasciato da PKI di AgID), i dati identificativi dell'Aggregato e le informazioni per la fatturazione elettronica da parte degli IDP. Le informazioni dell'Ente sono in questo caso localizzate anche in lingua inglese.

```
<md:EntityDescriptor
        [...]
        entityID="https://aggregatore/pri-ag-lite/estensione.aggregato"
        ID="_uniqueID"
        [...]
        xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:spid="https://spid.gov.it/saml-extensions">
    [...]
    <md:Organization>
        <md:OrganizationName xml:lang="it">
            Società Aggregata Nazionale S.p.A.
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">
            S.A.N.
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">
            https://societaaggregata.com/it/
        </md:OrganizationURL>
        <md:OrganizationName xml:lang="en">
            Società Aggregata S.p.A.
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="en">
            SAN
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="en">
            https://societaaggregata.com/en/
        </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregator">
        <md:Extensions>
            <spid:VATNumber>ITpartitaIVA_aggregatore</spid:VATNumber>
            <spid:FiscalCode>CF_aggregatore</spid:FiscalCode>
            <spid:PrivateServicesLightAggregator/>
            <spid:KeyDescriptor md:use="spid:validation">
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>
                            [...]CertificatoSubCA-AggregatoreBase64 [...]
                        </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
```

```
            </spid:KeyDescriptor>
        </md:Extensions>
        <md:Company>Soggetto Aggregatore s.r.l.</md:Company>
        <md:EmailAddress>email@aggregatore</md:EmailAddress>
        <md:TelephoneNumber>+39tel_aggregatore</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregated">
        <md:Extensions>
            <spid:VATNumber>ITpartitaIVA_aggregato</spid:VATNumber>
            <spid:FiscalCode>CF_aggregato</spid:FiscalCode>
            <spid:Private/>
        </md:Extensions>
        <md:Company>Società Aggregata Nazionale S.p.A.</md:Company>
    </md:ContactPerson>
   <md:ContactPerson contactType="billing">
        <md:Extensions
              xmlns:fpa="https://spid.gov.it/invoicing-extensions">
            <fpa:CessionarioCommittente>
                <fpa:DatiAnagrafici>
                    <fpa:IdFiscaleIVA>
                        <fpa:IdPaese>IT</fpa:IdPaese>
                        <fpa:IdCodice>02468135791</fpa:IdCodice>
                    </fpa:IdFiscaleIVA>
                    <fpa:Anagrafica>
                        <fpa:Denominazione>
                            Azienda_Destinataria_Fatturazione
                        </fpa:Denominazione>
                    </fpa:Anagrafica>
                </fpa:DatiAnagrafici>
                <fpa:Sede>
                    <fpa:Indirizzo>via [...]</fpa:Indirizzo>
                    <fpa:NumeroCivico>99</fpa:NumeroCivico>
                    <fpa:CAP>12345</fpa:CAP>
                    <fpa:Comune>nome_citta</fpa:Comune>
                    <fpa:Provincia>XY</fpa:Provincia>
                    <fpa:Nazione>IT</fpa:Nazione>
                </fpa:Sede>
            </fpa:CessionarioCommittente>
        </md:Extensions>
        <md:Company>Azienda_Destinataria_Fatturazione</md:Company>
        <md:EmailAddress>email@fatturazione</md:EmailAddress>
        <md:TelephoneNumber>+39telefono_fatture</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

Esempio di metadata di un Gestore *full* (codice attività: `pub-op-full`)

Il seguente esempio di metadata è relativo all'attività di un Gestore, `Gestore S.p.A.`, operante in modalità *full*, che è dunque relativo a *tutti* i servizi per i quali l'Aggregatore eroga direttamente servizi di PP.AA. online.

```
<md:EntityDescriptor
        [...]
        entityID="https://gestore/pub-op-full/"
        ID="_uniqueID"
        [...]
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:spid="https://spid.gov.it/saml-extensions">
    [...]
    <md:Organization>
        <md:OrganizationName xml:lang="it">
            Gestore S.p.A.
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">
            Gestore
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">
            https://gestoreonline.it/
        </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregator">
        <md:Extensions>
            <spid:IPACode>cIPA_gestore</spid:IPACode>
            <spid:VATNumber>ITpartitaIVA_gestore</spid:VATNumber>
            <spid:FiscalCode>CF_gestore</spid:FiscalCode>
            <spid:PublicServicesFullOperator/>
        </md:Extensions>
        <md:Company>Gestore S.p.A.</md:Company>
        <md:EmailAddress>email@gestoreonine.it</md:EmailAddress>
        <md:TelephoneNumber>+39telefono_gestore</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

Esempio di metadata di una P.A. Aggregata in modalità *full* (codice attività: `pub-ag-full`)

Il seguente esempio di metadata è relativo a una P.A., `Ente Locale Aggregato`, aggregata da un Aggregatore privato, `Soggetto Aggregatore s.r.l.` (operante in modalità *full*), nel quale sono specificati, nell'ordine, i dati identificativi dell'Aggregatore e i dati identificativi dell'Aggregato.

```
<md:EntityDescriptor
        [...]
        entityID="https://aggregatore/pub-ag-full/estensione.aggregato"
        ID="_uniqueID"
```

```
        [...]
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:spid="https://spid.gov.it/saml-extensions">
    [...]
    <md:Organization>
        <md:OrganizationName xml:lang="it">
            Ente Locale Aggregato
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">
            E.L.A.
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">
            https://ela.gov.it/spid/
        </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregator">
        <md:Extensions>
            <spid:VATNumber>ITpartitaIVA_aggregatore</spid:VATNumber>
            <spid:FiscalCode>CF_aggregatore</spid:FiscalCode>
            <spid:PublicServicesFullAggregator/>
        </md:Extensions>
        <md:Company>Soggetto Aggregatore s.r.l.</md:Company>
        <md:EmailAddress>email@aggregatore</md:EmailAddress>
        <md:TelephoneNumber>+39tel_aggregatore</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregated">
        <md:Extensions>
            <spid:IPACode>cIPA_aggregato</spid:IPACode>
            <spid:Public/>
        </md:Extensions>
        <md:Company>Ente Locale Aggregato</md:Company>
    </md:ContactPerson>
</md:EntityDescriptor>
```

Esempio di metadata di un Gestore Aggregato in modalità *full* (codice attività: `pub-ag-full`)

Il seguente esempio di metadata è relativo a un Gestore, `Gestore S.p.A.`, aggregato da un Aggregatore privato, `Soggetto Aggregatore s.r.l.` (operante in modalità *full*), nel quale sono specificati, nell'ordine, i dati identificativi dell'Aggregatore e i dati identificativi del Gestore Aggregato.

```
<md:EntityDescriptor
        [...]
        entityID="https://aggregatore/pub-ag-full/estensione.gestore"
        ID="_uniqueID"
```

```
        [...]
        xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
        xmlns:spid="https://spid.gov.it/saml-extensions">
    [...]
    <md:Organization>
        <md:OrganizationName xml:lang="it">
            Gestore S.p.A.
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">
            Gestore
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">
            https://gestoreonline.it
        </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregator">
        <md:Extensions>
            <spid:VATNumber>ITpartitaIVA_aggregatore</spid:VATNumber>
            <spid:FiscalCode>CF_aggregatore</spid:FiscalCode>
            <spid:PublicServicesFullAggregator/>
        </md:Extensions>
        <md:Company>Soggetto Aggregatore s.r.l.</md:Company>
        <md:EmailAddress>email@aggregatore</md:EmailAddress>
        <md:TelephoneNumber>+39tel_aggregatore</md:TelephoneNumber>
    </md:ContactPerson>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregated">
        <md:Extensions>
            <spid:IPACode>cIPA_gestore</spid:IPACode>
            <spid:VATNumber>ITpartitaIVA_gestore</spid:VATNumber>
            <spid:FiscalCode>CF_gestore</spid:FiscalCode>
            <spid:PublicServicesOperator/>
        </md:Extensions>
        <md:Company>Gestore S.p.A.</md:Company>
        <md:EmailAddress>email@gestoreonine.it</md:EmailAddress>
        <md:TelephoneNumber>+39tel_gestore</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

Norme transitorie

Il presente Avviso abroga e sostituisce l'Avviso SPID №19/2020 versione 3.0.

Al fine di facilitare il *roll-over* dei certificati elettronici non conformi al presente Avviso:

- sino al **30 novembre 2020** sono ancora accettati sia metadata che *nuovi* certificati elettronici – per

l'apposizione di sigilli elettronici sulle *request* o sui metadata stessi – la cui struttura è conforme a quanto stabilito con la versione 3.0 del presente Avviso;

- entro il **20 dicembre 2020** gli Aggregatori che utilizzano certificati *non* conformi al presente Avviso DEVONO comunicare una nuova edizione dei metadata coinvolti, contenenti sia i certificati in uso alla data, sia i nuovi certificati – conformi al presente Avviso – destinati a sostituirli;
- entro il **15 gennaio 2021** gli Aggregatori di cui al punto precedente DEVONO sostituire i suddetti metadata rimuovendo *tutti* i certificati elettronici non conformi al presente Avviso.

Gli IDP adeguano i propri sistemi per gestire le estensioni SAML `spid:KeyDescriptor`, di cui a pagina 9, entro 80 giorni dalla data di emanazione del presente Avviso.

Il Responsabile del progetto SPID