SPID – SISTEMA PUBBLICO PER L'IDENTITA' DIGITALE
Avviso nr. 19

02/03/2020

Struttura del metadata dei soggetti aggregati

Il metadata di un Ente *aggregato*, entrato nella federazione SPID per mezzo di un *aggregatore* di servizi (nella fattispecie, di un soggetto aggregatore di fornitori di servizi), contiene particolari estensioni SAML che permettono agli altri enti della federazione SPID, di individuare l'aggregatore che –amministrativamente e tecnicamente– si presenta nella federazione per conto dell'aggregato. Tali estensioni contengono anche i recapiti dei referenti designati sia dell'Ente aggregato che del proprio soggetto aggregatore.

L'aggregatore invia ad AgID –tramite canali di comunicazione a tale scopo individuati dall'Agenzia– il metadata per ciascun soggetto aggregato, ogni sua ulteriore modificazione e, eventualmente, revoca.

L'**aggregatore** è identificato *univocamente*, all'interno della federazione SPID, mediante un `entityID` corrispondente a un nome URL che soddisfi le seguenti regole sintattiche:

- comprende lo *schema* HTTPS (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. sia `https://registry.spid.gov.it/metadata/sp` che `https://agid.gov.it/en/` sono validi, invece `https://agid.gov.it/datapolicy.pdf` *non* è valido);
- *non* contiene *query string* o ulteriori frammenti (quali, ad es., `?id=1234567#data`).

Il metadata dell'Ente aggregato presenta caratteristiche tecniche realizzate mediante la presenza dei seguenti elementi figli (tutti con *namespace* `md`), ovvero dei seguenti attributi dell'elemento `EntityDescriptor`:

- `entityID` — Attributo che identifica univocamente l'aggregato, è valorizzato con una stringa ottenuta concatenando l'`entityID` dell'**aggregatore** a un percorso URL *relativo* (anch'esso privo di *query string* o ulteriori frammenti), unico per l'**aggregato** nel contesto dell'aggregatore. Per esempio, l'`entityID` di un Ente aggregato dal soggetto aggregatore il cui `entityID` è `https://entityID/aggregatore`, può risultare in una stringa del tipo `https://entityID/aggregatore/estensione.unica.aggregato`.
- `Organization` (1 occorrenza) — contiene le informazioni di base circa l'Ente **aggregato**, mantenendo la massima retrocompatibilità con implementazioni SPID che non distinguono tra aggregatori e aggregati. Contiene i seguenti elementi, ciascuno dei quali ripetuto almeno una volta valorizzato in lingua italiana e eventuali occorrenze facoltative in ulteriori lingue (tutte identificate mediante l'attributo `xml:lang`, obbligatoriamente presente negli elementi sotto indicati):
    - `OrganizationName` (1 o più occorrenze nel caso multilingua) — Come da Regole Tecniche SPID, contiene il nome dell'Ente **aggregato** (p.es. *`EnteAggregato`*).
    - `OrganizationDisplayName` (1 o più occorrenze nel caso multilingua) — valorizzato con:
        - Nel caso in cui i dati personali dei soggetti autenticati siano trattati dal soggetto aggregatore (ad esempio, nel caso in cui il servizio dell'aggregato sia gestito dall'aggregatore), una stringa contenente la denominazione dell'**aggregato**, così come

contenuto nel corrispondente elemento `OrganizationName` (di pari lingua), più il nome dell'**aggregatore** (p.es. *SoggettoAggregatore*), concatenati tra loro tramite la parola " **tramite** ".

Ad esempio:

EnteAggregato tramite *SoggettoAggregatore*

- Nel caso in cui i dati personali dei soggetti autenticati non siano trattati dal soggetto aggregatore (ad esempio, nel caso in cui il sistema di autenticazione sia installato dall'aggregatore presso i sistemi informatici dell'aggregato e l'aggregatore non entri in possesso di detti dati), una stringa contenente la denominazione dell'**aggregato**, così come contenuto nel corrispondente elemento `OrganizationName` (di pari lingua).

  Ad esempio:

  EnteAggregato

- `OrganizationURL` (1 o più occorrenze nel caso multilingua) — contiene l'URL di una pagina del sito web dell'**aggregato**, i cui contenuti sono nella lingua specificata dall'attributo `xml:lang`.

Il numero di occorrenze di `OrganizationName` , `OrganizationDisplayName` e `OrganizationURL` sono uguali: non è possibile usare una seconda occorrenza in altra lingua solo in una o due delle tre.

- `ContactPerson` (2 occorrenze) — contiene informazioni sia per l'aggregato che per l'aggregatore. Entrambe le istanze sono corredate dall'attributo `contactType` valorizzato come `other`; l'istanza per l'**aggregato** è corredata anche dall'attributo obbligatorio `spid:entityType` valorizzato come `spid:aggregated`; l'istanza per l'**aggregatore** è corredata invece dall'attributo obbligatorio `spid:entityType` valorizzato come `spid:aggregator`.
  Ciascuna occorrenza dell'elemento `ContactPerson` contiene i seguenti sotto-elementi (tutti con *namespace* `md` quando non altrimenti specificato):
  - `Company` (1 occorrenza) — Contiene il nome dell'organizzazione che è la persona giuridica che svolge il ruolo di punto di contatto, per l'aggregatore o l'aggregato cui l'elemento genitore (`ContactPerson`) si riferisce. Coincide rispettivamente con *SoggettoAggregatore* o con *EnteAggregato*.
  - `Extensions` (1 occorrenza) — Contenente *almeno* uno dei seguenti sotto-elementi:
    1. `IPACode` (0 o 1 occorrenza, *namespace* `spid`) — Contiene il codice IPA dell'aggregatore o dell'aggregato cui l'antenato diretto (`ContactPerson`) si riferisce.
    2. `VATNumber` (0 o 1 occorrenza, *namespace* `spid`) — Contiene la partiva IVA dell'aggregatore o dell'aggregato cui l'antenato diretto (`ContactPerson`) si riferisce. Se la partita IVA corrisponde al codice fiscale, va indicato solo in questa estensione.
    3. `FiscalCode` (0 o 1 occorrenza, *namespace* `spid`) — Contiene il codice fiscale dell'aggregatore o dell'aggregato cui l'antenato diretto (`ContactPerson`) si riferisce. Se il codice fiscale corrisponde alla partita IVA va indicato solo nell'estensione `VATNumber`.

Per un punto di contatto privato, può essere presente sia il numero di partita IVA che il codice fiscale (entrambi obbligatori se diversi fra loro); per un Ente pubblico, è presente il codice IPA (obbligatorio) e può essere presente il numero di partita IVA e/o il codice fiscale.

Si veda il seguente esempio di metadata nel quale sono veicolate le informazioni del soggetto aggregatore (soggetto privato) e del soggetto aggregato (pubblico).

```
<md:EntityDescriptor
        […]
        entityID="https://entityID/aggregatore/estensione.unica.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">
            EnteAggregato
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">
            EnteAggregato tramite SoggettoAggregatore
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">
            https://url-SP-aggregato
        </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregator">
        <md:Company>SoggettoAggregatore</md:Company>
        <md:Extensions>
            <spid:VATNumber>pIVA aggregatore</spid:VATNumber>
            <spid:IPACode>cIPA_aggregatore</spid:IPACode>
            <spid:FiscalCode>CF_aggregatore</spid:FiscalCode>
        </md:Extensions>
    </md:ContactPerson>
    <md:ContactPerson
          contactType="other"
          spid:entityType="spid:aggregated">
        <md:Company>EnteAggregato</md:Company>
        <md:Extensions>
            <spid:IPACode>cIPA_aggregato</spid:IPACode>
        </md:Extensions>
    </md:ContactPerson>
</md:EntityDescriptor>
```

Sul metadata di ciascun **aggregato** è apposto un sigillo elettronico avanzato creato dall'**aggregatore** mediante la chiave corrispondente al certificato di federazione proveniente dall'infrastruttura a chiave pubblica (PKI) che AgID ha istituito appositamente per la gestione fiduciaria della federazione SPID. Tale certificato di federazione contiene l'`entityID` dell'**aggregatore** in un'apposita estensione di certificato. Nel caso in cui il processo di autenticazione è effettuato presso i sistemi del soggetto aggregatore, la predetta chiave è utilizzata

dall'aggregatore per sottoscrivere anche le richieste di autenticazione inviate ai gestori di identità digitale.

Nel caso in cui il soggetto aggregatore installi presso il soggetto aggregato il sistema di autenticazione, al metadata di ciascun **aggregato** è sempre apposto un sigillo elettronico avanzato creato dall'**aggregatore** mediante la chiave corrispondente al certificato di federazione proveniente dall'infrastruttura a chiave pubblica (PKI) di AgID, mentre le richieste di autenticazione inviate ai gestori di identità digitale sono sottoscritte con una chiave corrispondente ad un certificato generato dal soggetto aggregatore per lo specifico soggetto aggregato tramite una subCA il cui certificato è fornito dall'infrastruttura a chiave pubblica (PKI) di AgID.

Il presente avviso sostituisce altro avviso erroneamente pubblicato in pari data con il medesimo numero.

Il Responsabile del progetto SPID

STEFANO ARBIA