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

STEFANO ARBIA