SPID – SISTEMA PUBBLICO PER L'IDENTITÀ DIGITALE
Avviso nr. 29 – Versione 3
02/11/2020

SPECIFICHE TECNICHE PER I CERTIFICATI ELETTRONICI E I METADATA DEI SERVICE PROVIDER PUBBLICI E PRIVATI

Premessa

Al fine di chiarire quali sono i soggetti eleggibili a entrare nella federazione SPID in qualità di fornitori di servizi (**SP**) Pubbliche Amministrazioni (PP.AA.) si rimanda all'Avviso SPID №28/2020.

Struttura dei certificati elettronici dei Service Provider

Al fine dell'interoperabilità del Sistema Pubblico delle Identità Digitali (SPID), i certificati di sigillo elettronico utilizzati dai SP pubblici e privati per convalidare i sigilli elettronici sono conformi alla RFC-5280 e a quanto regolato dal presente Avviso.
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 SP, così come indicata nei pubblici registri, come riportata nel tag XML `<OrganizationName>` del metadata del SP (esempio: "`Comune di Forlì`" e *non* "`COMUNE DI FORLI'`"; anche "`Agenzia per l'Italia Digitale`" e *non* "`Agenzia per l'italia digitale`").
    b. `commonName` (OID 2.5.4.3) — La denominazione che valorizza l'estensione `organizationName`, eventualmente senza esplicitazione degli acronimi, come riportata nel tag XML `<OrganizationDisplayName>` del metadata del SP (esempio: "`AgID`").
    c. `uri` (OID 2.5.4.83) — EntityID del SP, così come riportato nell'attributo `entityID` del tag XML `<EntityDescriptor>` del metadata del SP.
    d. `organizationIdentifier` (OID 2.5.4.97) — Un codice identificativo unico del SP all'interno della federazione SPID, conforme alla sintassi prevista dalla norma ETSI EN 319-412-1, §5.1.4:
        i. **SP pubblici** — in base al §5.1.4 punto 3 della suddetta norma, valorizzato con il prefisso '`PA:IT-`' seguito dal codice IPA dell'Ente — ad esempio, per il Comune di Roma (codice IPA '`c_h501`') tale estensione è valorizzata come "`PA:IT-c_h501`";
        ii. **SP privati** — la seguente alternativa di codici utilizzando, in ordine di preferenza:
            - il numero di partita IVA (in base al §5.1.4 punto 1 della suddetta norma), preceduto dal prefisso '`VAT`' seguito dal codice ISO 3166-1 α-2 del Paese, seguito dal carattere '`-`' (`0x2D`) (ad esempio, "`VAT`*`IT-12345678901`*");
            - per i soggetti *non* provvisti di partita IVA, il codice fiscale (in base al §5.1.4 punto 2 della suddetta norma), preceduto dal 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 SP (esempio: "`IT`");
    f. `localityName` (OID 2.5.4.7) — il nome completo della città ove è situata la sede legale del SP (esempio: "`Forlì`" e *non* "`Forli'`").

2. Nel campo **`CertificatePolicies`**:
    a. `policyIdentifier` — contenente quantomeno uno dei seguenti identificatori:
        i. **SP pubblici** — `spid-publicsector-SP` (OID 1.3.76.16.**4.2.1**);
        ii. **SP privati** — `spid-privatesector-SP` (OID 1.3.76.16.**4.3.1**).

    I certificati di sigillo elettronico conformi con la Determinazione AgID №121/2019 s.m.i.[1] – anche se non qualificati[2] – 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.

Gli SP pubblici POSSONO creare autonomamente i certificati elettronici necessari. I certificati possono anche essere di tipo *self-signed*. Qualora il SP pubblico utilizzi un certificato dedicato all'apposizione del sigillo elettronico sul proprio metadata e un altro certificato[3] dedicato all'apposizione di sigilli elettronici sulle proprie *request*, il presente Avviso si applica a tutti questi certificati.

A seguito dell'accreditamento presso AgID, i SP privati ricevono un **certificato di federazione**[3] emesso dall'infrastruttura a chiave pubblica (**PKI**) che AgID ha istituito appositamente per la gestione dell'intera federazione SPID. Al fine di ottenere detto certificato si deve far riferimento all'Avviso SPID №23/2016 s.m.i. e compilare il previsto modulo di richiesta. La chiave privata cui tale certificato afferisce è utilizzata dal SP privato per apporre sigilli elettronici avanzati sia sul proprio metadata che sulle proprie *request*.

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, i SP 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**.

Struttura dei metadata dei Service Provider

Oltre a quanto previsto dalle Regole Tecniche e dagli Avvisi SPID, i metadata SAML dei SP pubblici e privati valorizzano i tag figli (tutti con *namespace* `md`), ovvero i seguenti attributi del tag `EntityDescriptor`, seguendo le disposizioni di cui al presente Avviso. Ove occorrano estensioni proprie di SPID, è adeguatamente definito il *namespace* XML associato: `https://spid.gov.it/saml-extensions`.

---

[1] 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*.
[2] Ai sensi del Regolamento (UE) №910/2014 s.m.i..
[3] Per particolari esigenze, sono ammessi più certificati per servizi del medesimo SP.

- `entityID` (1 occorrenza) — Attributo valorizzato con l'EntityID, così come riportato nell'estensione `commonName` del certificato elettronico del SP. In caso il SP svolga più attività – come ad esempio quella di SP pubblico e di SP privato – si dota di metadata SAML differenti, ciascuno con un diverso 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[4] dei tag figli facoltativi sopra definiti.
- `Organization` (1 occorrenza) — Contiene vari tag, ciascuno dei quali ripetuto almeno una volta valorizzato in lingua italiana, più occorrenze facoltative localizzanti il medesimo nome in ulteriori lingue (identificate mediante l'attributo `xml:lang`, obbligatoriamente presente in tutti i tag figli):
  - `OrganizationName` (1 o più occorrenze) — Denominazione – *completa e per esteso* e con il corretto uso di minuscole, maiuscole, lettere accentate e altri segni diacritici – del SP, così come riportata nell'estensione `organizationName` del certificato elettronico del SP (esempio: "`Agenzia per l'Italia Digitale`").
  - `OrganizationDisplayName` (1 o più occorrenze) — Denominazione del SP – eventualmente in forma abbreviata (ad esempio senza esplicitare gli eventuali acronimi) e con il corretto utilizzo delle minuscole e maiuscole – così come riportata nell'estensione `commonName` del certificato elettronico del SP (esempio: "`AgID`").

    Durante la fase di autenticazione, gli IDP avvisano l'utente dell'invio degli attributi al SP, visualizzando il valore di questo tag per indicare il soggetto richiedente.
  - `OrganizationURL` (1 o più occorrenze) — Contiene l'URL di una pagina del sito web del SP relativa al servizio di autenticazione o ai servizi accessibili tramite essa, i cui contenuti sono

[4] 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`).

localizzati nella lingua specificata dal proprio attributo `xml:lang`.

Sussiste il medesimo numero di occorrenze di `OrganizationName`, `OrganizationDisplayName` e `OrganizationURL`: non vi sono ulteriori occorrenze in altre lingue solo di uno o due di essi.

- `ContactPerson` (1 o 2 occorrenze) — Tag utilizzato per veicolare le informazioni per contattare il soggetto cui il metadata afferisce. Ogni occorrenza è dotata dei seguenti attributi:
  - `contactType` — L'occorrenza *obbligatoria* di `ContactPerson` è valorizzata con `other`; l'ulteriore occorrenza, obbligatoria per i soli SP privati, è valorizzata con `billing`.

  L'occorrenza di `ContactPerson` con l'attributo `contactType` valorizzato come `other` contiene i seguenti tag (*namespace* `md`):

  - `Extensions` (1 occorrenza *obbligatoria*) — Contenente almeno uno dei seguenti tag (tutti con *namespace* `spid`):
    1. `IPACode` — Presente *solo* per il SP *pubblico*, è valorizzato con il codice IPA dell'Ente.
    2. `VATNumber` — Obbligatorio per il SP *privato* dotato di partita IVA (altrimenti facoltativo), è valorizzato comprensivo del codice ISO 3166-1 α-2 del Paese (senza spazi).
    3. `FiscalCode` — Obbligatorio per il SP *privato* non dotato di partita IVA (altrimenti facoltativo), è valorizzato con il codice fiscale del SP.
    4. `Public` — Tag vuoto, *obbligatorio* per il SP pubblico o, *in alternativa*,
    5. `Private` — Tag vuoto, *obbligatorio* per il SP privato.
  - `Company` (0 o 1 occorrenze) — Se presente, è valorizzato come il tag `OrganizationName` contenuto nel tag `Organization`.
  - `EmailAddress` (1 occorrenza, *obbligatorio*) — Contiene l'indirizzo di posta elettronica per contattare il SP. 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 SP; *senza spazi* e comprensivo del prefisso internazionale (esempio: "`+39`" per l'Italia).

Informazioni obbligatorie per la fatturazione

L'occorrenza di `ContactPerson` con l'attributo `contactType` valorizzato come `billing` è obbligatoria in caso sia presente l'estensione `Private` nel tag `Extensions` (dell'occorrenza di `ContactPerson` con l'attributo `contactType` valorizzato come `other`). 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[5] **FatturaPA** dell'Agenzia delle Entrate, contiene i tag minimi necessari alla suddetta individuazione fiscale.

[5] 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`.

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` (0 o 1 occorrenze) — Obbligatoriamente presente qualora il soggetto per l'emissione delle fatture sia distinto dal SP stesso (e 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*) — Contiene l'indirizzo di posta elettronica, *aziendale o istituzionale*, per contattare il soggetto 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.

Il seguente esempio di metadata è relativo a un SP privato (`Organizzazione`), nel quale sono specificati sia i dati identificativi del SP, che i dati per la fatturazione elettronica da parte degli IDP.

```
<md:EntityDescriptor
        [...]
        entityID="https://entityID.unico/dell/SP"
        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">
            Denominazione Completa dell'Organizzazione s.r.l.
        </md:OrganizationName>
        <md:OrganizationDisplayName xml:lang="it">
            Organizzazione
        </md:OrganizationDisplayName>
        <md:OrganizationURL xml:lang="it">
            https://organizzazione.com/it
        </md:OrganizationURL>
    </md:Organization>
    <md:ContactPerson contactType="other">
        <md:Extensions>
            <spid:VATNumber>IT12345678901</spid:VATNumber>
            <spid:FiscalCode>XYZABCAAMGGJ000W</spid:FiscalCode>
```

```
            <spid:Private/>
        </md:Extensions>
        <md:EmailAddress>spid@organizzazione.com</md:EmailAddress>
        <md:TelephoneNumber>+390123456789</md:TelephoneNumber>
    </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>
                            Destinatario_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>Destinatario_Fatturazione</md:Company>
        <md:EmailAddress>email@fatturazione.it</md:EmailAddress>
        <md:TelephoneNumber>telefono_fatture</md:TelephoneNumber>
    </md:ContactPerson>
</md:EntityDescriptor>
```

Norme transitorie

Il presente Avviso abroga e sostituisce l'Avviso SPID №29/2020 versione 2.0.

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 2.0 del presente Avviso;
- entro il **20 dicembre 2020** gli SP privati che usano certificati *non* conformi al presente Avviso DEVONO comunicare una nuova edizione del proprio metadata, contenente sia il certificato o i certificati in uso alla data, sia i nuovi certificati – conformi al presente Avviso – destinati a sostituirli;
- entro il **15 gennaio 2021** gli SP privati di cui al punto precedente DEVONO sostituire il proprio metadata

rimuovendo *tutti* i certificati elettronici non conformi al presente Avviso.

Il Responsabile del progetto SPID

STEFANO ARBIA