



SPID – SISTEMA PUBBLICO PER L'IDENTITÀ DIGITALE

Avviso nr. 29 – Versione 2.0

08/10/2020

**ULTERIORI 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. **commonName** (OID [2.5.4.3](#)) — EntityID del SP, così come riportato nell'attributo **entityID** del tag XML **<EntityDescriptor>** del metadata del SP.
- b. **organizationName** (OID [2.5.4.10](#)) — Denominazione *completa e per esteso* del SP, così indicata nei pubblici registri e come riportata nel tag XML **<OrganizationName>** del metadata del SP (esempio: "Comune di Forlì" e *non* "COMUNE DI FORLI");
- c. **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, "VATIT-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.
- d. **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");
- e. **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](#)).

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.

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 certificato¹ dedicato all'apposizione di sigilli elettronici sulle proprie *request*, il presente Avviso si applica ad entrambi.

A seguito dell'accreditamento presso AgID, i SP privati ricevono un **certificato di federazione**¹ 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 e 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 la *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 occorran estensioni proprie di SPID, è adeguatamente definito il *namespace* XML associato: <https://spid.gov.it/saml-extensions>.

- **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.
- **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

¹ Per particolari esigenze, sono ammessi più certificati per servizi del medesimo SP.



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 (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 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*) — Contiene 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, *obbligatoria* per il SP pubblico o, *in alternativa*,
 5. **Private** — Tag vuoto, *obbligatoria* per il SP privato.
- **Company** (0 o 1 occorrenze) — Se presente, è valorizzato come il tag **OrganizationName** contenuto nel tag **Organization**.
- **EmailAddress** (1 occorrenza, *obbligatoria*) — 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 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*) — Contiene i tag minimi necessari alla suddetta individuazione fiscale, secondo la normativa nazionale per le fatture elettroniche in formato XML. Ad esempio, adottando il *namespace* preposto dell'Agenzia delle Entrate, <http://ivaservizi.agenziaentrate.gov.it/docs/xsd/fatture/v1.2> (nel tag **Extensions** o in uno dei suoi antenati), si usano i tag **CessionarioCommittente** e, opzionalmente, il tag **TerzoIntermediarioSoggettoEmittente**, presi dallo standard **FatturaPA**, cioè utilizzando il seguente albero genealogico *minimo* di tag:
 - **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**, **NumeroCivico** (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 inerenti alla 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:Organization>
</md:EntityDescriptor>
```



```
</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=
    "http://ivaservizi.agenziaentrate.gov.it/docs/xsd/fatture/v1.2">
    <fpa:CessionarioCommittente>
      <fpa:DatiAnagrafici>
        <fpa:IdFiscaleIVA>
          <fpa:IdPaese>IT</fpa:IdPaese>
          <fpa:IdCodice>02468135791</fpa:IdCodice>
        </fpa:IdFiscaleIVA>
        <fpa:Anagrafica>
          <fpa:Denominazione>
            Destinatarario_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>Destinatarario_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 N°29/2020 versione 1.0.



AGID

Agenzia per l'Italia Digitale

spod

Sino al 14 novembre 2020 sono ancora accettati metadata, nuovi o aggiornati, la cui struttura e i cui certificati di sigillo ivi contenuti – per l'apposizione di sigilli elettronici sulle *request* o sui metadata – siano conformi a quanto stabilito con la precedente versione 1.0 del presente Avviso.

Entro il 15 dicembre 2020 i SP privati devono sostituire i loro metadata e i relativi certificati presenti nel registro SPID e non conformi al presente Avviso.

Il Responsabile del progetto SPID