

DIVENTARE FORNITORE DI SERVIZI



PROCEDURA TECNICA
PROCEDURA AMMINISTRATIVA

DIVENTARE FORNITORE DI SERVIZI



1. segui le regole tecniche di AgID per attivare SPID e le indicazioni per rendere riconoscibile l'accesso agli utenti; effettua i test necessari di implementazione della piattaforma e individua un referente tecnico per le interlocuzioni con AgID;
2. predisponi e rendi disponibili per i controlli di AgID il metadata che consentirà ai gestori di identità (identity provider - IDP) di configurare l'accesso ai servizi con SPID. Dopo i controlli, il collaudo del servizio e la firma della convenzione, AgID comunica il metadata ai gestori;
3. se l'accesso con SPID ai tuoi servizi prevede il secondo o il terzo livello di sicurezza, devi implementare anche il nodo italiano eIDAS che consente l'accesso ai servizi pubblici italiani dei cittadini dell'UE;
4. terminati i processi tecnici, dopo il riscontro positivo di AgID, puoi sottoscrivere la convenzione SPID tramite un referente amministrativo. Firmata la convenzione, AgID informa i gestori e successivamente i servizi diventeranno accessibili con SPID.



Regole tecniche

Le caratteristiche del Service Provider devono essere definite attraverso metadata conformi allo standard SAML v2.0 (SAML-Metadata) e rispettare le condizioni di seguito indicate



Regole tecniche

Nell'elemento <EntityDescriptor> deve essere presente il seguente attributo:

entityID (1 occorrenza) - Attributo valorizzato con l'EntityID, così come riportato nell'estensione uri 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.

Contiene l'url dell'applicativo su cui deve essere attivato lo SPID

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  xmlns:spid="https://spid.gov.it/saml-extensions"
  xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
  entityID="https://spid.serviceprovider.it"
  ID="_0j40cj0848d8e3jncjdjss...">
```

Regole tecniche

Deve essere presente l'elemento `<KeyDescriptor>` contenente 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

```
<md:KeyDescriptor use="signing">  
  [...]  
</md:KeyDescriptor>
```

Regole tecniche

Deve essere presente l'elemento `<Signature>` riportante la firma sui metadata. La firma deve essere prodotta secondo il profilo specificato per SAML (SAML-Metadata, cap. 3) utilizzando chiavi RSA almeno a 2048 bit e algoritmo di digest SHA-256 o superiore;

```
<ds:Signature xmlns:ds="http://www.w3.org/2000/09/xmldsig#">  
  [...]  
</ds:Signature>
```

Regole tecniche

Deve essere presente un solo 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;

```
<md:SPSSODescriptor
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
  AuthnRequestsSigned="true"
  WantAssertionsSigned="true">
  <md:KeyDescriptor use="signing">
    [...]
  </md:KeyDescriptor>
  <SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://spid.serviceprovider.it/slo-location"
    ResponseLocation="https://spid.serviceprovider.it/slo-location"/>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  <md:AssertionConsumerService
    index="0" isDefault="true"
    Location="https://spid.serviceprovider.it/sso-location"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  <md:AssertionConsumerService
    index="1"
    Location="https://spidSP.serviceProvider.it/sso-location"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  <md:AttributeConsumingService index="0">
    <md:ServiceName xml:lang="it">Set 0</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">Set 1</md:ServiceName>
    <md:RequestedAttribute Name="spidCode"/>
    <md:RequestedAttribute Name="fiscalNumber"/>
  </md:AttributeConsumingService>
</md:SPSSODescriptor>
```

Regole tecniche

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, riportante 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'attributo isDefault posto al valore true;

```

<md:SPSSODescriptor
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
  AuthnRequestsSigned="true"
  WantAssertionsSigned="true">
  <md:KeyDescriptor use="signing">
    [...]
  </md:KeyDescriptor>
  <SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://spid.serviceprovider.it/slo-location"
    ResponseLocation="https://spid.serviceprovider.it/slo-location"/>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  <md:AssertionConsumerService
    index="0" isDefault="true"
    Location="https://spid.serviceprovider.it/sso-location"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  <md:AssertionConsumerService
    index="1"
    Location="https://spidSP.serviceProvider.it/sso-location"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" />
  <md:AttributeConsumingService index="0">
    <md:ServiceName xml:lang="it">Set 0</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">Set 1</md:ServiceName>
    <md:RequestedAttribute Name="spidCode" />
    <md:RequestedAttribute Name="fiscalNumber" />
  </md:AttributeConsumingService>
</md:SPSSODescriptor>

```

Regole tecniche

Deve essere presente almeno un elemento `<SingleLogoutService>` indicante l'indirizzo del `SingleLogoutService` e riportante i seguenti attributi:

Location URL endpoint del servizio per la ricezione delle richieste di Single Logout;

Binding che può assumere uno dei valori

`urn:oasis:names:tc:SAML:2.0:bindings:SOAP`

`urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect`

Redirect

`urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST`

ed opzionalmente l'attributo:

ResponseLocation, URL endpoint del servizio per la ricezione delle risposte alle richieste di Single Logout.

```
<md:SPSSODescriptor
  protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol"
  AuthnRequestsSigned="true"
  WantAssertionsSigned="true">
  <md:KeyDescriptor use="signing">
    [...]
  </md:KeyDescriptor>
  <SingleLogoutService
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"
    Location="https://spid.serviceprovider.it/slo-location"
    ResponseLocation="https://spid.serviceprovider.it/slo-location"/>
  <NameIDFormat>urn:oasis:names:tc:SAML:2.0:nameid-format:transient</NameIDFormat>
  <md:AssertionConsumerService
    index="0" isDefault="true"
    Location="https://spid.serviceprovider.it/sso-location"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  <md:AssertionConsumerService
    index="1"
    Location="https://spidSP.serviceProvider.it/sso-location"
    Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"/>
  <md:AttributeConsumingService index="0">
    <md:ServiceName xml:lang="it">Set 0</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">Set 1</md:ServiceName>
    <md:RequestedAttribute Name="spidCode"/>
    <md:RequestedAttribute Name="fiscalNumber"/>
  </md:AttributeConsumingService>
</md:SPSSODescriptor>
```



Regole tecniche

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 (senza esplicitare gli eventuali acronimi) 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.

```
<md:Organization>  
  <OrganizationName xml:lang="it">Service provider</OrganizationName>  
  <OrganizationDisplayName xml:lang="it">Nome service provider</OrganizationDisplay  
  <OrganizationURL xml:lang="it">http://spid.serviceprovider.it</OrganizationURL>  
</md:Organization>
```



Regole tecniche

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.

```
<md:ContactPerson contactType="other">  
  <md:Extensions>  
    <spid:VATNumber>IT12345678901</spid:VATNumber>  
    <spid:FiscalCode>XYZABCAAMGGJ000W</spid:FiscalCode>  
    <spid:Private/>  
  </md:Extensions>  
  <md:EmailAddress>tech-info@example.org</md:EmailAddress>  
  <md:TelephoneNumber>+39 8472345634785</md:TelephoneNumber>  
</md:ContactPerson>
```



Regole tecniche

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):

IPACode — Presente solo per il SP pubblico, è valorizzato con il codice ipa dell'Ente.

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).

FiscalCode — Obbligatorio per il SP privato non dotato di partita iva (altrimenti facoltativo), è valorizzato con il codice fiscale del SP.

Public — Tag vuoto, obbligatorio per il SP pubblico o,

in alternativa,

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).



Regole tecniche

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 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, 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.

Regole tecniche

Informazioni obbligatorie per la fatturazione

Esempio: Contatti metadata SP per Fatturazione

```

1  <md:EntityDescriptor
2    entityID="https://entityID.unico/dell/SP"
3    ID="_uniqueID"
4    xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"
5    xmlns:spid="https://spid.gov.it/saml-extensions">
6    <md:Organization>
7      <md:OrganizationName xml:lang="it">
8        Denominazione Completa dell'Organizzazione s.r.l.
9      </md:OrganizationName>
10     <md:OrganizationDisplayName xml:lang="it">
11       Organizzazione
12     </md:OrganizationDisplayName>
13     <md:OrganizationURL xml:lang="it">
14       https://organizzazione.com/it
15     </md:OrganizationURL>
16   </md:Organization>
17   <md:ContactPerson contactType="other">
18     <md:Extensions>
19       <spid:VATNumber>IT12345678901</spid:VATNumber>
20       <spid:FiscalCode>XYZABCAAMGGJ000W</spid:FiscalCode>
21       <spid:Private/>
22     </md:Extensions>
23     <md:EmailAddress>spid@organizzazione.com</md:EmailAddress>
24     <md:TelephoneNumber>+390123456789</md:TelephoneNumber>
25   </md:ContactPerson>

```

```

26   <md:ContactPerson contactType="billing">
27     <md:Extensions
28       xmlns:fpa="https://spid.gov.it/invoicing-extensions">
29       <fpa:CessionarioCommittente>
30         <fpa:DatiAnagrafici>
31           <fpa:IdFiscaleIVA>
32             <fpa:IdPaese>IT</fpa:IdPaese>
33             <fpa:IdCodice>02468135791</fpa:IdCodice>
34           </fpa:IdFiscaleIVA>
35           <fpa:Anagrafica>
36             <fpa:Denominazione>
37               Destinatarario_Fatturazione
38             </fpa:Denominazione>
39           </fpa:Anagrafica>
40         </fpa:DatiAnagrafici>
41         <fpa:Sede>
42           <fpa:Indirizzo>via [...]</fpa:Indirizzo>
43           <fpa:NumeroCivico>99</fpa:NumeroCivico>
44           <fpa:CAP>12345</ fpa:CAP>
45           <fpa:Comune>nome_citta</fpa:Comune>
46           <fpa:Provincia>XY</fpa:Provincia>
47           <fpa:Nazione>IT</fpa:Nazione>
48         </fpa:Sede>
49       </fpa:CessionarioCommittente>
50     </md:Extensions>
51     <md:Company>Destinatarario_Fatturazione</md:Company>
52     <md:EmailAddress>email@fatturazione.it</md:EmailAddress>
53     <md:TelephoneNumber>telefono_fatture</md:TelephoneNumber>
54   </md:ContactPerson>
55 </md:EntityDescriptor>

```




Metadata

Esempio di metadata validato

<ds:SignatureValue> contiene la firma

```
<ds:SignatureValue> 3Sym1jjZokttmOZn+pz1qkhzKdWjccM+AoMnv+Cx4biDQbWyMykupk/qiDMyGPBgx+ziVz7KethF
TZHJpYgSkzgmfGBWfxxBNcciPT7gFfwVPRpdXDVOLEUtzVly+k109K0tavx8zosXJ7e9KMcfq6u untI5lQaxhw1+vZn05iwoMn37sFAKAE3NEGvwPXmg2MZUHpxafw4ufRPowOy4dcOS7en7jlVEyN1
Mjun85ALhrhjtA7TMQ1hldJ4Jrw7XQyUwwWZkSF+sk5pWDupmdT6DsC+gPB+Y2iKOpaaafpAwApD xFi0BbKHZFXoFGGEDCHGIc+oFQ1TvMqRHwvoc2j2o2QXj5ilfUjLRmEMLHti17rMPxbcV5GBZe/q
8wEUo6ZUnygt9czIpbRaSgCubkebnBDkZmirtIX9mQqr3rBQefY+D7xtavQUOKf1Zi2vTaMrF9G+ zGqNQVN5BE0gCoXsE4qQZ9Sj0kXPoh0vJuJuIpgzms5rx8iZKsTtikDPqsU+RuJi4B83KSQVnhd
GGrhhd8d+fezYtR44WvIuiznN/yDsp3j+E1B52FfrjtR0Jl8LVvZR6YSvS1rYagTmZVU111RK6tfp S73lprekTOqwSN+FQXsBxJT6GVRkD2Bocv8tInnim6rpZNIUDe2gNPuUOYBjpxjSJuvk+PEMaEo=
</ds:SignatureValue>
```




Metadata

Esempio di metadata validato

entityID contiene l'url dell'applicativo su cui deve essere attivato lo SPID

```
▼ <md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata"  
  xmlns:spid="https://spid.gov.it/saml-extensions" ID="_f3f3d1d0-f317-45fa-96e7-0799110f6f06"  
  entityID="https://www.comune. . . .it">
```



Metadata

Esempio di metadata validato

Location di <md:SingleLogoutService deve contenere il metodo presente sull'applicativo che deve essere chiamato per effettuare il Logout.

```
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https://www.comuneweb.it/SPID/SSOLogout.ashx"/>  
<md:SingleLogoutService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect"  
Location="https://servizi.comune.it/SpidSaml/LogoutRequest"/>
```



Metadata

Esempio di metadata validato

Location di <md:AssertionConsumerService deve contenere l'URL endpoint del servizio da chiamare 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'attributo isDefault posto al valore true;

```
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https://portaleservizi.comune. . . . .it/Spid . . . . . /AssertionConsumer"  
index="0" isDefault="true"/>
```

```
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https:// . . . . .comune.pluginpay.it/spidacs" index="0" isDefault="true"/>  
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https:// . . . . .comuneweb.it/SPID/SSOLogin.ashx" index="1"/>  
<md:AssertionConsumerService Binding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST"  
Location="https://servizi.comune. . . . .it/SpidSaml/ACS" index="2"/>
```

Metadata

Esempio di metadata validato

Poi vengono indicati gli attributi (md:RequestedAttribute) che devono essere passati a SPID.

```
▼ <md:AttributeConsumingService index="0">  
  <md:ServiceName xml:lang="it">Portale dei pagamenti del cittadino</md:ServiceName>  
  <md:RequestedAttribute Name="spidCode"/>  
  <md:RequestedAttribute Name="familyName"/>  
  <md:RequestedAttribute Name="name"/>  
  <md:RequestedAttribute Name="companyName"/>  
  <md:RequestedAttribute Name="fiscalNumber"/>  
  <md:RequestedAttribute Name="ivaCode"/>  
  <md:RequestedAttribute Name="email"/>  
  <md:RequestedAttribute Name="gender"/>  
  <md:RequestedAttribute Name="placeOfBirth"/>  
  <md:RequestedAttribute Name="countyOfBirth"/>  
  <md:RequestedAttribute Name="dateOfBirth"/>  
</md:AttributeConsumingService>
```

Metadata

Esempio di metadata validato



Se il metadata contiene un'aggregazione di servizi, allora troveremo definiti altri `<md:AttributeConsumingService index="1">` con index differenti e con i relativi attributi da prendere in considerazione per quel determinato servizio.

Metadata

Esempio di metadata validato

Poi vengono indicati gli attributi (md:RequestedAttribute) che devono essere passati a SPID.

Secondo servizio

```
▼ <md:AttributeConsumingService index="1">
  <md:ServiceName xml:lang="it">Accesso ai servizi ComuneWeb</md:ServiceName>
  <md:RequestedAttribute Name="spidCode"/>
  <md:RequestedAttribute Name="familyName"/>
  <md:RequestedAttribute Name="name"/>
  <md:RequestedAttribute Name="companyName"/>
  <md:RequestedAttribute Name="fiscalNumber"/>
  <md:RequestedAttribute Name="ivaCode"/>
  <md:RequestedAttribute Name="email"/>
  <md:RequestedAttribute Name="gender"/>
  <md:RequestedAttribute Name="placeOfBirth"/>
  <md:RequestedAttribute Name="countyOfBirth"/>
  <md:RequestedAttribute Name="dateOfBirth"/>
</md:AttributeConsumingService>
```



Metadata

Esempio di metadata validato

Poi vengono indicati gli attributi (md:RequestedAttribute) che devono essere passati a SPID.

Terzo servizio

```
▼ <md:AttributeConsumingService index="2">
  <md:ServiceName xml:lang="it">Istanze Online          Srl</md:ServiceName>
  <md:ServiceDescription xml:lang="it"> SISTEMA PER LA COMPILAZIONE E PRESENTAZIONE ON-LINE DELLE ISTANZE, DICHIARAZIONI E SEGNALAZIONI ALLA
  PUBBLICA AMMINISTRAZIONE </md:ServiceDescription>
  <md:RequestedAttribute Name="spidCode" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="name" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="gender" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="placeOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="ivaCode" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="companyName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="mobilePhone" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="address" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="expirationDate" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="digitalAddress" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="registeredOffice" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="idCard" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="countyOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="dateOfBirth" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="familyName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
  <md:RequestedAttribute Name="fiscalNumber" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"/>
</md:AttributeConsumingService>
```



Metadata

Esempio di metadata validato

Qui vengono indicati i dati dell'Ente

```
▼ <md:Organization>
  <md:OrganizationName xml:lang="it">Comune di ... </md:OrganizationName>
  <md:OrganizationDisplayName xml:lang="it">Comune ... </md:OrganizationDisplayName>
  <md:OrganizationURL xml:lang="it">https://www.comune. ... .it</md:OrganizationURL>
</md:Organization>
▼ <md:ContactPerson contactType="other">
  ▼ <md:Extensions>
    <spid:IPACode>c_ ... </spid:IPACode>
    <spid:Public/>
  </md:Extensions>
  <md:EmailAddress>comune. ... @pec. ... .it</md:EmailAddress>
</md:ContactPerson>
```



Metadata

Esempio di metadata validato

Per inviarlo, occorre inviare una email a spid.tech@agid.gov.it indicando le seguenti informazioni:

1. Nome ente (denominazione o ragione sociale) e alternativamente:
 1. se soggetto pubblico, Codice IPA
 2. se soggetto privato, Codice Fiscale o P.IVA
2. URL del metadata;
3. Se si tratta di aggiornamento o nuovo metadata;
4. URL del servizio al quale è presente il bottone “Entra con SPID” con il collegamento a SPID Validator;
5. Contatto riferimento tecnico (nominativo, e-mail, num. di telefono);
6. Contatto referente amministrativo (nominativo, e-mail, num. di telefono);

Il metadata deve essere reso disponibile su una URL 'https' del dominio.

Procedura amministrativa



Completata la procedura tecnica, AgID invierà al referente amministrativo un'e-mail di conferma con la copia della "Convenzione per l'adesione delle Pubbliche Amministrazioni al Sistema Pubblico per le Identità Digitali"

Procedura amministrativa



Agenzia per l'Italia Digitale
Presidenza del Consiglio dei Ministri



Upload Logo
Amministrazione

CONVENZIONE PER L'ADESIONE DELLE PUBBLICHE AMMINISTRAZIONI AL SISTEMA PUBBLICO PER LE IDENTITÀ DIGITALI

(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

Il del mese di dell'anno

TRA

L'Agenzia per l'Italia Digitale (di seguito "AgID"), codice fiscale n.97735020584,
in persona del Direttore e legale rappresentante pro tempore, con sede in
Roma - Viale Liszt 21,

E

L'amministrazione
(di seguito Amministrazione), con sede in:
Prov. () indirizzo: , cap
Cod.Fiscale/partita IVA: , codice iscrizione
all'Indice delle Pubbliche Amministrazioni (I.P.A.):
in persona del ,
(ruolo del firmatario nell'Amministrazione)

(nome e cognome del firmatario);

PREMESSO CHE

convenzione non utilizzabile per la sottoscrizione.
mento al sito dell'AgID.

Procedura amministrativa



Schema α
Fare riferir

1. l'articolo 64, comma 2-bis del Decreto legislativo n. 82/2005 (Codice dell'Amministrazione Digitale, di seguito "CAD") prevede che *"per favorire la diffusione di servizi in rete e agevolare l'accesso agli stessi da parte di cittadini e imprese, anche in mobilità, è istituito, a cura dell'Agenzia per l'Italia digitale, il sistema pubblico per la gestione dell'identità digitale di cittadini e imprese"* (di seguito "SPID");
2. l'articolo 64, comma 2-quater del CAD stabilisce che *"Il sistema SPID è adottato dalle pubbliche amministrazioni nei tempi e secondo le modalità definiti con il decreto di cui al comma 2-sexies"*;
3. l'articolo 64, comma 2-sexies del CAD stabilisce che *"Con decreto del Presidente del Consiglio dei ministri, [OMISSIS], sono definite le caratteristiche del sistema SPID, anche con riferimento:*
 - a) *al modello architetturale e organizzativo del sistema;*

Attoscrizione. Fare

CONVENZIONE PER L'ADESIONE DELLE PUBBLICHE AMMINISTRAZIONI
AL SISTEMA PUBBLICO PER LE IDENTITÀ DIGITALI
(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

- b) *alle modalità e ai requisiti necessari per l'accreditamento dei gestori dell'identità digitale;*
- c) *agli standard tecnologici e alle soluzioni tecniche e organizzative da adottare anche al fine di garantire l'interoperabilità delle credenziali e degli strumenti di accesso resi disponibili dai gestori dell'identità digitale nei riguardi di cittadini e imprese, compresi gli strumenti di cui al comma 1;*
- d) *alle modalità di adesione da parte di cittadini e imprese in qualità di utenti di servizi in rete;*
- e) *ai tempi e alle modalità di adozione da parte delle pubbliche amministrazioni in qualità di erogatori di servizi in rete;*
- f) *alle modalità di adesione da parte delle imprese interessate in qualità di erogatori di servizi in rete"*;

Procedura amministrativa

Schema convenzione non utilizzabile per la sofferenza al sito dell'AgID.

4. nella Gazzetta Ufficiale n. 285 del 9 dicembre 2014, è stato pubblicato il DPCM 24 ottobre 2014, recante *“Definizione delle caratteristiche del sistema SPID, nonché dei tempi e delle modalità di adozione del sistema pubblico per la gestione dell’identità digitale di cittadini e imprese (SPID) da parte delle pubbliche amministrazioni e delle imprese”* (di seguito DPCM);
5. il DPCM stabilisce le caratteristiche dello SPID, consentendo agli utenti di avvalersi di gestori dell’identità digitale e di gestori di attributi qualificati, per consentire ai fornitori di servizi qualificati erogati in rete l’immediata verifica della propria identità e di eventuali attributi qualificati che li riguardano;
6. l’art. 4 del DPCM prevede l’attivazione dello SPID da parte dell’AgID, che a tal fine è chiamata a svolgere le seguenti attività:
 - a) gestisce l’accreditamento dei gestori dell’identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni;
 - b) cura l’aggiornamento del Registro SPID e vigila sull’operato dei soggetti che partecipano allo SPID, anche con possibilità di conoscere, tramite il gestore dell’identità digitale, i dati identificativi dell’utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate;
 - c) stipula apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità;
7. l’art. 13, comma 1, del DPCM stabilisce che *“I fornitori di servizi possono aderire allo SPID stipulando apposita convenzione con l’Agenzia il cui schema è definito nell’ambito dei regolamenti attuativi di cui all’art. 4”*;
8. l’art. 14, comma 1, del DPCM stabilisce che *“le pubbliche amministrazioni che erogano in rete servizi qualificati, direttamente o tramite altro fornitore di servizi, consentono l’identificazione informatica degli utenti attraverso l’uso di SPID”*;
9. l’art. 14, comma 2, del DPCM stabilisce che *“le pubbliche amministrazioni di cui all’art. 2, comma 2, del CAD aderiscono allo SPID, secondo le modalità stabilite dall’Agenzia ai sensi dell’art. 4, entro i ventiquattro mesi successivi all’accreditamento del primo gestore dell’identità digitale”*;

Procedura amministrativa

(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

10. l'art. 14, comma 5, del DPCM stabilisce che *"Le pubbliche amministrazioni, in qualità di fornitori dei servizi, usufruiscono gratuitamente delle verifiche rese disponibili dai gestori di identità digitali e dai gestori di attributi qualificati"*;

11. l'art. 1 lettera i) del DPCM definisce come fornitore di servizi: *"il fornitore dei servizi della società dell'informazione definiti dall'art. 2, comma 1, lettera a), del decreto legislativo 9 aprile 2003, n. 70, o dei servizi di un'amministrazione o di un ente pubblico erogati agli utenti attraverso sistemi informativi accessibili in rete. I fornitori di servizi inoltrano le richieste di identificazione informatica dell'utente ai gestori dell'identità e ne ricevono l'esito"*;

12. l'art. 1 lettera i) del DPCM stabilisce, inoltre, che *"i fornitori di servizi, nell'accettare l'identità digitale, non discriminano gli utenti in base al gestore dell'identità digitale che l'ha fornita"*;

13. con Determinazione AgID n. 44/2015 del 28 luglio 2015, sono stati emanati i Regolamenti previsti dall'art. 4, commi 2 e 3, DPCM, concernenti:

- le modalità attuative per la realizzazione dello SPID;
- le regole tecniche;
- le modalità di accreditamento e vigilanza dei gestori di identità digitale;
- le procedure necessarie a consentire ai gestori dell'identità digitale, tramite l'utilizzo di altri sistemi di identificazione informatica conformi ai requisiti dello SPID, il rilascio dell'identità digitale.

TUTTO CIÒ PREMESSO SI CONVIENE E SI STIPULA QUANTO SEGUE

Art. 1 - Oggetto e finalità della convenzione

1 La presente Convenzione disciplina il rapporto fra AgID e l'Amministrazione nell'ambito del Sistema pubblico per le identità digitali (SPID) per l'espletamento da parte dell'Amministrazione di tutte le attività necessarie per l'adesione a SPID.

2. Sottoscrivendo il presente atto, l'Amministrazione si impegna a rispettare la normativa vigente che disciplina lo SPID nonché le regole e i relativi aggiornamenti emanati da AgID.

3. Entro il termine di dieci giorni dalla stipula della presente Convenzione, AgID dispone l'iscrizione dell'Amministrazione nell'apposito registro di cui all'art.1, comma 1, lett. s) del DPCM.

Art. 2 - Obblighi dell'Amministrazione

1. L'Amministrazione, a seguito dell'iscrizione nel Registro SPID, si obbliga:

- a) a comunicare ad AgID e mantenere aggiornato l'elenco dei servizi qualificati erogati in rete e le informazioni tecniche richieste da AgID per consentire la fruizione degli stessi previa autenticazione SPID;

Schema convenzione non utilizzabile per la sottoscrizione. Fare riferimento al sito dell'AgID.

Procedura amministrativa



Schema convenzione non utilizzabile per la sottoscrizione.
Fare riferimento al sito dell'AgID.

AL SISTEMA PUBBLICO PER LE IDENTITÀ DIGITALI
(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

- b) a comunicare ad AgID, per ciascuno dei servizi qualificati erogati in rete compresi nell'elenco, la lista degli attributi SPID necessari alla fruizione, i quali devono risultare pertinenti e non eccedenti in relazione alla tipologia e alle funzionalità offerte dal servizio;
- c) a inviare ad AgID una sintetica nota che, ai sensi di quanto previsto dall'art.6, comma 5, del DPCM e dall'art.3, comma 1, lett. b), del Regolamento AgID sulle modalità attuative, fornisca una motivazione in merito ai livelli di sicurezza adottati e agli attributi (identificativi, non identificativi e qualificati) richiesti per ciascuno dei servizi erogati;
- d) a porre in essere ogni attività strumentale connessa all'adesione allo SPID nel rispetto delle modalità definite da AgID in conformità al Regolamento recante le regole tecniche.
- e) a rispettare quanto specificato nelle "Note tecniche sulle interfacce e sulle Informazioni Idp/Sp" pubblicate sul sito AgID come previsto dall'appendice D del "Regolamento recante le modalità attuative per la realizzazione dello SPID" con riferimento all'accesso ai servizi qualificati erogati in rete e all'uso degli elementi grafici identificativi dello SPID;
- f) a comunicare tempestivamente all'indirizzo: protocollo@pec.agid.gov.it ogni malfunzionamento o incidente sulla sicurezza occorso al sistema di autenticazione fermo restando l'obbligo per le pubbliche amministrazioni di comunicare - entro e non oltre 24 ore dall'avvenuta conoscenza dall'accaduto - al Garante per la protezione dei dati personali e ad AgID eventuali violazioni ed intrusioni nei dati personali dei soggetti per i quali chiede la verifica dell'identità digitale, anche in conformità al Provvedimento del Garante per la protezione dei dati personali riguardante le misure di sicurezza e modalità di scambio dei dati personali tra amministrazioni pubbliche;
- g) a vincolarsi alla scrupolosa osservanza delle disposizioni contenute nel Decreto Legislativo 30 giugno 2003, n.196 e successive modifiche, in particolare per quanto concerne la sicurezza dei dati, gli adempimenti e la responsabilità nei confronti degli interessati, dei terzi e dell'Autorità del Garante per la protezione dei dati personali. In particolare, l'amministrazione si impegna a non acquisire attraverso lo SPID attributi e informazioni non necessari alla fruizione del servizio richiesto dall'utente;
- h) a registrare gli eventi relativi a richieste di accesso ai servizi (log) secondo quanto previsto nei regolamenti AgID;
- i) a garantire che agli eventi registrati (log) sia apposto un riferimento temporale che corrisponda alla scala di tempo UTC (IEN) di cui al decreto del Ministro dell'Industria del commercio ed artigianato 30 novembre 1993, n. 591, con una differenza non superiore ad un minuto primo;
- j) a garantire la disponibilità delle funzioni, l'applicazione dei modelli architettonici secondo le disposizioni previste dal DPCM e dai Regolamenti attuativi AgID;
- k) ad assistere l'utente nella risoluzione di eventuali problematiche che si dovessero verificare nel corso dell'autenticazione (*help desk* di primo livello), facendosi carico, se necessario, di indirizzare l'utente verso il

Procedura amministrativa

(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

gestore delle identità digitali coinvolto nella transazione (assistenza tecnica).

2. L'Amministrazione, inoltre, si impegna a collaborare con AgID nell'attività di monitoraggio e controllo e, in particolare, si obbliga:
 - a) ad inviare ad AgID, in forma aggregata, i dati da questa richiesti che possono essere utilizzati esclusivamente a fini statistici ed essere resi pubblici in forma aggregata. AgID, prima della pubblicazione, verifica che i dati resi pubblici siano effettivamente anonimi nel loro complesso, individuando la presenza di eventuali *outlier* statistici generati durante le fasi di analisi;
 - b) a dare immediata comunicazione ad AgID di ogni circostanza, reale o potenziale, che possa eventualmente inficiare la corretta esecuzione delle attività di cui alla presente Convenzione.

Art. 3 – Compiti dell'Agenzia per l'Italia Digitale

1. L'AgID cura l'attivazione dello SPID e sovrintende al corretto funzionamento del sistema, svolgendo, in particolare, le seguenti attività:
 - a) gestisce l'accreditamento dei gestori dell'identità digitale e dei gestori di attributi qualificati, stipulando con essi apposite convenzioni;
 - b) stipula delle Convenzioni con le pubbliche amministrazioni ed i privati aderenti a SPID in qualità di fornitori di servizi qualificati erogati in rete;
 - c) cura l'aggiornamento del registro SPID e vigila sull'operato dei soggetti che partecipano allo SPID, anche con possibilità di conoscere, tramite il gestore dell'identità digitale, i dati identificativi dell'utente e verificare le modalità con cui le identità digitali sono state rilasciate e utilizzate;
 - d) stipula apposite convenzioni con i soggetti che attestano la validità degli attributi identificativi e consentono la verifica dei documenti di identità.
2. L'AgID, nell'ambito delle proprie attività di vigilanza e controllo sullo SPID:
 - a) pubblica statistiche e dati aggregati sullo SPID;
 - b) riceve da tutti i soggetti di cui all'art. 3, comma 1, del DPCM le segnalazioni di malfunzionamenti o incidenti di sicurezza;
 - c) trasmette ai soggetti di cui all'art. 3, comma 1, del DPCM ogni informazione rilevante per la propria attività;
 - d) valuta l'applicazione di quanto previsto dai Regolamenti AgID, promuovendo la soluzione di eventuali problematiche di interoperabilità;
 - e) segnala all'Amministrazione le eventuali difformità riscontrate;
 - f) promuove l'adozione di criteri per rendere omogenei e congruenti a livello nazionale l'uso dei livelli di credenziali;
 - g) rende pubblici annualmente i risultati del proprio lavoro.

Schema convenzione non utilizzabile per la sottoscrizione.
Fare riferimento al sito dell'AgID.

Procedura amministrativa



Schema convenzione non utilizzabile per la sottoscrizione.
Fare riferimento al sito dell'AgID.

CONVENZIONE PER L'ADESIONE DEL SERVIZIO AMMINISTRATIVO
AL SISTEMA PUBBLICO PER LE IDENTITÀ DIGITALI
(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

Art. 4 – Trattamento dei dati

1. L'Amministrazione si impegna a trattare i dati personali nell'ambito dell'erogazione del servizio qualificato erogato in rete nel rispetto del principio di necessità e delle altre garanzie fissate dal Codice sulla protezione dei dati personali e per le finalità previste nell'art.64 del CAD e nell'art. 2, comma 2, del DPCM, secondo le modalità fissate nei Regolamenti attuativi dell'AgID.

Art. 5 – Durata, modifiche e integrazioni

1. La presente Convenzione ha durata quinquennale, a decorrere dalla sua sottoscrizione da parte dell'AgID, e non può essere oggetto di rinnovo tacito.
2. La presente convenzione è unica per tutte le Amministrazioni. Modifiche e/o integrazioni saranno possibili, acquisito il parere del Garante per la protezione dei dati personali, in presenza di accordo delle parti oltre che in tutti i casi sia necessario adeguarne il contenuto al mutamento della normativa e dei Regolamenti adottati da AgID.

Art. 6 – Figure di riferimento per l'attuazione della convenzione

1. Sia l'AgID che l'Amministrazione nominano un proprio Referente ai fini della corretta applicazione della presente Convenzione e della gestione delle relative comunicazioni.
2. AgID pubblica sul proprio sito istituzionale, nell'apposita sezione SPID, il nome del proprio Referente e il relativo indirizzo di Posta Elettronica Certificata (PEC); l'Amministrazione nomina quale proprio Referente: [redacted]
recapito PEC: [redacted].
3. Le parti si impegnano a comunicare tempestivamente ogni variazione del nominativo e dei recapiti dei referenti.

Art. 7 – Inadempimento e risoluzione della Convenzione

1. Quando nell'attività di valutazione, controllo o vigilanza, vengano riscontrati inadempimenti dell'Amministrazione degli obblighi assunti con la presente Convenzione nonché degli altri obblighi in capo ai fornitori di servizi previsti nel DPCM e nei Regolamenti attuativi del sistema SPID in capo ai Fornitori di Servizi, AgID invia una contestazione, prescrivendo ove necessario le attività che devono essere poste in essere al fine del ripristino della regolarità del servizio reso agli utenti.
2. Nei casi di violazione di particolare gravità oppure nel caso di mancato adeguamento dell'Amministrazione alle prescrizioni richieste, AgID nel termine assegnato ha diritto di dichiarare risolta *ipso jure* la presente convenzione.
3. Nel caso in cui l'Amministrazione cessi la propria attività di erogazione di servizi qualificati la presente convenzione è risolta *ipso jure*.

Procedura amministrativa



Schema convenzione non utilizzabile per la sottoscrizione.
Fare riferimento al sito dell'AgID.

AL SISTEMA PUBBLICO PER LE IDENTITÀ DIGITALI
(SCHEMA APPROVATO CON DETERMINAZIONE AGID N.14/2018)

Art. 8 - Disposizioni finali

1. La presente convenzione produce i suoi effetti a decorrere dalla data di sottoscrizione da parte di AgID.
2. Per quanto non espressamente previsto, si fa espresso rinvio al DPCM, ai Regolamenti SPID adottati da AgID e alle altre disposizioni vigenti in materia.

per l'AgID

per l'Amministrazione

Firmato digitalmente dal

Firmato digitalmente da

Direttore Generale AgID

[Redacted signature area]



Procedura amministrativa

La Convenzione deve essere restituita, compilata in tutte le sue parti e firmata digitalmente da un legale rappresentante dell'Ente presente nell'Indice dei domicili digitali della Pubblica Amministrazione e dei Gestori di Pubblici Servizi (IPA), ed inviata dalla PEC istituzionale presente in IPA, all'indirizzo protocollo@pec.agid.gov.it e per CC a spid.tech@agid.gov.it, insieme al file "ODS" per la comunicazione dei servizi (http://www.agid.gov.it/sites/default/files/repository_files/spid-comunicazione_servizi_pa.ods), indicando nell'oggetto delle e-mail esclusivamente la seguente dicitura: "00030 – Convenzione di adesione a SPID per SP pubblici - <Nome Ente>".

Se il file "ods" non è stato restituito insieme alla convenzione o se si tratta di un aggiornamento, deve essere inviato all'indirizzo protocollo@pec.agid.gov.it, mediante PEC istituzionale, presente in IPA (per le Pubbliche Amministrazioni) o nel Registro delle imprese (per i soggetti privati), indicando nell'oggetto dell'e-mail, esclusivamente, la seguente dicitura: "00010 elenco servizi pubblici in data <<AAAA/MM/GG>>", per i fornitori di servizi privati: "00011 elenco servizi privati in data <<AAAA/MM/GG>>".

La convenzione deve essere restituita entro 30 giorni solari dalla ricezione della suddetta e-mail di conferma.

La convenzione verrà restituita controfirmata dal Direttore Generale di AgID nel più breve tempo possibile.