AGID
Agenzia per l'Italia Digitale

spid

COME DIVENTARE SOGGETTI AGGREGATORI DI SERVIZI PUBBLICI

I Soggetti Aggregatori di servizi pubblici (nel seguito "Aggregatori") sono soggetti che offrono, tramite apposito servizio, a soggetti pubblici (nel seguito "Aggregati") la possibilità di rendere accessibili tramite credenziali SPID servizi online, individuando le attività necessarie a tale scopo.

L'Aggregatore, a seguito dell'iscrizione nel Registro SPID, può gestire in totale autonomia i rapporti con i soggetti Aggregati, nel rispetto della convenzione sottoscritta con AGID.

L'Aggregatore può gestire il sistema di autenticazione in modalità "*light*" e/o in modalità "*full*".

La modalità "*light*" è quella per la quale il Soggetto Aggregatore di servizi pubblici o privati garantisce l'attività di autenticazione tramite l'infrastruttura del Soggetto Aggregato, su cui è stata installata la soluzione fornita dall'Aggregatore. In questo caso, AgID rilascia un certificato di CA intermedia (*sub-CA*) che l'Aggregatore utilizza per generare certificati di sigillo elettronico per ciascun Aggregato.

La modalità "*full*" è quella per la quale il Soggetto Aggregatore di servizi pubblici o privati esegue l'attività di autenticazione tramite la propria infrastruttura. In questo caso, AgID rilascia direttamente un certificato di sigillo elettronico.

Il rilascio dei certificati elettronici è regolato dall'Avviso SPID №23.

Uno stesso Soggetto Aggregatore può operare sia in modalità "*full*" sia in modalità "*light*".

Le procedure da completare per l'adesione sono due, una tecnica e una amministrativa.

Procedura tecnica

Il sistema SPID si basa sul protocollo SAML2:

1. Consulta le regole tecniche, gli avvisi SPID e la tabella anomalie, con le indicazioni necessarie a guidarti durante l'implementazione di SPID e le linee guida interfacce e informazioni. Queste ultime hanno l'obiettivo di guidarti nell'utilizzo delle componenti grafiche necessarie a garantire la riconoscibilità di SPID tra gli utenti.

2. Implementa l'autenticazione con SPID sui tuoi servizi. Sul repository https://developers.italia.it/it/spid sono disponibili librerie per i diversi linguaggi di programmazione e risorse utili per l'integrazione ai quali puoi fare riferimento.

3. Elabora un metadata relativo ad un aggregato fittizio, per effettuare il collaudo finale, seguendo le indicazioni riportate nelle regole tecniche, nell'Avviso SPID №6 e nell'Avviso SPID №22.

4. **Accertati del corretto funzionamento della tua implementazione prima di richiedere ad AgID la verifica tecnica.** Verifica autonomamente la correttezza del metadata di cui al punto 3, usando lo *SPID Validator*, e la conformità della tua implementazione[1] ai requisiti tecnici, utilizzando in locale sia lo *SPID Validator* che lo ambiente di test (l'ambiente di test è anche disponibile online all'indirizzo https://idp.spid.gov.it). In particolare, occorre verificare il corretto funzionamento in relazione ad ognuno dei test indicati nel seguente documento SPID Quality Assessment Document. Per utilizzare l'ambiente di test online, occorre registrare il proprio metadata all'indirizzo https://idp.spid.gov.it/admin/databasesprecord/ Essendo l'ambiente di test online pubblico, i metadati registrati sono pubblicamente visibili. Per maggiori informazioni circa l'utilizzo dell'ambiente di test o per segnalare eventuali problemi fare riferimento al repository ufficiale GitHub.

5. Rendi disponibile il metadata di cui al punto 3 su una URL 'https' del tuo dominio e inserisci tra gli IdP del bottone "Entra con SPID" un ulteriore IdP del tool *SPID Validator*, il cui metadata è disponibile alla seguente URL: https://validator.spid.gov.it/metadata.xml.

   Compila e firma digitalmente in formato PAdES il modulo per l'Adesione a SPID e invialo a protocollo@pec.agid.gov.it e p.c. a spid.tech@agid.gov.it .

[1] SPID Validator non verifica che il metadata contenga quanto previsto specificatamente per i soggetti aggregatori nell'Avviso 19 e nel documento Struttura del metadata di test per soggetto aggregato.

6. AgID provvederà a verificare il metadata ricevuto e la correttezza dell'implementazione. Se necessario, saranno segnalate le modifiche necessarie a garantire il rispetto delle regole tecniche.

   Se AgID richiede delle modifiche dovrai ripetere la procedura a partire dal punto 3.

Procedura amministrativa

Completata la procedura tecnica, AgID invierà al referente amministrativo, indicato nel modulo di cui al punto 5 della procedura tecnica, la copia della convenzione e il modulo per la richiesta di emissione di certificato elettronico (CSR), in conformità con l'Avviso SPID №23.

La convenzione, il modulo e il CSR devono essere restituite, compilate e sottoscritte con firma elettronica qualificata, via PEC a protocollo@pec.agid.gov.it.

Entro pochi giorni la convenzione ti tornerà controfirmata dal Direttore Generale di AgID insieme al suddetto certificato elettronico.

Se non provvederai a restituire la convenzione firmata entro 30 giorni solari prendi immediati contatti con AgID per concordare altro termine, altrimenti i tuoi servizi saranno tolti dalla federazione e non saranno più accessibili con SPID.

Comunicazione dei metadata per gli Enti aggregati

A seguito della sottoscrizione della Convenzione da parte del Direttore Generale dell'AgID e della conseguente iscrizione nel Registro SPID il Soggetto Aggregatore può gestire in totale autonomia i rapporti con gli Aggregati, inviando ad AgID un solo metadata per ogni Aggregato secondo le seguenti modalità.

Verifica se hai già prodotto ed inviato ad AgID un metadata per un soggetto aggregato. In caso affermativo modifica[2] il metadata già presentato per

[2] Attenzione, se invii un nuovo metadata anziché modificare il precedente, andrai a sostituire l'ultimo al precedente con il risultato che i servizi precedenti non funzioneranno più! Modificando il metadata fai anche attenzione a non modificare l'entityID, non corrisponderebbe più a quanto contenuto nel certificato di firma delle asserzioni e vi sarebbero disservizi.

includere i nuovi servizi, altrimenti elabora un metadata come indicato nelle regole tecniche, nell'Avviso SPID №6 e nell'Avviso SPID №19.

Sigilla il metadata con la chiave privata afferente al certificato di sigillo elettronico rilasciato da AgID, se sei un Aggregatore "full" o se sei sia "full" che "light".

Se, invece, sei solo "light" genera, con la chiave privata afferente al certificato di CA intermedia (*sub-CA*) rilasciato da AgID, un certificato di sigillo elettronico a te intestato e utilizza la relativa chiave privata *esclusivamente* per sigillare i metadata da inviare ad AgID.

La comunicazione del metadata può essere effettuata esclusivamente i giorni lunedì, mercoledì e venerdì (se feriali) entro e non oltre le ore 15 con un'unica mail giornaliera, con oggetto "[Metadata Aggregatori]", contenente, *in un unico file ZIP in allegato:*

- un file XML per ogni metadata nuovo o aggiornato;
- un file JSON riepilogativo dei dati degli Aggregati interessati.

Un modello di esempio per il file JSON da compilare e allegare nel file ZIP è scaricabile da qui (file compresso); lo schema da seguire nel compilarlo è riportato in questa pagina.

Il nome dei file contenenti i metadata utilizza la seguente *naming convention*: il codice IPA (se SP pubblico) ovvero dalla P.IVA o, in alternativa, del codice fiscale (se SP privato) dell'**Aggregato**, seguito da *doppio underscore* "__", seguito dal codice IPA ovvero dal numero di partita IVA dell'**Aggregatore**, seguito dal suffisso "`.xml`".

Esempio di invio da Aggregatore con P.IVA 57575757575 del metadata:

- di un Aggregato privato con P.IVA 12345678901:

  `12345678901__57575757575.xml`

- di un Aggregato pubblico con codice IPA "`agid`":

```
agid__57575757575.xml
```

I nomi del file ZIP e del file JSON in esso contenuto utilizzano la seguente *naming convention*: "`md-aggr-`" seguito dal codice IPA ovvero dal numero di partita IVA dell'Aggregatore, seguito da "`_`", seguito dalla data in formato statunitense *AAAAMMGG*, seguito dal suffisso "`.zip`" e, rispettivamente, "`.json`".

Esempio di file ZIP inviato il 26 marzo 2020 da Aggregatore con numero di partita IVA 57575757575:

```
md-aggr-57575757575-20200326.zip
```

AgID provvederà a comunicare il metadata agli Identity Provider (IdP), dandone informazione all'Aggregatore e, tramite PEC, all'Aggregato.

Di norma, entro un giorno lavorativo[3], gli IdP provvedono al loro caricamento ed il tuo servizio sarà accessibile tramite SPID.

Supporto tecnico e amministrativo

Se hai bisogno di supporto nella fase tecnica e per i metadata puoi rivolgerti a spid.tech@agid.gov.it.

Se hai bisogno di supporto nella fase amministrativa e per la convenzione puoi rivolgerti a convenzioni.spid@agid.gov.it.

Riepilogo

I principali interventi tecnici che ti verranno chiesti

1. Interventi di implementazione del sistema SPID, utilizzando SAML2, nei propri applicativi web;

[3] Al massimo entro due giorni lavorativi.

2. Consegna di un metadata, come da regole tecniche e successivi avvisi, per la configurazione dei propri servizi presso gli IDP.

Le figure di riferimento necessarie per concludere il processo di adesione a SPID

1. Referente tecnico del Soggetto Aggregatore per tutte le attività di implementazione del sistema di autenticazione SPID;
2. Rappresentante legale per la firma della convenzione;
3. Referente amministrativo del Soggetto Aggregatore;
4. Referente amministrativo del Soggetto Aggregato.

Riferimenti

DPCM 24 ottobre 2014

Documentazione e regole tecniche

Avvisi

Linee guida interfacce e informazioni SPID per IdP e Sp

Repository Github Italia

Convenzione per soggetti aggregatori

Allegato alla Determinazione AGID №80/2018.

AGID
Agenzia per l'Italia Digitale

spid

Schema JSON per le comunicazioni tecniche tra AgID e altri soggetti in merito ai metadata degli SP SPID

Schema per la comunicazione agli IdP dei metadata di tutti gli SP da parte di AgID

Il file JSON con il quale l'Agenzia per l'Italia Digitale comunica agli IdP, con cadenza giornaliera, l'elenco dei metadata SAML per i SP oggetto di cambiamenti tecnici è un oggetto contenente i seguenti elementi, tutti *obbligatori*:

i. `dateTime` (string) — La data e l'ora (in fuso orario italiano) in cui il file JSON è preparato per l'invio da parte di AgID, secondo la sintassi "*YYYY-MM-DD*T*hh:mm:ss*".
ii. `metadata` (array) — Una lista non vuota di object, ciascuno relativo a un SP di cui comunicare l'azione.

Schema per la comunicazione ad AGID dei metadata degli SP aggregati da parte di un Soggetto Aggregatore

Con riferimento agli Avvisi SPID №19, №22, №23 e alla procedura per gli Aggregatori pubblicata sul sito dell'Agenzia per l'Italia Digitale, il file JSON con il quale gli Aggregatori comunicano ad AgID l'elenco dei metadata SAML per i propri Aggregati oggetto di cambiamenti tecnici è un oggetto contenente i seguenti elementi, tutti *obbligatori*:

iii. `aggregatorCode` (string) — Il numero di partita IVA (se ente di diritto privato) ovvero con il codice IPA (se Ente pubblico) del soggetto Aggregatore.
iv. `aggregatorName` (string) — La denominazione o ragione sociale completa dell'Aggregatore.
v. `entityID` (string) — L'`entityID` dell'Aggregatore, conforme all'Avviso SPID №19.
vi. `dateTime` (string) — La data e l'ora (in fuso orario italiano) in cui il file ZIP è preparato per l'invio ad AgID, secondo la sintassi "*YYYY-MM-DD*T*hh:mm:ss*".
vii. `metadata` (array) — Una lista non vuota di object, ciascuno relativo al soggetto Aggregato di cui comunicare l'azione.

Gli `entityID` di ciascun Aggregato, valorizzati dagli omonimi sotto-elementi all'interno dell'array `metadata`, sono anch'essi conformi all'Avviso SPID №19.

Componenti comuni dello schema

Gli oggetti JSON presenti nell'array `metadata` per ciascuno dei due tipi di file JSON sopra introdotti sono in numero di uno per ciascun SP e sono costituiti dai sotto-elementi elencati qui sotto. Tali sotto-elementi sono tutti *obbligatori*, salvo ove espressamente specificato:

1. `action` (string) — Verbo RESTful che consente di stabilire l'azione da intraprendere sul metadata corrispondente; è valorizzato dalle seguenti stringhe alternative:
   - `POST` — aggiunta di un metadata (subentro di un nuovo SP);
   - `PUT` — modifica di un metadata esistente (cambiamento dei servizi di un SP);
   - `DELETE` — rimozione di un metadata (esclusione del SP dalla federazione, ovvero interruzione della gestione di un Aggregato da parte di un Aggregatore); solo nel caso di tale valorizzazione, va omesso l'elemento, comunque facoltativo, `metadataUrl` (vedi sotto).

Si precisa che, nonostante la differenza semantica tra i due verbi `POST` e `PUT`, un scambio fra i due non deve risultare in un rifiuto nell'accettazione del JSON. In particolar modo, un metadata elencato con verbo `POST` a fronte di una pre-esistente versione dello stesso, risulta nell'aggiornamento del metadata esistente (come per effetto di un verbo `PUT`) e viceversa.

2. `entityCode` (string) — Il numero di partita IVA o, in alternativa, il codice fiscale, qualora il SP sia ente di diritto privato; il codice IPA, qualora il SP sia un Ente pubblico.
3. `entityID` (string) — L'`entityID` del SP.
4. `isPrivate` (boolean) — Booleano **vero**, qualora il SP sia un ente di diritto privato; **falso**, qualora il SP sia un Ente pubblico.
5. `metadataFilename` (string) — Il nome del file XML del metadata del SP (*senza* alcun percorso di filesystem né URL), e la cui *naming convention* rispetta la procedura indicata sul sito di AgID per tali file.
6. `metadataUrl` (string, *facoltativo*) — URL con schema HTTPS afferente al mittente del JSON, ove questo rende disponibile online il metadata del SP al destinatario.

Infine, anche se non necessario per la conformità del JSON allo schema del W3C, si consiglia di rispettare le seguenti indicazioni sintattiche aggiuntive:

- un elemento per riga di testo (incluse le parentesi di chiusura e apertura), ad eccezione di quelli di tipo `object` e `array`, per i quali i loro sotto-elementi saranno anch'essi in righe separate;
- adottare carattere di *newline* compatibile con sistemi Windows (cioè carattere "`\r\n`", cioè `0x0D0A` esadecimale);
- rispettare l'ordinamento degli elementi come elencati nel presente schema.

Segue un esempio di metadata json che un Aggregatore identificato da un numero di partita IVA `57575757575` invia ad AgID le informazioni circa:

- l'aggiunta di un Comune aggregato, identificato dal codice IPA `c_X000`;
- la modifica dei servizi di un Aggregato privato identificato tramite la P.IVA `12345678901`;
- l'interruzione della gestione di un'Unione di Comuni, identificato dal codice IPA `ucYYY`.

```
{
 "aggregatorCode": "57575757575",
 "aggregatorName": "Ragione sociale dell'Aggregatore",
 "entityID": "https://id.aggregatore/",
 "dateTime": "2020-03-27T17:24:16",
 "metadata":[
       {
             "action": "POST",
             "entityCode": "c_X000",
             "entityName": "Comune di XXXXXXXX",
             "entityID": "https://id.aggregatore/id.aggr/1",
             "isPrivate": false,
             "metadataFilename": "c_X000_57575757575.xml",
             "metadataUrl": "https://sito-
aggregatore/percorso/al/metadata/c_X000__57575757575.xml"
       },
       {
             "action": "PUT",
             "entityCode": "12345678901",
             "entityName": "Ragione sociale dell'Azienda",
```

```
            "entityID": "https://id.aggregatore/id.aggr/2",
            "isPrivate": true,
            "metadataFilename": "12345678901_57575757575.xml",
            "metadataUrl": "https://sito-
aggregatore/percorso/al/metadata/12345678901__57575757575.xml"
      },
      {
            "action": "DELETE",
            "entityCode": "ucYYY",
            "entityName": "Unione dei Comuni di YYYYYYYY",
            "entityID": "https://id.aggregatore/id.aggr/3",
            "isPrivate": false,
            "metadataFilename": "ucYYY__57575757575.xml"
      }
 ]
}
```