SPID OpenID Connect Federation

OpenID Connect Federation

SPID adotta le specifiche di OpenID Connect (OIDC) Federation 1.0 [OIDC-FED] che definiscono come le entità, intese come partecipanti ad una Federazione, possono riconoscersi ed ottenere i metadati di Federazione e i metadati per il protocollo OpenID Connect [OpenID.Core]. I metadati sono certificabili da un parte fidata che all'interno della Federazione SPID è AgID e corrisponde alla Autorità di Federazione.

SPID implementa OpenID Connect Federation 1.0 ed estende alcune funzionalità dello standard, ne realizza una implementazione concreta e produce le buone pratiche per la sua adozione.

OpenID Connect Federation

Affinché le parti si riconoscano all’interno della medesima Federazione delle identità è necessario che ognuna di queste ottenga la prova della reciproca aderenza ad un medesimo quadro regolatorio.

Le parti ottengono i metadati gli uni degli altri, contenenti le chiavi pubbliche per le operazioni di firma digitale e criptazione e le definizioni necessarie all'interscambio delle informazioni, secondo le regole prestabilite

.

Entità della Federazione

Le parti coinvolte all'interno di una Federazione OpenID Connect sono le seguenti:

Autorità di Federazione	Agenzia per l'Italia Digitale (AgID). Norma il funzionamento e le modalità di registrazione e riconoscimento dei partecipanti
Trust Anchor	Sistema gestito dalla AgID il cui compito è quello di pubblicare la configurazione della Federazione e le affermazioni di riconoscimento delle parti che afferiscono alla Federazione. Il Trust Anchor corrisponde alla Autorità di Federazione e rappresenta la Federazione stessa.
Intermediario	Soggetto Aggregatore (SA), facilita l'ingresso nella Federazione e PUÒ gestire le funzionalità per conto di un suo discendente (Aggregato), pubblica la propria configurazione all'interno della Federazione e le affermazioni di riconoscimento delle parti sue discendenti (Aggregati) in conformità alle regole definite dalla AgID.
Foglia	Entità definita dal protocollo OIDC come Relying Party e Provider OpenID
Entità	Partecipante alla Federazione. Trust Anchor, Intermediario o Foglia.

Acronimi

AdF	Autorità di Federazione, che è AgID.
OIDC	OpenID Connect
OIDC-FED	OIDC Federation 1.0.
IOF	Italian OIDC Federation 1.0.
SPID	Sistema Pubblico per la gestione dell'Identità Digitale
AgID	Agenzia per l'Italia Digitale.
SA	Soggetti Aggregatori.
TA	OIDC Federation Trust Anchor.
OP	OpenID Provider.
RP	Relying Party.
AA	Attribute Authority, OAuth Resource Server, Gestore degli Attributi qualificati.
TM	Trust Mark.
EC	Entity Configuration.
ES	Entity Statement.
URL	Uniform Resource Locator, corrispondente ad un indirizzo web.
JWT	Vedi [RFC7519].

Soggetti Aggregatori

I **soggetti aggregatori** sono pubbliche amministrazioni o privati che offrono a terzi (soggetti aggregati) la possibilità di rendere accessibili tramite lo SPID i rispettivi servizi.

Tali soggetti si distinguono in aggregatori di servizi pubblici e aggregatori di servizi privati.

I soggetti aggregatori possono svolgere per il soggetto aggregato la solo funzione di autenticazione con SPID oppure ospitare l'intero servizio.

Tali soggetti agevolano l'ingresso nella federazione SPID dei fornitori di servizi che non ritengono conveniente attivare presso di loro la struttura necessaria per esporre i propri servizi in rete tramite l'autenticazione con lo SPID.

Gestori attributi qualificati

La federazione SPID prevede l'esistenza dei **gestori di attributi qualificati** (Attribute Authorities). Questi sono potenzialmente tutti i soggetti che in base ad una norma hanno il potere di attestare "*[..] abilitazioni o autorizzazioni richieste dalla legge ovvero stati, qualità personali e fatti contenuti in albi, elenchi o registri pubblici o comunque accertati da soggetti titolari di funzioni pubbliche, ovvero gli altri dati, fatti e informazioni funzionali alla fruizione di un servizio attestati da un gestore di attributi qualificati, [..]*" come da art. 62 comma 2-*duodecies* del CAD

L'ingresso di questi soggetti nella federazione SPID consente ai fornitori di servizi di verificare stati personali (qualifiche, poteri, ecc.) delle persone fisiche che accedono ai loro servizi in rete.

Termini e definizioni

Entity configuration	Dichiarazione di una entità emessa per proprio conto, nella forma di JWT auto firmato [RFC7515] e contenente la configurazione di se stessa. Contiene le chiavi pubbliche di Federazione, il metadata OIDC, gli URL delle autorità sue superiori e i Trust Mark emessi da autorità riconoscibili nella Federazione che attestano l'aderenza del soggetto a determinati profili.
Entity statement	Dichiarazione di riconoscimento emessa da un'entità superiore (Trust Anchor o Intermediario) riguardante un'entità discendente (RP, OP o Intermediario) in formato JWT firmato [RFC7515], contenente la chiave pubblica del soggetto discendente, i Trust Mark emessi per i quali è emittente e la politica dei metadati da applicare ai metadati del soggetto.
Trust Mark	JWT firmato [RFC7515] dall'ente emittente e relativo ad un partecipante. Attesta la conformità di questo ai profili riconoscibili all'interno della Federazione (RP pubblico o privato, Soggetto Aggregatore Pubblico o Privato, etc.). La Foglia che acquisisce il marchio di fiducia durante la fase di onboarding deve includere questo nella sua Entity Configuration a mò di *Badge* di riconoscimento.
Metadata	Documento che descrive una implementazione di una entità OpenID Connect. Le implementazioni di ogni Entità condividono i metadati per stabilire una base di fiducia e interoperabilità.

Metadata policy	Il Trust Anchor pubblica le regole e le politiche da applicare sui metadata dei discendenti, specificando quali valori o sottoinsiemi di valori sono consentiti per un dato attributo di metadati.
Authority hint	Un *Array* di valori url corrispondenti agli identificativi delle entità superiori, Trust Anchor o Intermediario, che emettono un Entity Statement per i propri discendenti.
Metadata Discovery	Raccolta di Entity Configuration e Statement. Inizia da un'entità Foglia fino al raggiungimento del Trust Anchor.
Trust Chain	Procedura di validazione della sequenza di Entity Configuration e Statement raccolta mediante Metadata Discovery, il cui esito positivo è un metadata finale relativo ad una entità e la data di scadenza entro la quale questo deve essere aggiornato.
onboarding	Procedura di registrazione di una nuova entità all'interno della Federazione SPID
entity-type	All'interno dell Federazione le tipologie di Entità consentite sono: • openid_relying_party • openid_provider • federation_entity • oauth_authorization_server • trust_mark_issuer • oauth_resource

Configurazione della Federazione SPID

La configurazione della Federazione SPID è pubblicata dal Trust Anchor all'interno della sua Entity Configuration, presso un web path ben noto e corrispondente a **.well-known/openid-federation**.

Tutti i partecipanti DEVONO ottenere prima della fase di esercizio la configurazione della Federazione e mantenere quest'ultima aggiornata su base giornaliera. All'interno della Configurazione della Federazione è presente la chiave pubblica del Trust Anchor usata per le operazioni di firma, il numero massimo di Intermediari consentiti tra una Foglia e il Trust Anchor (**max_path length**) e le autorità abilitate all'emissione dei Trust Marks (**trust_marks_issuers**).

Modalità di partecipazione alla Federazione

Per aderire alla Federazione SPID una entità di tipo Foglia DEVE pubblicare la propria configurazione (Entity Configuration) presso il web endpoint **.well-known/openid-federation**.

Gli incaricati tecnici ed amministrativi della Foglia completano la procedura amministrativa per la registrazione di una nuova entità o l'aggiornamento di una preesistente definita dalla Autorità di Federazione o da un suo Intermediario(SA).

L'Autorità di Federazione o un suo Intermediario dopo aver effettuato tutti i controlli amministrativi e tecnici richiesti, registra le chiavi pubbliche della Foglia e rilascia una prova di adesione alla Federazione sotto forma di Trust Mark (TM)

La Foglia DEVE includere il TM all'interno della propria configurazione di Federazione (Entity Configuration) come prova del buon esito del processo di onboarding

L'Autorità di Federazione o un suo Intermediario DEVE pubblicare la dichiarazione di riconoscimento della Foglia (Entity Statement) contenente le chiavi pubbliche di federazione della Foglia e i TM a questa rilasciati. L'Autorità di Federazione o un suo Intermediario PUÒ pubblicare una politica dei metadata per forzare la modifica dei metadata OIDC della Foglia, nelle parti in cui questo sia necessario

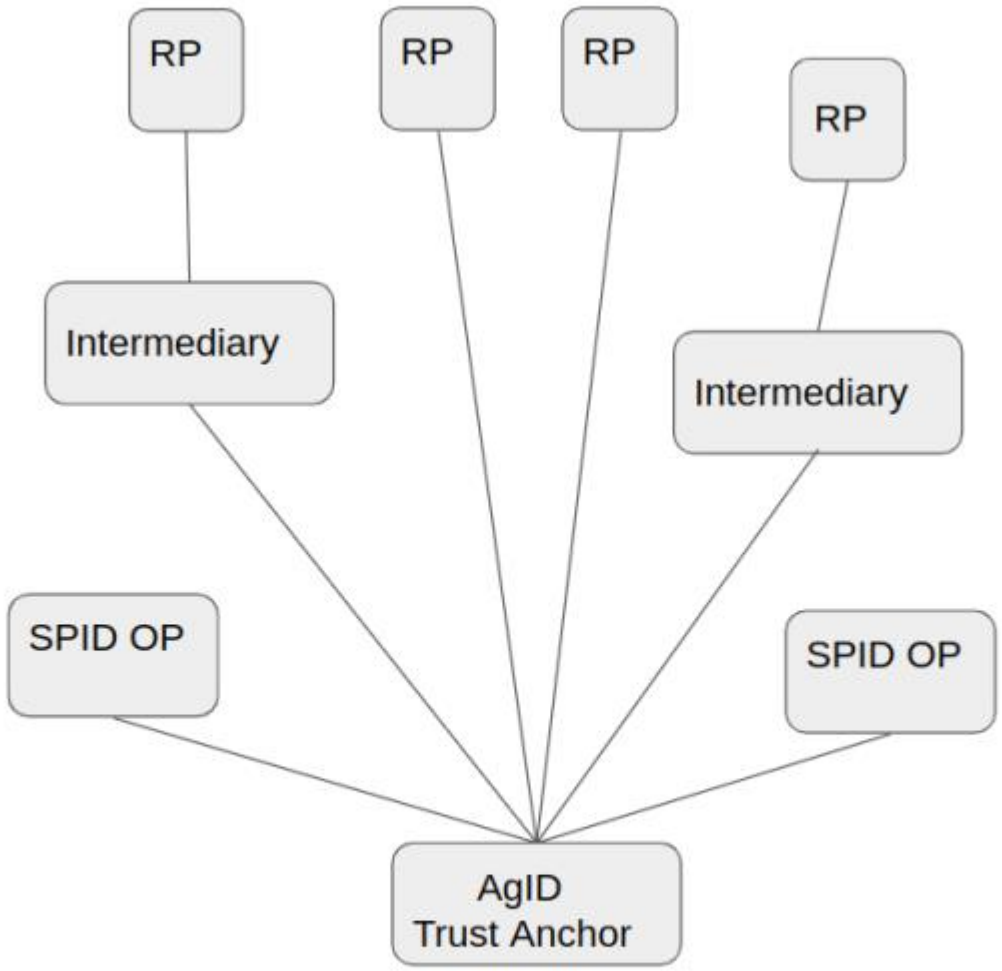


Figura 1: *Schema ad albero che rappresenta la struttura della Federazione. Alla Base l'Autorità di Federazione e a salire gli OP che non hanno intermediari, gli RP e gli Intermediari che a loro volta Aggregano altri RP.*

Modalità di riconoscimento e instaurazione della fiducia tra le parti

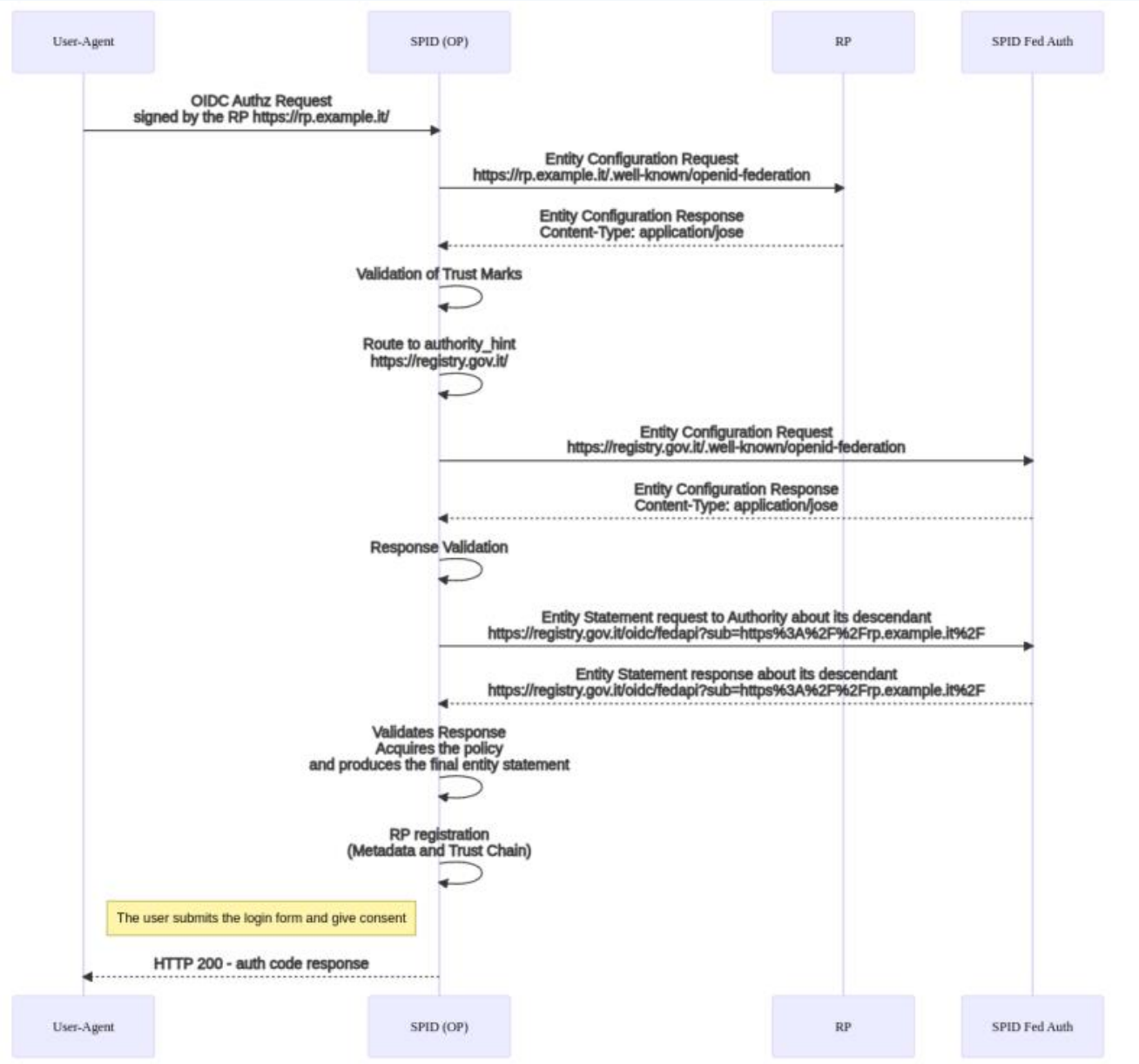
Modalità di mutuo riconoscimento tra RP e OP, le modalità con le quali le Foglie della Federazione SPID si riconoscono all'interno della medesima Federazione e ottengono le une i metadata delle altre.

Modalità di riconoscimento - Relying Party

1. Il RP ottiene la lista degli OP in formato JSON interrogando l'**endpoint list** disponibile presso il Trust Anchor. Per ogni soggetto contenuto nella risposta dell'**endpoint list** e corrispondente ad un OP, il RP richiede ed ottiene l'Entity Configuration *self-signed* presso l'OP.
2. Per ogni EC degli OP, il RP verifica la firma del contenuto adoperando la chiave pubblica ottenuta dall'Entity Statement rilasciato dalla Trust Anchor. Verificata la firma dell'Entity Configuration con la chiave pubblica pubblicata dalla Trust Anchor la fiducia è stabilita nei confronti del OP da parte del RP.
3. Il RP applica infine le politiche pubblicate dal Trust Anchor sui metadata del OP e salva il metadata finale associandolo ad una data di scadenza (claim **exp**). La data di scadenza corrisponde al valore di **exp** più basso ottenuto da tutti gli *statement* che compongono la **Trust Chain**. Periodicamente il RP aggiorna i metadati di tutti gli OP rinnovando la Trust Chain relativa a questi.
4. Ottenuti i metadati finali di tutti i Provider SPID, il RP genera lo SPID Button e lo pubblica all'interno della pagina di autenticazione destinata agli utenti.
5. La procedura di Metadata Discovery risulta semplificata per i RP SPID perché non è consentita all'interno della Federazione l'esistenza di Intermediari tra gli OP ed il loro Trust Anchor

Modalità di riconoscimento - OpenID Provider

Quando un Provider (OP) riceve una richiesta di autorizzazione da parte di un RP non precedentemente riconosciuto avviene la procedura di automatic client registration. Sono di seguito descritte le operazioni compiute dal OP per registrare un RP dinamicamente.



La registrazione di un RP dalla prospettiva di un OP che per la prima volta riceve una richiesta di autorizzazione dal RP e avvia il processo di Metadata Discovery e salvataggio della Trust Chain

Modalità di riconoscimento - OpenID Provider

1. L'OP estrae l'identificativo univoco (**client_id**) dall'oggetto *request* contenuto all'interno della *Authorization Request* ed effettua una richiesta di Entity Configuration presso il RP. Ottiene la configurazione *self-signed* del RP e convalida la firma dei Trust Marks riconoscibili all'interno della Federazione
2. Se il RP non espone all'interno della sua configurazione nessun Trust Mark riconoscibile per il profilo di RP il Provider DEVE rifiutare l'autorizzazione con un messaggio di errore di tipo unauthorized_client conforme alla Linee Guida OpenID Connect SPID.
3. Se il Provider convalida con successo almeno un Trust Mark per il profilo RP contenuto all'interno della configurazione del RP richiedente, estrae le entità superiori contenute nel claim authority_hints ed avvia la fase di Metadata Discovery. Ne consegue il calcolo della Trust Chain e l'ottenimento del metadata finale

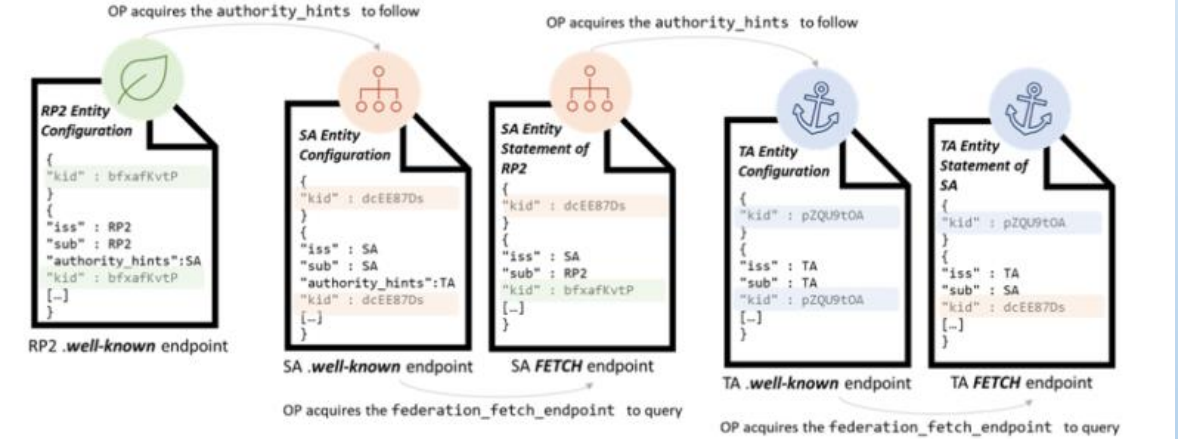


Figura 3: La procedura di Metadata Discovery a partire dalla Foglia fino al Trust Anchor. Si noti come dall'Entity Statement rilasciato da un superiore si ottiene la chiave pubblica per la validazione dell'Entity Configuration dell'entità discendente.

Modalità di riconoscimento - OpenID Provider

4. Durante il Metadata Discovery, il Provider richiede ad una o più di una entità superiore (*Un RP può esporre più di una entità superiore all'interno del proprio claim di authority_hints. Si pensi ad un RP che partecipa sia alla Federazione SPID che a quella CIE. Inoltre un RP può risultare come aggregato di molteplici intermediari, se questi SPID o CIE.)* l'Entity Statement relativo al RP e ottiene la chiave pubblica con la quale valida la configurazione del RP, fino a giungere al Trust Anchor. Infine applica la politica dei metadata pubblicata dal Trust Anchor e salva il risultante metadata finale del RP associandolo ad una data di scadenza, oltre la quale rinnoverà il metadata secondo le modalità di rinnovo della Trust Chain
5. Ottenuto il metadata finale, il Provider valida la richiesta del RP secondo le modalità definite all'interno delle Linee Guida OpenID Connect SPID
6. Nei casi in cui un RP avesse come entità superiore un SA e non direttamente la TA, la procedura di acquisizione e validazione dell'Entity Configuration del RP avviene mediante l'Entity Statement pubblicato dal SA nei confronti del RP e mediante la convalida dell'Entity Configuration del SA con l'Entity Statement emesso dalla TA in relazione al SA. Se la soglia del massimo numero di intermediari verticali, definita dal valore di **max_path_length**, venisse superata, l'OP blocca il processo di Metadata Discovery e rigetta la richiesta del RP

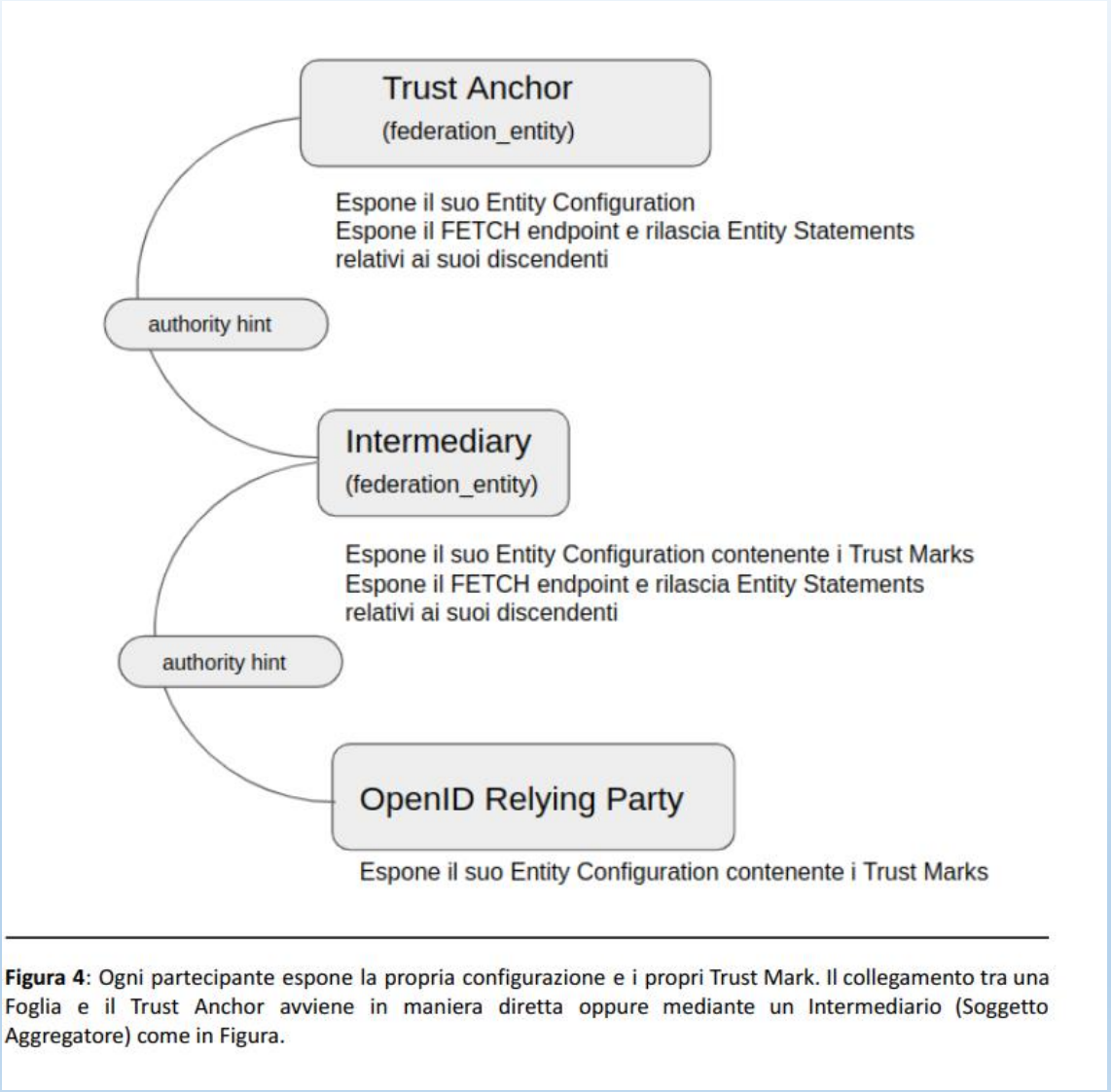


Figura 4: Ogni partecipante espone la propria configurazione e i propri Trust Mark. Il collegamento tra una Foglia e il Trust Anchor avviene in maniera diretta oppure mediante un Intermediario (Soggetto Aggregatore) come in Figura.

Modalità di accesso alla Entity Configuration

Per individuare per un determinato soggetto l'URL per il download della Entity Configuration occorre usare la risorsa attraverso la quale un partecipante pubblica la sua configurazione (Entity Configuration) corrispondente al webpath **.well-known/openid-federation** e DEVE essere appesa all'URL che identifica il soggetto

Esempi:

- con identificativo del soggetto pari a **https://rp.example.it** il risultante URL di Entity Configuration è **https://rp.example.it/.well-known/oidc-federation**.
- con identificativo del soggetto pari **https://rp.servizi-spid.it/oidc/** il risultante URL di Entity Configuration è **https://rp.servizi-spid.it/oidc/.well-known/oidc-federation**.

Se l'URL che identifica il soggetto non presenta il simbolo di slash finale ("/") è necessario aggiungerlo prima di appendere il web path della risorsa **well-known**.

Trust Mark

I Trust Mark, letteralmente tradotti come marchi di fiducia, sono oggetti JSON firmati in formato Jose e rappresentano la dichiarazione di conformità a un insieme ben definito di requisiti di fiducia e/o di interoperabilità o un accordo tra le parti coinvolte all'interno della Federazione. I Trust Marks sono rilasciati principalmente durante il processo di registrazione di una nuova entità di tipo Foglia (onboarding) dal Trust Anchor o suoi Intermediari.

Lo scopo principale di questi marchi di fiducia è quello di esporre alcune informazioni non richieste dal protocollo OpenID Connect Core ma che risultano utili in contesto Federativo

I Trust Marks riconoscibili all'interno della Federazione SPID sono emessi e firmati dalla AgID (TA) o suoi intermediari (SA) o dai Gestori di attributi qualificati (AA) se definiti all'interno del **claim trust_mark_issuers** pubblicato all'interno dell'Entity Configuration del TA. Ogni partecipante DEVE esporre nella propria configurazione (EC) i Trust Mark rilasciati dalle autorità emittenti.

I Trust Mark rappresentano il primo filtro per l'instaurazione della fiducia tra le parti, sono elementi indispensabili per avviare la risoluzione dei metadati. In loro assenza una entità non è riconoscibile come partecipante all'interno della Federazione SPID.

Trust Mark

All’interno della Federazione SPID i Trust Mark presentano degli identificativi univoci (claim **id**) in formato URL che adottano la seguente struttura:

https:// <domain> / <entity_type> / [<trustmark_profile> /] [estensione /]

(La notazione indica che l’elemento è opzionale e non obbligatorio)

Alcuni esempi non normativi sono di seguito riportati:

- profilo RP public: https://registry.spid.gov.it/openid_relying_party/public/
- profilo SA private di tipo full o light: https://registry.spid.gov.it/federation_entity/private/
- profilo AA: https://registry.spid.gov.it/oauth_resource/public/

Composizione dei Trust Mark

I claim definiti all'interno dei Trust Marks aderiscono a quanto definito all'interno dello standard **OIDC Federation 1.015** di seguito riportati.

Claim	Tipo	Descrizione
iss	String	RICHIESTO. URL che identifica univocamente l'Autorità che lo ha emesso.
sub	String	RICHIESTO. URL che identifica univocamente il soggetto per il quale il Trust Mark è stato emesso.
id	String	RICHIESTO. Identificativo univoco del Trust Mark.
iat	UTC Timestamp	RICHIESTO. Quando è stato emesso questo marchio di fiducia. Espresso come "*Seconds Since the Epoch*" [RFC7519].
logo_uri	String	OPZIONALE. Un URL che punta al logo rappresentante il Trust Mark.
exp	UTC Timestamp	RICHIESTO. Momento oltre il quale non sarà più valido. Espresso come "*Seconds Since the Epoch*" [RFC7519] e corrispondente o inferiore alla durata della validità della convenzione amministrativa di adesione alla Federazione.
ref	String	OPZIONALE. URL che punta a informazioni presenti sul web relative a questo marchio di fiducia

La seguente tabella riassume i profili di TM supportati all'interno della Federazione SPID e identificati dal claim "id".

Tipo	Descrizione	Entità
public	Indica che il RP l'entity statement afferisce ad una Pubblica Amministrazione.	RP , OP, SA, AA
private	Indica che il RP l'entity statement afferisce ad una organizzazione privata.	RP, OP, SA, AA

Trust Mark - SPID

Agli attributi dei TM definiti nella tabella precedente, i Trust Mark SPID aggiungono i seguenti.

Claims	Description
organization_type	RICHIESTO. Specifica se l'ente appartiene alla pubblica amministrazione italiana o al settore privato (private or public).
id_code	RICHIESTO. Codice di identificazione dell'organizzazione; a seconda del valore del tipo di organizzazione deve essere indicato il codice IPA (per il tipo di organizzazione pubblica) o il numero di partita IVA (per quello privato).
email	RICHIESTO. Email istituzionale o PEC dell'organizzazione.
organization_name	RICHIESTO. Il nome completo dell'entità che fornisce i servizi.
sa_profile	RICHIESTO per SA. Specifica il profilo dell'Aggregatore, esempio: **full** o **light**.

Trust Mark

esempio non normativo di un marchio di fiducia emesso da AgID per un SA privato di tipo full.

```
"trust_marks": [
 {
  "id":"https://registry.spid.gov.it/federation_entity/private/",
  "trust_mark": "..."
 }
]
```

Dove il contenuto del JWT firmato all'interno del claim **trust_mark** corrisponde a:

```
{
  "id":"https://registry.spid.gov.it/federation_entity/private/",
  "iss": "https://registry.spid.gov.it",
  "sub": "https://intermediary.example.it",
  "iat": 1579621160,
  "organization_type": "private",
  "sa_profile": "full",
  "id_code": "12345678900",
  "email": "email_or_pec@example.it",
  "organization_name": "Full name of the SA",
  "ref": "https://reference_to_some_documentation.example.it/"
}
```

Un'entità intermediaria (SA) è riconoscibile come emittente di Trust Mark

Trust Mark

esempio non normativo di un Trust Mark emesso da un Soggetto Aggregatore a favore di un RP suo discendente.

```
"trust_marks": [
 {
  "id":"https://registry.spid.gov.it/openid_relying_party/public/",
  "trust_mark": ...
  }
]
```

Dove il contenuto del JWT firmato all'interno del claim **trust_mark** corrisponde al seguente esempio non normativo.

```
{
  "id":"https://registry.spid.gov.it/openid_relying_party/public/",
  "iss": "https://intermediary.example.it",
  "sub": "https://rp.example.it",
  "iat": 1579621160,
  "organization_type": "public",
  "id_code": "123456",
  "email": "email_or_pec@rp.it",
  "organization_name": "Full name of the RP",
  "ref": "https://reference_to_some_documentation.it/"
}
```

Validazione dei Trust Mark

Esistono due modi per validare un Trust Mark:

1. Validazione **statica**. Il Trust Mark viene validato mediante il certificato pubblico dell'autorità che lo ha emesso (claim **iss**), sulla base della corrispondenza del claim **sub** con il medesimo claim della Entity Configuration in cui è contenuto e sulla base del valore di scadenza (claim **exp**)

2. Validazione dinamica. I partecipanti della federazione possono interrogare l'endpoint trust mark status erogato dal suo emittente (claim iss) per la verifica in tempo reale dei TM da lui emessi.

Tutti gli emittenti di Trust Mark DEVONO esporre un endpoint di *trust mark status* per consentire la validazione **dinamica**

Disattivazione dei Trust Mark

Un Trust Mark può essere revocato in qualsiasi momento. In caso di esclusione di un Soggetto Aggregato da parte della Autorità di Federazione, questa comunica al Soggetto Aggregatore l’esclusione dell'Aggregato. Di conseguenza il SA revoca il TM per il suo discendente.

Pubblicazione dei Trust Marks

La TA definisce i TM e gli emittenti di questi abilitati nella Federazione mediante il claim **trust_mark_issuers**, presente all'interno del proprio Entity Configuration. Il valore del claim **trust_mark_issuers** è composto da un oggetto JSON, avente come chiavi gli id dei TM e come valori la lista degli emittenti abilitati.

Di seguito un esempio non normativo dell'oggetto **trust_mark_issuers** all'interno della Entity Configuration del TA

```
"trust_marks_issuers":{
    "https://registry.spid.gov.it/openid_relying_party/public/":[
      "https://registry.spid.gov.it/",
      "https://public.intermediary.spid.it/"
    ],
    "https://registry.spid.gov.it/openid_relying_party/private/":[
      "https://registry.spid.gov.it/",
      "https://private.other.intermediary.it/"
    ],
    “https://deleghedigitali.gov.it/openid_relying_party/sgd/”: [
      “https://deleghedigitali.gov.it”
    ]
  }
```

I TM emessi per le Foglie DEVONO essere pubblicati dalle stesse all'interno della proprie Entity Configuration, all'interno del claim **trust_marks**. Questo è composto da lista di oggetti JSON, ognuno di questi DEVE contenere almeno i **claim id** e **trust_mark**, il primo identifica il TM, il secondo contiene il JWT firmato del TM

Entity Statement e Configuration

Un Entity Configuration è un Metadata di federazione in formato Jose e firmato dal soggetto che lo emette e riguardante se stesso, all'interno del quale i valori dei claim **iss** e **sub** contengono il medesimo valore (URL).

Un Entity Statement è un documento di riconoscimento che una Autorità di Federazione o suo Intermediario emette per uno specifico soggetto, suo discendente, individuato all'interno del claim **sub**.

Entity Statement e Configuration - Firma

La firma dei JWT avviene mediante l'algoritmo RSA SHA-256 (RS256), tutti i partecipanti DEVONO supportare questo algoritmo di firma all’interno della Federazione. Tutte le operazioni di firma relative agli Entity Statements, Entity Configuration e Trust Mark sono condotte con le chiavi pubbliche di Federazione

Entity Statement e Configuration – Attributi (Claims)

Entity Configuration e Statement presentano i seguenti claim comuni

Nome	tipo	descrizione
iss	String	RICHIESTO. Identificativo dell'entità che lo emette.
sub	String	RICHIESTO. Identificativo del soggetto a cui è riferito.
iat	Unix Timestamp	RICHIESTO. Data di emissione.
exp	Unix Timestamp	RICHIESTO. Data di scadenza.
jwks	JWKS	RICHIESTO. Un JSON Web Key Set (JWKS) [RFC7517] che rappresenta la parte pubblica delle chiavi di firma dell'entità interessata. Ogni JWK nel set JWK DEVE avere un ID (claim **kid**).
trust_marks	JSON array	RICHIESTO per tutti i partecipanti fatta esclusione del Trust Anchor. Un array JSON contenente i Trust Mark. Vedere la Sezione Trust Mark.

Entity Statement e Configuration – Attributi (Claims)

Gli oggetti Entity Configuration delle Entità di tipo Foglia contengono in aggiunta ai claim comuni anche i seguenti:

Nome	tipo	descrizione
authority_hints	Array di URLs	RICHIESTO. Contiene una lista di URL delle entità superiori, quali TA o SA che POSSONO emettere un Entity Statement relativo a questo soggetto.
metadata	JSON object	RICHIESTO. Ogni chiave dell'oggetto JSON rappresenta un identificatore del tipo di metadati e ogni valore DEVE essere un oggetto JSON che rappresenta i metadati secondo lo schema di metadati di quel tipo. Una configurazione di entità PUÒ contenere più dichiarazioni di metadati, ma solo una per ogni tipo di metadati (<**entity_type**>).

Entity Statement e Configuration – Attributi (Claims)

Gli oggetti Entity Configuration della Federation Authority che è AgID, contiene in aggiunta ai claim comuni anche i seguenti:

Nome	tipo	descrizione
constraints	JSON object	RICHIESTO e include l'elemento **max_path_length** al quale viene assegnato un valore Integer. Indica il numero massimo di intermediari consentiti tra una Foglia e il suo Trust Anchor.
trust_marks_issuers	JSON array	RICHIESTO. Indica quali autorità sono considerate attendibili nella federazione per l'emissione di specifici Trust Mark, questi assegnati mediante il proprio identificativo univoco.

Entity Statement e Configuration – Attributi (Claims)

Gli Entity Statement emessi dal Trust Ancor o suo Intermediario per i propri diretti discendenti, contengono in aggiunta ai claim comuni anche i seguenti:

Nome	tipo	descrizione
metadata_policy	JSON object	OPZIONALE. Oggetto JSON che descrive un criterio di metadati. Ogni chiave dell'oggetto JSON rappresenta un identificatore del tipo di metadati e ogni valore DEVE essere un oggetto JSON che rappresenta la politica dei metadati in base allo schema di quel tipo di metadati. Si rimanda alla specifica [OIDC-FED#Section.5.1] per i dettagli implementativi.
trust_marks	JSON array	RICHIESTO. Un array JSON contenente i Trust Mark emessi da se stesso per il soggetto discendente.

Metadata

OIDC-FED utilizza i claim dei Metadata così come definiti all'interno delle specifiche di OpenID Connect Discovery 1.0 e OpenID Connect Dynamic Client Registration 1.0 [OpenID.Discovery, OpenID.Registration] rispettivamente per OP e RP.

In OIDC-FED il Metadata OIDC relativo a RP e OP viene definito all'interno del claim "**metadata**" e del suo sotto claim "<**entity_type**>", all'interno dell'Entity Configuration, come oggetto JSON

Ogni Entità DEVE esporre all'interno dei propri Metadata i seguenti claim come obbligatori

Nome	tipo	valore
organization_name	String	OBBLIGATORIO. Nome dell'organizzazione
jwks	JSON	OBBLIGATORIO in assenza del claim **signed_jwks_uri**. JSON Web Key Set [RFC7517#appendix-A.1]
signed_jwks_uri	String	OBBLIGATORIO in assenza del claim **jwks**. URL del JWT auto firmato e verificabile con la chiave pubblica di Federazione (jwk).

Metadata
OpenID Connect Provider Metadata

È il Metadata che gli OP pubblicano con l'identificativo "openid_provider", come segue.

```
   "metadata":{
      "openid_provider": { ... },
      "federation_entity": { ... }

}
```

Se un OP non dispone all'interno dei propri Metadata dei claim **client_registration_types_supported** e/o **request_authentication_methods_supported** i valori da intendersi come impliciti sono i seguenti

Nome	**tipo**	**valore**
client_registration_types_supported	String	"automatic"

request_authentication_methods_supported	JSON Object	{
		"authorization_endpoint":[
		"request_object"
		]
		}

Metadata
OpenID Connect Relying Party Metadata

È il Metadata che i RP pubblicano con l'identificativo "openid_relying_party", come segue

```
   "metadata":{
      "openid_relying_party": { ... },
      "federation_entity": { ... }
}
```

Se un RP non dispone all'interno dei propri Metadata dei claim **client_registration_types** i valori da intendersi come impliciti sono i seguenti

Nome	**tipo**	**valore**
client_registration_types	String	"automatic"

Metadata
OpenID Connect Federation Entity Metadata

È il Metadata che il Trust Anchor, o suo Intermediario, pubblica con l'identificativo **federation_entity**. Questa tipologia caratterizza il TA e i suoi Intermediari. Di seguito la struttura del Metadata di federation_entity

```
   "metadata":{
      "federation_entity": { ... }
}
```

L'oggetto federation_entity è composto dai seguenti claim

Nome	tipo	descrizione
federation_fetch_endpoint	URL	RICHIESTO, url presso il quale sono pubblicati gli Entity Statements in formato JWT dei soggetti discendenti.
federation_list_endpoint	URL	RICHIESTO, url presso il quale è possibile ottenere la lista dei discendenti in formato JSON.
federation_resolve_endpoint	URL	RICHIESTO, url presso il quale è possibile ottenere i trust mark validati,il Metadata finale e la Trust Chain, relativamente ad un soggetto.
federation_status_endpoint	URL	RICHIESTO, url presso il quale è possibile validare l'assegnazione di un Trust Mark ad uno specifico soggetto.
homepage_uri	URL	url della pagina web del Trust Anchor o SA.
organization_name	String	Nome umanamente leggibile di questa Entità.

Metadata
Trust Mark issuer Metadata

Questo è il tipo di Metadata che tutte le entità abilitate ad emettere TM pubblicano con l'identificativo **trust_mark_issuer**, come segue

```
"metadata":{
   "trust_mark_issuer": { ... }
```

Essendo l'endpoint status già presente all'interno dei Metadata di federation_entity, TA e SA adottano la definizione federation_status_endpoint e non è richiesto loro di configurare questo tipo di Metadata in aggiunta

Nome	**tipo**	**descrizione**
status_endpoint	URL	url presso il quale è possibile validare l'assegnazione di un Trust Mark ad uno specifico soggetto

Metadata
Attribute Authority Metadata

Di seguito illustrata la struttura di Metadata che identifica un'Entità di tipo Attribute Authority

```
   "metadata":{
      "oauth_authorization_server": { ... },
      "oauth_resource": { ... },
      "federation_entity": { ... }
}
```

Metadata
Attribute Authority Metadata

Di seguito i claim del Metadata di tipo oauth_authorization_server

Nome	Tipo	Descrizione	Standard di riferimento
issuer	Stringa	Identificativo univoco della Attribute Authority.	[RFC8414]
token_endpoint	Stringa	URL che il RP deve chiamare per scambiare un *Grant Token* con un *Access Token* (token exchange).	[RFC8414]
jwks	Oggetto JSON	Un JSON Web Key Set (JWKS) che rappresenta la parte pubblica delle chiavi di firma dell'entità interessata. Ogni JWK nel set JWK DEVE avere un ID (claim **kid**).	[RFC7517]
scopes_supported	JSON array	Lista di OAuth 2.0 **scope** che la AS supporta.	[RFC8414]
response_types_supported	JSON array	Lista dei valori "response_type" supportati dalla AA. Nel contesto di token exchange (profilo AA protected) viene supportato solo il valore token.	[RFC8414]
grant_types_supported	JSON array	Lista di OAuth 2.0 grant type che la AS supporta.	[RFC8414] [RFC8693]
token_endpoint_auth_methods_supported	JSON array	Array contenente i metodi di autenticazione supportati dal Token Endpoint. Deve essere presente solo il valore **private_key_jwt**	[RFC8414]
token_endpoint_auth_signing_alg_values_supported	JSON array	Array contenente l'elenco degli algoritmi di firma JWS supportati dal Token Endpoint per la firma del JWT utilizzato nell'autenticazione **private_key_jwt**	[RFC8414]
op_policy_uri	Stringa	URL dove è disponibile la privacy policy del servizio AA. Può essere presente più di una occorrenza opportunamente localizzata in più lingue.	[RFC8414]
dpop_signing_alg_values_supported	JSON array	Array contenente l'elenco degli algoritmi di firma JWS supportati dalla AA per la DPoP proof.	draft-ietf-oauth-dpop-03 [OAuth-DPoP]

Metadata
Attribute Authority Metadata

Il Metadata di “oauth_resource” contiene i seguenti parametri

Nome	Tipo	Descrizione	Standard di riferimento
logo_uri	Stringa	OBBLIGATORIO. URL del logo in formato SVG.	[RFC7591]
resource	JSON array	OBBLIGATORIO. Una o più URL che identificano gli endpoint delle risorse protette.	draft-jones-oauth-resource-metadata-01 [OAuth-RS]

Metadata Policy

Il TA o suo Intermediario possono pubblicare politiche sui metadati relative ai propri discendenti all'interno degli Entity Statements relativi a questi.

Ciascuna di queste politiche di metadati presenta le seguenti caratteristiche:

- Consiste in una o più policy claim
- Ogni policy claim si applica a un claim di metadati (es: **client_id**, **grant_types** ...).
- Ogni policy claim è composta da uno o più operatori, che possono essere modificatori di valore o controlli di valore (ad esempio, **value**, **one_of**, **subset_of** ...)
- Un operatore di policy può apparire solo una volta in un oggetto **metadata_policy**.

Per la descrizione degli operatori delle politiche dei metadati, le restrizioni sulle voci dei criteri, l'applicazione dei criteri e l'estensione del linguaggio dei criteri si fa riferimento a [OIDC-FED] "5.1. Metadata Policy".

Soggetti Aggregatori

In questa sezione sono specificate le modalità implementative dei Soggetti Aggregatori in contesto Federativo. Un SA o Intermediario di Federazione è un soggetto che provvede alla registrazione di Foglie di tipo Relying Party e per le quali emette dei Trust Mark riconoscibili dalla AgID e all'interno della Federazione.

Un SA può registrare RP preesistenti e già conformi allo standard OIDC-FED, afferenti a domini esterni al proprio oppure mascherare dietro di sé i propri discendenti. Nel primo caso il SA è di tipo Trasparente (Aggregatore Light) mentre nel secondo caso è di tipo Proxy (Aggregatore Full).

Gli Aggregatori Light registrano RP preesistenti e conformi a OIDC-FED e pubblicano gli entity statement a questi riferiti.

Gli Aggregatori Full provvedono a costruire una interfaccia di autenticazione e federazione per conto dei propri aggregati, mediante risorse web solitamente esposte all'interno del proprio dominio. Questa tipologia di Aggregatore espone le seguenti risorse per ogni suo aggregato:

- **.well-known/openid-federation**, contenente un subject identifier del RP univoco;
- Authorization callback endpoint per l'acquisizione dell'auth code da parte del OP (**redirect_uri**).

Soggetti Aggregatori

Il Soggetto Aggregatore di tipo Full DEVE aggiungere il codice IPA (per il tipo di organizzazione pubblica) o il numero IVA (per quello privato) o il codice fiscale, espressi secondo la norma [EN319-412-1] Paragrafi 5.1.3 e 5.1.4, all'interno del webpath all'interno del **client_id** che identifica l'aggregato:

<SA_dominio> / <IPACODE|VATNUMBER|CODICEFISCALE> /

Nella seguente tabella sono presenti alcuni esempi non normativi per evidenziare le differenze tra gli aggregati Light e Full, dove per l'aggregato Full si usa la variabile $IDCODE ad identificare il soggetto aggregato

	Light mode	**Full mode**
client_id	https://www.rp.it/	https://spid.sa.it/$IDCODE/
redirect_uri	https://www.rp.it/callback/	https://spid.sa.it/$IDCODE/callback/
authorization endpoint	https://www.rp.it/authorize/	https://spid.sa.it/$IDCODE/authorize/
entity configuration	https://www.rp.it/.well-known/openid-federation	https://spid.sa.it/$IDCODE/.well-known/openid-federation

Endpoint di Federazione – Endpoint comuni a tutti

.well-known/openid-federation

Risorsa pubblica attraverso la quale un partecipante pubblica la sua configurazione (EntityConfiguration)

Endpoint di Federazione – Endpoint comuni a tutti

Resolve Entity Statement endpoint

Risorsa pubblica attraverso la quale un partecipante rende noto il Metadata finale calcolato su una Trust Chain precedentemente elaborata e relativa ad un altro soggetto.

L'Entità che espone questo endpoint rende noti i Trust Marks, i metadati e la Trust Chain, relativi alle Entità da esso riconosciute.

Un RP che espone questo endpoint rende noti i metadati degli OP da esso riconosciuti e viceversa.

Questo endpoint DEVE essere esposto da tutti i partecipanti della Federazione per rendere trasparenti le operazioni di analisi delle problematiche dovute al disallineamento dei metadati tra le Entità.

Questo endpoint richiede obbligatoriamente i seguenti parametri in fase di HTTP Request

Claim	**tipo**	**descrizione**
sub	URL	Identificativo dell'Entità per la quale si chiede di ottenere i Trust Mark e i Metadata.
anchor	URL	Identificativo del TA.

Endpoint di Federazione – Endpoint per Trust Anchor ed Intermediari

Il Trust Anchor e i suoi Intermediari (federation_entity) DEVONO in aggiunta esporre al pubblico i seguenti *endpoint*:

Fetch entity statement endpoint

Il recupero degli Entity Statement viene effettuato presso questo endpoint secondo le modalità definite all'interno di OIDC-FED "7.1. Fetching Entity Statements".

Trust mark status endpoint

L'assegnazione di un Trust Mark ad un soggetto viene effettuato presso questo endpoint secondo le modalità definite all'interno di OIDC-FED "7.4. Trust Mark Status".

Entity Listing endpoint

Per ottenere la lista dei discendenti registrati presso la TA o un suo Intermediario è possibile interrogare questo endpoint secondo le modalità descritte in OIDC-FED "7.3. Entity Listings". Ai parametri esistenti già definiti nella specifica, si aggiunge per SPID il parametro entity_type come filtro sul tipo di entità dei discendenti (<entity-type>).

Differenze con OIDC Federation 1.0

Client Registration

SPID supporta esclusivamente **automatic_client_registration**. La modalità **implicit** è da intendersi come non supportata.

Listing endpoint

In SPID viene adottato il parametro aggiuntivo **entity_type** a quelli esistenti nello Standard [OIDC-FED] per questo endpoint, con lo scopo di ottenere un filtro sulla tipologia delle entità discendenti. Questa esigenza consente nello specifico di filtrare entità di tipo **federation_entity**, **openid_relying_party**, **openid_provider, oauth_authorization_server** e **oauth_resource**.

Trust Mark

In OIDC-FED l'uso dei Trust Mark non è obbligatorio. In SPID l'esposizione dei Trust Mark è obbligatoria. Per approfondimenti sulla ragione dell'obbligo dei Trust Mark si rimanda alla sezione "Considerazioni di Sicurezza".

Claim non supportati negli Entity Statement

Poiché SPID non necessita di alcun claim aggiuntivo in ambito federativo, non necessita dei claim **crit**. Inoltre non sono supportati i claim **aud**, **naming_constraints**, **policy_language_crit** e **trust_anchor_id**. L'eventuale presenza di questi claim non presenta alcuna implicazione, questi verranno semplicemente ignorati fino ad ulteriori avvisi che li normino

Sicurezza

Trust Mark come deterrente contro gli abusi

L'implementazione dei Trust Mark e il filtro su questi in fase di Metadata Discovery risulta necessario contro gli attacchi destinati al consumo delle risorse. Un OP attaccato con un numero ingente di connessioni presso il suo endpoint di *authorization*, contenenti **client_id** e **authority_hints** fasulli, produrrebbe svariate connessioni verso sistemi di terze parti nel tentativo di trovare un percorso verso la TA e instaurare la fiducia con il richiedente.

L'OP DEVE validare staticamente il TM oppure DEVE escludere a priori la richiesta ove il TM non risultasse presente, in caso di assenza o non validità di un TM la procedura di Metadata Discovery NON DEVE essere avviata e NON DEVE creare di conseguenza connessioni verso sistemi di terze parti.

Sicurezza

Numero Massimo di authority_hints

All'interno di una Federazione il Trust Anchor decide quante intermediazioni consentire tra di lui e le Foglie, mediante la *constraint* denominata **max_path_lenght**. Questo tipo di relazione è di tipo verticale, dalla foglia alla radice. Questo attributo se valorizzato ad esempio con un valore numerico intero pari a 1 indica che soltanto un SA è consentito tra una Foglia e il TA.

Ogni Foglia DEVE pubblicare i suoi superiori all'interno della lista contenuta nel claim **authority_hints**. Una Foglia all'interno della Federazione PUÒ avere superiori afferenti a diverse Federazioni, si pensi a CIE id per esempio. L'analisi dei superiori disponibili introduce un modello di navigazione orizzontale, ad esempio un OP tenta di trovare il percorso più breve verso il Trust Anchor attraverso tutti gli URL contenuti all'interno dell'array **authority_hints** prima di fare un ulteriore movimento verticale, a salire, verso uno degli Intermediari presenti in questo array.

La soglia **max_path_lenght** si applica per la navigazione verticale e superata questa soglia senza aver trovato il TA la procedura di Metadata Discovery DEVE essere interrotta. Si faccia l'esempio di un RP discendente di un 1 SA che quest'ultimo a sua volta è discendente di un altro SA, essendo il valore di **max_path_lenght** pari a uno e superata questa soglia senza aver trovato il Trust Anchor, la procedura DEVE essere interrotta.

Allo stesso tempo la specifica OIDC Federation 1.0 non definisce un limite per il numero di **authority_hints**, questo perché nessun Trust Anchor può limitare il numero di Federazioni alle quali un partecipante può aderire. Per questa ragione è utile che gli implementatori adottino un limite massimo del numero di elementi consentiti all'interno dell'Array **authority_hint**. Questo per evitare che un numero esagerato di URL contenuti nella lista di **authority_hints**, dovuto ad una cattiva configurazione di una Foglia, produca un consumo di risorse eccessivo

Sicurezza

Resolve Entity Statement

Questo endpoint DEVE rilasciare i Metadata, i Trust Marks e la Trust Chain già precedentemente elaborata e NON DEVE innescare una procedura di Metadata Discovery ad ogni richiesta pervenuta, a meno che questo endpoint non venga protetto con un meccanismo di autenticazione dei client, come ad esempio **private_key_jwt** [OIDC-CORE].

Buone Pratiche

Specializzare le chiavi pubbliche OpenID Core e Federation

È buona pratica usare chiavi pubbliche specializzate per i due tipi di operazioni, Core e Federation.

Modalità di aggiornamento dei Metadata OpenID Core

L'interoperabilità tra i partecipanti funziona mediante i Metadata ottenuti dal calcolo e dalla conservazione delle Trust Chain. Questo significa che se un OP al tempo T calcola la Trust Chain per un RP e questo al tempo T+n modifica i propri Metadata, l'OP di conseguenza potrebbe incorrere in problematiche di validazione delle richieste di autorizzazione del RP, fino a quando non avrà aggiornato la Trust Chain relativa a questo.

La buona pratica per evitare le interruzioni di servizio relative alle operazioni di OIDC Core è quella di aggiungere le nuove chiavi pubbliche all'interno degli oggetti *jwks* senza rimuovere i valori preesistenti. Oppure, ad esempio, i nuovi *redirect_uri*.

In questa maniera dopo il limite massimo di durata delle Trust Chain, definito con il claim **exp** e pubblicato nella Entity Configuration della TA, si ha la certezza che tutti i partecipanti abbiano rinnovato le loro Trust Chain, e sarà possibile agli amministratori della Foglia rimuovere le vecchie definizioni in cima alla lista.

Periodo di grazia per le Trust Chain scadute

In una Federazione distribuita come quella di OIDC-FED è possibile che al tempo T+x un OP necessiti di aggiornare alcune Trust Chain, relative a diversi RP, prossime alla scadenza. Si faccia l'esempio che parte di questi RP risultino aggregati da una SA e i servizi di questo risultino temporaneamente non raggiungibili.

In questi casi, ove vi fosse l'impossibilità di aggiornare una Trust Chain a causa di irraggiungibilità dei servizi web di federazione, è possibile continuare ad utilizzare le Trust Chain scadute fino ad un massimo di 24 ore successive al primo tentativo di aggiornamento. All'interno di questo intervallo temporale "di grazia" sono comunque necessari periodici tentativi di aggiornamento