OpenID Connect in SPID

SPID

SPID (Sistema Pubblico di Identità Digitale) è la chiave di accesso a tutti i servizi digitali della pubblica amministrazione ed a svariati del settore privato. Consiste in un singolo set di credenziali (username e password) che rappresenta l'identità digitale e personale dei cittadini italiani, consentendo loro di essere riconosciuti e di accedere in modo sicuro e personalizzato ai servizi digitali.

Il sistema di identificazione attraverso SPID si basa su tre diversi livelli di sicurezza progressivamente più rigorosi, richiesti dai servizi durante la fase di accesso e correlati al tipo di attività che l'utente sta per svolgere. Per ottenere le credenziali SPID esistono diversi IdP, ad esempio TIM id, POSTE id, aruba.it id, e ognuno di essi può garantire al cliente un certo livello di sicurezza raggiungibile.

I tre livelli sono:

1. Accesso con semplice nome utente e password (SPIDL1).
2. Stesso del punto 1 pi`u un codice temporaneo, un OTP (One Time Password), come ad esempio un SMS o il supporto offerto dall'applicazione mobile (per smartphone e tablet) (SPIDL2).
3. Richiede altri tipi di soluzioni di sicurezza, come un dispositivo fisico (ad esempio una smart card) rilasciato dall'identity provider (SPIDL3).

OpenID Connect in SPID

Le caratteristiche di OpenID Connect rispetto allo standard attualmente utilizzato da Spid (Saml - Security Assertion Markup Language) sono maggiore sicurezza; maggiore facilità di integrazione in sistemi eterogenei (single-page app, web, backend, mobile, IoT); migliore integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile.

Termini e definizioni

Essendo le funzionalità simili, ritroviamo gli stessi concetti di SAML 2.0 anche in OpenID Connect:

SAML 2.0	**OpenID Connect**
Assertion	*ID Token*
Attribute query	*UserInfo Endpoint*
Authentication request	*Authentication request*
ForceAuthn	*prompt=login*
Identity Provider (IdP)	*OpenID Provider (OP)*
IdP metadata	*OpenID Provider metadata*
Issuer	*Issuer*
Logout	*Revoke*
NameID policy	*Subject identifier type*
Passive Authentication	*prompt=none*
Service Provider (SP)	*Relying Party (RP)*
SP metadata	*Client metadata*
Subject	*Subject Identifier*
Attributes	*Claims*

OpenID Provider e Relyng Party

Per OpenID Provider (OP) e *Relying Party (RP)* si intendono rispettivamente i Gestori dell'identità digitale (Identity Provider - IdP) e i Fornitori di servizi (Service Provider - SP) di cui al DPCM 24 ottobre 2014, "Definizione delle caratteristiche del sistema pubblico per la gestione dell'identità digitale di cittadini e imprese (SPID), nonché dei tempi e delle modalità di adozione del sistema SPID da parte delle pubbliche amministrazioni e delle imprese."

Metadata

I metadata sono strutture dati contenenti le informazioni di OpenID Provider (OP) e di Relying Party (RP), mantenute e distribuite dal Registro SPID a tutti i soggetti della federazione, secondo le modalità definite dall'Agenzia per l'Italia Digitale, al fine di consentirne la configurazione nei rispettivi sistemi.

OpenID Provider (OP) Metadata Esempio


```
{
  "issuer": "https://op.fornitore_identita.it",
  "authorization_endpoint": "https://op.fornitore_identita.it/auth
  "token_endpoint": "https://op.fornitore_identita.it/token",
  "userinfo_endpoint": "https://op.fornitore_identita.it/userinfo"
  "introspection_endpoint": "https://op.fornitore_identita.it/intr
  "revocation_endpoint": "https://op.fornitore_identita.it/revoke"
  "end_session_endpoint": "https://op.fornitore_identita.it/logout
  "jwks_uri": "https://registry.spid.gov.it/...",
  "id_token_encryption_alg_values_supported": [
      "..."
  ],
  "userinfo_signing_alg_values_supported": [
      "..."
  ],
  "request_object_encryption_enc_values_supported": [
      "..."
  ],
  "token_endpoint_auth_methods_supported": ["private_key_jwt"],
  "userinfo_encryption_alg_values_supported": [
      "..."
  ],
  "claims_supported":[
    "https://attributes.spid.gov.it/spidCode",
    "https://attributes.spid.gov.it/name",
    "https://attributes.spid.gov.it/familyName",
    "https://attributes.spid.gov.it/placeOfBirth",
    "https://attributes.spid.gov.it/countyOfBirth",
    "https://attributes.spid.gov.it/dateOfBirth",
    "https://attributes.spid.gov.it/gender",
    "https://attributes.spid.gov.it/companyName",
    "https://attributes.spid.gov.it/registeredOffice",
    "https://attributes.spid.gov.it/fiscalNumber",
    "https://attributes.spid.gov.it/ivaCode",
    "https://attributes.spid.gov.it/idCard",
    "https://attributes.spid.gov.it/mobilePhone",
    "https://attributes.spid.gov.it/email",
    "https://attributes.spid.gov.it/address",
    "https://attributes.spid.gov.it/expirationDate",
    "https://attributes.spid.gov.it/digitalAddress"
  ],
  "acr_values_supported":[
    "https://www.spid.gov.it/SpidL1",
```

Elementi nei metadata OP

- **issuer**: identificativo per l'OP (con schema HTTPS), tipicamente il bae URL. Deve corrispondere al valore di iss nel token ID emesso dall'OP. Corrisponde all'attributo entityID in SAML e rappresenta la chiave unica per identificare l'IdP.
- **Authorization_endpoint**: URL per l'endpoint di autorizzazione, al quale il client verrà reindirizzato per avviare il flusso di utenticazione.
- **token_endpoint**: URL per l'endpoint del token che la RP utilizzer`a per scambiare il codice ricevuto alla fine del processo di autenticazione con un access token.
- **Userinfo_endpoint**: URL per lo user info endpoint che la RP pu`o invocare per ottenere gli attributi autorizzati dall'utente.
- **Introspection_endpoint**: URL per l'introspection endpoint che restituisce informazioni su un token.
- **Revocation_endpoint**: URL per l'endpoint di revoca che revoca un refresh token o access token precedentemente emesso per la RP richiedente.
- **Jwks_uri**: URL per il jwks che è un json contenente i seguenti parametri:
  - kty: famiglia dell'algoritmo crittografico adottato.
  - alg: algoritmo adottato
  - use: uso previsto per la chiave pubblica, signature (sig) o encryption (enc).
  - kid: identificatore univoco della chiave.
  - n: modulo (pem standard).
  - e: esponente (pem standard)
- ***Provider_name***: nome del provider OpenID.
- ***Provider_url***: URL del provider OpenID.
- altri campi contenenti gli algoritmi supportati.
- ***Acr_values supported***: array contenente i livelli SPID supportati dall'OP. Uno o pi`u tra:
  - *https://www.spid.gov.it/SpidL1*
  - *https://www.spid.gov.it/SpidL2*
  - *https://www.spid.gov.it/SpidL3*

Relying Party Metadata Esempio


```
{
  "client_id": "https://rp.spid.agid.gov.it",
  "redirect_uris": [
    "https://rp.spid.agid.gov.it/callback1/",
    "https://rp.spid.agid.gov.it/callback2/"
  ],
  "jwks_uri": "https://registry.spid.gov.it/...",
  "jwks": {
    "keys": [
     {
      "kty": "RSA",
      "alg": "RS256",
      "use": "sig",
      "kid": "e27671d73a2605ccd454413c4c94e25b3f66cdea",
      "n": "vmyoDT6ND_YJa1ItdvULuTJr2pw4MvN3Z5kmSiJBm9glVoakcDEBGF
      "e": "ABAB"
     }
    ]
  },
  "response_types": ["code"],
  "grant_types": ["authorization_code", "refresh_token"],
  "client_name": "Agenzia per l'Italia Digitale",
  "client_name#en": "Agency for Digital Italy"
}
```

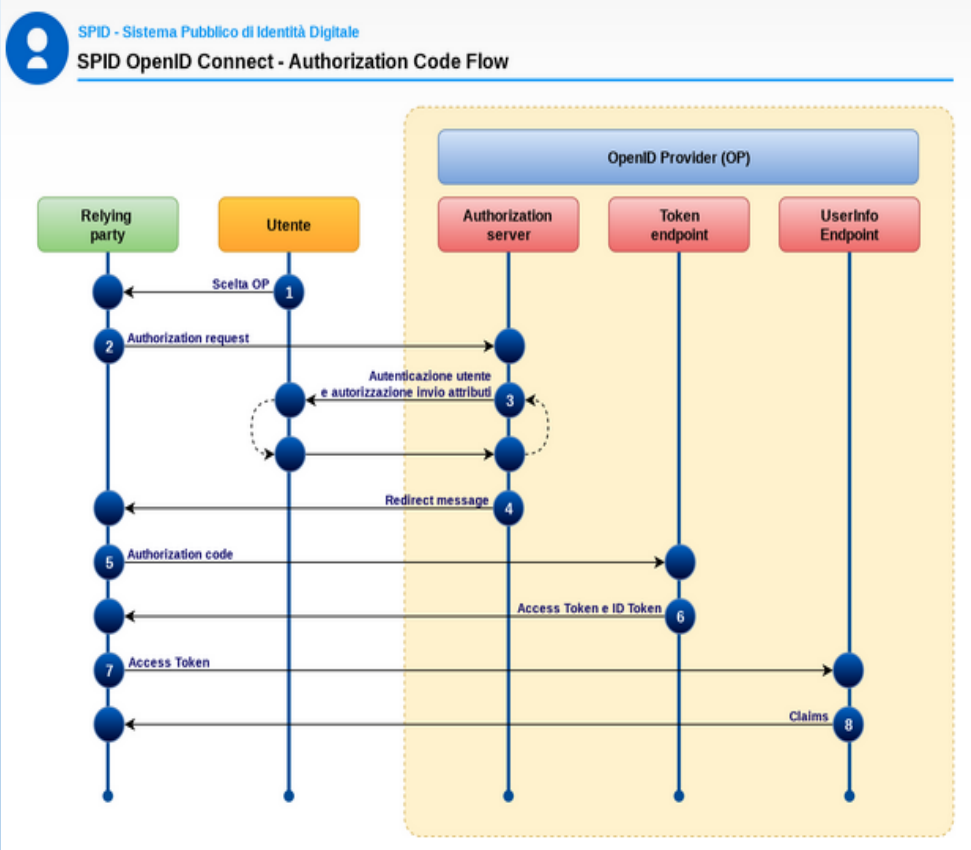
Elementi nei metadati dell'RP

- **client_id**: URI per identificare univocamente la RP, come da registro SPID.
- **redirect_uris**: elenco di URI di call-back utilizzati dalla RP. Il protocollo HTTPS è obbligatorio. Uno di essi deve essere presente nella richiesta di autenticazione.
- **jwks_uri**: stesso formato di quello presente nei metadati dell'OP.
- **client_name**: nome della RP da mostrare nelle pagine di autenticazione e consenso.
- **response_types**: deve contenere solo il valore code code
- **grant_types**: deve contenere solo i valori authorization code e refresh toke

Flusso

Il modello di flusso è l' «**OpenID Connect Authorization Code Flow**» che è infatti l'unico flusso previsto da iGov.

L'Authorization code flow restituisce un codice di autorizzazione che può essere scambiato per un ID token e/o un access token. Questo flusso è anche la soluzione ideale per sessioni lunghe o aggiornabili attraverso l'uso del refresh token. L'Authorization code flow ottiene l'authorization code dall'authorization endpoint dell'OpenID Provider e tutti i token sono restituiti dal token endpoint.



#	Da	A	Azione
1	**Utente**	**RP**	L'Utente, nella pagina di accesso del Relying Party (RP), seleziona, sul pulsante SPID, l'OpenID Provider (OP) con cui autenticarsi
2	**RP**	**OP Authorization server**	Il Relying Party (RP) prepara un'authenticati on request e la invia all'Authorizati on Endpoint dell'OpendID Provider selezionato dall'utente
3	**OP Authorization Server**	**Utente**	L'OpendID Provider (OP) richiede all'utente l'inserimento delle credenziali, secondo il livello SPID richiesto dal Relying Party (RP), all'utente a cui chiede, una volta autenticato, di autorizzare gli attributi richiesti dal Relying Party (RP)
4	**OP Authorization Server**	**RP**	L'OpenID Provider reindirizza l'utente verso il Redirect URI specificato dal RP, passando un authorization code
5	**RP**	**OP Token endpoint**	L'RP invia l'authorization code ricevuto al Token endpoint dell'OP
6	**OP Token endpoint**	**RP**	L'OP Token endpoint rilascia un ID Token, un Access token, e se richiesto un Refresh token
7	**RP**	**UserInfo endpoint**	L'RP valida l'ID token e registra nella propria sessione tutti i token ricevuti. Per chiedere gli attributi che erano stati autorizzati dall'utente al punto 3, invia l'Access token allo UserInfo endpoint dell'OP
8	**OP Userinfo endpoint**	**RP**	L'OP rilascia gli attributi richiesti

Authorization Endpoint (Authentication Request)

Per avviare il processo di autenticazione, il RP manda l'utente all'Authorization Endpoint dell'OP selezionato passando in POST o GET una richiesta in formato JWT.

Tale richiesta DEVE essere firmata e cifrata, secondo le modalità definite dall'Agenzia per l'Italia Digitale.

Esempio (chiamata HTTP):

https://op.spid.agid.gov.it/auth?
request=eyJhbGciOiJSUzI1NiIs
ImtpZCI6ImsyYmRjIn0.ew0KICJpc3MiOiAiczZCaGRSa3F0MyIsDQogI
mF1ZCI6ICJod
HRwczovL3NlcnZlci5leGFtcGxlLmNvbSIsDQogInJlc3BvbnNlX3R5cGUi
OiAiY29kZS
BpZF90b2tlbiIsDQogImNsaWVudF9pZCI6ICJzNkJoZFJrcXQzIiwNCiAic
mVkaXJlY3R
fdXJpIjogImh0dHBzOi8vY2xpZW50LmV4YW1wbGUub3JnL2NiIiwNCi
Aic2NvcGUiOiAi
b3BlbmlkIiwNCiAic3RhdGUiOiAiYWYwaWZqc2xka2oiLA0KICJub25jZ
SI6ICJuLTBTN
l9XekEyTWoiLA0KICJtYXhfYWdlIjogODY0MDAsDQogImNsYWltcyI6IA
0KICB7DQogIC
AidXNlcmluZm8iOiANCiAgICB7DQogICAgICJnaXZlbl9uYW1lIjogeyJlc
3NlbnRpYWw iOiB0cnVlfSwNCiAgICAgIm5p

Esempio (contenuto del JWT**):**

{
client_id=https%3A%2F%2Frp.spid.agid.gov.it
code_challenge=qWJlMe0xdbXrKxTm72EpH659bUxAxw80
code_challenge_method=S256
nonce=MBzGqyf9QytD28eupyWhSqMj78WNqpc2
prompt=login
redirect_uri=https%3A%2F%2Frp.spid.agid.gov.it%2Fcallback1%2F
response_type=code
scope=openid
acr_values=https://www.spid.gov.it/SpidL1 https://www.spid.gov.it/SpidL2
claims={
"id_token":{
"nbf": { essential: true},
"jti": { essential: true}
},
"userinfo":{
"https://attributes.spid.gov.it/name": null,
"https://attributes.spid.gov.it/familyName": null
},
}
state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd
}

Elementi Authentication Request

Parametro	Descrizione	Valori ammessi	Obbligatorio
client_id	URI che identifica univocamente il RP come da Registro SPID.	Deve corrispondere ad un valore nel Registro SPID.	SI
code_challenge	Un challenge per PKCE da riportare anche nella successiva richiesta al Token endpoint.	V. paragrafo 6.1 «Generazione del code_challenge per PKCE»	SI
code_challenge_method	Metodo di costru zione del challen ge PKCE.	È obbligatorio specificare il valore **S256**	SI
nonce	Valore che serve ad evitare attacchi Reply, generato casualmente e non prevedibile da terzi. Questo valore sarà restituito nell'ID Token fornito dal Token Endpoint, in modo da consentire al client di verificare che sia uguale a quello inviato nella richiesta di autenticazione.	Stringa di almeno 32 caratteri alfanumerici.	SI
prompt	Definisce se l'OP deve occuparsi di eseguire una richiesta di autenticazione all'utente o meno.	**consent**: l'OP chiederà le credenziali di autenticazione all'utente (ma solo se non è già attiva una sessione di Single Sign-On) e successivamente chiederà il consenso al trasferimento degli attributi (valore consigliato). **consent login:** l'OP chiederà sempre le credenziali di autenticazione all'utente e successivamente chiederà il consenso al trasferimento degli attributi (valore da utilizzarsi limitatamente ai casi in cui si vuole forzare la riautenticazion e)	SI

Proof Key for Code Exchange è un'estensione per OAuth 2.0 al fine di evitare possibili attacchi messi in atto intercettando il codice di autorizzazione.

Elementi Authentication Request

redirect_uri	URL dove l'OP reindirizzerà l'utente al termine del processo di autenticazione.	Deve essere uno degli URL indicati nel client metadata (v. paragrafo 3.2).	SI
response_type	Il tipo di credenziali che deve restituire l'OP.	**code**	SI
Scope	Lista degli scope richiesti.	**openid** (obbligatorio). **offline_access** se specificato, l'OP rilascerà oltre all'*access token* anche un *refresh token* necessario per instaurare sessioni lunghe revocabili. L'uso di questo valore è consentito solo se il client è un'applicazione per dispositivi mobili che intenda offrire all'utente una sessione lunga revocabile.	SI

Elementi Authentication Request

acr_values	Valori di riferimento della classe di contesto dell'autenticazione richiesta. Stringa separata da uno spazio, che specifica i valori "acr" richiesti al server di autorizzazione per l'elaborazione della richiesta di autenticazione, con i valori visualizzati in ordine di preferenza.	https://www.spid.gov.it/SpidL1 https://www.spid.gov.it/SpidL2 https://www.spid.gov.it/SpidL3	SI
Claims	Lista dei claims (attributi) che un RP intende richiedere per il servizio e livello SPID richiesto.	v. paragrafo 5.1	SI
State	Valore univoco utilizzato per mantenere lo stato tra la request e il callback. Questo valore verrà restituito al client nella risposta al termine dell'autenticaz ione. Il valore deve essere significativo esclusivamente per il RP e non deve essere intellegibile ad altri.	Stringa di almeno 32 caratteri alfanumerici.	SI
response_mode	Definisce la modalità di risposta del Form*	form_post	SI
ui_locales	Lingue preferibili per visualizzare le pagine dell'OP. L'OP può ignorare questo parametro se non dispone di nessuna delle lingue indicate.	Lista di codici RFC5646 separati da spazi.	NO

Claims

Il parametro claims definisce gli attributi e il livello SPID richiesti. all'interno dell'elemento «userinfo» si elencano gli attributi, da richiedere come chiavi di oggetti JSON, i cui valori devono essere null. Gli attributi elencati sotto «userinfo» sono disponibili al momento della chiamata allo UserInfo Endpoint.

```
{
 "userinfo":
  {
   "https://attributes.spid.gov.it/familyName":
    {
     "essential": true
    }
  },
}
```

Se il Relying Party è privato, gli OpenID Provider devono controllare che gli attributi richiesti rientrino tra quelli che essi, in base alla convenzione, possono utilizzare.

Generazione del code_challenge per PKCE

PKCE (Proof Key for Code Exchange, RFC7636) è un'estensione del protocollo OAuth 2.0 finalizzata ad evitare un potenziale attacco attuato con l'intercettazione dell'authorization code, soprattutto nel caso di applicazioni per dispositivi mobili. Consiste nella generazione di un codice (*code verifier*) e del suo hash (*code challenge*). Il *code challenge* viene inviato all'OP nella richiesta di autenticazione.

Quando il client contatta il Token Endpoint al termine del flusso di autenticazione, invia il *code verifier* originariamente creato, in modo che l'OP possa confrontare che il suo hash corrisponda con quello acquisito nella richiesta di autenticazione.

Il *code verifier* deve avere una lunghezza compresa tra 43 e 128 caratteri e deve essere generato con un algoritmo crittografico ad alta entropia.

Il *code challenge* deve essere generato con algoritmo SHA256.

Authentication response

Un'Authentication response è un messaggio di risposta di autorizzazione OAuth 2.0 restituito dall'authorization endpoint dell'OpenID Provider (OP) al termine del flusso di autenticazione. L'OP reindirizzerà l'utente al redirect_uri specificato nella richiesta di autorizzazione, aggiungendo nella post i parametri in risposta.

https://op.spid.agid.gov.it/resp?
code=usDwMnEzJPpG5oaV8x3j&
state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd

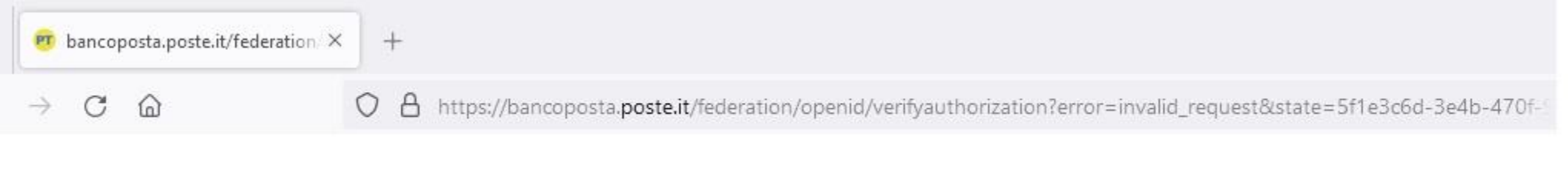
Parametro	Descrizione	Valori ammessi
code	Codice univoco di autorizzazione (*authorization code*) che il client poi passerà al Token Endpoint, secondo le modalità definite dall'Agenzia per l'Italia Digitale.	
state	Valore state incluso nell'Authentication request. Il client è tenuto a verificarne la corrispondenza.	Deve essere lo stesso valore indicato dal client nella Authorization Request.

Errori

In caso di errore, l'OP visualizza i messaggi definiti dalle Linee Guida UX SPID. Nei casi in cui tali linee guida prescrivono un redirect dell'utente verso il RP, l'OP effettua il redirect verso l'URL indicata nel parametro **redirect_uri** della richiesta (solo se valido, ovvero presente nel client metadata), con i seguenti parametri.

https://op.spid.agid.gov.it/resp?
error=invalid_request&
error_description=request%20malformata&
state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd

Parametro	Descrizione	Valori ammessi
error	Codice dell'errore	
error_description	Descrizione più dettagliata dell'errore, finalizzata ad aiutare lo sviluppatore per eventuale debugging. Questo messaggio non è destinato ad essere visualizzato all'utente (a tal fine si faccia riferimento alle Linee Guida UX SPID).	
state	Valore *state* incluso nell'Authentication Request.	Il client è tenuto a verificare che corrisponda a quello inviato nella Authentication Request.



Codici Errori

Scenario	Codice errore
L'OP ha negato l'accesso a causa di credenziali non valide o non adeguate al livello SPID richiesto.	**access_denied**
Il client_id indicato nella richiesta non è riconosciuto.	**invalid_client**
La richiesta non è valida a causa della mancanza o della non correttezza di uno o più parametri.	**invalid_request**
Sono stati richiesti degli scope non validi.	**invalid_scope**
L'OP ha riscontrato un problema interno.	**server_error**
L'OP ha riscontrato un problema interno temporaneo.	**temporarily_unavailable**

Token Endpoint (richiesta token)

Il Token Endpoint rilascia *access token*, *ID Token* e *refresh token*, vi sono due scenari distinti in cui il client chiama il Token Endpoint:

1. al termine del flusso di autenticazione descritto nel paragrafo precedente, il Client chiama il Token Endpoint inviando l'Authorization code ricevuto dall'OP (code=usDwMnEzJPpG5oaV8x3j) per ottenere un *ID Token* e un *access token* (necessario per poi chiedere gli attributi/claim allo UserInfo Endpoint) ed eventualmente un refresh token (se è stata avviata una sessione lunga revocabile);
2. in presenza di una sessione lunga revocabile, il Client chiama il Token Endpoint inviando il *refresh token* in suo possesso per ottenere un nuovo *access token*.

Request

Esempio di richiesta con authorization code (caso 1):

POST https://op.spid.agid.gov.it/token?
client_id=https%3A%2F%2Frp.spid.agid.gov.it&
client_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWI
iOiIxMjM0NTY3ODkwIiwibmFtZSI6IlNQSUQiLCJhZG1pbiI6dHJ1ZX0.LVyRDPVJm0S9
q7oiXcYVIIqGWY0wWQlqxvFGYswLF88&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-as sertion-type%3Ajwt-bearer&
code=usDwMnEzJPpG5oaV8x3j&
code_verifier=9g8S40MozM3NSqjHnhi7OnsE38jklFv2&
grant_type=authorization_code

Esempio di richiesta con refresh token (caso 2):

POST https://op.spid.agid.gov.it/token?
client_id=https%3A%2F%2Frp.spid.agid.gov.it&
client_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWI
iOiIxMjM0NTY3ODkwIiwibmFtZSI6IlNQSUQiLCJhZG1pbiI6dHJ1ZX0.LVyRDPVJm0S9
q7oiXcYVIIqGWY0wWQlqxvFGYswLF88&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-as sertion-type%3Ajwt-bearer&
grant_type=refresh_token&
refresh_token=8xLOxBtZp8

Elementi chiave nella richiesta del token

Parametro	Descrizione	Valori ammessi	Obbligatorio
client_id	URI che identifica univocamente il RP come da Registro SPID.		SI
client_assert ion	JWT firmato con la chiave privata del Relying Party contenente i seguenti parametri: **iss**: Identificatore del RP registrato presso gli OP e che contraddistingu e univocamente l'entità nella federazione nel formato Uniform Resource Locater (URL); corrisponde al client_id usato nella richiesta di autenticazione **sub**: uguale al parametro **iss** **aud**: URL del Token Endpoint dell'OP **iat**: data/ora in cui è stato rilasciato il JWT in formato UTC **exp**: data/ora di scadenza della request in formato UTC. **jti**: Identificatore univoco per questa richiesta di autenticazione, generato dal client casualmente con almeno 128bit di entropia.	**iat**: secondo le modalità definite dall'Agenzia per l'Italia Digitale. **exp**: secondo le modalità definite dall'Agenzia per l'Italia Digitale.	SI

Client_assert ion_type		Deve assumere il seguente valore: **urn:ietf:para ms:oauth:client - assertion-type :jwt-bearer**	SI
Code	Codice di autorizzazione restituito nell'Authentica tion response.		Solo se **grant_type** è **authorization _code**
code_verifier	Codice di verifica del code_challenge (v paragrafo 5.2)		Solo se **grant_type** è **authorization _code**
grant_type	Tipo di credenziale presentata dal Client per la richiesta corrente.	Può assumere uno dei seguenti valori: **authorization _code refresh _token**	SI
refresh_token			Solo se **grant_type** è **refresh_token**

Esempio di token response

Dopo avere ricevuto e validato la Token request dal client, il Token endpoint dell'OpenID Provider (OP) restituisce una response che include ID Token e Access Token e un eventuale Refresh Token, in formato JWT e firmati secondo le modalità definite dall'Agenzia per l'Italia Digitale.

Access Token e ID Token devono essere formati secondo le indicazioni dello standard "International Government Assurance Profile (iGov) for OAuth 2.0 - Draft 03, paragrafo 3.2.1, "JWT Bearer Tokens".


```
{
 "access_token": "dC34Pf6kdG...",
 "token_type": "Bearer",
 "refresh_token": "wJ848BcyLP...",
 "expires_in": 1800,
 "id_token": "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY..."
}
```

Elementi chiave nella token response

Parametro	Descrizione	Valori ammessi
access_token	L'access token, in formato JWT firmato, consente l'accesso allo UserInfo endpoint per ottenere gli attributi.	
token_type	Tipo di *access token* restituito.	Deve essere valorizzato sempre con **Bearer**
refresh_token	Il *refresh token*, in formato JWT firmato, consente di chiamare nuovamente il Token Endpoint per ottenere un nuovo *access token* e quindi recuperare una sessione lunga revocabile.	
expires_in	Scadenza dell'*access token*, in secondi.	Secondo le modalità definite dall'Agenzia per l'Italia Digitale.
id_token	ID Token in formato JWT, firmato e cifrato.	

ID Token

L’ID Token è un JSON Web Token (JWT) che contiene informazioni sull’utente che ha eseguito l’autenticazione. I Client devono eseguire la validazione dell’ID Token.

Esempio


```
{
 "iss": "https://rp.spid.agid.gov.it/",
 "sub": "OP-1234567890",
 "aud": "https://op.spid.agid.gov.it/auth",
 "acr": "https://www.spid.gov.it/SpidL2",
 "at_hash": "qiyh4XPJGsOZ2MEAyLkfWqeQ",
 "iat": 1519032969,
 "nbf": 1519032969,
 "exp": 1519033149,
 "jti": "nw4J0zMwRk4kRbQ53G7z",
 "nonce": "MBzGqyf9QytD28eupyWhSqMj78WNqpc2"
}
```

Elementi chiave dell'ID token

Parametro	Descrizione	Validazione
Iss	Identificatore dell'OP che lo contraddistingue univocamente nella federazione nel formato Uniform Resource Locator (URL).	Il client è tenuto a verificare che questo valore corrisponda all'OP chiamato.
Sub	Per il valore di questo parametro fare riferimento allo standard "OpenID Connect Core 1.0", paragrafo 8.1. "Pairwise Identifier Algorithm".	
Aud	Contiene il client ID.	Il client è tenuto a verificare che questo valore corrisponda al proprio client ID.
Acr	Livello di autenticazione effettivo. Può essere uguale o superiore a quello richiesto dal client nella Authentication Request.	

at_hash	Hash dell'Access Token; il suo valore è la codifica base64url della prima metà dell'hash del valore access_token, usando l'algoritmo di hashing indicato in **alg** nell'header dell'ID Token.	Il client è tenuto a verificare che questo valore corrisponda all'*access token* restituito insieme all'ID Token.
Iat	Data/ora di emissione del token in formato UTC.	

Nbf	Data/ora di inizio validità del token in formato UTC. Deve corrispondere con il valore di **iat**.	{
		userinfo: {…}
		id_token: {
		acr: {…},
		nbf: { essential: true},
		jti: { essential: true }
		}
		}

Exp	Data/ora di scadenza del token in formato UTC, secondo le modalità definite dall'Agenzia per l'Italia Digitale.	
Jti	Identificatore unico dell'ID Token che il client più utilizzare per prevenirne il riuso, rifiutando l'ID Token se già processato. Deve essere di difficile individuazione da parte di un attaccante e composto da una stringa casuale.	
Nonce	Stringa casuale generata dal Client per ciascuna sessione utente ed inviata nell'Authentication Request (parametro nonce), finalizzata a mitigare attacchi replay.	Il client è tenuto a verificare che coincida con quella inviata nell'Authentication Request.

Errori

In caso di errore, l'OP restituisce un codice HTTP 401 con un JSON nel body avente gli elementi di seguito indicati.

Esempio:

```
{
  "error": "invalid_client",
  "error_description: "client_id non riconosciuto."
}
```

Parametro	Descrizione	Valori ammessi
Error	Codice dell'errore	
error_description	Descrizione più dettagliata dell'errore, finalizzata ad aiutare lo sviluppatore per eventuale debugging. Questo messaggio non è destinato ad essere visualizzato all'utente (a tal fine si faccia riferimento alle Linee Guida UX SPID).	

Codici Errore

Scenario	Codice errore
Il client_id indicato nella richiesta non è riconosciuto.	**invalid_client**
Il parametro **grant_type** contiene un valore non corretto.	**unsupported_grant_type**
I parametri **grant_type**, **code**, **code_verifier**, **access_token** non sono validi.	**invalid_grant**
La richiesta non è valida a causa della mancanza o della non correttezza di uno o più parametri.	**invalid_request**
L'OP ha riscontrato un problema interno.	**server_error**
L'OP ha riscontrato un problema interno temporaneo.	**temporarily_unavailable**

UserInfo Endpoint (attributi)

Lo UserInfo Endpoint è una risorsa protetta OAuth 2.0 che restituisce attributi dell'utente autenticato. Per ottenere gli attributi richiesti dal Relying Party, il client inoltra una richiesta allo UserInfo endpoint utilizzando l'Access token. Il risultato è presentato in JSON e contiene una raccolta di coppie nome e valore.

Lo UserInfo Endpoint deve supportare l'uso dei metodi HTTP GET e HTTP POST definiti in RFC 2616 [RFC2616], accettare i token di accesso come utilizzo di token bearer OAuth 2.0 [RFC6750] e supportare l'uso di Cross Origin Resource Sharing (CORS) e/o altri metodi appropriati per consentire ai client Java Script di accedere all'endpoint.

GET https://op.spid.agid.gov.it/userinfo
Authorization: Bearer dC34Pf6kd

Response

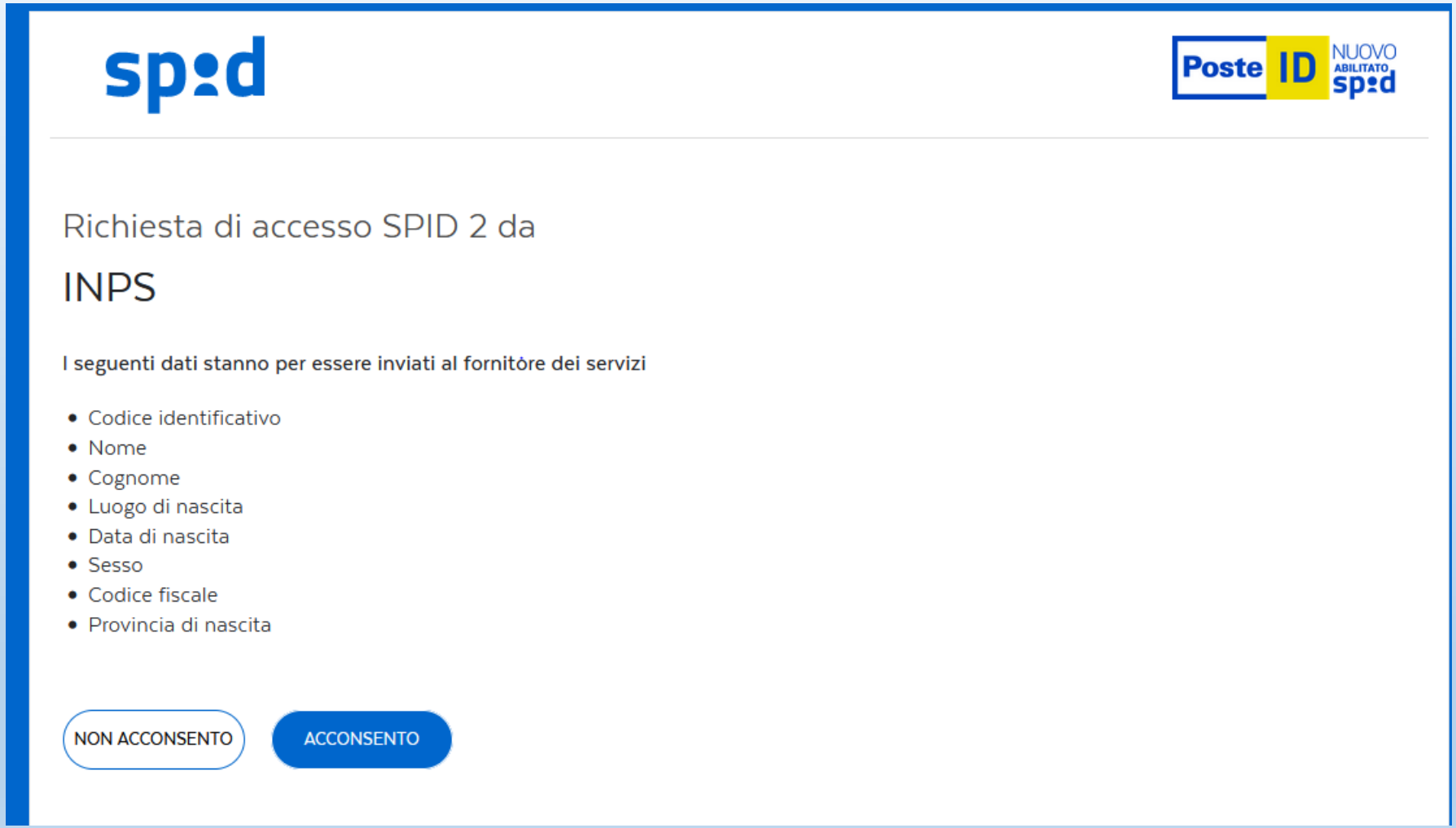
La response dello UserInfo Endpoint deve essere firmata e cifrata secondo le modalità definite dall'Agenzia per l'Italia Digitale. Lo UserInfo Endpoint restituisce i claim autorizzati nella Authentication Request.

Esempio:


```
{
  "iss": "https://op.fornitore_identita.it",
  "aud": "https://rp.fornitore_servizio.it",
  "iat": 1519032969,
  "nbf": 1519032969,
  "exp": 1519033149,
  "sub": "OP-1234567890",
  "https://attributes.spid.gov.it/name": "Mario",
  "https://attributes.spid.gov.it/familyName": "Rossi",
  "https://attributes.spid.gov.it/fiscalNumber": "MROXXXXXXXXXXXXX"
}
```


Parametro	Descrizione	Valori ammessi
sub	Identificatore del soggetto, coincidente con quello già rilasciato nell'ID Token.	Il RP deve verificare che il valore coincida con quello contenuto nell'ID Token.
aud	Identificatore del soggetto destinatario della response	
iss	URI che identifica univocamente il RP come da Registro SPID (client_id).	Il RP deve verificare che il valore coincida con il proprio client_id.
<attributo>	I claim richiesti al momento dell'autenticazione	

In caso di errore di autenticazione, lo UserInfo Endpoint restituisce un errore "HTTP 401".


spid
Poste ID NUOVO ABILITATO spid
Richiesta di accesso SPID 2 da
INPS
I seguenti dati stanno per essere inviati al fornitore dei servizi
Codice identificativo
Nome
Cognome
Luogo di nascita
Data di nascita
Sesso
Codice fiscale
Provincia di nascita
NON ACCONSENTO
ACCONSENTO

Introspection Endpoint (verifica validità token)

L'Introspection Endpoint esposto dall'OP consente ai RP di ottenere informazioni su un token in loro possesso, come ad esempio la sua validità.

La richiesta all'Introspection Endpoint consiste nell'invio del token su cui si vogliono ottenere informazioni unitamente ad una Client Assertion che consente di identificare il RP che esegue la richiesta.

Esempio:
POST https://op.spid.agid.gov.it/introspection?
client_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWI
iOiIxMjM0NTY3ODkwIiwibmFtZSI6IlNQSUQiLCJhZG1pbiI6dHJ1ZX0.LVyRDPVJm0S9 q7oiXcYVIIqGWY0wWQlqxvFGYswLF88&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-as sertion-type%3Ajwt-bearer&
client_id=https%3A%2F%2Frp.spid.agid.gov.it&
token=eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE0MTg3MDI0MTQsImF1ZCI6WyJl
NzFmYjcyYS05NzRmLTQwMDEtYmNiNy1lNjdjMmJjMDAzN2YiXSwiaXNzIjoiaHR0cHM6X
C9cL2FzLXZhLmV4YW1wbGUuY29tXC8iLCJqdGkiOiIyMWIxNTk2ZC04NWQzLTQzN2MtYW
Q4My1iM2YyY2UyNDcyNDQiLCJpYXQiOjE0MTg2OTg4MTR9.FXDtEzDLbTHzFNroW7w27R
Lk5m0wprFfFH7h4bdFw5fR3pwiqejKmdfAbJvN3_yfAokBv06we5RARJUbdjmFFfRRW23
cMbpGQCIk7Nq4L012X_1J4IewOQXXMLTyWQQ_BcBMjcW3MtPrY1AoOcfBOJPx1k2jwRkY tyVTLWlff6S5gK-
ciYf3b0bAdjoQEHd_IvssIPH3xuBJkmtkrTlfWR0Q0pdpeyVePkMSI 28XZvDaGnxA4j7QI5loZYeyzGR9h70xQLVzqwwl1P0-
F_0JaDFMJFO1yl4IexfpoZZsB3 HhF2vFdL6D_lLeHRy-H2g2OzF59eMIsM_Ccs4G47862w

Introspection Endpoint – Elementi chiave

Parametro	Descrizione	Valori ammessi
client_assertion	JWT firmato con la chiave privata del Relying Party contenente gli stessi parametri documentati per le richieste al Token Endpoint.	L'OP deve verificare la validità di tutti i campi presenti nel JWT, nonché la validità della sua firma in relazione al parametro **client_id**.
client_assertion_ty pe		**urn:ietf:params:oau th:client-assertion-t ype:jwt-bearer**
client_id	URI che identifica univocamente il RP come da Registro SPID.	L'OP deve verificare che il client_id sia noto.
token	Il token su cui il RP vuole ottenere informazioni.	

Introspection Endpoint - Response

L'Introspection Endpoint risponde con un oggetto JSON definito come segue.

Esempio:

```
{
  "active": true,
  "scope": "foo bar",
  "exp": 1519033149,
  "sub": "OP-1234567890",
  "client_id": "https://rp.agid.gov.it/"
}
```

Parametro	Descrizione	Valori ammessi
active	Valore booleano che indica la validità del token. Se il token è scaduto, è revocato o non è mai stato emesso per il client_id chiamante, l'Introspection Endpoint deve restituire **false**.	
scope	Lista degli scope richiesti al momento dell'Authorization Request.	
exp	Scadenza del token.	
sub	Identificatore del soggetto, coincidente con quello già rilasciato nell'ID Token.	Il RP deve verificare che il valore coincida con quello contenuto nell'ID Token.
client_id	URI che identifica univocamente il RP come da Registro SPID.	Il RP deve verificare che il valore coincida con il proprio client_id.

Introspection Endpoint - Errori

In caso di errore, l'OP restituisce un codice HTTP 401 con un JSON nel body avente gli elementi di seguito indicati.

Parametro	Descrizione
Error	Codice dell'errore (v. tabella sotto)
error_description	Descrizione più dettagliata dell'errore, finalizzata ad aiutare lo sviluppatore per eventuale debugging. Questo messaggio non è destinato ad essere visualizzato all'utente (a tal fine si faccia riferimento alle Linee Guida UX SPID).

Esempio:

```
{
 "error": "invalid_client",
 "error_description: "client_id non riconosciuto."
}
```

Scenario	Codice errore
Il client_id indicato nella richiesta non è riconosciuto.	**invalid_client**
La richiesta non è valida a causa della mancanza o della non correttezza di uno o più parametri.	**invalid_request**
L'OP ha riscontrato un problema interno.	**server_error**
L'OP ha riscontrato un problema interno temporaneo.	**temporarily_unavailable**

Revocation Endpoint (logout)

Il Revocation Endpoint consente al RP di chiedere la revoca di un *access token* o di un *refresh token* in suo possesso. Lo stato del token può essere verificato inviandolo al introspection endpoint

Quando l'utente esegue il logout, o quando la sua sessione presso il RP scade (in base alle policy decise da quest'ultimo), il RP deve chiamare questo endpoint per revocare l'*access token* e l'eventuale *refresh token* in suo possesso.

L'OP dovrà revocare il token specificato nella richiesta e dovrà terminare la sessione di Single Sign-On se ancora attiva. Eventuali altri token attivi per l'utente dovranno invece essere mantenuti validi.

```
https://idp-poste.poste.it/jod-idp-retail/federation/openid-logout?
iss=agent_idp_ppay&sid=_iTn4JADNOdMwe4BttSoWBedusPvCBQnz3w7yceKlpAMMzyHoUwCPzAGt4tghXcKuJaXLIyb6vXywRdLulgVd5B8HVyvnSAH9bABOcKstIM&sigalg=ht
tp%3A%2F%2Fwww.w3.org%2F2001%2F04%2Fxmldsig-more%23rsa-sha256&sig=GBRR7DUPVlEr9LOhNQWg66oIuCz
%2Firo4Bed6frrwfnk30Xa4ckpKojdtdtZTwdt4Thnx3uiWy%2Bir%0A3vP4PJquAPRpibFa6eUEv5yLEnDq3vyVIuTj%2BJyogCTYcn8MBQGeAiv9Bi8k0pbX4Pa0urYTnzRT
%0Ak39lRY%2B6fdv4NsJSuXo92Lr4o5bcIjxmd1Mee5OQ08BFbOMwL%2BeFfvoCUtFuDKB5bN7VwUJ65J2z%0A5MpS%2BiCqz0iB40hYMDsJ4BSdjbViu6D
%2BL3%2FTo2GvSNHpjs23vgigFGIN1lKrQ%2BbWbHxeOf4Pvigg%0A0Jltrzn7Drp9CYaCQGRjHHr%2BgVBE9fwiyBUFeA%3D%3D
```

Revocation Endpoint - Request

La richiesta al Revocation Endpoint consiste nell'invio del token che si vuole revocare unitamente ad una Client Assertion che consente di identificare il RP che esegue la richiesta.

Esempio:
POST https://op.spid.agid.gov.it/revoke?
client_assertion=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6IlNQSUQiLCJhZG1pbiI6dHJ1ZX0.LVyRDPVJm0S9q7 oiXcYVIIqGWY0wWQlqxvFGYswLF88&
client_assertion_type=urn%3Aietf%3Aparams%3Aoauth%3Aclient-asser tion-type%3Ajwt-bearer&
client_id=https%3A%2F%2Frp.spid.agid.gov.it&
token=eyJhbGciOiJSUzI1NiJ9.eyJleHAiOjE0MTg3MDI0MTQsImF1ZCI6WyJl
NzFmYjcyYS05NzRmLTQwMDEtYmNiNy1lNjdjMmJjMDAzN2YiXSwiaXNzIjoiaHR0cHM6
XC9cL2FzLXZhLmV4YW1wbGUuY29tXC8iLCJqdGkiOiIyMWIxNTk2ZC04NWQzLTQzN2Mt
YWQ4My1iM2YyY2UyNDcyNDQiLCJpYXQiOjE0MTg2OTg4MTR9.FXDtEzDLbTHzFNroW7w
27RLk5m0wprFfFH7h4bdFw5fR3pwiqejKmdfAbJvN3_yfAokBv06we5
RARJUbdjmFFfR
RW23cMbpGQCIk7Nq4L012X_1J4IewOQXXMLTyWQQ_BcBMjcW3Mt
PrY1AoOcfBOJPx1k2 jwRkYtyVTLWlff6S5gK-
ciYf3b0bAdjoQEHd_IvssIPH3xuBJkmtkrTlfWR0Q0pdpeyV
ePkMSI28XZvDaGnxA4j7QI5loZYeyzGR9h70xQLVzqwwl1P0-
F_0JaDFMJFO1yl4Iexf poZZsB3HhF2vFdL6D_lLeHRy-
H2g2OzF59eMlsM_Ccs4G47862w

Parametro	Descrizione	Valori ammessi
client_assertion	JWT firmato con la chiave privata del Relying Party contenente gli stessi parametri documentati per le richieste al Token Endpoint.	L'OP deve verificare la validità di tutti i campi presenti nel JWT, nonché la validità della sua firma in relazione al parametro **client_id**.
client_assertion_ty pe		**urn:ietf:params:oauth:client-assertion-type:jwt-bearer**
client_id	URI che identifica univocamente il RP come da Registro SPID.	L'OP deve verificare che il client_id sia noto.
Token	Il token su cui il RP vuole ottenere informazioni.	

Revocation Endpoint - Response

Il Revocation Endpoint risponde con un codice HTTP 200, anche nel caso in cui il token indicato non esista o sia già stato revocato (in modo da non rilasciare informazioni).

Sessioni lunghe revocabili

Per applicazioni mobili in cui l'RP intenda offrire un'esperienza utente che non passi per il reinserimento delle credenziali SPID ad ogni avvio, è possibile beneficiare di sessioni lunghe revocabili. Per adottare questo tipo di sessione, la RP deve impostare nella authentication request lo scope *offline access* per ottenere successivamente anche un refresh token dopo il consenso esplicito dell'utente

Sessioni lunghe revocabili - Ambiti e limiti di utilizzo

1. Al primo avvio dell'applicazione l'Utente deve essere informato della possibilità di utilizzare la sessione lunga revocabile, per mantenere un'autenticazione di SPID di livello 1 che consenta all'applicazione di ricevere notifiche o effettuare azioni richieste dalla RP, anche quando l'Utente "non sia presente";
2. Le applicazioni mobili che fanno uso di sessioni lunghe revocabili sono tenute a richiedere all'utente, ad ogni avvio o attivazione, un PIN locale oppure un fattore biometrico.
3. In fase di installazione o di prima configurazione, l'applicazione chiede all'utente di registrare il fattore di autenticazione da utilizzare per ogni avvio successivo al primo.
4. Quando l'Utente avvia nuovamente l'applicazione, questa deve richiedere all'Utente il fattore di autenticazione scelto in fase di installazione o di prima configurazione e consentire l'accesso alle funzioni del RP fruibili con il Livello 1 di SPID.
5. Nel caso in cui sia necessario accedere all'applicazione con un livello superiore a SPID di Livello 1, occorre effettuare una nuova autenticazione SPID in base al livello richiesto.

Infine, l'OP deve includere una pagina raggiungibile dall'utente che mostri loro le attuali longterm session attive con la possibilit`a di revocarle. In caso di modifica della password, l'OP deve inoltre fornire la possibilit`a di revocare tutte le attuali long-term session attive dell'utente

Sessioni lunghe revocabili - Request

Per poter utilizzare le sessioni lunghe revocabili, l'RP include nella Authentication Request:

- lo scope "offline_access", al fine di ottenere un refresh token utilizzabile dietro espressa consenso dell'utente;
- il parametro "acr_values" contenente una delle seguenti opzioni:
  - il livello SPID 1;
  - il livello SPID 2 + il livello SPID 1.
  - il livello SPID 3 + il livello SPID 1.

Gestione delle sessioni

- Al fine di poter gestire le sessioni lunghe revocabili e poter rilasciare un refresh token per il Livello 1 di SPID anche a seguito di un'autenticazione di Livello 2 o 3 di SPID, è ammessa l'instaurazione, per ogni livello di SPID, di una sessione di autenticazione associata ad un determinato utente titolare di identità digitale, mantenuta dal gestore dell'identità digitale.
- Gli OP devono includere all'interno della "Pagina di gestione dell'identità SPID", descritta nelle Linee Guida UX SPID, un'interfaccia per visualizzare le sessioni lunghe revocabili attive, dove l'utente possa revocarle singolarmente o in massa.
- In caso di modifica della password richiesta dall'utente, l'OP deve prevedere la possibilità di revocare tutte le sessioni lunghe attive.

Gestione dei log

OpenID Provider e Relying party devono conservare i log di ogni autenticazione e devono essere mantenuti per un tempo pari a 24 mesi.

In particolare devono essere conservate le evidenze di:

rilascio di ID e access token a fronte di autenticazione;

rilascio di refresh token a fronte di autenticazione;

rilascio di ID e access token a fronte di utilizzo del refresh token.

Per ogni rilascio devono essere conservati JWT costituenti richiesta e risposta, occorre, inoltre, tracciare le chiamate e le relative risposte effettuate verso ogni endpoint.

Le tracciature devono essere mantenute nel rispetto del codice della privacy sotto la responsabilità dell'OpenID Provider o del Relying Party e l'accesso ai dati di tracciatura deve essere riservato a personale incaricato.

Al fine di garantire la confidenzialità potrebbero essere adottati meccanismi di cifratura dei dati o impiegati sistemi di basi di dati (DBMS) che realizzano la persistenza cifrata delle informazioni.

Per il mantenimento devono essere messi in atto meccanismi che garantiscono l'integrità e il non ripudio.