Linee Guida OpenID Connect in SPID

Release bozza

AGID

13 feb 2020

Indice dei contenuti

consultation

La consultazione pubblica relativa alle Linee Guida OpenID Connect in SPID è attiva dal **27 agosto** al **26 settembre 2019**.

CAPITOLO 1

Introduzione

1.1 Scopo

Le Linee Guida vengono emesse ai sensi dell'articolo 71 del decreto legislativo 7 marzo 2005, n. 82 e successive modifiche e integrazioni (di seguito CAD) e della Determinazione AgID n. 160 del 2018 recante «Regolamento per l'adozione di linee guida per l'attuazione del Codice dell'Amministrazione Digitale».

OpenID Connect è un layer di identità basato su JSON/REST che si posiziona sopra al protocollo OAuth 2.0. La sua filosofia di design è «rendi semplici le cose semplici e rendi possibili le cose complicate». Mentre OAuth 2.0 è un protocollo di delega delle autorizzazioni di accesso generico, consentendo così il trasferimento di dati arbitrari e non definisce i modi per autenticare gli utenti o comunicare informazioni su di essi, OpenID Connect offre un layer di identità sicuro, flessibile e interoperabile in modo che le identità digitali possano essere facilmente utilizzate su servizi desktop e mobile.

OpenID Connect non si occupa solo di autenticazione ma può essere anche utilizzato per autorizzazione, delega e API access management.

I suoi punti di forza sono:

- facilità di integrazione;
- abilità di integrare applicazioni su diverse piattaforme, single-page app, web, backend, mobile, IoT;
- permette integrazione di componenti di terze parti in modalità sicura, interoperabile e scalabile;
- risolve diverse problematiche di sicurezza riscontrate in OAuth 2.0;
- è utilizzato da un gran numero di servizi social e di pagamento.

Per tutti questi motivi, le presenti linee guide intendono normare l'utilizzo di OpenID Connect nel Sistema Pubblico di Identità Digitale italiano (SPID).

1.2 Gruppo di lavoro

La redazione del documento è stata curata dal gruppo di lavoro composto da:

- Agenzia per l'Italia Digitale;
- Agenzia delle Entrate;
- Aruba S.p.A.;
- Comune di Roma;
- CSI Piemonte;
- Infocert S.p.A.;
- INPS;
- In.Te.S.A. S.p.A.;
- Istituto Poligrafico e Zecca dello Stato;
- Lepida S.p.A.;
- Lombardia Informatica S.p.A.;
- Namirial S.p.A.;
- Net Studio S.p.A.;
- Poste Italiane S.p.A.;
- Regione Toscana;
- Register.it S.p.A.;
- Sielte S.p.A.;
- Sistemi Informativi S.r.l.;
- Sogei S.p.A.;
- Team per la Trasformazione Digitale;
- TI Trust Technologies S.r.l.

I soggetti destinatari delle presenti linee guida sono: i Gestori dell'identità digitale e i Fornitori di servizi 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".

Le presenti Linee Guida entreranno in vigore 6 mesi dopo la loro adozione da parte dell'Agenzia per l'Italia Digitale.

CAPITOLO 2

Riferimenti e sigle

2.1 Riferimenti Normativi

- [Reg. UE n.910/2014] Regolamento (UE) n. 910/2014 del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE;
- [D.Lgs. 82/2005] Decreto legislativo 7 marzo 2005, n. 82 e s.m.i. recante "Codice dell'amministrazione digitale";
- [DPCM 24 ottobre 2014] recante "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.";
- [Regolamento recante le regole tecniche] (articolo 4, comma 2, DPCM 24 ottobre 2014) e s.m.i.;
- [Regolamento recante le modalità attuative per la realizzazione dello SPID] (articolo 4, comma 2, DPCM 24 ottobre 2014) e s.m.i.

2.2 Standard di riferimento

SPID OpenID Connect è basato sul profilo iGov (openid-gov-profile) di OpenID Connect, *International Government Assurance Profile (iGov) for OpenID Connect 1.0*, con la seguente personalizzazione:

- paragrafo 4,2 di openid-igov-openid-connect-1_0: Scope: viene utilizzato solo lo scope «openid» e non «bio», «profile» e «doc» come suggerito dal profilo iGov;
- paragrafo 3,7 e 2,5 di openid-igov-openid-connect-1_0: I metadata degli attori sono distribuiti secondo le modalità definite dall'Agenzia per l'Italia Digitale.

Riferimenti

https://openid.net/specs/openid-igov-openid-connect-1_0-ID1.html
http://openid.net/specs/openid-igov-oauth2-1_0-02.html

2.3 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*

Ai fini delle presenti Linee Guida, 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."

CAPITOLO 3

Metadata

I metadata sono strutture dati contenenti le informazioni di OpenID Provider (OP) e di Relying Party (RP), mantenute e distribuite dal Registry 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.

3.1 OpenID Provider (OP) Metadata

Il formato del metadata deriva da quanto specificato nel documento *«OpenID Connect Discovery 1.0»*, del quale costituisce un sottoinsieme con alcuni campi in aggiunta.

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/introspect",
  "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": [
      "..."
```

(continues on next page)

(continua dalla pagina precedente)

```
  ],
  "id_token_encryption_enc_values_supported": [
      "..."
  ],
  "id_token_signing_alg_values_supported": [
      "..."
  ],
  "request_object_encryption_alg_values_supported": [
      "..."
  ],
  "token_endpoint_auth_signing_alg_values_supported": [
      "..."
  ],
  "request_object_signing_alg_values_supported": [
      "..."
  ],
  "userinfo_encryption_enc_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",
    "https://www.spid.gov.it/SpidL2",
    "https://www.spid.gov.it/SpidL3
  ],
  "request_parameter_supported": true,
  "subject_types_supported":["public"],
  "op_name": "Agenzia per l'Italia Digitale",
  "op_name#en": "Agency for Digital Italy",
  "op_url": "https://www.agid.gov.it",
  "op_url#en": "https://www.agid.gov.it/en"
}
```

Esempio di risorsa jwks_uri:

```
{
  "keys": [
    {
     "kty": "EC",
```

(continues on next page)

(continua dalla pagina precedente)

```
      "kid": "sig-ec256-0",
      "use": "sig",
      "crv": "P-256",
      "x": "2jM2df3IjB9VYQ0yz373-6EEot_1TBuTRaRYafMi5K0",
      "y": "h6Zlz6XReK0L-iu4ZgxlozJEXgTGUFuuDl7o8b_8JnM"
     },
     {
      "kty": "EC",
      "kid": "enc-ec256-0",
      "use": "enc",
      "crv": "P-256",
      "x": "QI31cvWP4GwnWIi-Z0IYHauQ4nPCk8Vf1BHoPazGqEc",
      "y": "DBwf8t9-abpXGtTDlZ8njjxAb33kOMrOqiGsd9oRxr0"
     }
    ]
}
```

Elemento	Descrizione
Issuer	L'identificatore dell'OP (con schema HTTPS), tipicamente l'URL base. Deve essere identico al valore di iss negli ID Token prodotti dall'OP. L'issuer corrisponde al entityID che viene utilizzato in SAML e che rappresenta la chiave univoca con cui è identificato il fornitore di identità.
authorization_endpoint	URL dell'Authorization Endpoint, al quale il Client viene reindirizzato per iniziare il flusso di autenticazione.
token_endpoint	URL del Token Endpoin, che il RP deve chiamare per scambiare il codice ricevuto al termine dell'autenticazione con un access_token.
userinfo_endpoint	URL dello UserInfo Endpoint, che il RP può chiamare per ottenere i claim autorizzati dall'utente.
introspection_endpoint	URL dell'Introspection Endpoint (v. più avanti) che restituisce informazioni su un token.
revocation_endpoint	URL del Revocation Endpoint (v. più avanti) che revoca un *refresh token* o un *access token* già rilasciato al RP chiamante.
jwks_uri	Url del registry dove è localizzato il jwks che è un json array composto dai seguenti parametri: • *kty:* famiglia dell'algoritmo crittografico utilizzato • *alg:* algoritmo utilizzato • *use:* utilizzo della chiave pubblica per firma (sig) o encryption (enc) • *kid:* identificatore univoco della chiave • *n:* modulus (standard pem) • *e:* esponente (standard pem)
provider_name	Nome dell'OpenID Provider. Può essere specificato in più lingue apponendo al nome dell'elemento il suffisso «#» seguito dal codice RFC5646. Un nome di default senza indicazione della lingua è sempre presente.
provider_url	URL dell'OpenID Provider. Può essere specificato in più lingue apponendo al nome dell'elemento il suffisso «#» seguito dal codice RFC5646. Un valore di default senza indicazione della lingua è sempre presente.
request_object_signing_alg_valu es_supported	Array contenente gli algoritmi di firma supportati per il JWS dei Request Object. L'OP deve supportare RS256 e può supportare anche altri algoritmi definiti in rfc7518 (3.1): https://tools.ietf.org/html/rfc7518#section-3.1
request_object_encryption_alg_v alues_supported	Array contenente gli algoritmi di cifratura (**alg**) supportati per il JWS dei Request Object, come definito in rfc7518 (4.1): https://tools.ietf.org/html/rfc7518#section-4.1
request_object_encryption_enc_v alues_supported	Array contenente gli algoritmi di cifratura (**enc**) supportati per il JWS dei Request Object, come definito in rfc7518 (5.1): https://tools.ietf.org/html/rfc7518#section-5.1
id_token_signing_alg_values_sup ported	Array contenente gli algoritmi di firma supportati per il JWS dell'ID Token. L'OP deve supportare RS256 e può supportare anche altri algoritmi definiti in rfc7518 (3.1): https://tools.ietf.org/html/rfc7518#section-3.1
id_token_encryption_alg_values_ supported	Array contenente gli algoritmi di cifratura (**alg**) supportati per il JWS dell'ID Token, come definito in rfc7518 (4.1): https://tools.ietf.org/html/rfc7518#section-4.1
id_token_encryption_enc_values_ supported	Array contenente gli algoritmi di cifratura (**enc**) supportati per il JWS dell'ID Token, come definito in rfc7518

Riferimenti

https://openid.net/specs/openid-connect-discovery-1_0.html#ProviderMetadata

3.2 Client Metadata (Relying Party Metadata)

Il formato del metadata deriva da quanto specificato nel documento *«OpenID Connect Discovery 1.0»*, del quale costituisce un sottoinsieme con alcuni campi in aggiunta.

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_YJa1ItdvULuTJr2pw4MvN3Z5kmSiJBm9glVoakcDEBGF4b5c7WDh2P...",
      "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"
}
```

Elemento	Descrizione
client_id	URI che identifica univocamente il RP come da Registro SPID.
redirect_uris	Array di URI di redirezione utilizzati dal client (RP). Deve esserci un match esatto tra uno degli URI nell'array e quello utilizzato nell'Authentication request. Non è ammesso l'uso dello schema http (è obbligatorio HTTPS); tuttavia gli URI possono seguire eventuali schemi custom (ad es. *myapp://*) al fine di supportare applicazioni mobili. *Come raccomandato dal Garante per la Protezione dei Dati Personali, l'URL non dovrebbe contenere informazioni utili ad individuare lo specifico servizio a cui l'utente intende accedere. Si raccomanda dunque di reindirizzare verso un sistema di access management che a sua volta rimanderà l'utente allo specifico servizio.*
jwks_uri	Array contenente la chiave pubblica in formato JSON Web Key (JWK) e quindi composto dai seguenti parametri: • *kty:* famiglia dell'algoritmo crittografico utilizzato • *alg:* algoritmo utilizzato • *use:* utilizzo della chiave pubblica per firma (sig) o encryption (enc) • *kid:* identificatore univoco della chiave • *n:* modulus (standard pem) • *e:* esponente (standard pem).
client_name	Nome del RP da visualizzare nelle schermate di autenticazione e richiesta di consenso. Può essere specificato in più lingue apponendo al nome dell'elemento il suffisso «#» seguito dal codice RFC5646. Un nome di default senza indicazione della lingua è sempre presente.
response_types	Array dei valori di response_type previsti da OAuth 2.0 che il client userà nelle richieste di autenticazione. Deve contenere il solo valore **code**.
grant_types	Array dei valori di grant_type previsti da OAuth 2.0 che il client userà nelle richieste al Token Endpoint. Deve contenere i soli valori **authorization_code** e **refresh_token**.

Riferimenti

https://openid.net/specs/openid-connect-registration-1_0.html#ClientMetadata

CAPITOLO 4

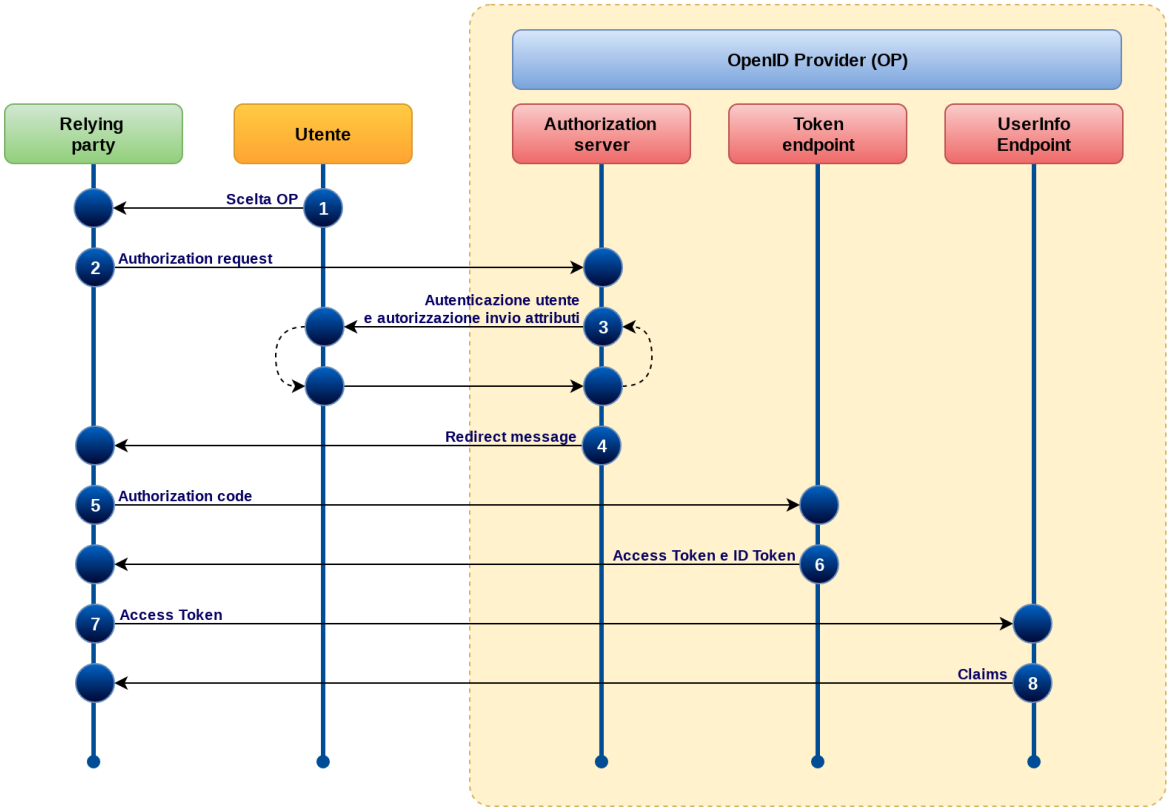
Flusso

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

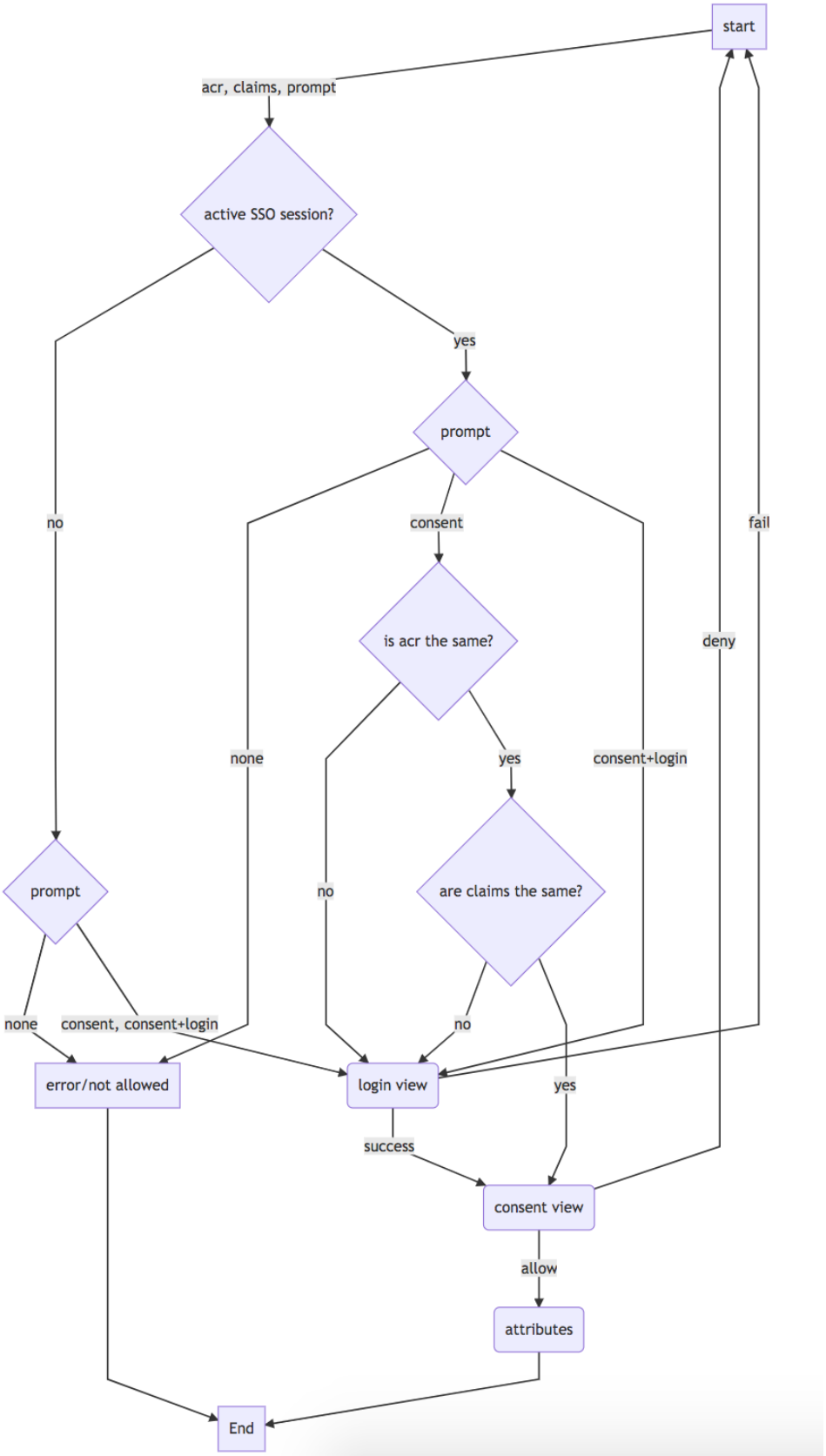
L'Authorization code flow restituisce un codice di autorizzazione che può essere scambiato per un ID token e/o un access token; Questo flusso è anche la soluzione ideale per sessioni lunghe o aggiornabili attraverso l'uso del refresh token. L'Authorization code flow ottiene l'authorization code dall'authorization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

SPID - Sistema Pubblico di Identità Digitale

SPID OpenID Connect - Authorization Code Flow



#	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


start
acr, claims, prompt
active SSO session?
yes
prompt
no
consent
fail
is acr the same?
deny
none
yes
consent+login
prompt
no
are claims the same?
none
consent, consent+login
no
error/not allowed
login view
yes
success
consent view
allow
attributes
End

4.1 Applicazioni per dispositivi mobili

Nel caso di applicazioni mobili rimane il requisito di seguire l'Authorization Code Flow descritto sopra.

In tale contesto, nel diagramma di cui al paragrafo precedente, l'elemento identificato come Relying Party sta ad identificare l'insieme della applicazione residente sul dispositivo mobile e del suo eventuale backend.

Le richieste al Token Endpoint e allo UserInfo Endpoint possono pertanto essere inviate sia dall'applicazione sia dal suo backend; lo scambio di informazioni tra l'applicazione mobile e il suo eventuale backend non sono normate dal presente documento, ferma restando la raccomandazione di prevedere meccanismi di trasmissione e archiviazione sicuri che impediscano a terze parti di venire in possesso dell'Access Token.

Per inviare la Authentication Request all'OP è possibile usare il browser o una webview, purché protetta con i meccanismi più sicuri messi a disposizione dai sistemi operativi al fine di ottenere il massimo isolamento dall'applicazione chiamante. A tal fine si consiglia l'uso della libreria AppAuth e si rinvia alle indicazioni contenute nelle Linee Guida User Experience SPID.

Si rimanda a RFC8252 per ulteriori specifiche tecniche e raccomandazioni di sicurezza da applicarsi in caso di applicazioni mobili.

Riferimenti

RFC8252: OAuth 2.0 for Native Apps (https://tools.ietf.org/html/rfc8252)

CAPITOLO 5

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.ew0KICJpc3MiOiAiczZCaGRSa3F0MyIsDQogImF1ZCI6ICJod
HRwczovL3NlcnZlci5leGFtcGxlLmNvbSIsDQogInJlc3BvbnNlX3R5cGUiOiAiY29kZS
BpZF90b2tlbiIsDQogImNsaWVudF9pZCI6ICJzNkJoZFJrcXQzIiwNCiAicmVkaXJlY3R
fdXJpIjogImh0dHBzOi8vY2xpZW50LmV4YW1wbGUub3JnL2NiIiwNCiAic2NvcGUiOiAi
b3BlbmlkIiwNCiAic3RhdGUiOiAiYWYwaWZqc2xka2oiLA0KICJub25jZSI6ICJuLTBTN
l9XekEyTWoiLA0KICJtYXhfYWdlIjogODY0MDAsDQogImNsYWltcyI6IA0KICB7DQogIC
AidXNlcmluZm8iOiANCiAgICB7DQogICAgInaXZlbl9uYW1lIjogeyJlc3NlbnRpYWw
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
```

(continues on next page)

(continua dalla pagina precedente)

```
 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
}
```

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 auten-	SI

Riferimenti:

http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest
http://openid.net/specs/openid-igov-oauth2-1_0-02.html#rfc.section.2.1.1
http://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.2.1
http://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.2.4
http://openid.net/specs/openid-connect-core-1_0.html#JWTRequests
*https://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html#FormPostesponseMode

5.1 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.

Riferimenti:

http://openid.net/specs/openid-connect-core-1_0.html#IndividualClaimsRequests

5.2 Generazione del code_challenge per PKCE

PKCE (Proof Key for Code Exchange, RFC7636[1]) 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.

Riferimenti:

[1] https://tools.ietf.org/html/rfc7636

http://openid.net/specs/openid-igov-oauth2-1_0-02.html#rfc.section.3.1.7
https://tools.ietf.org/html/rfc7636

CAPITOLO 6

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.

Riferimenti:

https://tools.ietf.org/html/rfc6749#section-4.1.2
http://openid.net/specs/openid-connect-core-1_0.html#AuthRequestValid ation

6.1 Response

Se l'autenticazione è avvenuta con successo, l'OpenID Provider (OP) Authorization server, reindizza l'utente con i seguenti parametri:

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.

6.2 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.

Esempio:

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

Parametro	Descrizione	Valori ammessi
error	Codice dell'errore (v. tabella sotto)	
error_description	Descrizione più dettagliata dell'errore, finalizzata ad aiutare lo sviluppatore in un 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.

Di seguito i codici di errore:

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**

Riferimenti:

https://tools.ietf.org/html/rfc6749#section-4.1.2.1

CAPITOLO 7

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*.

Riferimenti:

https://tools.ietf.org/html/rfc6749#section-3.2
http://openid.net/specs/openid-connect-core-1_0.html#TokenEndpoint
http://openid.net/specs/openid-igov-oauth2-1_0-02.html#rfc.section.2.1.2
http://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.2.2

7.1 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

Parametro	Descrizione	Valori ammessi	Obbligatorio
client_id	URI che identifica univocamente il RP come da Registro SPID.		SI
client_assertion	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_assertion_type		Deve assumere il seguente valore: **urn:ietf:params: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**

7.2 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..."
}
```

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 (v. paragrafo dedicato).	

7.3 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 di ID Token:

```
{
 "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"
}
```

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.

Riferimenti:

http://openid.net/specs/openid-connect-core-1_0.html#IDToken https://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.3.1

7.4 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 (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).	

Di seguito i codici di 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**

Riferimenti:

https://tools.ietf.org/html/rfc6749#section-5.2 http://openid.net/specs/openid-connect-core-1_0.html#TokenErrorResponse

CAPITOLO 8

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 dC34Pf6kdG
```

Riferimenti:

```
http://openid.net/specs/openid-connect-core-1_0.html#UserInfo
https://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.4
```

8.1 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,
```

(continues on next page)

(continua dalla pagina precedente)


```
  "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": "MROXXXXXXXXXXXX"
}
```


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".

CAPITOLO 9

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.

Riferimenti:

https://tools.ietf.org/html/rfc7662
http://openid.net/specs/openid-igov-oauth2-1_0-02.html#rfc.section.3.2.2

9.1 Request

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

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_type		**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.	

9.2 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.

9.3 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 (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).	

Di seguito i codici di errore:

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**

Riferimenti:

https://tools.ietf.org/html/rfc7662#section-2.3

CAPITOLO 10

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.

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.

Riferimenti:

https://tools.ietf.org/html/rfc7009

10.1 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.eyJzdWIiOi
IxMjM0NTY3ODkwIiwibmFtZSI6IlNQSUQiLCJhZG1pbiI6dHJ1ZX0.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_yfAokBv06we5RARJUbdjmFFfR
RW23cMbpGQCIk7Nq4L012X_1J4IewOQXXMLTyWQQ_BcBMjcW3MtPrY1AoOcfBOJPx1k2
jwRkYtyVTLWlff6S5gK-ciYf3b0bAdjoQEHd_IvssIPH3xuBJkmtkrTlfWR0Q0pdpeyV
ePkMSI28XZvDaGnxA4j7QI5loZYeyzGR9h70xQLVzqwwl1P0-F_0JaDFMJFO1yl4Iexf
poZZsB3HhF2vFdL6D_lLeHRy-H2g2OzF59eMIsM_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_type		**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.	

10.2 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).

CAPITOLO 11

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.

11.1 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 unicamente notifiche o call to action da parte dello SP, 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.

11.2 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.

11.3 Refresh Token

Se nella Request è incluso lo scope "offline_access", il Token Endpoint dell'OP restituisce oltre all'*access token* anche un *refresh token*.

11.4 Introspection

Ad ogni successivo avvio della propria applicazione, il RP può inviare una richiesta all'Introspection Endpoint per verificare che l'*access token* in suo possesso sia ancora valido.

In caso negativo, deve inviare una richiesta al Token Endpoint con il *refresh token* in suo possesso, per ottenere un nuovo *access token*.

Nel caso in cui il Token Endpoint rifiuti la concessione di un nuovo *access token*, l'utente dovrà effettuare un nuovo login SPID.

11.5 Esempio

Un RP fornisce servizi per i quali è necessaria un'autenticazione di liv 1 o di livello 2.

Il RP, per consentire l'accesso, effettua una richiesta di autenticazione, all'OP con acr_values=https://www.spid.gov.it/SpidL2 https://www.spid.gov.it/SpidL1

L'"authorization server" autentica l'utente, sulla base del Livello SPID richiesto dal RP (Livello 1 o Livello 2 o Livello 3), c.d. "autenticazione originaria", e rilascia un unico "access_token" sia per il Livello SPID 1 sia per il Livello SPID richiesto dal SP, con una scadenza di 15 minuti, e rilascia un "refresh_token" per il solo livello SPID 1 con scadenza 30 giorni.

L'OP consente l'accesso sia al livello «SPID1» sia al livello «SPID2» per 15 mins mediante l'"access_token".

Quando l'"access_token" scade, l'OP non consente l'accesso con tale l'access token e il RP deve ottenere un nuovo «access_token» tramite nuova autenticazione oppure tramite una «richiesta di refresh».

Il RP effettua una "richiesta di refresh" con il refresh_token.

Il "token endpoint" verifica la validità del refresh_token, e se nella richiesta di autenticazione originaria era presente nell'"acr_values" il livello "SPID1", rilascia un nuovo ID Token valido esclusivamente per il livello «SPID1» con scadenza a 30 giorni dall'autenticazione originaria.

Esempio (chiamata HTTP):

```
https://op.spid.agid.gov.it/auth?request=eyJhbGciOiJSUzI1NiIs ImtpZCI6ImsyYmRjIn0.ew0KICJpc3MiOiAiczZCaGRSa3F0MyIsD
HRwczovL3NlcnZlci5leGFtcGxlLmNvbSIsDQogInJlc3BvbnNlX3R5cGUiOiAiY29kZS Bp-
ZF90b2tlbiIsDQogImNsaWVudF9pZCI6ICJzNkJoZFJrcXQzIiwNCiAicmVkaXJlY3R fd-
XJpIjogImh0dHBzOi8vY2xpZW50LmV4YW1wbGUub3JnL2NiIiwNCiAic2NvcGUiOiAi
b3BlbmlkIiwNCiAic3RhdGUiOiAiYWYwaWZqc2xka2oiLA0KICJub25jZSI6ICJuLTBTN
l9XekEyTWoiLA0KICJtYXhfYWdlIjogODY0MDAsDQogImNsYWltcyI6IA0KICB7DQogIC
AidXNlcmluZm8iOiANCiAgICAgICB7DQogICAgICAgICJnaXZlbl9uYW1lIjogeyJlc3NlbnRpYWw
iOiB0cnVlfSwNCiAgICAgICAgIm5p
```

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 offline_access,
   acr_values=https://www.spid.gov.it/SpidL2 https://www.spid.gov.it/SpidL1,
   claims={
       "userinfo":{
           "https://attributes.spid.gov.it/name": null,
           "https://attributes.spid.gov.it/familyName": null
       },
    }&
   state=fyZiOL9Lf2CeKuNT2JzxiLRDink0uPcd
}
```

Parametro	Descrizione	Valori ammessi	Obbligatorio
client_id	URI che identifica univocamente il client ad un valore RP come da Registro SPID.	Deve corrispondere nel Registro SPID.	SI
code_challenge	Un challenge per PKCE da riportare nella successiva richiesta al Token endpoint.	V. paragrafo 6.1 «Generazione del code_challenge per PKCE»	SI
code_challenge_method	Metodo di costruzione del challenge PKCE	È obbligatorio specificare il valore **S256**	SI
Nonce	Valore che serve ad evitare attacchi Reply, generato casualmente e non prevedibile da 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 le credenziali di 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 riautenticazione)	SI
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
Claims	Lista dei claims (attributi) che un RP intende richiedere per il servizio.	vedi paragrafo 5.1	SI
acr_values	Livello minimo SPID richiesto.	Se sono richiesti più livelli, occorre indicarli in ordine di preferenza, separati da uno spazio.	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'autenticazione. Il valore deve essere significativo esclusivamente per il RP e non deve essere intellegibile ad altri.	Stringa di almeno almeno 32 caratteri alfanumerici.	SI
response_mode	http://openid.net/specs/oauth-v2-form-post-response-mode-1_0.html#FormPostResponseMode	form_post	SI
ui_locales	Lingue preferibili per visualizzare le pagine dell'OP. L'OP può ignorare	Lista di codici RFC5646 separati da spazi.	NO

Esempio Refresh (chiamata HTTP):

```
POST /token HTTP/1.1
Host: server.example.com
Content-Type: application/x-www-form-urlencoded
client_id=https%3A%2F%2Frp.spid.agid.gov.it
&grant_type=refresh_token
&refresh_token=8xLOxBtZp8
&scope=opened
```

Parametro	Descrizione	Valori ammessi
client_id	URI che identifica univocamente il RP come da Registro SPID.	Deve corrispondere alm valore del client_id della authentication request.
grant_type	Tipo di credenziale presentata dal Client per la richiesta corrente.	Deve assumere il valore: **refresh_token**
refresh_token		
Scope		openid

Nel caso in cui il Token Endpoint rifiuti la concessione di un nuovo *ID token* e *access token*, l'utente dovrà effettuare un nuovo login SPID.

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.

Se la Refresh Request è valida, l'OpenID Connect Provider restituisce un ID Token con i seguenti parametri:

Parametro	Descrizione	Valori ammessi
Iss	Identificatore dell'OP che lo contraddistingue univocamente nella federazione nel formato Uniform Resource Locator (URL).	Deve essere lo stesso indicato nell'ID Token emesso nell'autenticazione originaria.
Sub	Per il valore di questo parametro fare riferimento allo standard "OpenID Connect Core 1.0", paragrafo 8.1. "Pairwise Identifier Algorithm".	Deve essere lo stesso indicato nell'ID Token emesso nell'autenticazione originaria.
Aud	Contiene il client ID.	Deve essere lo stesso indicato nell'ID Token emesso nell'autenticazione originaria.
Acr	Livello di autenticazione ammesso a seguito di richiesta di refresh	https://www.spid.gov.it/SpidL1
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**.	
Exp	Data/ora di scadenza del token in formato UTC	
Jti	Identificatore unico dell'ID Token che il client può 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.

Il refresh token ottenuto con la richiesta di autenticazione ha una validità massima di 30 giorni, entro i quali potrà essere utilizzato un numero illimitato di volte. Allo scadere dei 30 giorni non potrà più essere utilizzato e sarà necessario rieseguire l'autenticazione completa.

Riferimenti:

http://openid.net/specs/openid-connect-core-1_0.html#AuthRequest
http://openid.net/specs/openid-igov-oauth2-1_0-02.html#rfc.section.2.1.1
http://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.2.1
http://openid.net/specs/openid-igov-openid-connect-1_0-02.html#rfc.section.2.4
http://openid.net/specs/openid-connect-core-1_0.html#JWTRequests

11.6 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.

CAPITOLO 12

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.