SPID – SISTEMA PUBBLICO PER L'IDENTITÀ DIGITALE
Avviso nr. 41 – Versione 2.0
23/03/2023

INTEGRAZIONE LL.GG. "OPENID CONNECT IN SPID"

METADATA OPENID PROVIDER

Gli OpenID Provider (OP) devono usare "jwks" o "signed_jwks_uri" come normato di seguito:

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

Per il "signed_jwks_uri" è necessario che la URL afferisca allo stesso dominio, di titolarità dell'OP, sul quale è pubblicato il metadata.

L'elemento "op_name" è rinominato in "organization_name".

L'elemento "op_uri" è rinominato in "homepage_uri".

Gli elementi "request_object_encryption_alg_values_supported" e "request_object_encryption_enc_values_supported" non devono essere inclusi nel metadata fino a diversa indicazione di AGID.

Gli elementi "id_token_encryption_alg_values_supported" e "id_token_encryption_enc_values_supported" non devono essere inclusi nel metadata fino a diversa indicazione di AGID.

METADATA CLIENT

I Relying Party (RP) devono usare "jwks" o "signed_jwks_uri" come normato di seguito:

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

REGISTRO SPID OPENID CONNECT

Gli RP e gli Aggregatori devono attuare quanto previsto nel Regolamento "SPID OpenID Connect Federation" ss.mm.ii. emanato da AGID.
Fino alla completa attuazione del suddetto Regolamento gli OP devono esporre quantomeno l'end point ".well-known/openid-federation", contenente nel claim metadata almeno il metadata del tipo **openid_provider**.

ALGORITMI CRITTOGRAFICI

Per tutte le richieste e le risposte HTTP deve essere utilizzando il protocollo TLS nella versione più recente disponibile.

Tutti i partecipanti devono pubblicare gli algoritmi supportati di criptazione e firma all'interno dei propri metadata. Tali algoritmi sono utilizzati per tutte le operazioni di cifratura e firma previsti da Federation.

La lunghezza delle chiavi RSA deve essere pari o superiore a 2048 bit. Si raccomanda una lunghezza di 4096 bit.

I seguenti algoritmi DEVONO essere supportati:

ALGORITMI	OPERAZIONI	RIFERIMENTO
RS256	Signature	OpenID.Core and RFC7518.
RS512	Signature	RFC7518
RSA-OAEP	Key Encryption	RFC7518.
RSA-OAEP-256	Key Encryption	RFC7516.
A128CBC-HS256	Content Encryption	RFC7516.
A256CBC-HS512	Content Encryption	RFC7516.

E' RACCOMANDATO il supporto per i seguenti algoritmi:

ALGORITMI	OPERAZIONI	RIFERIMENTO
ES256	Signature	OpenID.Core and RFC7518.
ES512	Signature	RFC7518.
PS256	Signature	RFC7518.
PS512	Signature	RFC7518.

I seguenti algoritmi NON DEVONO essere supportati:

ALGORITMI	OPERAZIONI	RIFERIMENTI
none	Signature	RFC7518.
RSA_1_5	Key Encryption	RFC7516.
HS256	Signature	RFC7518.
HS384	Signature	RFC7518.
HS512	Signature	RFC7518.

Quando nelle Linee Guida OpenID Connect in SPID viene indicato che il contenuto deve essere firmato e cifrato è necessario prima firmare e poi cifrare.

AUTHORIZATION REQUEST

L'implementazione del valore "verify" per il parametro "prompt" è sospesa fino a indicazione contraria di AGID.

AUTHORIZATION CODE

L'Authorization Code deve essere realizzato nella forma di UUID (https://tools.ietf.org/html/rfc4122) o in altra forma che fornisca almeno le medesime garanzie.
L'Authorization Code deve avere un periodo di validità pari a 5 minuti e bisogna verificare che non sia stato usato precedentemente.

PKCE

Il "code verifier" e il "code challenge" devono essere realizzati in base a quanto stabilito nel RFC 7636, "Proof Key for Code Exchange by OAuth Public Clients" (https://datatracker.ietf.org/doc/html/rfc7636).

REQUEST TOKEN

La differenza tra "iat" e "exp" è a discrezione del Client.

TOKEN ENDPOINT RESPONSE

Il parametro "expires_in" nella Response Token non deve essere superiore a 300 secondi.

ID TOKEN

Il parametro "exp" nell'ID Token deve essere pari a "iat" + 5 minuti
L'ID Token deve avere un periodo di validità pari a 5 minuti e bisogna verificare che non sia stato usato precedentemente.
Il parametro "exp" nell'ID Token rilasciato a seguito di richiesta di refresh deve essere pari a "iat" + 30 giorni – tempo dell'autenticazione originaria.
[Vedere schema per il flusso con refresh]

ACCESS TOKEN

Il parametro "exp" nell'Acces Token deve essere pari a "iat" + 15 minuti.
L'Access Token deve avere un periodo di validità pari a 15 minuti e deve essere riutilizzabile fino alla scadenza.
L'Access Token deve contenere i seguenti parametri:

- client_id
- sub
- scope

RESPONSE USERINFO

Nella header del JWT contenuto nella response del userinfo endpoint è necessario anche il parametro:

cty	(Content Type) Deve essere valorizzato con JWT

REFRESH

La differenza tra "iat" è "exp" può essere di massimo 30 giorni.
La validità del refresh token deve essere calcolata a partire dall'autenticazione originaria.
Il caso d'uso previsto è il Refresh a rotazione a 30 gg:

- t1 : RP effettua autenticazione con offline_access, quindi ottiene refresh_token RT1 (30gg)
- t2 = t1 + 4gg : dopo 4gg da t1 RP fa richiesta a /token presentando RT1. OP rilascia nuovo access_token e nuovo refresh_token RT2 con validità 30gg da t1 (26gg)
- t3 = t1 + 27gg : dopo 27gg da t1 RP fa richiesta a /token presentando RT2. OP rilascia nuovo access_token e nuovo refresh_token RT3 con validità 30gg da t1 (3gg)

[vedere schema per il flusso con refresh token].

TEMPI DI VALIDITA' DEI TOKEN

I Token devono rimanere validi fino alla loro scadenza
La scadenza di un token non incide sulla scadenza dei token collegati.
In caso di rinnovo a seguito dell'utilizzo del refresh token, i precedenti token devono essere resi inutilizzabili, se non già scaduti.

TOLLERANZE

La tolleranza in eccesso o in difetto sui valori "iat" e "exp" deve essere massimo di 3 minuti.

TEMPI DI RISPOSTA

I vari tempi di risposta devono essere compatibili con il tempo totale di risposta previsto dagli SLA allegati alla Convenzione.

TRACCIATURE

- ### TRACCIATURE OPENID PROVIDER

Ai fini della tracciatura l'OpenID Provider dovrà mantenere un Registro delle transazioni contenente i tracciati delle richieste di autenticazione servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà rendere persistente per ogni transazione l'identificativo dell'identità digitale (spidCode) interessata dalla transazione e tutti i messaggi scambiati con il rispettivo RP. Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi.
I messaggi memorizzati nel registro sono i seguenti:

- <AuthenticationRequest>
- <AuthenticationResponse>
- <TokenRequest>
- <TokenResponse>
- <UserInfoRequest>
- <UserInfoResponse>
- <RevocationRequest>
- <RevocationResponse>

e, per ogni messaggio, ove applicabili, potrebbero essere indicizzate ai fini di ricerca e consultazione le seguenti informazioni:

- authorization code
- client_id
- jti
- iss
- sub
- iat
- exp

- ### TRACCIATURE RELYING PARTY

Il comma 2 dell'articolo 13 del DPCM obbliga i fornitori di servizi (relying party) alla conservazione per ventiquattro mesi delle informazioni necessarie a imputare alle singole identità digitali le operazioni effettuate sui propri sistemi. A tal fine un RP dovrà mantenere un Registro delle transazioni contenente i tracciati delle richieste verso i diversi endpoint servite negli ultimi 24 mesi. L'unità di memorizzazione di tale registro dovrà rendere persistente per ogni transazione tutti i messaggi scambiati con il rispettivo OP. Al fine di consentire una facile ricerca e consultazione dei dati di tracciature potrebbe essere opportuno memorizzare in ogni record informazioni direttamente estratte dai suddetti messaggi.
I messaggi memorizzati nel registro potrebbero essere i seguenti:

- <AuthenticationRequest>
- <AuthenticationResponse>
- <TokenRequest>
- <TokenResponse>
- <UserInfoRequest>
- <UserInfoResponse>
- <RevocationRequest>
- <RevocationResponse>

e, per ogni messaggio, ove applicabili, potrebbero essere indicizzate ai fini di ricerca e consultazione le seguenti informazioni:

- authorization code
- client_id
- jti
- iss

- sub
- iat
- exp

- MANTENIMENTO TRACCIATURE

Le tracciature devono essere mantenute nel rispetto del codice della privacy sotto la responsabilità titolare del trattamento dell'Identity Provider. e l'accesso ai dati di tracciatura deve essere riservato a personale incaricato. Al fine di garantire la confidenzialità potrebbero essere adottai 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.

PARAMETRI COMUNI DEI JWT (FIRMATI)

L'header è costituito dalle seguenti informazioni:

Parametro	Descrizione
Typ	OPZIONALE. Ove fosse assente viene considerato "JWT" come definito da https://datatracker.ietf.org/doc/html/rfc7519#section-5.1
Alg	valorizzato con l'identificativo JWA dell'algoritmo crittografico utilizzato.
Kid	ID della chiave utilizzata per sigillare il token

Il payload è costituito dalle seguenti informazioni:

Parametro	Descrizione
Jti	identificativo unico del token.
Iss	deve corrispondere al soggetto mittente.
Aud	deve corrispondere al soggetto destinatario
Iat	istante di generazione del JWT codificato come NumericDate come indicato in RFC 7519 – JSON Web Token (JWT)
Exp	istante di scadenza del JWT codificato come NumericDate come indicato in RFC 7519 – JSON Web Token (JWT)

Non sono vietati ulteriori parametri necessari, sia nell'header sia nel payload, con valori opachi.

LOGOUT

I token rilasciati da OP sono validi fino all'istante di scadenza indicato nel parametro exp.
La revoca anticipata di un token e la conseguente chiusura della sessione sull'OP può essere richiesta dal RP tramite l'endpoint di Revocation.

CODICI DI ERRORE

I codici di errore relativi al Cap. 6 Par. 2 delle Linee Guida OpenID Connect in SPID sono i seguenti:

ERRORE	DESCRIZIONE	CODICE HTTP
access_denied	L'OP ha negato l'accesso a causa di credenziali non valide o non adeguate al livello SPID richiesto (**RFC 6749#section-4.1.2.1**).	*302 Found*
unauthorized_client	Il client non è autorizzato a richiedere un authorization code (**RFC 6749#section-4.1.2.1**).	*200 con pagina di cortesia*
invalid_request	La richiesta non è valida a causa della mancanza o della non correttezza di uno o più parametri (**RFC 6749#section-4.1.2.1**).	*302 Found*
invalid_scope	Sono stati richiesti degli scope non validi (**RFC 6749#section-4.1.2.1**).	*302 Found*
server_error	L'OP ha riscontrato un problema interno (**RFC 6749#section-4.1.2.1**).	*302 Found*
temporarily_unavailable	L'OP ha riscontrato un problema interno temporaneo (**RFC**	*302 Found*

	6749#section-4.1.2.1).	
unsupported_response_type	Il response_type richiesto non è supportato (**RFC 6749#section-4.1.2.1**).	*302 Found*
login_required	L'OP richiede l'autenticazione da parte dell'utente (OpenID.Core#AuthError).	*302 Found*
consent_required	L'OP richiede il consenso esplicito da parte dell'utente (OpenID.Core#AuthError).	*302 Found*
request_uri_not_supported	L'OP non supporta l'uso del parametro *request_uri* (OpenID.Core#AuthError).	*302 Found*
registration_not_supported	L'OP non supporta l'uso del parametro *registration* (OpenID.Core#AuthError).	*302 Found*
invalid_request_object	Il parametro *request* contiene un *Request Object* non valido (OpenID.Core#AuthError).	*302 Found*

I codici di errore relativi al Cap. 7 Par. 4 delle Linee Guida OpenID Connect in SPID sono i seguenti:

CLAIM	**DESCRIZIONE**	**CODICE HTTP**
invalid_client	Problemi durante la client authentication (ad esempio, il client_id è conosciuto, non è fornita l'autenticazione del client o il metodo di autenticazione non è supportato) (**RFC 6749#section-5.2**).	*401 Unauthorized*
unsupported_grant_type	Il parametro grant_type contiene un valore non corretto (**RFC 6749#section-5.2**).	*400 Bad Request*
invalid_grant	I parametri grant_type, code, code_verifier, access_token non sono validi (**RFC 6749#section-5.2**).	*400 Bad Request*
invalid_request	La richiesta non è valida a causa della mancanza o della non correttezza di uno o più parametri (**RFC 6749#section-5.2**).	*400 Bad Request*
server_error	L'OP ha riscontrato un problema interno (**RFC 6749#section-5.2**).	*400 Bad Request*
temporarily_unavailable	L'OP ha riscontrato un problema interno temporaneo (**RFC 6749#section-5.2**).	*400 Bad Request*

I codici di errore relativi al Cap. 8 delle Linee Guida OpenID Connect in SPID sono gli stessi del Cap. 7 Par. 4

I codici di errore relativi al Cap. 9 Par. 3 delle Linee Guida OpenID Connect in SPID sono i seguenti:

CLAIM	**DESCRIZIONE**	**CODICE HTTP**
invalid_client	Problemi durante la client authentication (ad esempio, il client_id è conosciuto, non è fornita l'autenticazione del client o il metodo di autenticazione non è supportato)	*401 Unauthorized*

	(**RFC 6749#section-5.2**).	
invalid_request	La richiesta non è valida a causa della mancanza o della non correttezza di uno o più parametri (**RFC 6749#section-5.2**).	*400 Bad Request*
server_error	L'OP ha riscontrato un problema interno (**RFC 6749#section-5.2**).	500
temporarily_unavailable	L'OP ha riscontrato un problema interno temporaneo (**RFC 6749#section-5.2**).	503

I codici di errore relativi al Cap. 10 delle Linee Guida OpenID Connect in SPID sono gli stessi del Cap. 9 Par. 3

USER EXPERIENCE OPENID CONNECT IN SPID

In attesa delle Linee Guida User Experience SPID (Linee Guida UX SPID) resta valida la User Experience già prevista dalle vigenti regole tecniche SPID.

INTROSPECTION

Se il parametro "active" è valorizzato con "false" non è necessario restituire anche gli altri parametri.

SINGLE SIGN ON

Fino all'emanazione di apposita regolamentazione non è prevista l'instaurazione di una sessione di autenticazione associata ad un determinato utente titolare di identità digitale, mantenute da un Gestore dell'identità digitale (OP) nei confronti di diversi Fornitori di servizi (RP).

Pertanto, con il termine "sessioni di SSO" indicato nelle LLGG OIDC SPID si intende: la sessione di autenticazione associata ad un determinato utente titolare di identità digitale, mantenuta da un Gestore dell'identità digitale (OP) nei confronti di un singolo Fornitore di servizi (RP).

GESTIONE SESSIONI OIDC-SAML

Fino all'emanazione di apposite regole tecniche, non è necessario che OIDC e SAML debbano condividere le sessioni.

PAIRWISE IDENTIFIER

L'OP può individuare autonomamente un valore ricollegabile al Client per il "sector_identifier_uri" in caso non sia stato possibile usando i criteri indicati nella specifica OIDC (https://openid.net/specs/openid-connect-core-1_0.html#PairwiseAlg.).

REVOCHE DEI TOKEN

La revoca di un token da parte dell'utente determina anche la revoca dei token collegati.

CIFRATURA HTTPS

Vale quanto già previsto nell'Avviso SPID n. 1

INDICAZIONE DEI LIVELLI IN ACR

L'OP ha facoltà di effettuare l'autenticazione ad un livello superiore a quello richiesto dal RP, come per SAML.
Il RP deve richiedere sempre il solo livello minimo richiesto per l'autenticazione.
Ad es. con la seguente richiesta: "acr_values=https://www.spid.gov.it/SpidL2" l'OP può effettuare l'autenticazione sia con il livello 2 sia con il livello 3.
Nel caso di "offline_access" il RP deve sempre indicare il solo livello minimino richiesto per l'autenticazione, seguito dal livello 1, ai fini della creazione e gestione delle sessioni lunghe revocabili.
Ad es. con la seguente richiesta: "acr_values=https://www.spid.gov.it/SpidL2 https://www.spid.gov.it/SpidL1" l'OP può effettuare l'autenticazione sia con il livello 2 sia con il livello 3, considerando il livello 1 solo ai fini della creazione e gestione delle sessioni lunghe revocabili.
Se il livello minimo richiesto per l'autenticazione è il Livello 1, il RP può indicare:
"acr_values=https://www.spid.gov.it/SpidL1 l'OP può effettuare l'autenticazione sia con il livello 1 sia con il livello 2

sia con il livello 3, considerando, l'indicazione del RP anche ai fini della creazione e gestione delle sessioni lunghe revocabili.
Se il RP indica nella "authentication request" con "off line access" prima il livello 1 e poi il livello minimino richiesto per l'autenticazione
Ad es.: con la seguente richiesta: "acr_values=https://www.spid.gov.it/SpidL1 https://www.spid.gov.it/SpidL2", l'OP restituisce l'errore "invalid_request".

Il Responsabile del progetto SPID

ENRICA MASSELLA DUCCI TERI

Firmato digitalmente da ENRICA MASSELLA DUCCI TERI
Data: 2023.03.23 19:45:14 +01'00'

OPENID CONNECT AUTHORIZATION CODE FLOW
CON REFRESH TOKEN A 30 GG