draft-lodderstedt-oauth-jwt-introspection-response-01

Vladimir Dzhuvinov, Torsten Lodderstedt

IETF-102
July 17 2018, Montreal

What is it?

- Proposes an additional JWT-based response type for Token Introspection (RFC 7662)

```
HTTP/1.1 200 OK
Content-Type: application/json

 {
   "sub": "Z5O3upPC88QrAjx00dis",
   "aud": "https://protected.example.net/resource",
   "extension_field": "twenty-seven",
   "scope": "read write dolphin",
   "iss": "https://server.example.com/",
   "active": true,
   "exp": 1419356238,
   "iat": 1419350238,
   "client_id": "l238j323ds-23ij4",
   "username": "jdoe"
  }
```

```
HTTP/1.1 200 OK
Content-Type: application/jwt

eyJraWQiOiIxIiwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiJaNU8zdXBQQzg4UXJBa
ngwMGRpcyIsImF1ZCI6Imh0dHBzOlwvXC9wcm90ZWN0ZWQuZXhhbXBsZS5u
ZXRcL3Jlc291cmNlIiwiZXh0ZW5zaW9uX2ZpZWxkIjoidHdlbnR5LXNldmVuIiwic2
NvcGUiOiJyZWFkIHdyaXRlIGRvbHBoaW4iLCJpc3MiOiJodHRwczpcL1wvc2Vyd
mVyLmV4YW1wbGUuY29tXC8iLCJhY3RpdmUiOnRydWUsImV4cCI6MTQxOTM
1NjIzOCwiaWF0IjoxNDE5MzUwMjM4LCJjbGllbnRfaWQiOiJsMjM4ajMyM2RzLTI
zaWo0IiwidXNlcm5hbWUiOiJqZG9lIn0.HEQHf05vqVvWVnWuEjbzUnPz6JDQVR
69QkxgzBNq5kk-sK54ieg1STazXGsdFAT8nUhiiV1f_Z4HOKNnBs8TLKaFXokhA
0MqNBOYI--2unVHDqI_RPmC3p0NmP02Xmv4hzxFmTmpgjSy3vpKQDihOjhwN
Bh7G81JNaJqjJQTRv_1dHUPJotQjMK3k8_5FyiO2p64Y2VyxyQn1VWVlgOHlJw
hj6BaGHk4Qf5F8DHQZ1WCPg2p_-hwfINfXh1_buSjxyDRF4oe9pKy6ZB3ejh9qI
Mm-WrwltuU1uWMXxN6eS6tUtpKo8UCHBwLWCHmJN7KU6ZojmaISspdS23lEL
Alyw
```

Why?

- High assurance level use cases such as payments & electronic signing require signed access tokens due to auditing/non-repudiation requirements
- Use of structured access tokens not always possible
- Example:
  - Integrated authorization for multiple services (e.g. sign a contract + initiate corresponding payment) operated by different providers
  - Cannot use single JWT carrying all necessary data (privacy)
- Token Introspection (RFC 7662) better fits but currently lacks signed responses

JWT Introspection Request

- RS requests JWT response using Accept header value `application/jwt`

```
POST /introspect HTTP/1.1
   Host: server.example.com
   Accept: application/jwt
   Content-Type: application/x-www-form-urlencoded

   token=2YotnFZFEjr1zCsicMWpAA
```

JWT Introspection Response

```
HTTP/1.1 200 OK
   Content-Type: application/jwt

   eyJraWQiOiIxIiwiYWxnIjoiUlMyNTYifQ.eyJzdWIiOiJaNU8zdXBQQzg4UXJBa
   ngwMGRpcyIsImF1ZCI6Imh0dHBzOlwvXC9wcm90ZWN0ZWQuZXhhbXBsZS5uZXRcL
   3Jlc291cmNlIiwiZXh0ZW5zaW9uX2ZpZWxkIjoidHdlbnR5LXNldmVuIiwic2Nvc
   GUiOiJyZWFkIHdyaXRlIGRvbHBoaW4iLCJpc3MiOiJodHRwczpcL1wvc2VydmVyL
   mV4YW1wbGUuY29tXC8iLCJhY3RpdmUiOnRydWUsImV4cCI6MTQxOTM1NjIzOCwia
   WF0IjoxNDE5MzUwMjM4LCJjbGllbnRfaWQiOiJsMjM4ajMyM2RzLTIzaWo0Iiwid
   XNlcm5hbWUiOiJqZG9lIn0.HEQHf05vqVvWVnWuEjbzUnPz6JDQVR69QkxgzBNq5
   kk-sK54ieg1STazXGsdFAT8nUhiiV1f_Z4HOKNnBs8TLKaFXokhA0MqNBOYI--2u
   nVHDqI_RPmC3p0NmP02Xmv4hzxFmTmpgjSy3vpKQDihOjhwNBh7G81JNaJqjJQTR
   v_1dHUPJotQjMK3k8_5FyiO2p64Y2VyxyQn1VWVlgOHlJwhj6BaGHk4Qf5F8DHQZ
   1WCPg2p_-hwfINfXh1_buSjxyDRF4oe9pKy6ZB3ejh9qIMm-WrwltuU1uWMXxN6e
   S6tUtpKo8UCHBwLWCHmJN7KU6ZojmaISspdS23lELAlyw
```

Request Processing

- AS determines what algorithms to employ and whether sign or sign+enc
- RS may supply configuration via Dynamic Client registration posing as a client
- Configuration values follow patterns established by OpenID Connect Dynamic Client Registration for UserInfo
  - `introspection_signed_response_alg`
  - `introspection_encrypted_response_alg`
  - `introspection_encrypted_response_enc`

Status

- Considered WG feedback from IETF-101, focus on RS/AS non-repudiation
- Published revision -01
  - Incorporated feedback from the list (Thanks to Neil Madden & Petteri Stenius!)
  - Added explicit request for JWT introspection response
  - Added security considerations on Cross-JWT Confusion
  - Made `iss` and `aud` claims mandatory in introspection response (Cross-JWT Confusion)
  - Added OAuth Server Metadata parameters to publish algorithms supported for signing and encrypting the introspection response
  - Added IANA registration of new parameters for OAuth Server Metadata and Client Registration