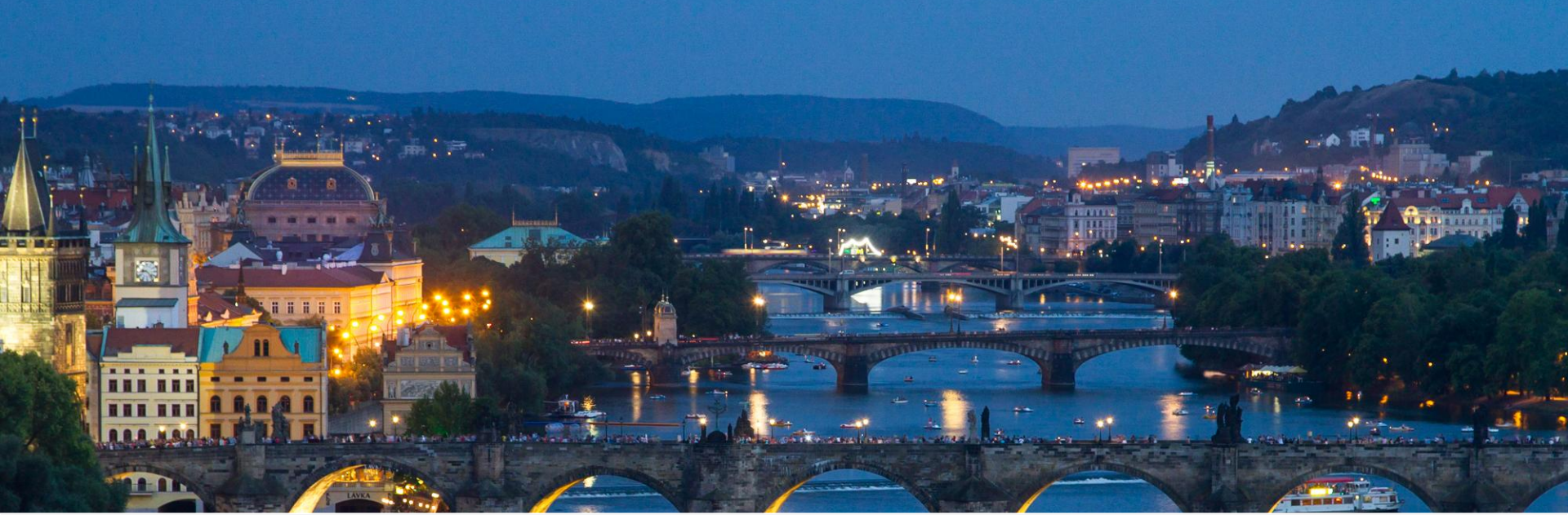
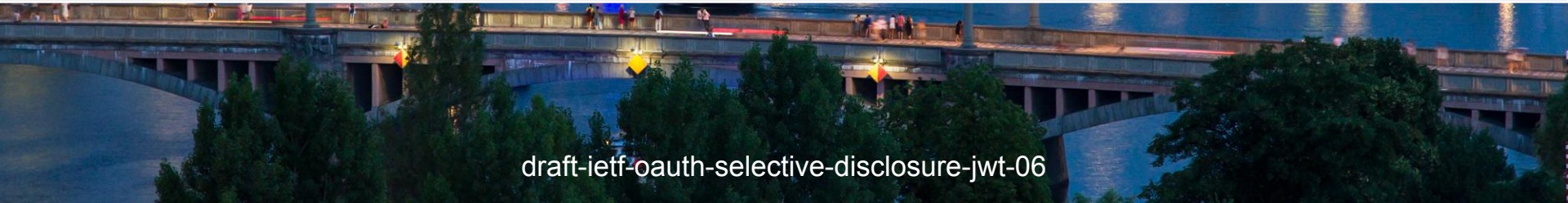


SD-JWT

‘Simple’ is a feature.



draft-ietf-oauth-selective-disclosure-jwt-06

IETF OAuth WG Draft

https://datatracker.ietf.org/doc/draft-ietf-oauth-selective-disclosure-jwt/

Daniel Fett
Authlete

Kristina Yasuda
Microsoft

Brian Campbell
Ping

What’s new in -06?

Format change:

- Added hash of Issuer-signed part and Disclosures in KB-JWT

Clarifications and restructuring:

- Restructured sections around data formats and Example 1
- More precise wording around storing artifacts with sensitive data
- Ensured claims that control validity are checked after decoding payload
- The claim name _sd or ... must not be used in a disclosure

Other changes:

- Fixed minor issues in some examples
- Added IANA media type registration request for the JSON Serialization
- Added JWT claims registration requests to IANA
- Updated JSON Serialization to remove the kb_jwt member and allow for the disclosures to be conveyed elsewhere
- Expanded the Enveloping SD-JWTs section to also discuss enveloping JSON serialized SD-JWTs

Hash in KB-JWT

Issuer

Issuance

End-User
(Holder)

Presentation

Verifier

SD-JWT
plain-text claims
+ hashed Disclosures

✓ signed
by Issuer

Disclosures
salt + claim name + claim value

SD-JWT
plain-text claims
+ hashed Disclosures

✓ signed
by Issuer

<u>Selected</u> Disclosures
salt + claim name + claim value

Holder-Binding JWT

nonce
audience
etc.

✓ signed
by Holder

holder's public key

Issuer

Issuance

SD-JWT
plain-text claims
+ hashed Disclosures

✓ signed by Issuer

Disclosures
salt + claim name + claim value

New: _sd_hash, a hash over the Issuer-signed JWT and the selected Disclosures (REQUIRED)

End-User
(Holder)

Presentation

SD-JWT
plain-text claims
+ hashed Disclosures

✓ signed by Issuer

Selected Disclosures
salt + claim name + claim value

Holder-Binding JWT

nonce
audience
_sd_hash
etc.

✓ signed by Holder

holder's public key

Verifier

Example Presentation


```
eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIkNyUWU3UzVrcUJBSHQtbk1ZWGdjNmJkd
DJTSDVhVFkxc1VfTS1QZ2tqUEkiLCAiSnpZakg0c3ZsaUgwUjNQeUVNZmVadTZKdDY5d
TVxZWhabzdGN0VQWWxTRSIsICJQb3JGYnBLdVZ1Nnh5bUphZ3ZrRnNGWEFiUm9jMkpHb
EFVQTJCQTRvN2NJIiwgIlRHZjRvTGJnd2Q1SlFhSHlLVlFaVTlVZEdFMHc1cnREc3Jae
mZVYW9tTG8iLCAiWFFfM2tQS3QxWHlYNOtBTmtxVlI2eVoyVmE1TnJQSXZQWWJ5TXZSS
0JNTSIsICJYekZyendzYOO2R242QOpEYzZ2Vks4QmtNbmZHOHZPUOtmcFBJWmRBZmRFI
iwgImdiT3NJNEVkcTJ4Mkt3LXc1d1BFemFrb2I5aFYxY1JEMEFUTjNvUUw5SkOiLCAia
nN1OXlWdWx3UVFsaEZsTV8zSmx6TWFTRnpnbGhRRzBEcGZheVF3TFVLNCJdLCAiaXNzI
jogImh0dHBzOi8vaXNzdWVyLmV4YW1wbGUuY29tIiwgImlhdCI6IDE2ODMwMDAwMDAsI
CJleHAiOiAxODgzMDAwMDAwLCAic3ViIjogInVzZXJfNDIiLCAibmFOaW9uYWxpdGllc
yI6IFt7Ii4uLiI6ICJwRm5kamtaX1ZDem15VGE2VWpsWm8zZGgta284YUlLUWM5RGxHe
mhhVllvIn0sIHsiLi4uIjogIjdDZjZKa1B1ZHJ5M2xjYndIZ2VaOGtoQXYxVTFPU2xlc
lAwVmtCSnJXWjAifVOsICJfc2RfYWxnIjogInNoYS0yNTYiLCAiY25mIjogeyJqd2siO
iB7Imt0eSI6ICJFQyIsICJjcnYiOiAiUCOyNTYiLCAieCI6ICJUQOFFUjE5WnZ1MO9IR
jRqNFcOdmZTVm9ISVAxSUxpbERsczd2Q2VHZW1jIiwgInkiOiAiWnhqaVdXYlpNUUdIV
ldLVlEOaGJTSWlyc1ZmdWVjQOU2dDRqVDlGMkhaUSJ9fXO.OeQrinudSFTXNysz2NuNQ
rwWJv-P9gQ-Ce3wWEYZkxngeA4GKfPfApdNzBa4OdH1urt8tXhW2WQl-IOOv8teuw~Wy
JlbHVWNU9nM2dTTklJOEVZbnN4QV9BIiwgImZhbWlseV9uYW11IiwgIkRvZSJd~WyJBS
ngtMDk1VlBycFROTjRRTU9xUk9BIiwgImFkZHJlc3MiLCB7InNOcmVldF9hZGRyZXNzI
jogIjEyMyBNYWluIFNOIiwgImxvY2FsaXR5IjogIkFueXRvd24iLCAicmVnaW9uIjogI
kFueXNOYXRlIiwgImNvdW5OcnkiOiAiVVMifVO~WyIyR0xDNDJzS1F2ZUNmR2ZyeU5ST
jl3IiwgImdpdmVuX25hbWUiLCAiSm9obiJd~WyJsa2x4RjVqTVlsR1RQVW92TU5JdkNB
IiwgIlVTIlO~eyJhbGciOiAiRVMyNTYiLCAidHlwIjogImtiK2p3dCJ9.eyJub25jZSI
6ICIxMjMONTY3ODkwIiwgImF1ZCI6ICJodHRwczovL3ZlcmlmaWVyLmV4YW1wbGUub3J
nIiwgImlhdCI6IDE2OTgwNzc3OTAsICJfc2RfaGFzaCI6ICIzNHQ4dkNDX2NfdlZMbk9
hZEJOd2gOZEZ2QkVyU2w5ektPcXdtNmloVF9VIn0.ZlotfwqF9NUTRAShrd8jGSJEB6e
3Z3EKm-AD5udfzggxfK-lQM4TCKbHK81eVO88YTKl-UfM7WSyQpx5wpNpZw
```


Key-Binding JWT Body:


```
{
  "nonce": "1234567890",
  "aud": "https://verifier.example.org",
  "iat": 1698077790,
  "_sd_hash": "34t8vCC_c_vVLnOadBtwh4dFvBErSl9zKOqwm6ihT_U"
}
```

Next Steps

Next Steps

- Neil's comments on cryptography — will address (#359, #360, TBD)
- More issues on issue tracker but nothing major
- Approaching Working Group Last Call?
  - Format (mostly) stable for some time now
  - No expected breaking changes
  - At least nine implementations