IETF 120, Vancouver
OAuth WG
July 2024

Selective Disclosure for JWTs (SD-JWT)

Daniel Fett (Authlete), Kristina Yasuda (Keio University), Brian Campbell (Ping Identity)

Rough Agenda:

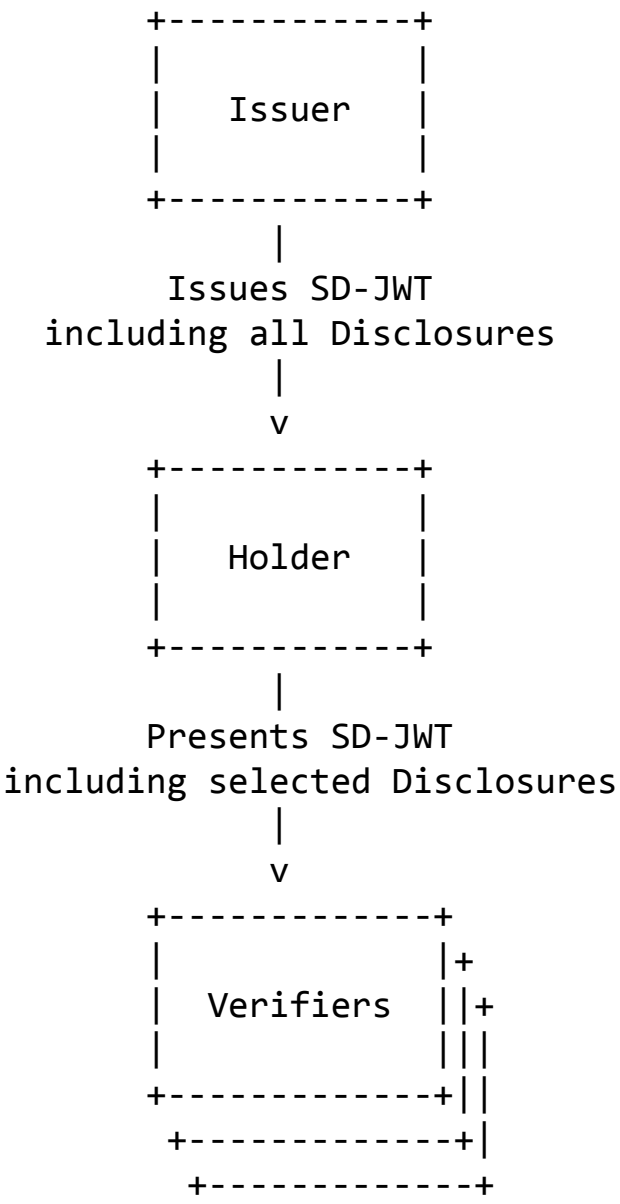
- Overview / refresher (again)
- Changes since last time
- Open issues/questions
- Next steps!

SD-JWT

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

Abstracting the Abstract

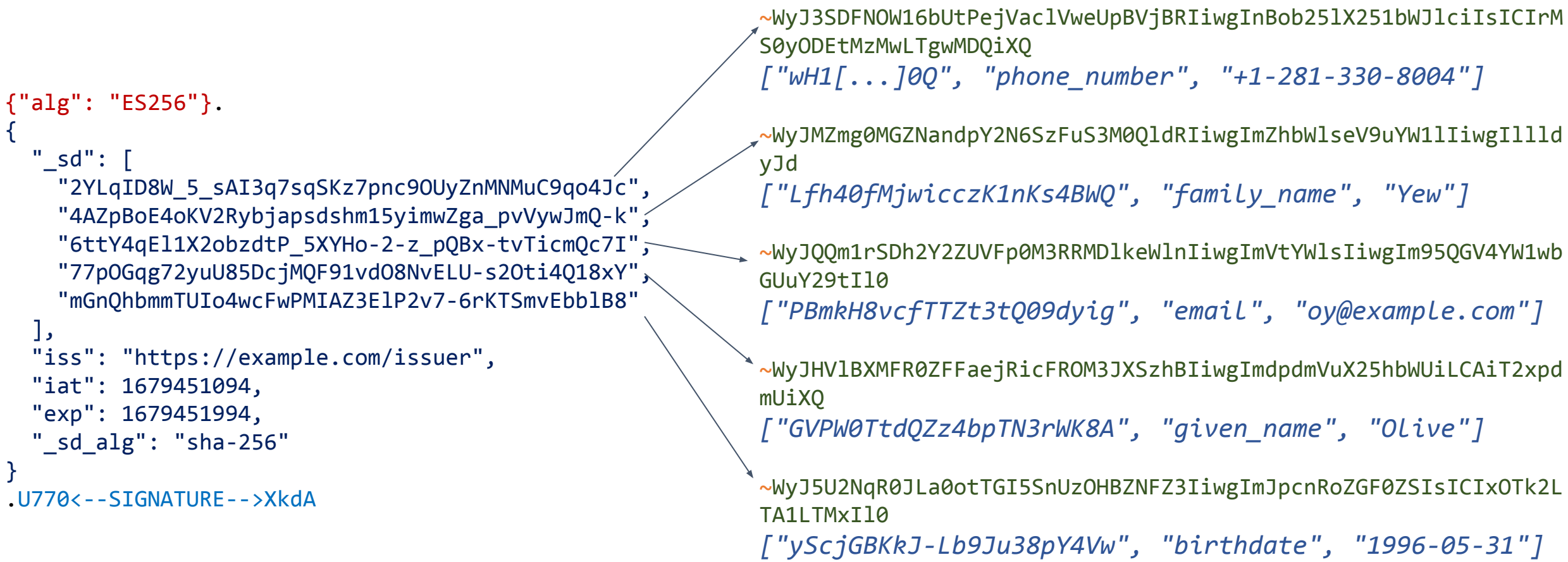
- SD-JWT is a salted-hash-based mechanism for selective disclosure of individual elements of a JSON object used as the payload of a JWS structure
- Mainly SD-JWT is for selective disclosure of JWT claims
- Aims to be easy to implement by leveraging familiar, established, and widely used data formats and cryptographic algorithms



Illustrated SD-JWT

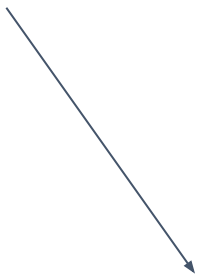

```
eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5jOU9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNXlpb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WFlIby0yLXpfcFFCe
C10dlRpY21RYzdJIiwgIjc3cE9HcWc3Mnl1VTg1RGNqTVFGOTF2ZE84TnZFTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUlvNHdjRndQTUlBWjNFbFAydjctNnJLVFNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBzOi8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImlhdCI6I
DE2Nzk0NTEwOTQsICJleHAiOiAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p17lZ0zH0cMlFJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hViy39Muzmjy_XkdA~WyJHVlBXMFR0ZFFaejRicFROM3JXSzhBIiwgImdpdmVuX2
5hbWUiLCAiT2xpdmUiXQ~WyJMZmg0MGZNandpY2N6SzFuS3M0QldRIiwgImZhbWlseV9
uYW1lIiwgIllldyJd~WyJQQm1rSDh2Y2ZUVFp0M3RRMDlkeWlnIiwgImVtYWlsIiwgIm
95QGV4YW1wbGUuY29tIl0~WyJ3SDFNOW16bUtPejVaclVweUpBVjBRIiwgInBob25lX2
51bWJlciIsICIrMS0yODEtMzMwLTgwMDQiXQ~WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ
3IiwgImJpcnRoZGF0ZSIsICIxOTk2LTA1LTMxIl0~
```

Disclosures



Selecting Disclosure(s)


```
{"alg": "ES256"}.
{
  "_sd": [
    "2YLqID8W_5_sAI3q7sqSKz7pnc9OUyZnMNMuC9qo4Jc",
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",
    "77pOGqg72yuU85DcjMQF91vdO8NvELU-s2Oti4Q18xY",
    "mGnQhbmmTUIo4wcFwPMIAZ3ElP2v7-6rKTSmvEbblB8"
  ],
  "iss": "https://example.com/issuer",
  "iat": 1679451094,
  "exp": 1679451994,
  "_sd_alg": "sha-256"
}
.U770<--SIGNATURE-->XkdA
```


```
~WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZGF0ZSIsICIxOTk2LTA1LTMxIl0
["yScjGBKkJ-Lb9Ju38pY4Vw", "birthdate", "1996-05-31"]
```

Presenting the SD-JWT
(i.e., without a KB-JWT)

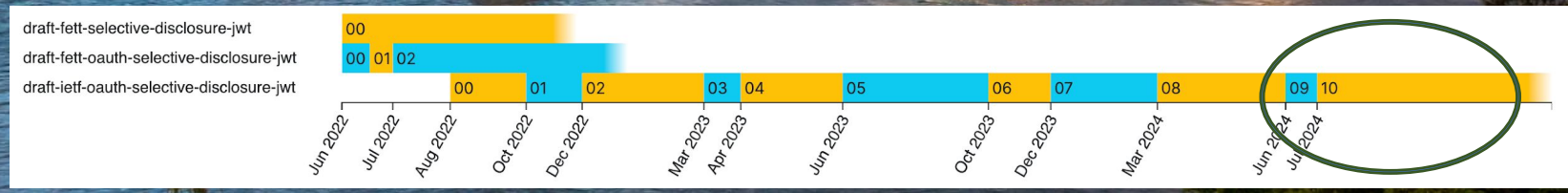

```
eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5jOU9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNXlpb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WFlIby0yLXpfcFFCe
C10dlRpY21RYzdJIiwgIjc3cE9HcWc3Mnl1VTg1RGNqTVFGOTF2ZE84TnZFTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUlvNHdjRndQTUlBWjNFbFAydjctNnJLVFNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBzOi8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImlhdCI6I
DE2Nzk0NTEwOTQsICJleHAiOiAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p17lZ0zH0cMlFJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hViy39Muzmjy_XkdA~WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZG
F0ZSIsICIxOTk2LTA1LTMxIl0~
```

Presenting the SD-JWT+KB
(i.e., with a KB-JWT)


```
eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5jOU9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNXlpb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WFlIby0yLXpfcFFCe
C10dlRpY21RYzdJIiwgIjc3cE9HcWc3Mnl1VTg1RGNqTVFGOTF2ZE84TnZFTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUlvNHdjRndQTUlBWjNFbFAydjctNnJLVFNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBzOi8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImlhdCI6I
DE2Nzk0NTEwOTQsICJleHAiOiAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p17lZ0zH0cMlFJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hViy39Muzmjy_XkdA~WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZG
F0ZSIsICIxOTk2LTA1LTMxIl0~eyJhbGciOiAiRVMyNTYiLCAidHlwIjogImtiK2p3dC
J9.eyJub25jZSI6ICIxMjM0NTY3ODkwIiwgImF1ZCI6ICJodHRwczovL3ZlcmlmaWVyL
mV4YW1wbGUub3JnIiwgImlhdCI6IDE3MDkzNDI1Mzd9.v_S9JlF_338--5VTk1kTjJTc
8NQQbNAgQyGj7eH1hAO5s-QEXAt8FAw1zXhJAmy0DMfCQLbGWQ5aoODa2q5igg
```

```
{"nonce": ”123", "aud": "https://verifier.example.org",
   "iat": 1709212154, "sd_hash": "GOnZn[...]iHvfQ"}
```

Since IETF 119 Brisbane…



© Brian Campbell

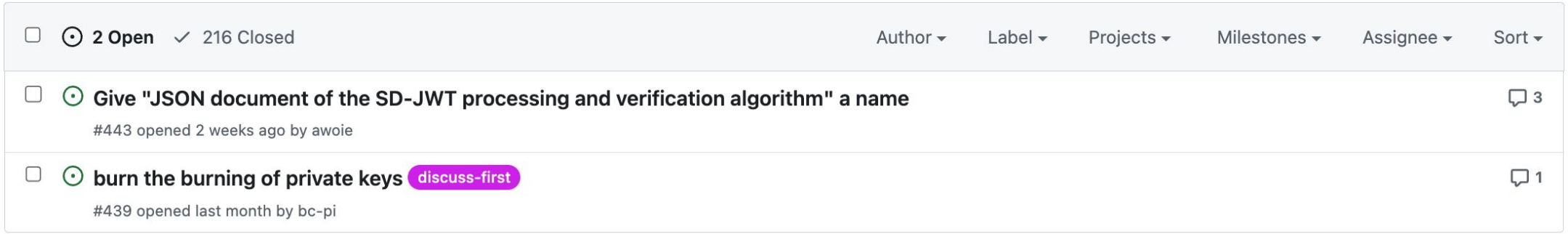
What's new in -09?

- Distinguished SD-JWT from SD-JWT+KB
- Provide ABNF for the SD-JWT, SD-JWT+KB, and various constituent parts
- New structure for JSON-serialized SD-JWTs/KB-JWTs to better align with JAdES
- Attempt to better explain how salt in the Disclosure makes guessing the preimage of the digest infeasible
- Consolidate salt entropy and length security consideration subsections
- Unnumbered most of the examples for improved clarity
- More definitive language around the exclusive use of the cnf claim for enabling Key Binding

What's new in -10?

- Add a section clarifying recursive disclosures and their interdependencies
- Editorial updates/fixes

Open Issues


2 Open
216 Closed
Author
Label
Projects
Milestones
Assignee
Sort
Give "JSON document of the SD-JWT processing and verification algorithm" a name
#443 opened 2 weeks ago by awoie
3
burn the burning of private keys
discuss-first
#439 opened last month by bc-pi
1

Next Steps

Getting to no SD-JWT presentation in IETF 122 Bangkok

© Brian Campbell