

Full Disclosure: Behind the Scenes of SD-JWT



Brian **Campbell**

Distinguished Engineer
Ping Identity
@ __b_c

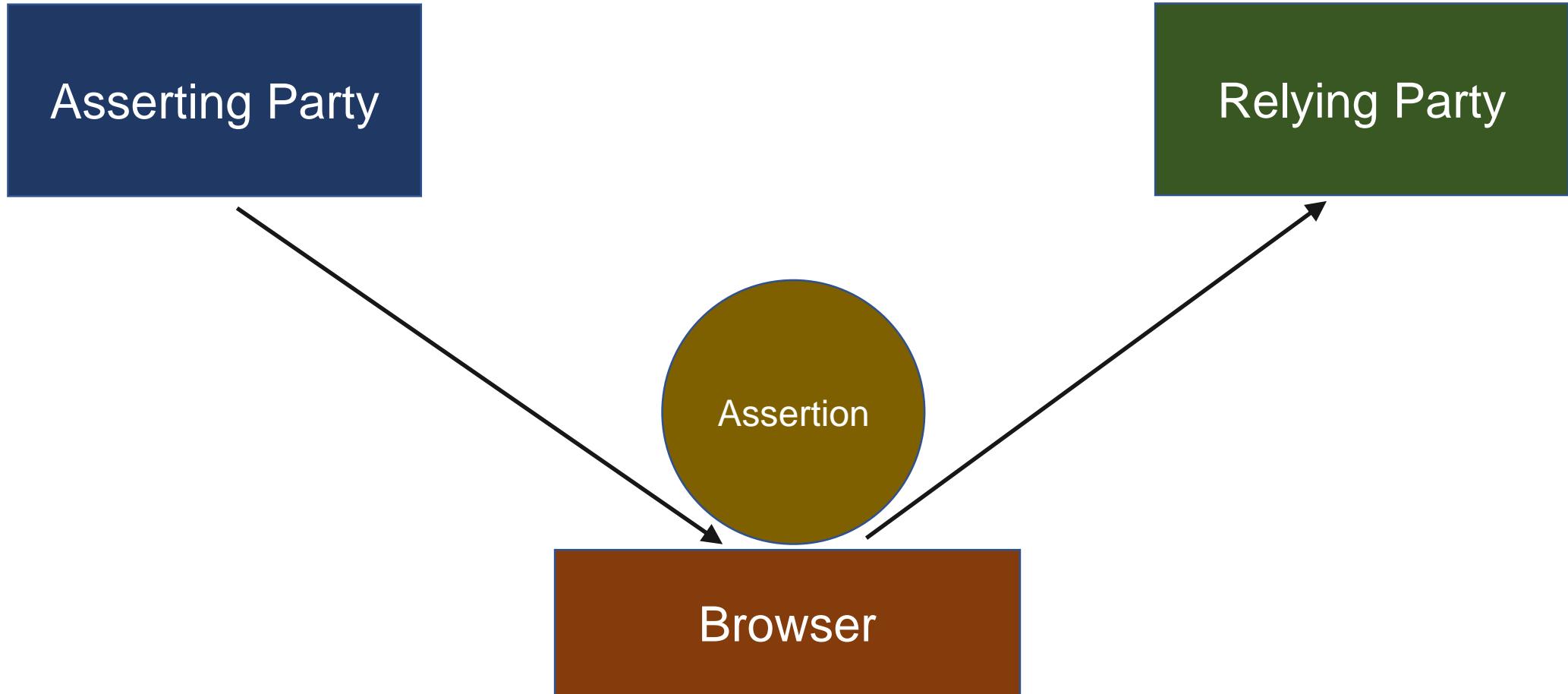
Reviewer, Review Thyself

(aka Rough Agenda)

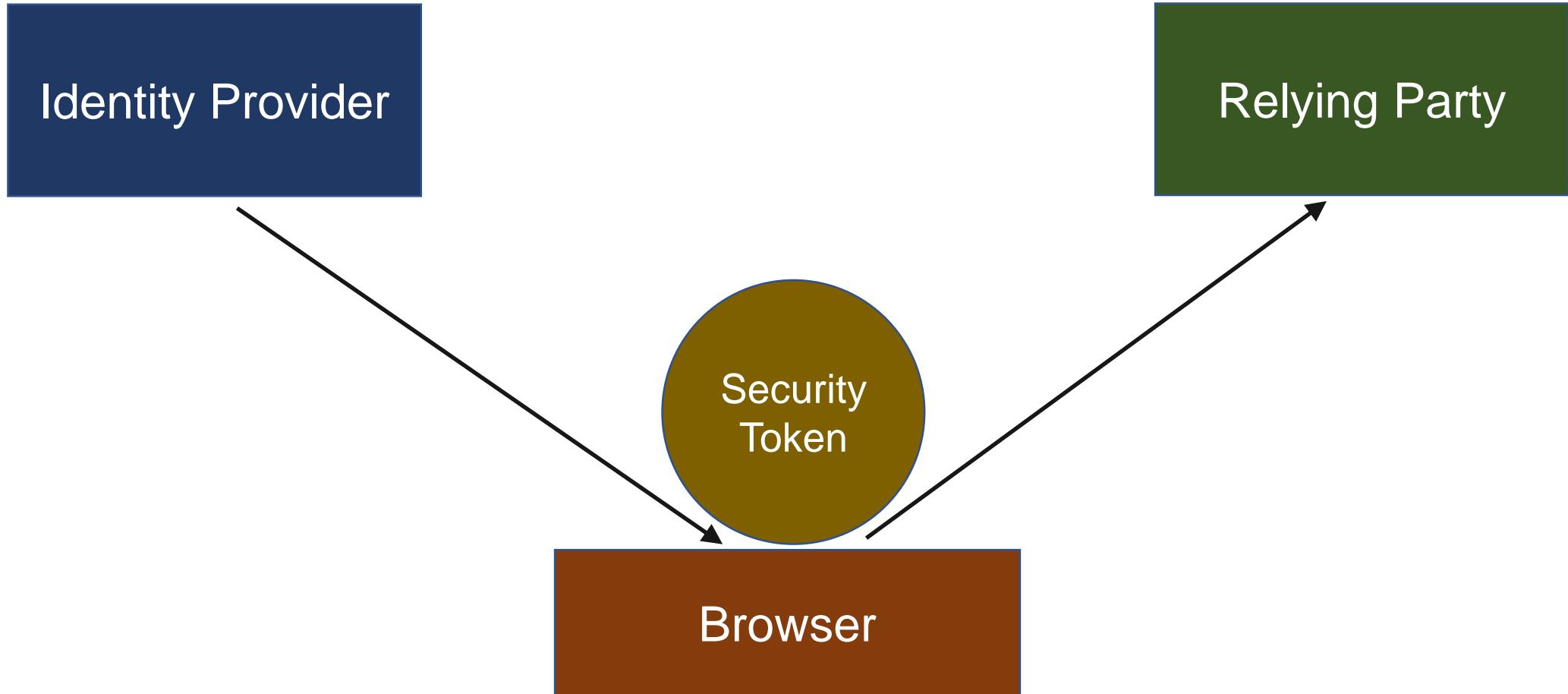
- Rough Agenda (meta)
- Brief history of tokens
- Briefer future of tokens
- Selective disclosure (SD) and JSON Web Token (JWT)
- My journey to SD-JWT (with photos, of course)
- Basic workings of SD-JWT
- Miscellaneous/closing considerations



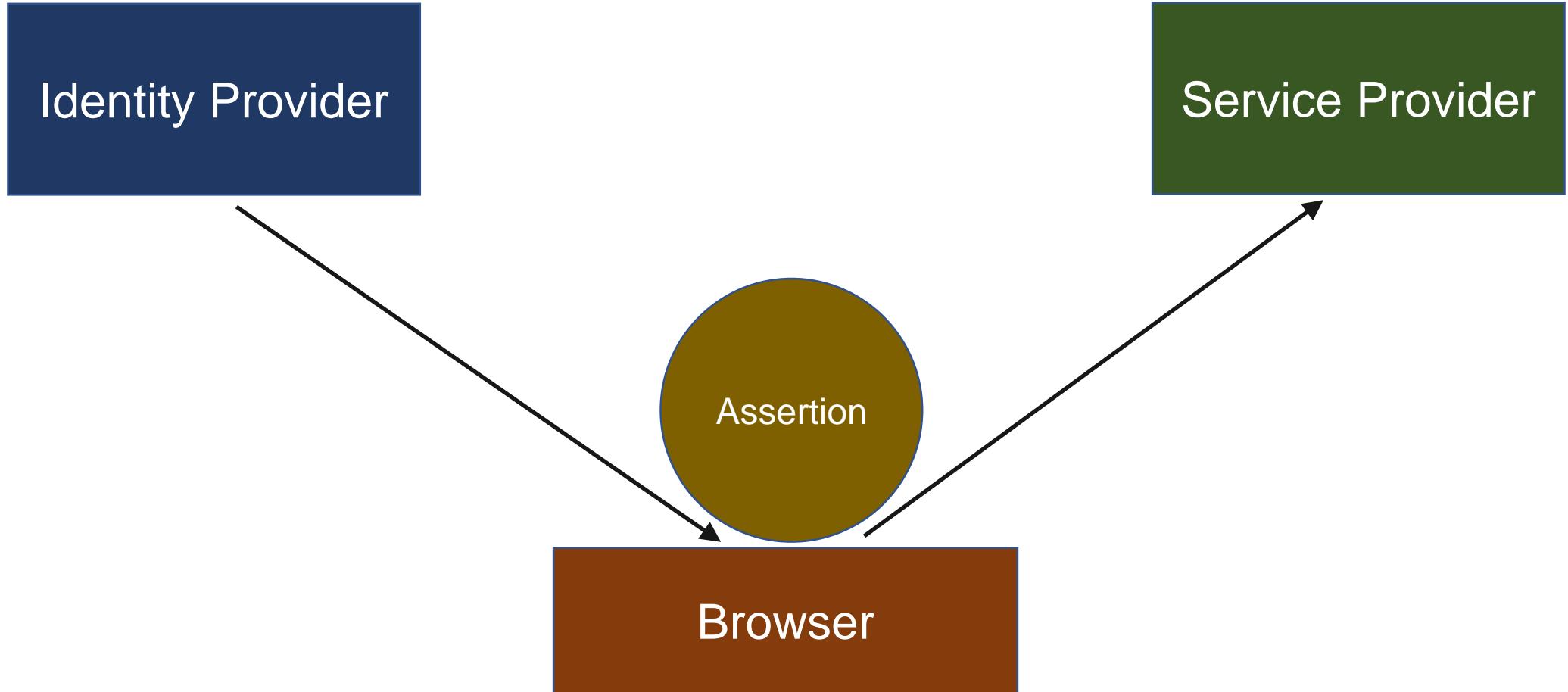
A Token History of Tokens: SAML 1.x SSO



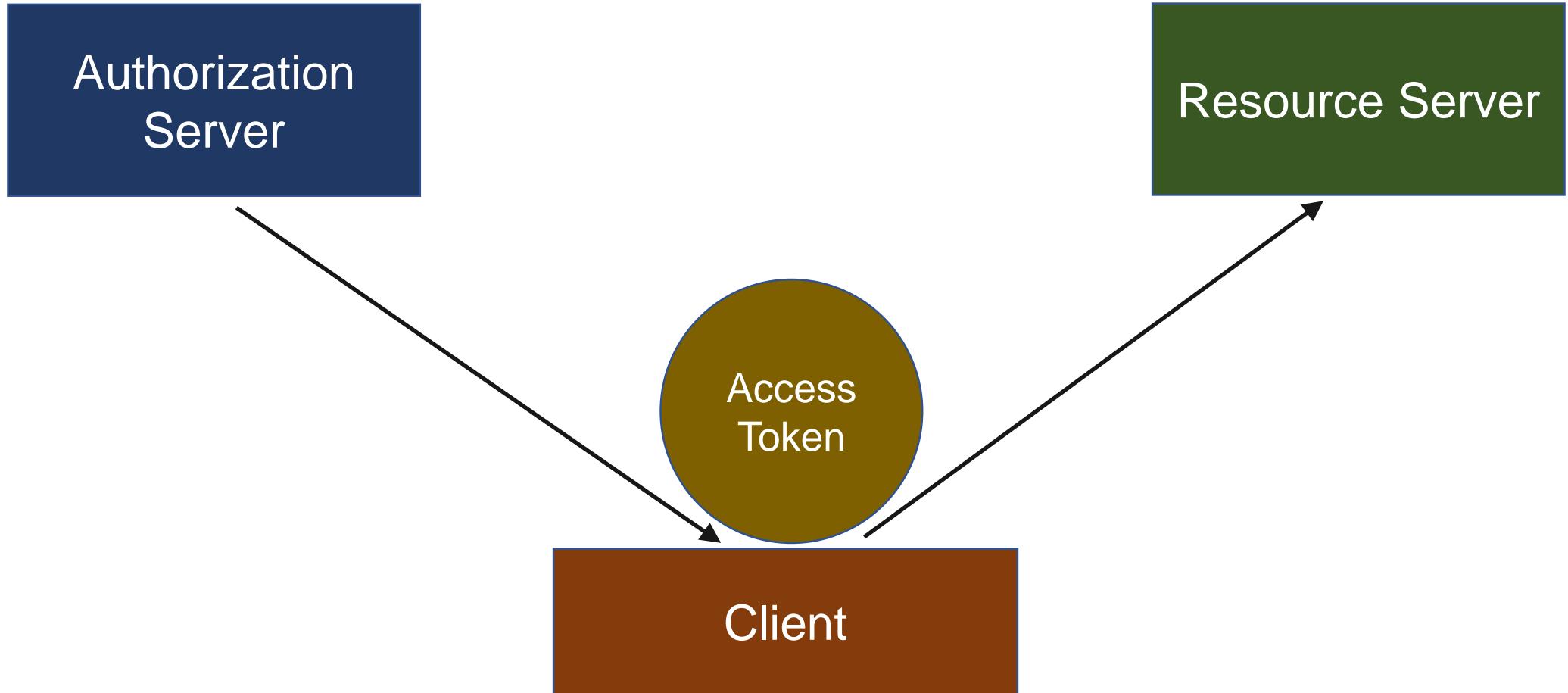
A Token History of Tokens: WS-Federation



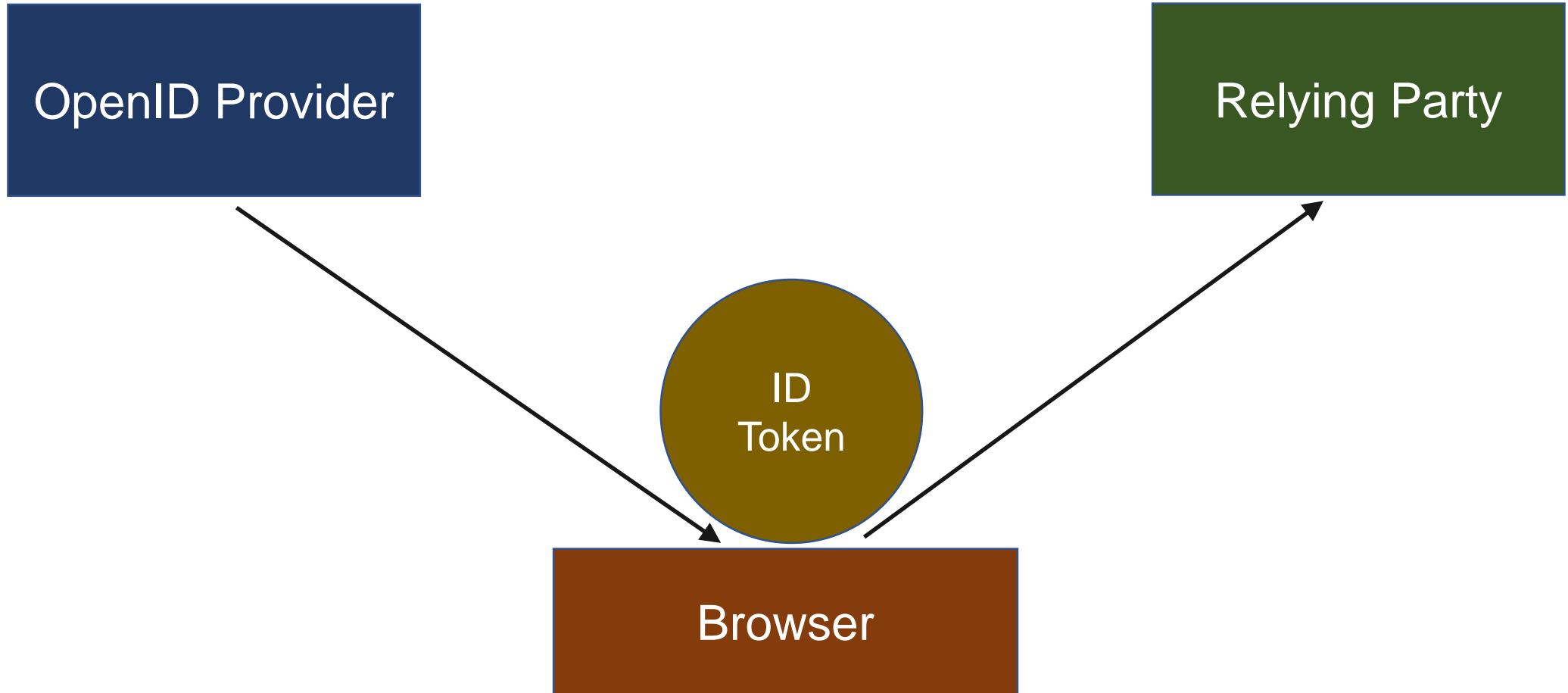
A Token History of Tokens: SAML 2.0 SSO



A Token History of Tokens: OAuth 2.0



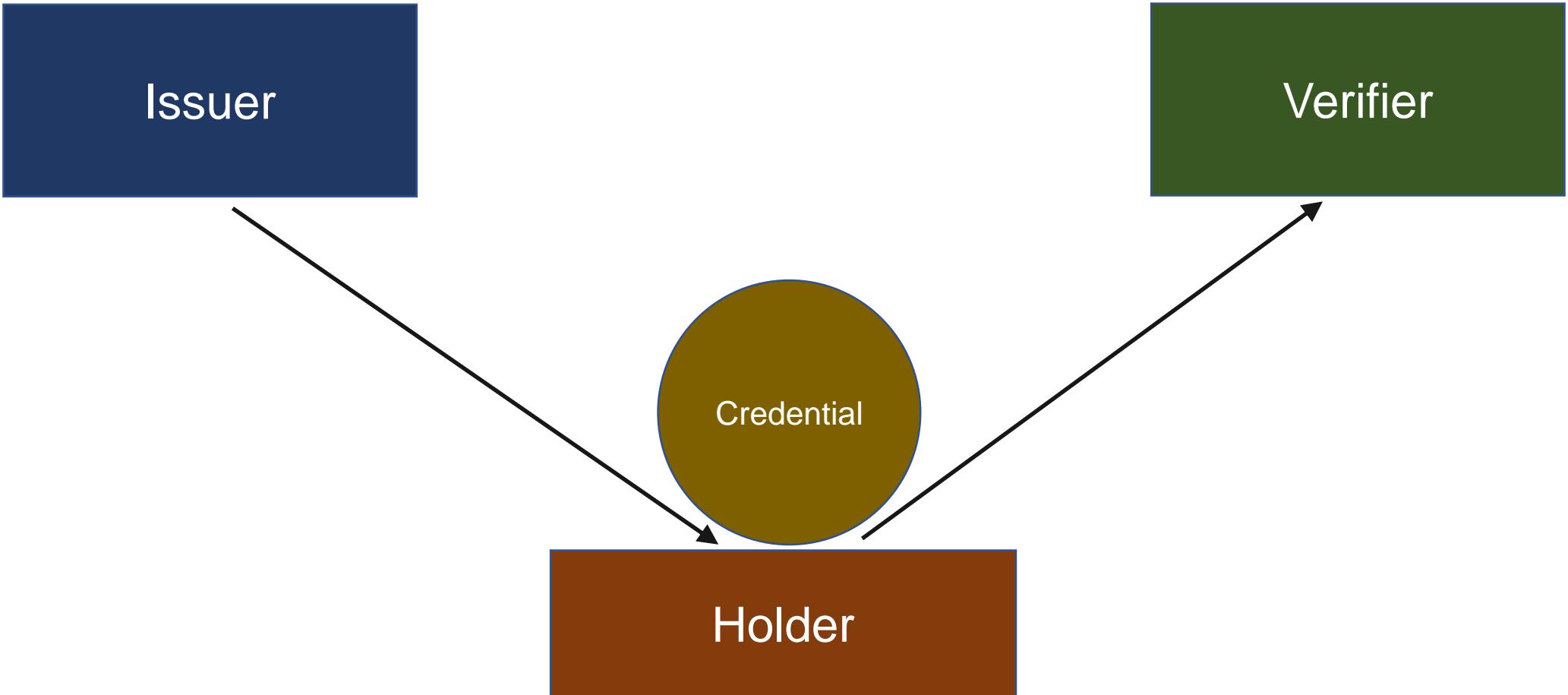
A Token History of Tokens: OpenID Connect



The Future of Tokens

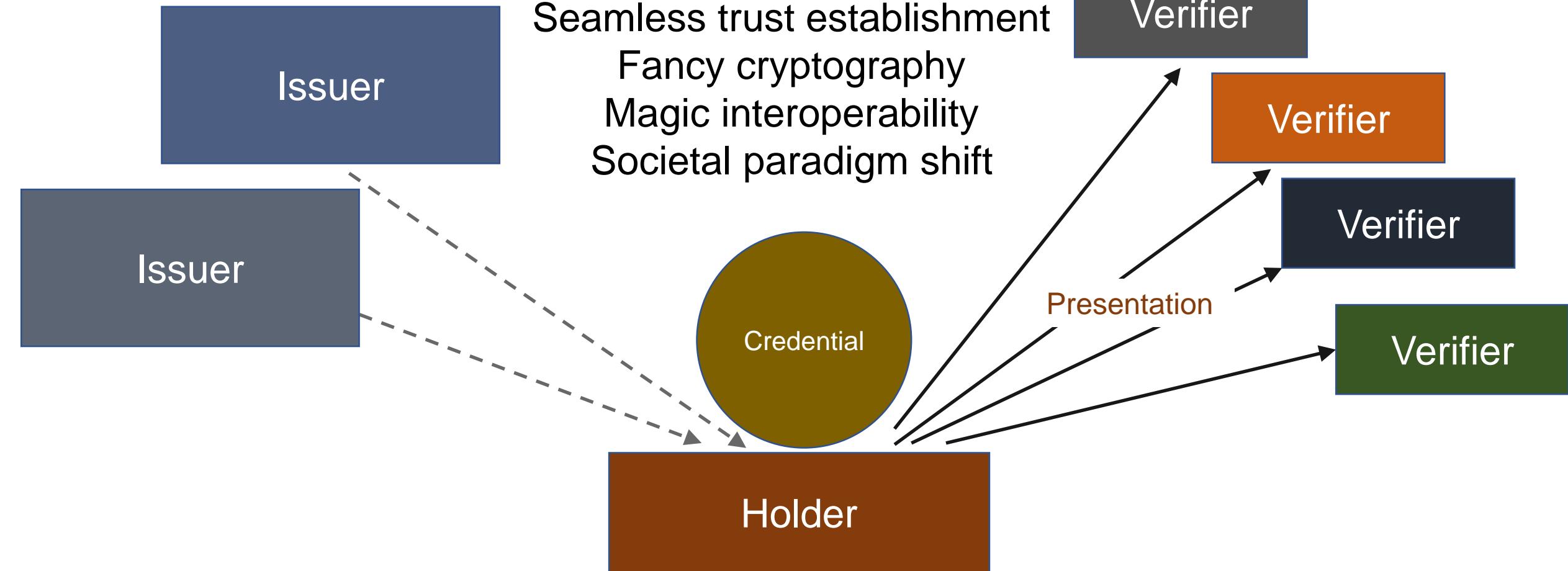
Wait for it...

The Future of Tokens!



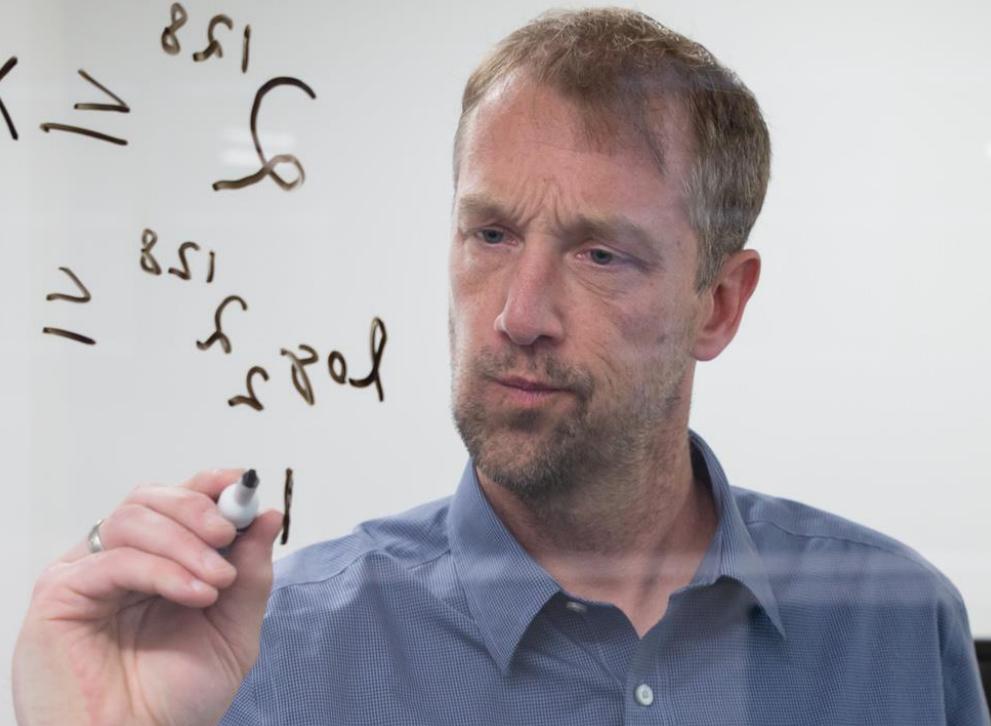
Well, Actually...

Improved privacy
User control
Reduced data retention
Seamless trust establishment
Fancy cryptography
Magic interoperability
Societal paradigm shift



Full Disclosure:

$$\begin{aligned} & \text{or } X_1 \geq 5 \\ & \text{or } X_{\text{rest}} \geq 5_{\text{rest}} \end{aligned}$$

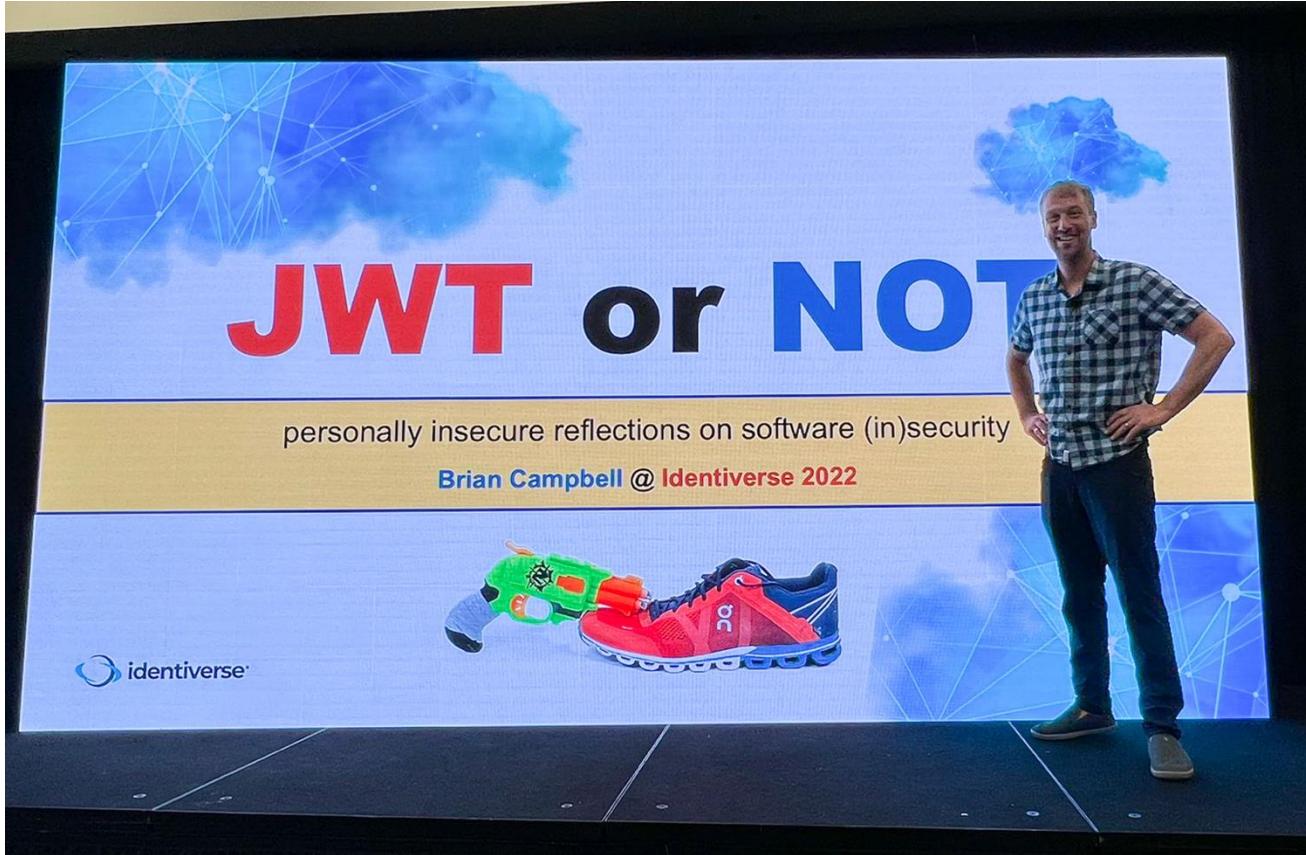


I'm just not that smart...

(tend to ignore or dismiss things I don't understand while clinging to things I do)

Which brings us to SD-JWT

(something in this future to cling to)



"Selective disclosure refers to the practice of releasing information to some individuals or organizations while withholding it from others."

- A Generative Artificial Intelligence

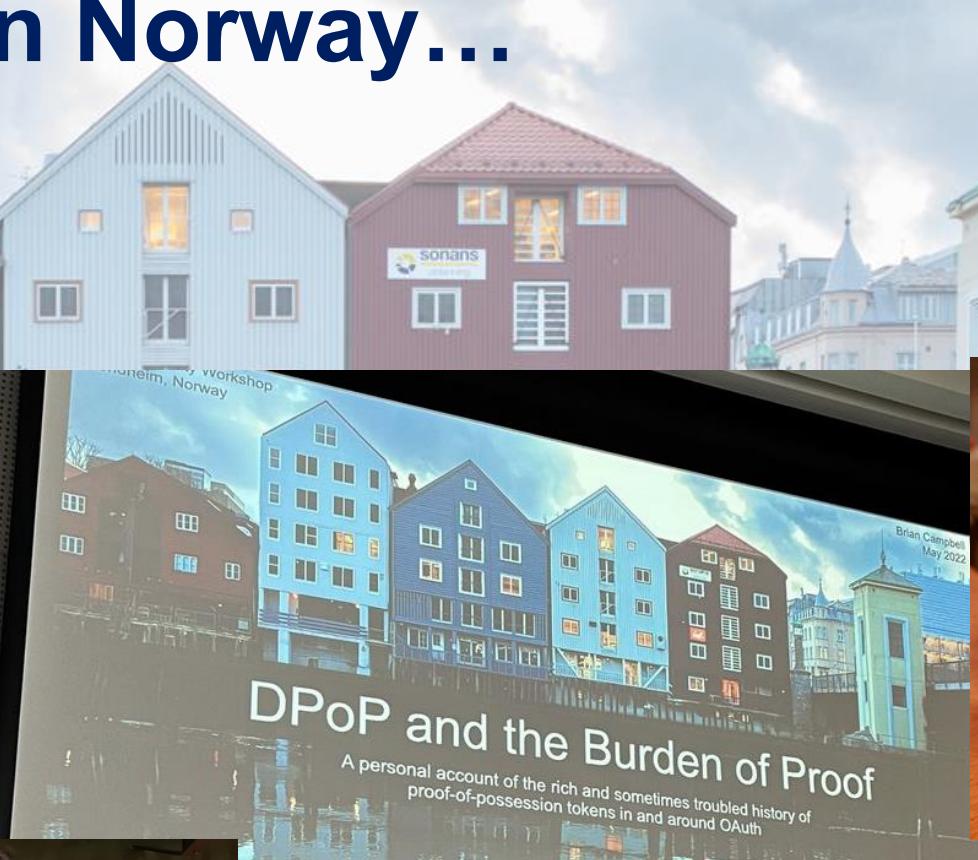
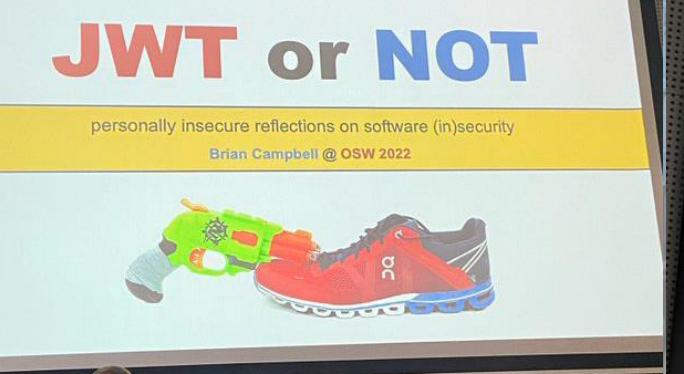
I do know something about JWT and can grasp selective disclosure
(even without the help of AI but it didn't hurt)

A photograph of a row of traditional Norwegian wooden buildings (rørosbygninger) built on stilts over a body of water. The buildings are painted in various colors, including red, blue, white, and grey. Some have signs for "sonans" and "frok". The water in the foreground is calm, reflecting the lights from the windows of the buildings. The sky is overcast with some clouds.

SD-JWT was Conceived at OSW '22

in Trondheim, Norway

I was in Norway...



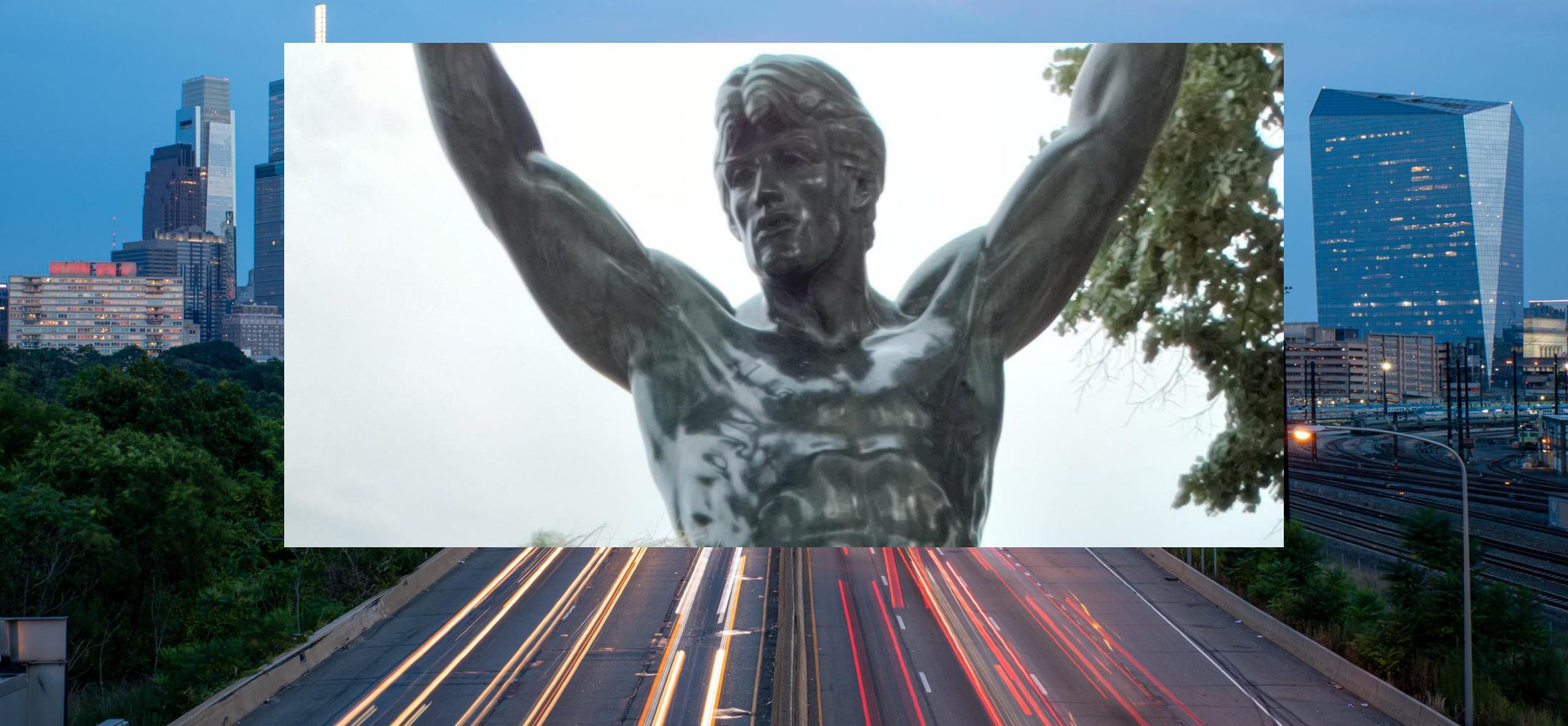
Slack, Email, and Some Midsummer Day's Zooms



SD-JWT Debuted at IETF 114 in Philadelphia



“Adopted” by the OAuth WG Shortly Thereafter



Hey look kids,
there's Big Ben!



Refined format and processing at IETF 115 in London

Selective Disclosure for JWTs (S X)

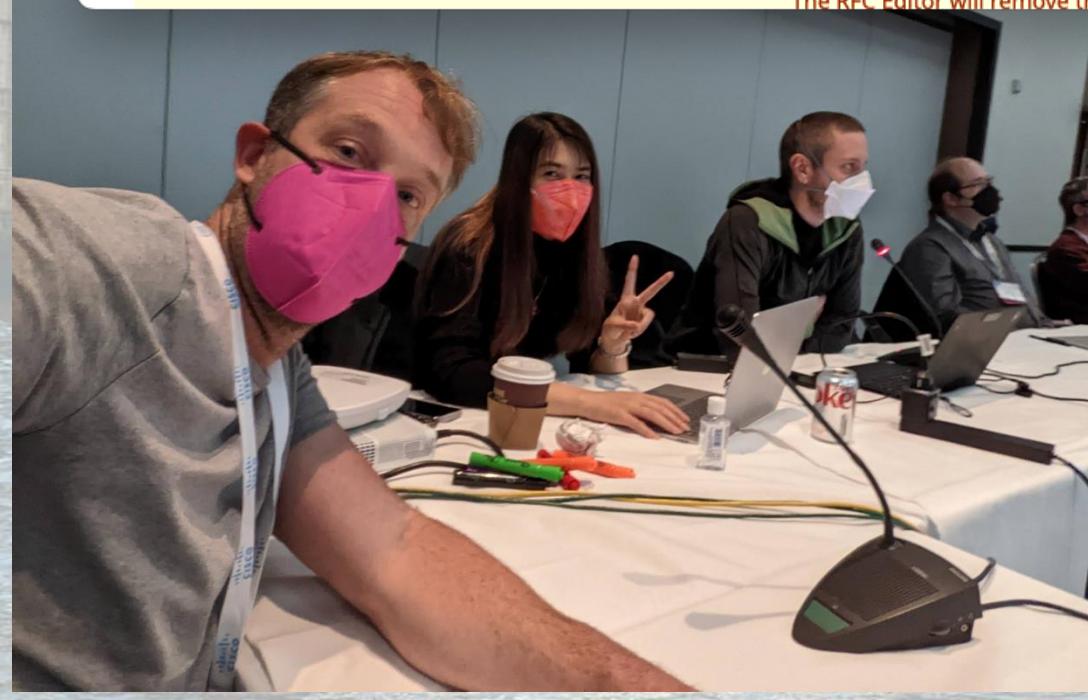
Workgroup: Web Authorization Protocol
Internet-Draft: draft-ietf-oauth-selective-disclosure-jwt-02
Published: 7 December 2022
Intended Status: Standards Track
Expires: 10 June 2023
Authors: D. Fett K. Yasuda B. Campbell
yes.com Microsoft Ping Identity

Selective Disclosure for JWTs (SD-JWT)

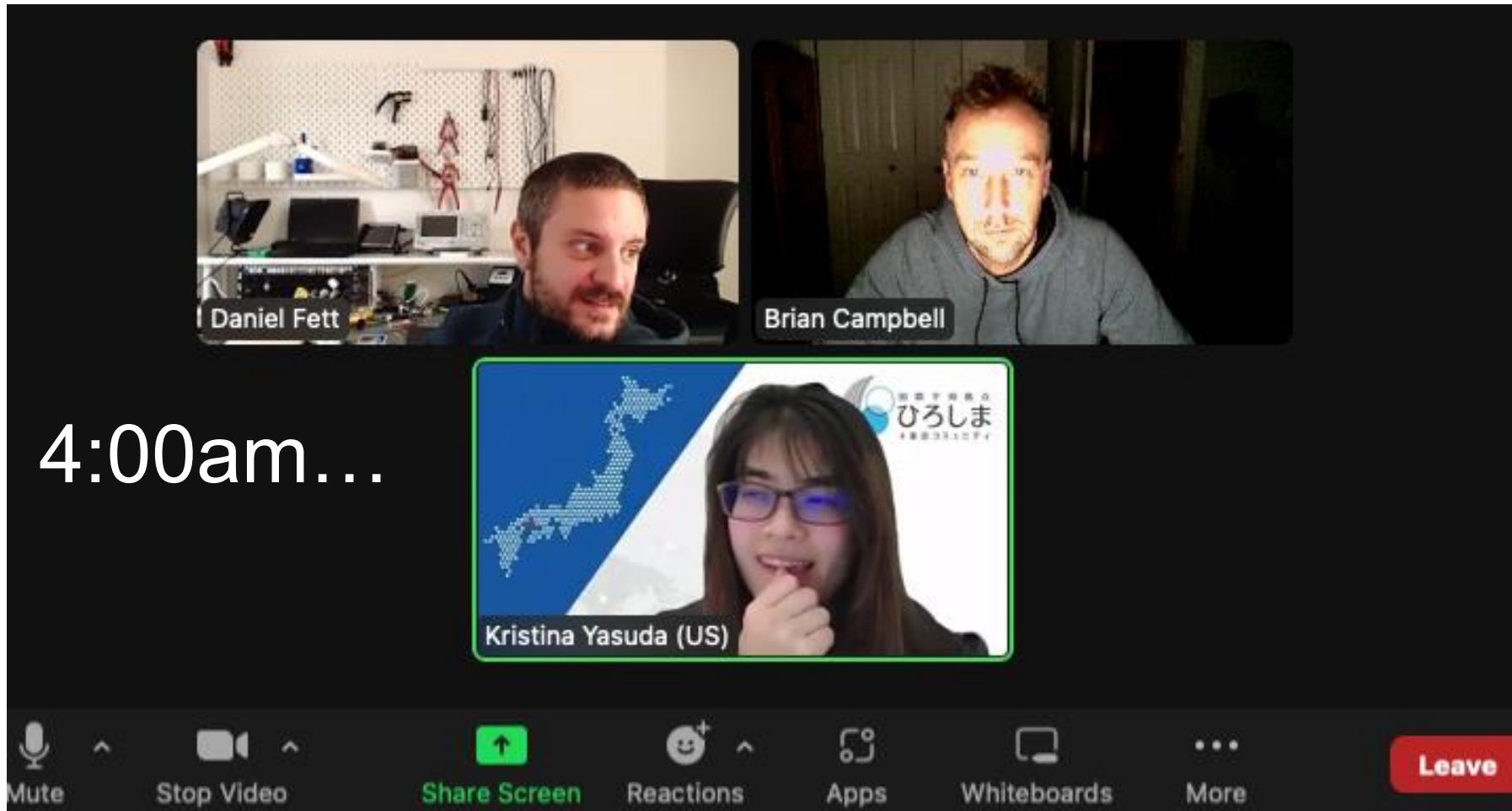
Abstract

This document specifies conventions for creating JSON Web Token (JWT) documents that support selective disclosure of JWT claims.

The RFC Editor will remove this note



Be careful what you wish for, lest it come true



Gratuitous Transition Slide...

(also from IETF 115 in London)



into the basic technical workings of SD-JWT

A JWT

eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5j0U9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNX1pb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WF1Iby0yLXpfcFFCe
C10d1RpY21RYzdJIiwgIjc3cE9HcWc3Mn11VTg1RGNqTVFGOTF2ZE84TnZTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUl1vNHdjRndQTU1BWjNFbFAydjctNnJLVFNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBz0i8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImhdCI6I
DE2Nzk0NTEwOTQsICJleHAiOiAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p17lZ0zH0cM1FJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hViy39Muzmjy_XkdA

An SD-JWT! (Issuance)

eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5j0U9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNX1pb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WF1Iby0yLXpfcFFCe
C10dlRpY21RYzdJIiwgIjc3cE9HcWc3Mn11VTg1RGNqTVFGOTF2ZE84TnZTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUl1vNHdjRndQTU1BWjNFbFAydjctNnJLVFNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBz0i8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImhdCI6I
DE2Nzk0NTEwOTQsICJleHAi0iAxNjc5NDUx0Tk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p171Z0zH0cM1FJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hViY39Muzmjy_XkdA~WyJHV1BXMFROZFFaejRicFROM3JXSzhBIiwgImdpdmVuX2
5hbWUiLCAiT2xpdmUiXQ~WyJMZmg0MGZNandpY2N6SzFuS3M0QldRIiwgImZhbWlseV9
uYW1lIiwgI111dyJd~WyJQQm1rSDh2Y2ZUVFp0M3RRMD1keWlnIiwgImVtYWlsIiwgIm
95QGV4YW1wbGUuY29tI10~WyJ3SDFNOW16bUtPejVac1VweUpBVjBRIiwgInBob25lX2
51bWJ1ciIsICIrMS0yODEtMzMwLTgwMDQiXQ~WyJ5U2NqR0JLa0otTGI5SnUzOHBNFZ
3IiwgImJpcnRoZGF0ZSIisICIxOTk2LTA1LTMxI10

```
{"alg": "ES256"},  
{
```

```
    "_sd": [  
        "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMNMuC9qo4Jc",  
        "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
        "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
        "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
        "mGnQhbmmTUIo4wcFwPMIAZ3ElP2v7-6rKTSmvEbb1B8"
```

```
],  
    "iss": "https://example.com/issuer",  
    "iat": 1679451094,  
    "exp": 1679451994,  
    "_sd_alg": "sha-256"
```

```
}
```

```
.U770FULq_s_BrHAAJr6Wt831834p17lZ0zH0cM1FJ_hYYGUFIbrvdMPgGvmtKWFQp  
UsV2hViy39Muzmjy_XkdA~WyJHV1BXMFR0ZFFaejRicFROM3JXSzhBIiwgImdpdmVuX2  
5hbWUiLCAiT2xpdmUiXQ~WyJMZmg0MGZNandpY2N6SzFuS3M0Q1dRIiwgImZhbWlseV9  
uYW1lIiwgI111dyJd~WyJQQm1rSDh2Y2ZUVFp0M3RRMD1keWlnIiwgImVtYWlsIiwgIm  
95QGV4YW1wbGUuY29tI10~WyJ3SDFNOW16bUtPejVac1VweUpBVjBRIiwgInBob251X2  
51bWJ1ciIsICIrMS0yODEtMzMwLTgwMDQiXQ~WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ  
3IiwgImJpcnRoZGF0ZSIIsICIxOTk2LTA1LTmxI10
```

Inside the SD-JWT

Inside the SD-JWT

```
{"alg": "ES256"}  
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3ElP2v7-6rKTSmvEbb1B8"  
  ],  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}  
.U770<--SIGNATURE-->XkdA  
~~~~~WyJHV1BXMFROZFFaejRicFROM3JXSzhBIiwgImdpdmVuX2  
5hbWUiLCAiT2xpdmUiXQ~WyJMZmg0MGZNandpY2N6SzFuS3M0Q1dRIiwgImZhbWlseV9  
uYW1lIiwgI111dyJd~WyJQQm1rSDh2Y2ZUVFp0M3RRMD1keWlnIiwgImVtYWlsIiwgIm  
95QGV4YW1wbGUuY29tI10~WyJ3SDFNOW16bUtPejVac1VweUpBVjBRIiwgInBob25lX2  
51bWJlciIsICIrMS0yODEtMzMwLTgwMDQiXQ~WyJ5U2NqR0JLa0otTGI5SnUz0HBZNFZ  
3IiwgImJpcnRoZGF0ZSIIsICIxOTk2LTA1LTMxI10
```

Hashes -> Disclosures

```
{"alg": "ES256"},  
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
  ],  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}  
• U770<--SIGNATURE-->XkdA
```

The diagram illustrates the relationship between the data in the JSON object and the resulting hashes. Five arrows point from the five strings in the '_sd' array to five distinct green-colored hash values. The green hash values are:
1. ~WyJ3SDFNOW16bUtPejVac1VweUpBVjBRIiwgInBob251X251bWJlciIsICIrM
2. S0yODEtMzMwLTgwMDQiXQ
3. ~WyJMZmg0MGZNandpY2N6SzFuS3M0QldRIiwgImZhbWlseV9uYW1lIiwgIlld
4. yJd
5. ~WyJQQm1rSDh2Y2ZUVFp0M3RRMD1keWlnIiwgImVtYWlsIiwgIm95QGV4YW1wb
GUuY29tI10
6. ~WyJHViBXMFROZFFaejRicFROM3JXSzhBIiwgImdpdmVuX25hbWUiLCAiT2xpdm
mUiXQ
7. ~WyJ5U2NqR0JLa0otTGI5SnUzOHBNFZ3IiwgImJpcnRoZGF0ZSIisICIxOTk2L
TA1LTmxI10

Inside the Disclosures

```
{"alg": "ES256"},  
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
  ],  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}  
U770<--SIGNATURE-->XkdA
```



Selecting a Disclosure

```
{"alg": "ES256"},  
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
  ],  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}  
• U770<--SIGNATURE-->XkdA  
  
~WyJ5U2NqR0JLa0otTGI5SnUzOHBNFZ3IiwgImJpcnRoZGF0ZSIIsICIxOTk2L  
TA1LTmxIl0  
[ "yScjGBKkJ-Lb9Ju38pY4Vw", "birthdate", "1996-05-31" ]
```

Selecting a Disclosure

eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5jOU9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNXlpb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WF1Iby0yLXpfcFFCe
C10d1RpY21RYzdJIiwgIjc3cE9HcWc3Mnl1VTg1RGNqTVFGOTF2ZE84TnZTFUtczJPd
Gk0UTE4eFkilCAibUduUWhibW1UVUl vNHdjRndQTUlBWjNFbFAydjctNnJLVF NtdkViY
mxCOCJdLCAiaXNzI jogImh0dHBz0i8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImlhCI6I
DE2Nzk0NTEwOTQsICJleHAi0iAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGETMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p171Z0zH0cM1FJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hViy39Muzmjy_XkdA

~WyJ5U2NqR0JLa0otTGI5SnUz0HBZNFZ3IiwgImJpcnRoZGF
0ZSI sICIxOTk2LTA1LT MxI10

The SD-JWT Presentation

eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5jOU9VeVpuTU5NdUM5cW80SmMiLCAiNEFacEJvRTRvS1YyUnliamFwc2RzaG0xNXlpb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WF1Iby0yLXpfcFFCe
C10d1RpY21RYzdJIiwgIjc3cE9HcWc3Mn1VTg1RGNqTVFGOTF2ZE84TnZTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUl vNHdjRndQTU1BWjNFbFAydjctNnJLVNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBz0i8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImhdCI6I
DE2Nzk0NTEwOTQsICJleHAiOiAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p171Z0zH0cM1FJ_hYYGUFIbrvdMPgGvmtKWFQp
UsV2hVi y39Mu zmjy_XkdA~WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZG
F0ZSI sICIxOTk2LTA1LT MxIl0~

Consuming the SD-JWT Presentation

eyJhbGciOiAiRVMyNTYifQ.eyJfc2QiOiBbIjJZTHFJRDhXXzVfc0FJM3E3c3FTS3o3c
G5jOU9VeVpuTU5NdUM5cW80SmMilCAiNEFacEJvRTRvS1YyUn1iamFwc2RzaG0xNX1pb
XdaZ2FfcHZWeXdKbVEtayIsICI2dHRZNHFFbDFYMm9iemR0UF81WF1Iby0yLXpfcFFCe
C10d1RpY21RYzdJIiwgIjc3cE9HcWc3Mn11VTg1RGNqTVFGOTF2ZE84TnZTFUtczJPd
Gk0UTE4eFkiLCAibUduUWhibW1UVUl1vNHdjRndQTU1BWjNFbFAydjctNnJLFNtdkViY
mxCOCJdLCAiaXNzIjogImh0dHBz0i8vZXhhbXBsZS5jb20vaXNzdWVyIiwgImlhdCI6I
DE2Nzk0NTEwOTQsICJleHAiOiAxNjc5NDUxOTk0LCAiX3NkX2FsZyI6ICJzaGEtMjU2I
n0.U770FULq_s_BrHAAJr6Wt831834p171Z0zH0cM1FJ_hYYGUFibrvdMPgGvmtKWFQp
UsV2hViy39Muzmjy_XkdA

~WyJ5U2NqR0JLa0otTGI5SnUz0HBZNFZ3IiwgImJpcnRoZGF0ZSIIsICIxOTk2LTA1LTmxIl0

Consuming the SD-JWT Presentation

```
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMNMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qE11X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
,  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}
```

WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZGF0ZSI_{sICI}xOTk2LTA1LTMxIl0

Consuming the SD-JWT Presentation

```
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMNMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
,  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}
```



```
WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZGF0ZSI↑sICIxOTk2LTA1LT↓MxI10  
[ "yScjGBKkJ-Lb9Ju38pY4Vw", "birthdate", "1996-05-31" ]
```

Consuming the SD-JWT Presentation

```
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMNMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
,  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}
```

WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZGF0ZSI[↑]ICIxOTk2LTA1LTmxIl0
["yScjGBKkJ-Lb9Ju38pY4Vw", "birthdate", "1996-05-31"]



Consuming the SD-JWT Presentation

```
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMNMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qE11X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3ElP2v7-6rKTSmvEbb1B8"  
,  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}
```

WyJ5U2NqR0JLa0otTGI5SnUzOHBZNFZ3IiwgImJpcnRoZGF0ZSI[↑]sICIxOTk2LTA1LTmxIl0
["yScjGBKkJ-Lb9Ju38pY4Vw", "birthdate", "1996-05-31"]



Consuming the SD-JWT Presentation

```
{  
  "_sd": [  
    "2YLqID8W_5_sAI3q7sqSKz7pnc90UyZnMNMuC9qo4Jc",  
    "4AZpBoE4oKV2Rybjapsdshm15yimwZga_pvVywJmQ-k",  
    "6ttY4qEl1X2obzdtP_5XYHo-2-z_pQBx-tvTicmQc7I",  
    "77p0Gqg72yuU85DcjMQF91vd08NvELU-s20ti4Q18xY",  
    "mGnQhbmmTUIo4wcFwPMIAZ3E1P2v7-6rKTSmvEbb1B8"  
,  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
  "_sd_alg": "sha-256"  
}
```



"birthdate", "1996-05-31"

Virtual Reconstructed Claims of the Presented SD-JWT

```
{  
  "birthdate": "1996-05-31",  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
}
```

"birthdate", "1996-05-31"



Virtual Reconstructed Claims of the Presented SD-JWT

```
{  
  "birthdate": "1996-05-31",  
  "iss": "https://example.com/issuer",  
  "iat": 1679451094,  
  "exp": 1679451994,  
}
```

A Disclosable Claim Values Can be Any JSON Type



Disclosable Content also (Recursively) Nestable

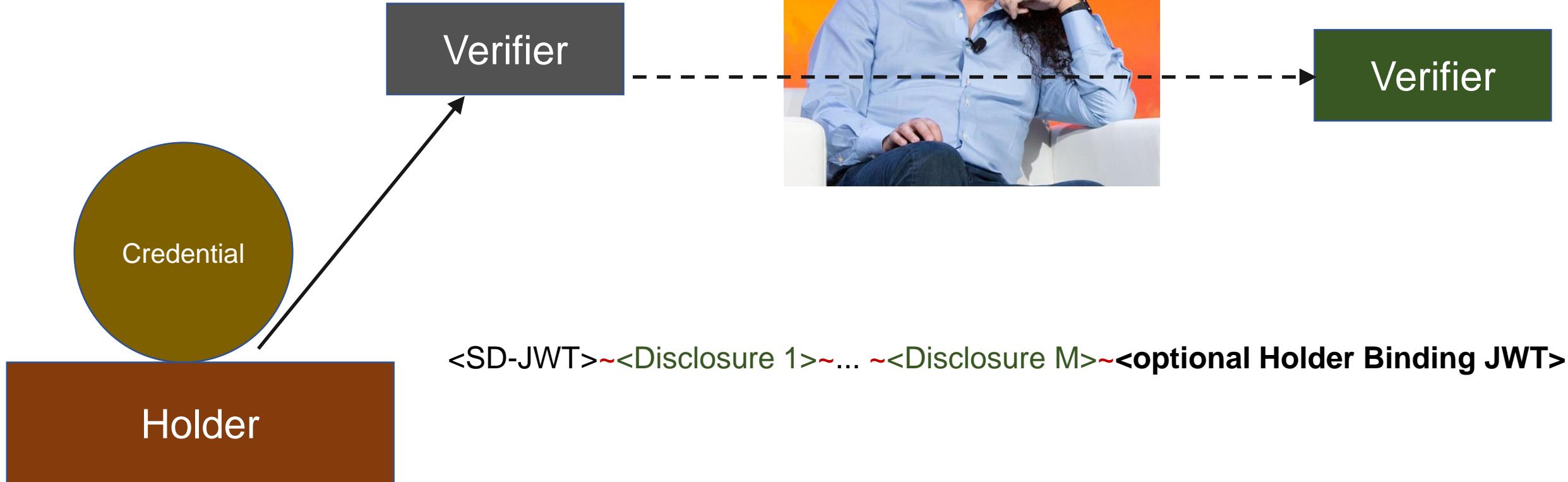
```
{  
  "iss": "https://example.com/issuer",  
  "iat": 1516239022,  
  "exp": 1735689661,  
  "sub": "6c5c0a49-b589-431d-bae7-219122a9ec2c",  
  "address": {  
    "_sd": [  
      "G_FeM1D-U3tDJcHB7pwTNEElLa19FE9PUs0k1HgeM1c",  
      "K1G6HEM6XWbymEJDfyDY4k1JkQ99iTuNG0LQXnE9mQ0",  
      "X96Emv4S9uzFUGkU8Mm01FzUwEtDNeT-ToXw3Fx9AfI",  
      "ffPGyxFBnNA1r60g2f796Hqq3dBGtaOogpnIBgRGdyY"  
    ]  
  },  
  "_sd_alg": "sha-256"  
}
```

```
{  
  "iss": "https://example.com/issuer",  
  "iat": 1516239022,  
  "exp": 1735689661,  
  "sub": "6c5c0a49-b589-431d-bae7-219122a9ec2c",  
  "_sd": [  
    "Lot9gM9V00iyFS4FOR1ykwz-V-fB_xwF63jWemIH4d0"  
  ],  
  "_sd_alg": "sha-256"  
}  
  
~WyJGcDBqLTd6Q2FOVFdmX3dLNjdzeGlnIiwgImFkZHJlc3MiLCB7Il9zZCI6I  
FsiMXpnc3U5RmU2YmtiUVk5ekpzZ1BUbzF1Q1BNVm00G00RFmeEpUWVN1MCI  
SICJES3ROX3FXX2hheVlDR0NLaWhTMz1NM3NvYnMxUlR1a3hhS25NYkUxNy1RI  
iwgImgYRHh4RTgwQzdxUld4Q1Fqd1I5NmRhNDZqcjJCOGJMU1J3QWRiW1NSbG8  
iLCAidWRGV0Z4XzkxTmdDamhMVEhKQXZ2QUh3T1QydmxIQnNXeFBJT3hLM11kb  
yJdfV0  
  
[  
  "Fp0j-7zCaNTWf_wK67sxig",  
  "address",  
  {  
    "_sd": [  
      "1zgsu9Fe6bkbQY9zJsPTo1uBPMV148m4EafxJTYSu0",  
      "DKtN_qW_hayYCGCKihS39M3sobs1RTekxaKnMbE17-Q",  
      "h2DxxE80C7qRWxCQjwR96da46jr2B8bLSRwAdbZSRlo",  
      "udFWFx_91NgCjhLTHJAvvAHwNT2vlHBsWxPIOxK2Ydo"  
    ]  
  }  
]
```



Another Gratuitous Transition Slide...
(from IETF 114 in Philly)
out of the basic technical workings of SD-JWT

Know Your Audience



Others Receiving Votes (limitations/considerations/etc.)

- Inherent explicit linkability by colluding verifiers
- Opportunities for implicit linkability and leakage abound (not unique to SD-JWT)
- Revocation (with privacy) out of scope
- SD-JWT is just a draft
- In a crowded “market”



Gratuitous Closing Slide...

(from Trondheim, Norway)

A wide-angle night photograph of the Nidelva river in Trondheim, Norway. The scene is framed by traditional Norwegian wooden buildings with red roofs on both banks. The water in the center reflects the warm lights from the buildings and a bridge in the background. The sky is a deep blue.

Thanks!
[time permitting] Questions?