

Token Status List

A simple and scalable credential revocation/status mechanism
[Formerly known as JWT CWT Status List]

Tobias Looker, Paul Bastian, Christian Bormann

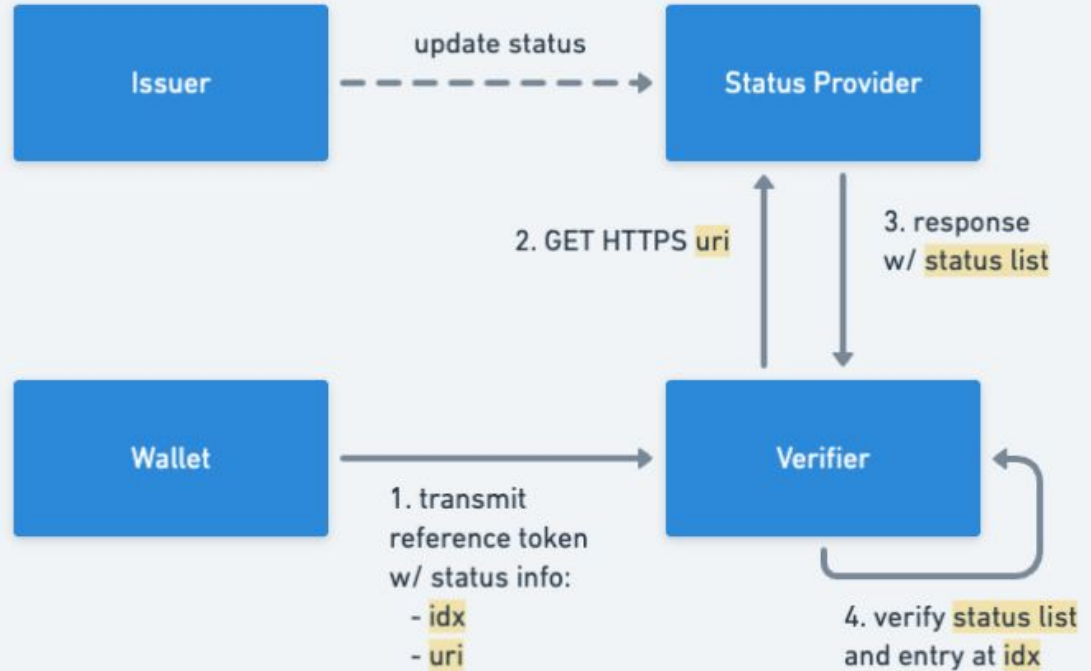


A Refresher - The Problem

How to enable the issuer of a token (e.g CWT or JWT) to communicate dynamic status information about a token after it is issued and before it expires.

Example - An SD-JWT Verifiable Credential where the Issuer would like to communicate whether the credential is revoked or not.

Big picture





Changes: -01

- Rename title of the draft
add design consideration to the introduction
- **Change status claim to in referenced token to allow re-use for other mechanisms**
- Add IANA Registry for status mechanisms
- Restructure the sections of this document
- **Add option to return an unsigned Status List**
- Changing compression from gzip to zlib
- Change typo in Status List Token sub claim description
- Add access token as an example use-case



Changes: -02

- add ttl claim to Status List Token to convey caching
- relax requirements on referenced token
- clarify Deflate / zlib compression
- make a reference to the Issuer-Holder-Verifier model of SD-JWT VC
- add COSE/CWT/CBOR encoding



01 - Change status claim to “cnf” style registry

- We expect different status mechanisms to be used based on use-cases and requirement
- Instead of “status” defining the status list reference, we introduced a mechanism similar to the confirmation claim
- Ability to re-use the general mechanism and add other status mechanisms

```
{
  "iss": "https://example.com",
  "status": {
    "idx": 0,
    "uri": "https://example.com/statuslists/1"
  }
}
```



```
{
  "iss": "https://example.com",
  "status": {
    "status_list": {
      "idx": 0,
      "uri": "https://example.com/statuslists/1"
    }
  }
}
```



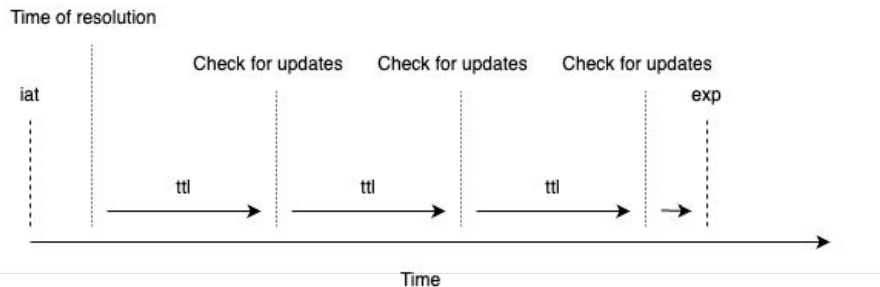
01 - Option to return unsigned status list

- Support for a simpler option that places trust in TLS, rather than application level signatures.
- Akin in some ways to the unsigned authorisation metadata option in OAuth2.
- Enable status list repudiation.

02 - Add ttl claim to convey caching

In order to convey the intended update interval of a status list, we have defined a new JWT and CWT claim for expressing the *time to live* for a token. When applied to the status list this enables a way for a consumer of a status list to know when to check for updates. The main alternative considered was an absolute timestamp for update checking which was dismissed because:

1. It synchronizes refresh/update requests from consumers.
2. It enables communicating a reoccurring update/refresh interval instead of a single point-of-time without having to resign the status list when there are no updates.



02 - Add COSE/CWT/CBOR encoding

- We have added text and examples for:

- [Status List in CBOR Format](#)
- [Status List Token in CWT Format](#)
- [Referenced Token in CWT Format](#)
- [Referenced Token in other COSE/CBOR Format](#)

```
a2 # map(2)
64 # string(4)
62697473 # "bits"
01 # uint(1)
63 # string(3)
6c7374 # "lst"
4a # bytes(10)
78dadbb918000217015d #
"xÚÛ¹\x18\x00\x02\x17\x01]"
```

```
d2 # tag(18)
84 # array(4)
53 # bytes(19)
a20126106e7374617475736c # "\x01&\x10nstatusl"
6973742b637774 # "ist+cwt"
a1 # map(1)
04 # uint(4)
42 # bytes(2)
3132 # "12"
58 60 # bytes(96)
a502782168747470733a2f2f # "\x02x!https://"
6578616d706c652e636f6d2f # "example.com/"
7374617475736c697374732f # "statuslists/"
31017368747470733a2f2f65 # "1\x01shttps://e"
78616d706c652e636f6d061a # "xample.com\x06\x1a"
648c3fca041a8898c3ca19ff # "d\x8c?"
Ê\x04\x1a\x88\x98ÃÊ\x19ÿ"
fe56a2646269747301636c73 # "bVçdbits\x01cls"
744a78dadbb918000217015d # "tJxÚÛ¹\x18\x00\x02\x17\x01]"
58 40 # bytes(64)
3fd60a6d10eb4b4131f1f6c1 # "?ð\x0am\x10ëKA1ñóÁ"
2fb365ae27b969e8e8df0b4f # "/³e@' :ièèß\x0bO"
4029815b679cb1051c1c9eb3 #
"@)\x81[g\x9c±\x05\x1c\x1c\x9e³"
6aa72f6f17bcfdb5ed443bdf # "j$/o\x17¼ÿµiD;ß"
c2339568ab42949169b413e7 # "Ã3\x95h«B\x94\x91i´\x13ç"
```



02 - Add COSE/CWT/CBOR encoding

- We have added text and examples for:

- [Status List in CBOR Format](#)
- [Status List Token in CWT Format](#)
- [Referenced Token in CWT Format](#) →
- [Referenced Token in other COSE/CBOR Format](#)

```
18(
  [
    / protected / << {
      / alg / 1: -7 / ES256 /
    } >>,
    / unprotected / {
      / kid / 4: h'3132' / '13' /
    },
    / payload / << {
      / iss / 1: "https://example.com",
      / status / 65535: {
        "status_list": {
          "idx": "0",
          "uri": "https://example.com/statuslists/1"
        }
      }
    }
  ] >>,
  / signature / h'...'
)
```



Discussion: Provide all StatusLists

- Provide a URL/List/Directory with URLs to all StatusList
 - This enables Verifiers to fetch all relevant StatusLists, e.g. in the morning for potential offline verification throughout the day
- Github issue: <https://github.com/oauth-wg/draft-ietf-oauth-status-list/issues/27>
- Options
 - Define status list path structure like `<some-host>/<some-path>/<status-list>/<id>` where the parent path contains a list of `<ids>`
 - `.well-known/` path
 - additional URL inside the `status_list` claim
 - URL provided by the Issuer metadata
- Data Structure to be defined



Discussion: Identifier List?

- As we introduce a registry for status mechanisms in JSON/CBOR, two candidates exist:
 - Status-List (this spec)
 - Status-Attestation (Giuseppe's proposal - OCSP-stapling like)
- We also see increased demand for a simple CRL-like mechanism
 - ISO mdoc folks are interested in this (--> **time sensitive**)
 - Putting this into the StatusList specification may overload and confuse people
 - Is there consensus for adding another, separate IETF specification for this?
- Call for Feedback:
 - Option 1 : separate Draft
 - Option 2 : add to Status List



Discussion: status IANA Registration?

- We are currently planning to create a registry for status mechanisms similar to how the confirmation claim (“cnf”) works
- This should apply for both the JOSE and COSE world (and the mechanisms could be used by mdoc)
- Do we create a registry each in the JWT and CWT IANA documents?



Further Open Topics

- Validation Rules to be more detailed
- Security considerations to be more detailed
- Add more and fix some examples
- Status Object as header?
- Drop authorization considerations for Status List?
- Comparison of status mechanisms -> informational RFC Draft?

Questions?





Example: Referenced Token

```
{
  "alg": "ES256",
  "kid": "11"
}
.
{
  "iss": "https://example.com",
  ... //other claims
  "status": {
    "status_list": {
      "uri": "https://example.com/statuslists/1",
      "idx": 5
    }
  }
}
```

Extension point for other status mechanisms

URI of the status list token

Index in the status list

Example: Status List in JWT

```
eyJhbGciOiJIUzI1NiIsImtpZCI6IjEyIiwidHlwIjoiYm9ja3RhdHVzIGlzdCtqd3QifQ.eyJleHAiOjE2MDc1MTc3NzAsImldCI6MTY0NjkxMjk3MCwiaXNzIjoiaHR0cHM6Ly9leGFtcGxlLmNvbSIsIn0YXR1c19saXN0Ijp7ImJpdHMiOjIsImxzdCI6Ikg0c0lBTW9faKdRQ196dnA4aE1BWkxSTE1RTUFBQUEifSwic3ViIjoiaHR0cHM6Ly9leGFtcGxlLmNvbS9zdGF0dXNsaXN0cy8xIn0.8uaUXshaJdG WGjvwPwaa2Gtt0M7-M7dG09rXaz3x99LCdG5tKb-ARL1ezquLT s63VeudYWqpdg4HpN-D2h0kg
```

```
{
  "alg": "ES256",
  "kid": "12",
  "typ": "statuslist+jwt"
}
.
{
  "exp": 1687517770,
  "iat": 1686912970,
  "iss": "https://example.com",
  ... //other claims
  "status_list": {
    "bits": 1,
    "lst": "H4sIAMo_jGQC_zvp8hMAZLRMLMQMAAAA"
  },
  "sub": "https://example.com/statuslists/1"
}
```

Example: How it fits together

```
"status_list": {  
  "status_list": {  
    "idx": 5  
    "uri": "https://example.com/statuslists/1",  
  }  
}
```

```
"sub": "https://example.com/statuslists/1"  
"status_list": {  
  "bits": 1,  
  "lst": "H4sIAMo_jGQC_zvp8hMAZLRMQMAAAA"  
}
```

0x0 = VALID
0x1 = INVALID

1	0	0	1	0	1	0	0	0	1	0	0
---	---	---	---	---	---	---	---	---	---	---	---

Deflate zlib





Links

Datatracker -> <https://datatracker.ietf.org/doc/draft-ietf-oauth-status-list/>

Git Repository -> <https://github.com/oauth-wg/draft-ietf-oauth-status-list>

Current Editors Copy -> <https://oauth-wg.github.io/oauth-sd-jwt-vc/#go.draft-ietf-oauth-sd-jwt-vc.html>