Token Status List

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

- Refresher
- Discussion
- 2. WGLC

Tobias Looker, Paul Bastian, Christian Bormann

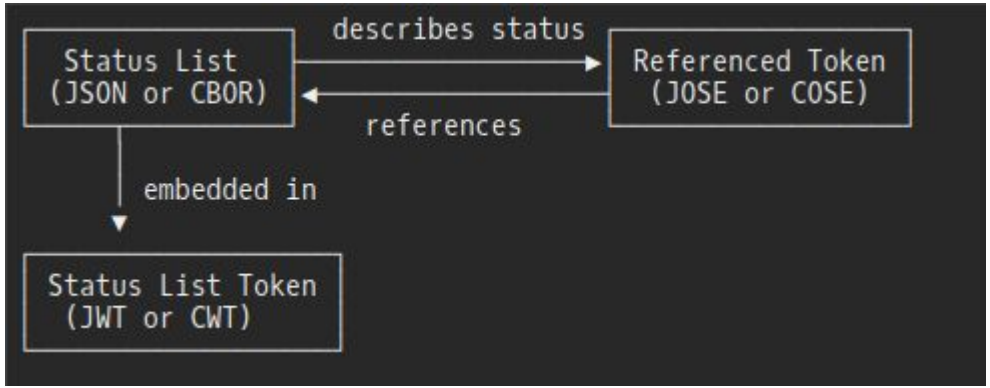
Key Facts

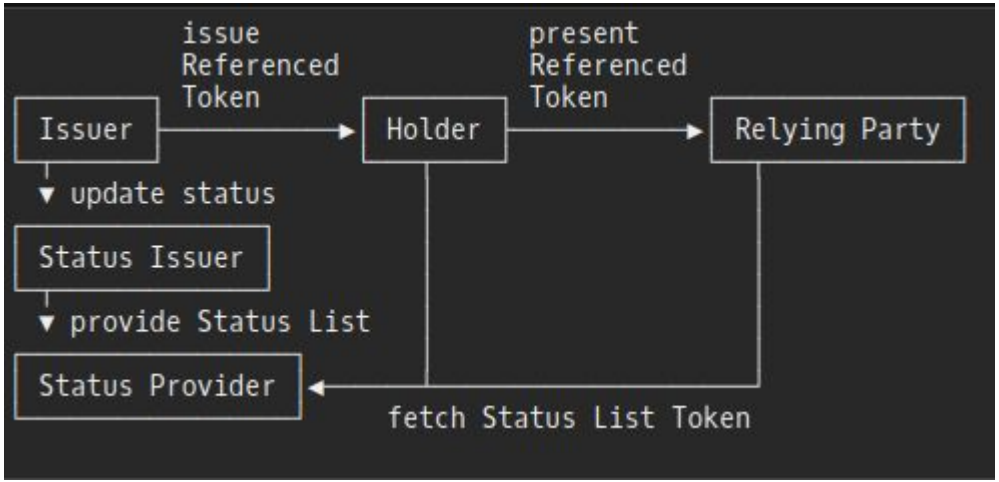
The most important facts:

- Scalable Revocation Mechanism
- Similar privacy properties as CRL
- Simple to understand, easy to implement
- Referenced by SD-JWT VC and ISO 18013-5 mdoc Amendment
- Named by ARF 1.4
- Tested at various interop events and hackathons
- Establishes an extension point and IANA registry for status mechanisms

Big Picture

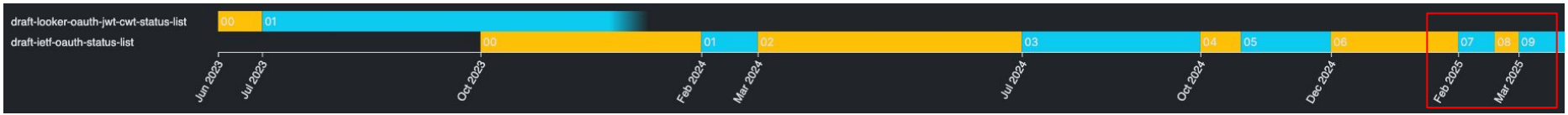
- Architecture of Status List





- Architecture of Status List
- Referenced Token = Credential
  - SD-JWT VC
  - ISO mdoc
  - Any other

Changes since Interims call 01/25



changes in -07

- **add recommendations for Key Resolution and Trust Management**
- **add extended key usage extensions for x509**
- Relying Parties avoiding correlatable Information
- editorial changes on terminology and Referenced Tokens
- clarify privacy consideration around one time use reference tokens
- explain the Status List Token size dependencies
- explain possibility to chunk Status List Tokens depending on Referenced Token's expiry date
- add short-lived tokens in the Rationale
- rename Status Mechanism Methods registry to Status Mechanisms registry
- changes as requested by IANA review
- emphasize that security and privacy considerations only apply to Status List and no other status mechanisms
- differentiate unlinkability between Issuer-RP and RP-RP

changes in -07 (cont)

- **add more test vectors for the status list encoding**
- **add prior art**
- updated language around application specific status type values and assigned ranges for application specific usage
- add short security considerations section for mac based deployments
- **privacy considerations for other status types like suspended**
- fix aggregation_uri text in referenced token
- mention key resolution in validation rules
- add considerations about External Status Issuer or Status Provider

changes in -08 and -09

- **introduce dedicated section for compressed byte array of the Status List**
- **fix Status List definitions**
- Add CDDL for CBOR StatusList encoding
- add diagram for Status List Aggregation for further explanation
- rename "chunking" of Status List Tokens (for scalability reasons) into "divide .. up"
- Holders may also fetch and verify Status List Tokens
- Update terminology for referenced token and Status List Token
- update acknowledgments
- **Fix cwt typ value to full media type**

Status Quo

- Received lots of good feedback since first WGLC
  - we feel we have incorporated all actionable feedback
  - A lot of the feedback resulted in editorial changes
- Finalize remaining discussion on X.509 as Referenced Token
- We believe all major points were discussed & addressed

Status List for X.509 Certificates

Mailing List discussion:
https://mailarchive.ietf.org/arch/msg/oauth/_vc8RgYVMOl3ekRTFd7nbGyDo9c/

We also brought it up at OSW to get more people involved in the discussion

Our current position as editors: *do not include in this draft, but do not prevent it - if there is interest in this extension, it should can happen in a separate draft in a more appropriate working group.*

Size comparison

A request for a size comparison of a status list vs CRL was suggested to be added informatively to the draft.

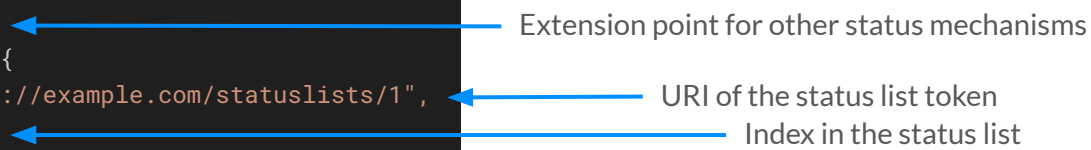
To address this we intend to add a comparison chart as potential last addition in the annex of the draft

Ask for 2. WGLC

Backup

Example: Referenced Token

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



Example: Status List in JWT

```
eyJhbGciOiJFUzI1NiIsImtpZCI6IjEyIiwidHlwIjoic3RhdHVzbGlzdCtqd3QifQ.eyJleHAiOjE2ODc1MTc3NzAsImlhdCI6MTY4NjkxMjk3MCwiaXNzIjoiaHR0cHM6Ly9leGFtcGxlLmNvbSIsInN0YXR1c19saXN0Ijp7ImJpdHMiOjIsImxzdCI6Ikg0c0lBTW9fakdRQ196dnA4aE1BWkxSTE1RTUFBQUEifSwic3ViIjoiaHR0cHM6Ly9leGFtcGxlLmNvbS9zdGF0dXNsaXN0cy8xIn0.8uaUXshaJdGWGjvwPwaa2Gtt0M7-M7dGO9rXaz3x99LCdG5tKb-ARL1ezqguLTs63VeudYWqpdg4HpN-D2hOkg
```

```
{
    "alg": "ES256",
    "kid": "12",
    "typ": "statuslist+jwt"
}
.
{
    "exp": 1687517770,
    "iat": 1686912970,
    "iss": "https://example.com",
    … //other claims
    "status_list": {
        "bits": 1,
        "lst": "H4sIAMo_jGQC_zvp8hMAZLRLMQMAAAA"
    },
    "sub": "https://example.com/statuslists/1"
}
```

Example: How it fits together