Can we improve certificate/JWT/CWT revocation?

Hannes Tschofenig

<Hannes.Tschofenig@siemens.com>

A lot has been said about certificate revocation already

- **Long-lived certificates** require a story for revocation. Solutions are available but usage remains “mixed”.

- Certificate Revocation Lists (RFC 5280)
- Online Certificate Status Protocol (OCSP) + extensions for stapling in TLS (see RFC 6961) and other protocols
- CRLite (Mozilla)
- CRLSets (Google)

- Reducing the lifetime of certificates is also frequently being proposed (and used).

JSON Web Tokens (JWTs) have now become certificates as well

- With the proof-of-possession extension (see RFC 7800) JWTs (RFC 7519) have effectively become certificates.
- With OAuth, these JWTs (when used as access tokens) are generally short-lived and created for use with specific relying parties.

- The work on **Verifiable Credentials** turns them into long-lived certificates.

  → JWTs require revocation.

- Same is true for CBOR Web Tokens (CWTs, RFC 8392) and the proof-of-possession extension defined in RFC 8747.

Status Lists

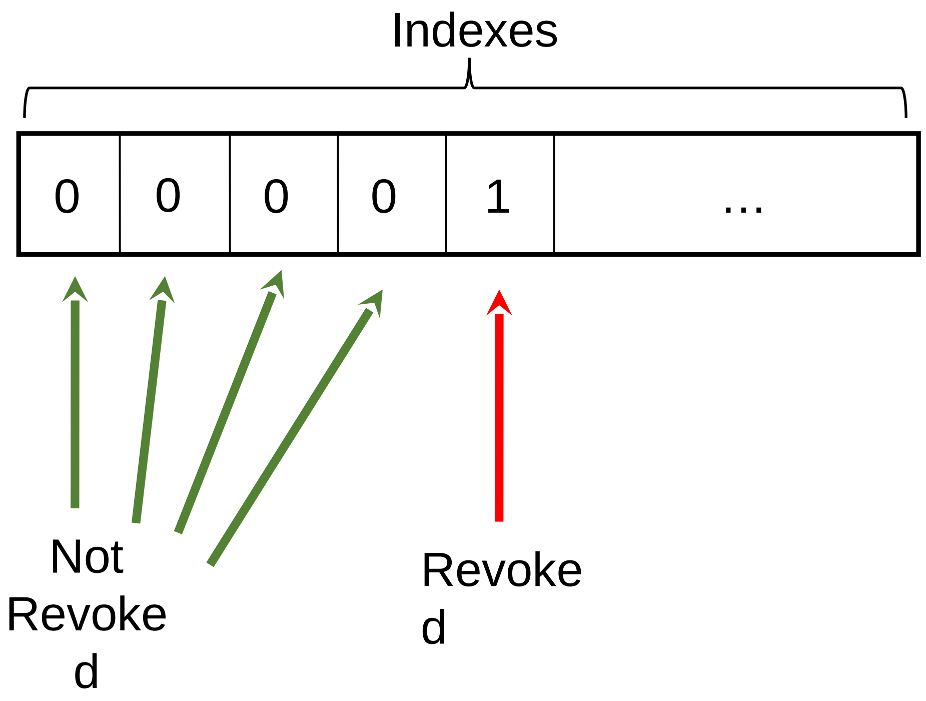
- New work in OAuth WG to define **new revocation mechanism**.

- Mimics the “Let’s Revoke” concept (academic publication, focused on X.509 certificates)

- Prior work also in the W3C on Verifiable Credentials Status List v2021 (w3.org)

What are Status Lists?

- Issuer adds a URL to the status list and an index to the JWT (or CWT)
- Issuer maintains information about revoked JWTs/CWTs in a bit string – called status list.
- Verifier fetches this status list by
  - Downloading the status list from the URL provided in the JWT/CWT
  - Retrieves the bit position based on the index value.
- The status list (containing the bit string) itself is again a JWT/CWT.
- To reduce the size of the bit string, apply GZIP.
- To make it bigger again then apply base64encoding ;-)



Indexes

0	0	0	0	1	…

Not Revoked

Revoked

Your experience is needed!

- Is this a useful concept?
- If it is useful for JWTs/CWTs, should it be applied to X.509 certificates as well?
- Is there room for improvement?

Come to the OAuth WG and tell us!