W3C CREDENTIALS COMMUNITY GROUP

Bitstring Status List

Agenda

01

Overview

What does it do?

02

Privacy Considerations

Why did we build it?

03

How it Works

What makes it tick?

04

Discussion

Questions and answers

01

Overview

Bitstring Status List

A privacy-preserving, space-efficient, and high-performance mechanism for publishing status information, such as suspension or revocation, of Verifiable Credentials.

- Provide status information for long-lived credentials.
- Do it in a way that doesn't violate an individual's privacy.
- Make it space efficient and easy to implement.

The full specification is here: https://www.w3.org/TR/vc-bitstring-status-list/

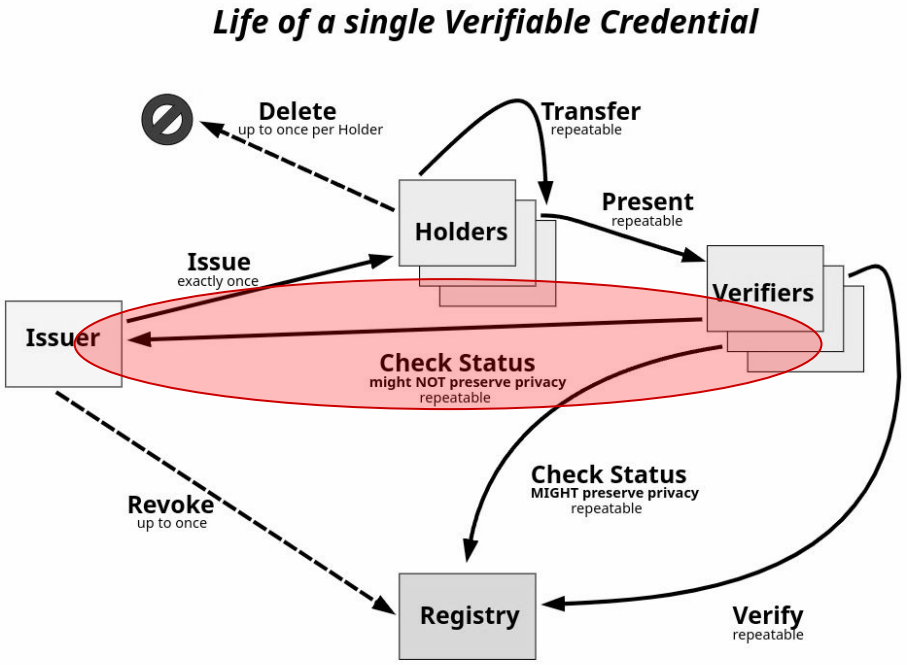
02

Privacy Considerations

Protect Against Tracking By Issuer

One goal is to prevent tracking by the issuer of the Verifiable Credential

- Issuer must not be able to guess who the subject is
- Holder should be able to deliver status list themselves
- Use infrastructure to increase privacy: Content Distribution Networks, Caching, and Oblivious HTTP



Protect Against Statistical Analysis

Another goal is to prevent analysis of group statistics

- Ensure that index allocation leaks as little information as possible
- Ensure that status changes leak as little information as possible

03

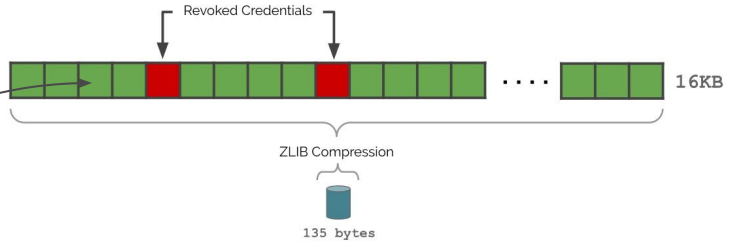
How it Works

Issuance

When a VC is issued, it gets assigned a "purpose", such as "revocation" and a position in a status list.

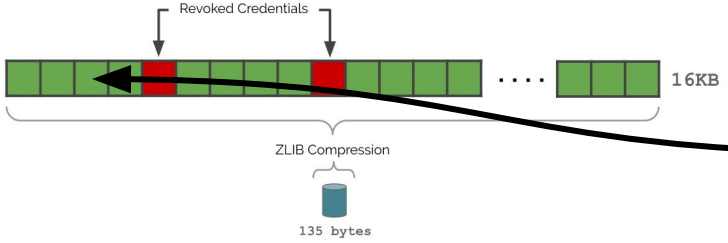
EXAMPLE 17: Usage of the status property

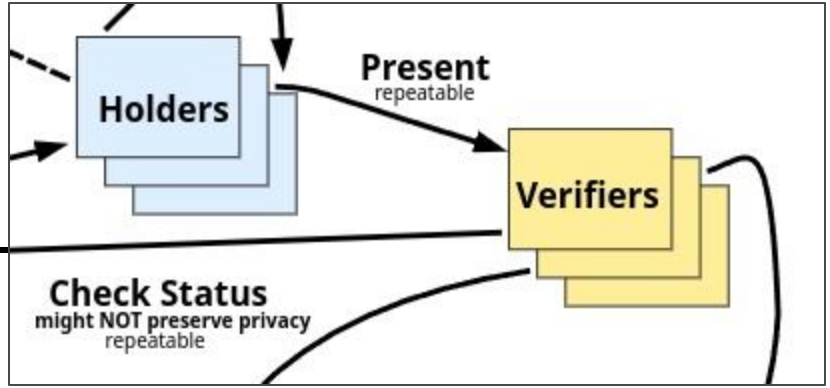
```
{
  "@context": [
    "https://www.w3.org/ns/credentials/v2",
    "https://w3id.org/vc/status-list/2021/v1"
  ],
  "id": "http://university.example/credentials/3732",
  "type": ["VerifiableCredential", "ExampleDegreeCredential"],
  "issuer": "https://university.example/issuers/14",
  "validFrom": "2010-01-01T19:23:24Z",
  "credentialSubject": {
    "id": "did:example:ebfeb1f712ebc6f1c276e12ec21",
    "degree": {
      "type": "ExampleBachelorDegree",
      "name": "Bachelor of Science and Arts"
    }
  },
  "credentialStatus": {
    "id": "https://university.example/credentials/status/3#94567",
    "type": "BitstringStatusListEntry",
    "statusPurpose": "revocation",
    "statusListIndex": "94567",
    "statusListCredential": "https://university.example/credentials/status/3"
  }
}
```



Verification

When a VC is verified, the list is downloaded, and the entry, which is only known to the holder and the verifier, is checked to see if it has changed.





Does it work?

Bitstring Status List addresses the requirements because:

- The Issuer doesn't know which individual's status is being checked in a list of 100,000+ entries. Individual privacy is preserved*.
- Observers of the list can't tell the number of entities or depend on their status because of randomness and dummy values. Group privacy is preserved*.
- Each entry only requires a single bit of storage and multiple bits of the same value are highly compressible. Storage efficiency is achieved.
- The status list can be delivered to the Verifier by the Holder.

* as long as the Issuer isn't a bad actor.

Could it be better?

Yes.

What if we could also support stronger unlinkability using a scalable Zero-Knowledge-based revocation scheme?

- AnonCredsv2 has done some work in this area.
- ALLOSAUR has some benefits; could we apply it to VCs via **credentialStatus**?
- Anyone know of anything else that would improve status checking?

04

Discussion

Discussion

Do you have any questions?

public-credentials@w3.org

https://w3c-ccg.github.io/