Status Registry Practices

Suggest Edits

ThecredentialStatus of a VC provides a flexible means of updating a credential's current state, such as to enable revoking or suspending it. An implementor must decide what credential status method(s) to support; there is no default method.

Privacy Considerations

The following considerations should be taken into account when choosing a status method:

1. Updating the status (e.g., revoking it) should not result in additional data being disclosed about the subject or holder
2. Issuers should avoid the need to "phone home" during verification* Note that phoning home also introduces an availability requirement on issuer services for verification to occur.
3. If "phone home" is used, Issuers should prefer methods that minimize behavioral data about the credential holder
4. Specifically, Issuers should avoid the need for Verifiers to perform a request correlatable to a specific individual

The VC Data Model'sprivacy considerations section contains additional considerations relevant to credential status implementations.

Status List 2021

A common approach that's simple to implement, size-efficient, and enables "herd privacy" for individuals is theStatus List 2021 method, which Verite uses.

The status list is a base 64 encoded, zlib compressed bitstring. That is, each bit corresponds to the revoked or active status of a credential. When issuing a credential, the credentialStatus object includes two critical properties: a url to fetch the revocation list and the index in the list that corresponds to the given credential. Notice that credentials are themselves immutable, so these properties must be determined in advance, at issuance. The revocation list is itself a verifiable credential. However, since webservers can always change what is returned at a given URL, the returned revocation list is essentially mutable.

For comparison, note that a simpler approach might be a single URL that returns the status of a single credential. However, each time a verifier checked the URL, it would leak activity back about the individual credential holder to the issuer. In contrast, the approach described here can contain the status for about 16KB worth, or 131,072 credentials. The verifier performs a request that compactly encodes the status for the batch, and the verifier selects the specific index they want to check. This means the issuer doesn't learn which specific credential the verifier was checking, allowing herd privacy for users.

You can read more about Verite's implementation in theRevoking a Credential tutorial.

Latency and Freshness Considerations

Verifiable Credentials from the Verite system should not be accepted or assumed to remain indefinitely valid; we recommend checking them at each relying transaction:

1. activation, i.e., issuance date is in the past and not the future, meaning it is currently in force),
2. non-expiration, i.e., its expiration date is in the future, and
3. active status, i.e., its status has not been set to "revoked" or "suspended" by the issuer.

That third check, since it is expressed in each credential as a URL, can be re-checked even if the underlying VC is unknown to the verifier, has not been retained, etc. Since non-sanctions or non-PEP status is an ongoing state monitored by most issuers of KYC/KYB credentials, issuers should choose carefully how frequently to update the status lists for their credentials, and verifiers/relying parties should understand precisely how to check these, as many usecases will require them to re-check them often. Updated5 months ago