Credential State

Suggest Edits

VC ecosystems enable credential subjects to store and share their credentials directly, outside of the issuer's domain. Nevertheless, in many cases, issuers must be able to specify when a credential is no longer valid, such as when a credential has expired or has been revoked. Verifiable Credentials expose dials to update the state of the credential in a manner consistent with the VC design goal of minimizing dependencies on the issuer.

Concepts

Expiration

Most credentials are intended to be valid for only for a certain period of time:

- A credit score credential may be considered valid only for days or hours after it was issued
- A KYC credential may expire after a few months or a year of issuance

Issuers may indicate that the credential is not to be considered after a certain date through the VC field expirationDate .

Status

Beyond expiry, VCs support a general notion of status. This is used by issuers to specify other updates to a credential's validity -- the most common being to revoke a credential (whether it was issued in error or found to be obtained through fraudulent means).

VCs contain a field credentialStatus for this purpose. Implementers are free to define their own states such as "suspended".

Details

The following two optional properties of a Verifiable Credential are used by verifiers when determining whether to accept a credential:

- expirationDate
- : optional ISO 8601 formatted string indicating when the credential is no longer validdetails
- credentialStatus
- : property whose
- type
- property defines a method for determining credential status, such a way to determine whether the credential has been revoked or suspendeddetails

During verification, expirationDate is evaluated and interpreted uniformly through comparison with the current date (possibly factoring in a delta), but credentialStatus must be evaluated based on the instructions indicated by the type . This might include instructions for looking up a list of revoked credential ids, identifying the status of a credential as an index in a bit vector, or use of a cryptographic accumulator. Verification libraries would typically allow for this flexibility through use of a status plugin model.

The choice of credentialStatus implementation allows for multiple credential states; i.e., a credential issuer might want to indicate a credential is "active", "suspended", or "revoked". However, most existing implementations are intended to support two states -- "active" and "revoked".

Verifiers may apply additional criteria to determine whether to accept a credential, such as their own fitness for purpose considerations.

Expiration and revocation considerations

Expiration and Revocation Tradeoffs

While expiration and revocation are semantically different, the VC design goals of enabling privacy while minimizing issuer dependencies result in common tradeoffs for implementers:

- For an VC with a long lifespan that the issuer may need to revoke, devising and deploying a privacy-preserving, yet decentralized revocation mechanism may seem prohibitive from an implementation perspective. For this reason, some issuers choose to set more aggressive expiration dates to avoid or reduce the need to revoke credentials.
- At the same time, an overly aggressive expiration date requires the credential subject to frequently re-request the credential, again increasing the dependency on the issuer.

To that end,Status Registry Practices expands on approaches to achieve privacy-preserving revocation (or more generally, status) methods.

Interpretation of a Revoked Status

Revocation does not always mean the credential subject has become ineligible for the given type of credential; sometimes it is used to correct information within the credential. Unless explicitly provided by the specific credential status implementation, a verifier is not intended to assume a reason for revocation. An issuer may provide a "revocation reason", but should be mindful of the possible privacy impact of the information provided.

Renewing or Refreshing a Credential

Issuers or subjects may want to refresh or renew a credential for a variety of reasons: in addition to updating the data in the credential (a name change, for example), subjects may want to update their identifier if they have lost control of cryptographic keys and rotation/recovery is not possible. For reasons such as this, some issuers may set an expirationDate that precedes the actual ending validity of a credential. In this case, the issuer is recommended to specify arefresh service via a refreshService field for convenience to the credential subject.

Expiration Date, in practice

expirationDate is commonly used for purposes like a trade certification, or a license that must be renewed every year. But it is also useful for credentials that become out of date quickly, like a credit score. Updated3 months ago * Table of Contents * * Concepts * * * Expiration * * * Status * * Details * * Expiration and revocation considerations * * * Expiration and Revocation Tradeoffs * * * Interpretation of a Revoked Status * * * Renewing or Refreshing a Credential * * * Expiration Date, in practice