Self-Review Questionnaire: Security and Privacy

Specs:

RTCQuicTransport:
https://w3c.github.io/webrtc-quic/#privacy-security

3.1. Does this specification deal with personally-identifiable information?

Yes, see section 6.4: Persistent Information

3.2. Does this specification deal with high-value data?

No

3.3. Does this specification introduce new state for an origin that persists across browsing sessions?

Yes, see section 6.4: Persistent Information

3.4. Does this specification expose persistent, cross-origin state to the web?

No

3.5. Does this specification expose any other data to an origin that it doesn't currently have access to?

Yes - see "impact on same origin policy" in the spec.

3.6. Does this specification enable new script execution/loading mechanisms?

No

3.7. Does this specification allow an origin access to a user's location?

No

3.8. Does this specification allow an origin access to sensors on a user's device?

No

3.9. Does this specification allow an origin access to aspects of a user's local computing environment?

No

3.10. Does this specification allow an origin access to other devices?

No, although it does allow communication of data between browsers and other devices.

3.11. Does this specification allow an origin some measure of control over a user agent's native UI?

No

3.12. Does this specification expose temporary identifiers to the web?

Yes

- **QUIC self-signed certificates & certificate fingerprints**

3.13. Does this specification distinguish between behavior in first-party and third-party contexts?

No

3.14. How should this specification work in the context of a user agent's "incognito" mode?

No difference.

3.15. Does this specification persist data to a user's local device?

No

3.16. Does this specification have a "Security Considerations" and "Privacy Considerations" section?

RTCQuicTransport:
https://w3c.github.io/webrtc-quic/#privacy-security

3.17. Does this specification allow downgrading default security characteristics?

No