This document describes perceived status of WebRTC identity as of May 2018.

Identity is at the moment section 8 of the WebRTC 1.0 specification.
It has been implemented in Firefox, but according to the Firefox developer, there are no active users of the feature.

At the IETF hackathon in London March 2018, the interface was explored - it was clear that it's possible to write identity providers according to the spec, but the security properties of the identity providers demonstrated weren't immediately obvious (apart from the insecure ones).

One of the demos showed how one could use an existing login (google login in this case) to build an identity provider (without needing to ask for help from the login provider). So we know this is possible.

Specification and process relationships

The identity specification is part of the W3C WebRTC 1.0 specification.
The rules for W3C specifications are that each feature must have 2 implementations in order to advance, and that specifications should (as in "most of the time") only reference documents at the same or higher maturity level.

The requirement to have an identity function is embedded in draft-ietf-rtcweb-security-arch section 5.6, where it shows how one needs identity in order to establish trust in identity between WebRTC endpoints without trusting the signalling provider to mediate such trust. (This document is currently in "issue raised at WGLC" state, and not yet approved by the IESG.)

The requirement for identity is embedded in RFC 7478 (the WebRTC requirements document) - "the browser must support a mechanism for cryptographically binding media and data security keys to the user identity (see R-ID-BINDING in [RFC5479])".

The security-arch document is a normative reference from the RTCWEB overview document (draft-ietf-rtcweb-overview). Thus, a conformant RTCWEB endpoint must support identity.

Issues with the current spec

The spec has not been used as a basis for a production service, so we do not know if it needs to be changed. Recent discussions on the webrtc list indicate some uncertainty about whether the identity needs to be bound to the origin or can be used across origins, for instance.

There's also been a thread asking exactly how the identity is bound with the TLS keying material - at the moment, the answer seems to be "it's in the same SDP blob as the a=fingerprint", which is not an answer with any cryptographic verification applied to it.

What we can conclude from the current state

The maturity of the identity spec seems to be significantly different from the rest of WebRTC 1.0, and progress has been slow. There are a number of bugs of long standing on identity (23 currently tagged with "identity related"). Since WebRTC 1.0 went to Candidate Recommendation, 80+ pull requests have been merged, yet none of the "identity related" issues has been closed.

On a pure W3C process basis, we need to isolate the identity provider specification from the rest of the WebRTC 1.0 specification, so that it can be updated, modified or replaced independent of the main specification.

On an IETF process basis, we need to make sure there is a stable reference for the requirement to implement identity assertions. This means that we should at least get the identity specification document published at the same time as we replace it with a reference in the main specification. (Also needed for W3C sanity).

Next steps

The logical step seems to be to break Identity out into its own specification, and let that progress independently of Webrtc-pc. This would also allow us to assign new editors to that part of the specification, without asking them to take responsibility for the WebRTC 1.0 spec.

This retains Identity as a part of the WebRTC protocol suite, but does not make it a blocker for progressing WebRTC 1.0 into a stable specification.