This message was sent to secdir on July 17th 2021:
https://mailarchive.ietf.org/arch/msg/secdir/ijoxNV3tjqYw1WOKI7T5O0JYts0/
Editing has been disabled.

Benjamin, Roman, and the IETF Security Area Directorate,

I am writing on behalf of the Chairs, Staff, and Members of multiple current chartered W3C Working Groups related to Verifiable Credentials[1] (VCs) and Decentralized Identifiers[2] (DIDs). The outcome of this message also could affect future W3C Working Groups currently in the pre-chartering process related to RDF Dataset Canonicalization and Hashing, and Linked Data Integrity[3].

TL;DR: There are two requests in this message. The first is from the DID WG, for a best-effort security review of the Decentralized Identifier Core specification[4] by an appropriate IETF group. The second is from the current VC and DID WGs, on behalf of themselves and the above-mentioned pre-charter WGs, to set up regular and recurring security reviews of specific W3C specifications that will be developed over the next several years, in a capacity that is more coupled than a traditional W3C-IETF liaison relationship.

Both requests are further detailed in the rest of this message.

Review of DID Core Specification

Mark Nottingham, Co-Chair of the HTTP WG, recently inquired about the security and privacy reviews that were performed on DID Core. The W3C DID WG has performed multiple security and privacy reviews on the specification[6], per the W3C process. In addition to those reviews, we are hoping that the IETF secdir or CFRG will guide us toward receiving additional security reviews on the specification. What would be the best path to getting an initial best-effort security review of the DID Core specification, and subsequent security reviews every six months or so on iterations of that specification?

I will note two important considerations. The first is that the initial DID WG charter expires in September 2021, the specification comes out of the 2nd W3C Candidate Recommendation phase in mid-July 2021, and according to W3C Process, the DID WG has enough implementation experience (32 implementations for many features) to move on to the W3C Proposed Recommendation phase. The second consideration is that the DID WG has only defined a data model and has not defined any cryptographic algorithms or protocols in this iteration of the specification. That said, the specification is expected to be used with cryptographic systems, and furthermore, protocol work might be included in the work of a re-chartered (future) group. Thus, we desire more eyes on the specification, especially from IETF Security Area Directorate and IRTF CFRG.

Benjamin and Roman, what mechanism would be most effective for achieving a timely, best-effort review of the W3C Decentralized Identifiers specification?

Targeted Engagement with Future DID and VC-related work at W3C

This message was sent to secdir on July 17th 2021:
https://mailarchive.ietf.org/arch/msg/secdir/ijoxNV3tjqYw1WOKI7T5O0JYts0/
Editing has been disabled.

Since the Recommendation of the W3C Verifiable Credentials specification[7], and the expected Recommendation of the W3C Decentralized Identifiers specification[4], there has been increased movement in government and the private sector towards issuing credentials for a variety of use cases in a production capacity. As a result, it is highly likely that both the W3C Verifiable Credentials WG and the W3C Decentralized Identifiers WG will be re-chartered to maintain and/or advance the work.

In addition, new cryptographic packaging formats and protocols[3][8] based on active IETF work[9][10] and/or RFCs are expected to be advanced in parallel. The chartered W3C Working Groups are requesting a more direct liaison relationship that goes beyond periodic reviews of the specifications under development by these groups. Ideally, participants in the IETF Security Area would be active members of these W3C Working Groups with an additional liaison relationship to groups like the IRTF CFRG. There is a strong expectation that newly chartered groups that are related to the technologies mentioned throughout this email will request the same type of relationship.

Benjamin and Roman, what mechanism would be most effective for setting up this more formal and active relationship between the IETF Security Area and the W3C Working Groups mentioned above?

Thank you for your time in considering the questions that we have put forward in this message. We know that this is only the beginning of the discussion, so don't expect definitive answers in initial responses, but hope for some concrete guidance on next steps.

On behalf of the Editors, Chairs, and Staff contacts for W3C Verifiable Credentials WG and the W3C Decentralized Identifiers WG,

-- manu

[1]https://www.w3.org/2017/vc/WG/
[2]https://www.w3.org/2019/did-wg/
[3]https://w3c.github.io/lds-wg-charter/
[4]https://w3c.github.io/did-core/
[5]https://github.com/w3c/did-core/issues/768
[6]https://github.com/w3c/did-core/issues/768#issuecomment-869209663
[7]https://www.w3.org/TR/vc-data-model/
[8]https://w3c.github.io/lds-wg-charter/explainer.html
[9]https://datatracker.ietf.org/doc/draft-irtf-cfrg-pairing-friendly-curves/
[10]https://datatracker.ietf.org/doc/draft-irtf-cfrg-bls-signature/