2019-09-18 Meeting Notes

1. PR Discussion: Zmix
   a. Dan: it's not clear how some of the stuff works.
      i. Dan: more cryptographic detail needed?
   b. Manu: goal to express functionality, not too much cryptographic detail.
   c. TODO: Manu and Dan to add cryptographic background and references to Zmix RFC
   d. TODO: we need to modify the RFC requirements to include cryptographic background and references.

2. RFC PR Discussion: PS Signatures and Delegatable Credentials
   a. Lovesh: some RFCs to go over here.
   b. Mike and Manu: we could reform the RFCs.
      i. In addition to background references...
      ii. Do we need such an emphasis on the API?
      iii. Not slowing down the RFC process as much as lack of reviews.
   c. Encryption API in final comment form
   d. PS Signatures and Verifiable Encryption–can we move to final comment period?
      i. Hope to merge by next meeting

3. Code PR Discussion
   a. Focus: Bulletproofs, BBS+ Signatures, and an improvement to PS Signatures.
   b. BBS+ Sigs: we got sidetracked on a lot of other things.