2019-09-04 Meeting Notes

NOTE: Jon Geater ran the call but didn't have Admin credentials so couldn't record. However he did display and read out the antitrust notice before starting.

1. Open PRs
   a. Loves working on PR-36. Already a few kloc: reviews welcome. Finalising code complete within a week.
   b. Question mark over MIT-licensed code incursion. Upcoming commit makes this clear but does not remove the license altogether: we think this is OK but it's not strictly Apace 2.0 (though it is broadly considered 'compatible')

2. Open RFCs
   a. Encryption API - to be covered in next major agenda item
   b. ZMix: review overdue - Mike to do a presentation next time, hopefully will un-block the conceptual thinking around the next 3.
   c. Verifiable encryption - already has several approvals and the code is merged. Any objection to completing this one? Please review and urgently speak up if you DON'T like it! ACTION: Lovesh to ping the Ursa chat and we'll move to final comment in next meeting.
   d. RFC PR-10 Proof of values in a vector commitment - one unresolved comment from Dmitry re optimisation, one concern from Manu remaining regarding the interface and what it's trying to achieve. ACTION Some constructive conversation soon the call about how to retarget the RFC to be more likely to succeed. Lovesh to talk to Dmitry and Manu to clear up the residual concerns.
   e. RFC PR-11 anoncreds signature scheme - Again code is merged already, residual concerns over exactly how the change is presented and bounding what it promises.
   f. Need to better formalise the RFC approval system to stop them from lying around for a long time. Need strong control of design changes but can't let inaction block changes...Agenda items for next week. ACTION agenda item for the next meeting to decide the criteria and philosophy for accepting general changes. Good litmus test for any controversial topic is: "do we have a strong use case need from a hyperledger framework?"

3. Unbound RFC for PKCS#11 provider
   a. Quick discussion on expectations: only ECDSA and a handful of hash algorithms are supported in the standard so it comes to a more grotty mix of vendor extensions. This makes it much less broadly applicable and vendor-neutral than we'd hoped and all vendors will have to provide Vendor Extensions to make a decent set of algs work. Nobody objects to this per se so the RFC will be pushed in the next couple of days and discussed next time.

4. Encryption API (RFC 6 in final comment period)
   a. Figure out what to do for a modular block cipher mode (in case projects use native block cipher calls).
      i. Request for better examples for developers - ACTION Dan to explicitly requests that as a comment against the EAP review
      ii. Happy with the change to Markdown
      iii. ACTION: Think about naming conventions
      iv. Please review!!

5. Accommodating Sovereign Crypto
   a. SKIPPED to next meeting: this will come out in the wash of the modular crypto thinking from the above topics.

6. Delegatable Credentials:
      Code is here: https://github.com/lovesh/signature-schemes/tree/delegatable/delg_cred_cdd
   b. Covered the limitation that there is no privacy among delegators...but that's OK, Hyperledger is Enterprise permission blockchain, and in those use cases you don't want unknown parties assuming your authority.
   c. Agreed it's worth bringing forward to full proposal.