

Proposal for a CFRG Crypto Review Panel

Alexey Melnikov (CFRG co-chair)

Kenny Paterson (CFRG co-chair)

Motivation

- CFRG is a volunteer-led activity relying on goodwill of its participants to provide review of documents.
- This can result in documents not receiving enough scrutiny, or examination only being forthcoming over an unacceptably long period of time.

Mission for CFRG Review Panel (1/2)

The CFRG Review Panel will ensure that CFRG chairs have at their disposal sufficient resources and lightweight processes to provide critical, objective, timely and consistent review of documents.

Mission (2/2)

- Any recommendations coming out of panel reviews will not be binding on CFRG, but are intended to provide high-quality input to **augment** (and not replace) the usual development process for CFRG drafts.
- Reviews will identify issues - both security issues and deployment issues - but not necessarily low-level nits and typos.
- Reviews will also identify relevant research, or the need for further research.

Proposed review process

- If chairs decide that a document would benefit from a panel review, they will select one or more reviewers and request a review within a given time period (typically 2 to 4 weeks). Alternatively we might have a Secretary.
- Reviews will be made public via the CFRG mailing list.
- A document's authors may identify conflicts of interest with particular panel members, and vice versa.
- Disagreements or grievances with the reviews, recommendations, mode of operation, etc. should be brought to the CFRG chairs first, with the IRTF chair being the next level of escalation.
- Not every CFRG draft needs to be reviewed by the panel; documents that are not CFRG drafts (but of potential interest to CFRG) may also be reviewed by the panel.

Proposed appointment process

- The CFRG chairs will make appointments to the Review Panel.
- The panel will be composed of 6-8 members; it may be increased in size should the document stream being handled by CFRG increase further in size.
- Reviewers will be appointed to the panel for a period of 2 years, renewable.
- The CFRG chairs will endeavour to ensure that the Review Panel has a balanced composition covering the main technical areas of relevance to CFRG.
- Individuals may self-nominate or nominate others for panel membership.
- Being a panel member represents a commitment to review documents in a timely and thorough fashion; reviewers' panel membership can be rescinded at any time at the discretion of the CFRG chairs.

Discussion

- Good Idea? Can people see problems with the proposed approach?
- Other comments?
- Volunteers?