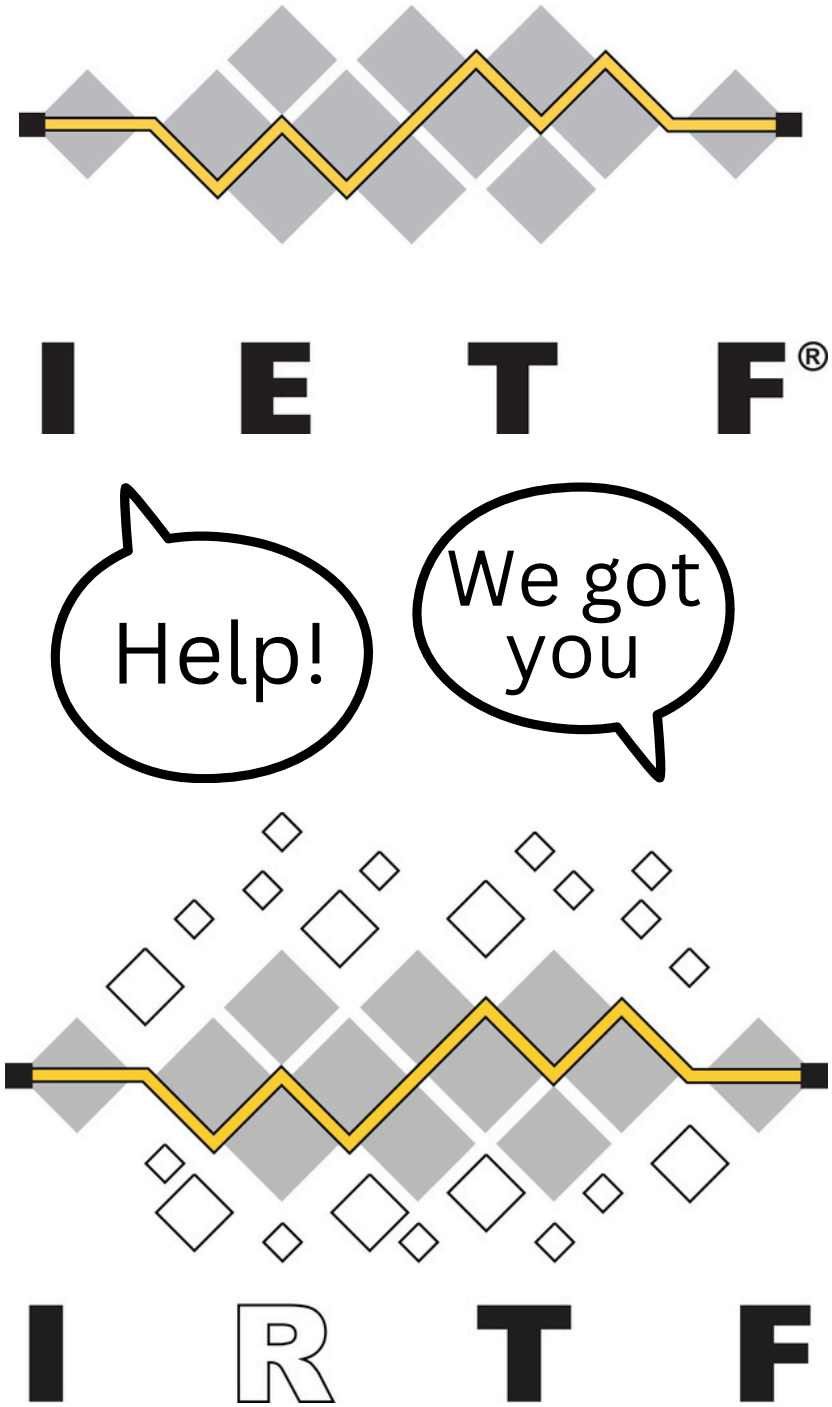
KEM COMBINERS PROCESS UPDATE

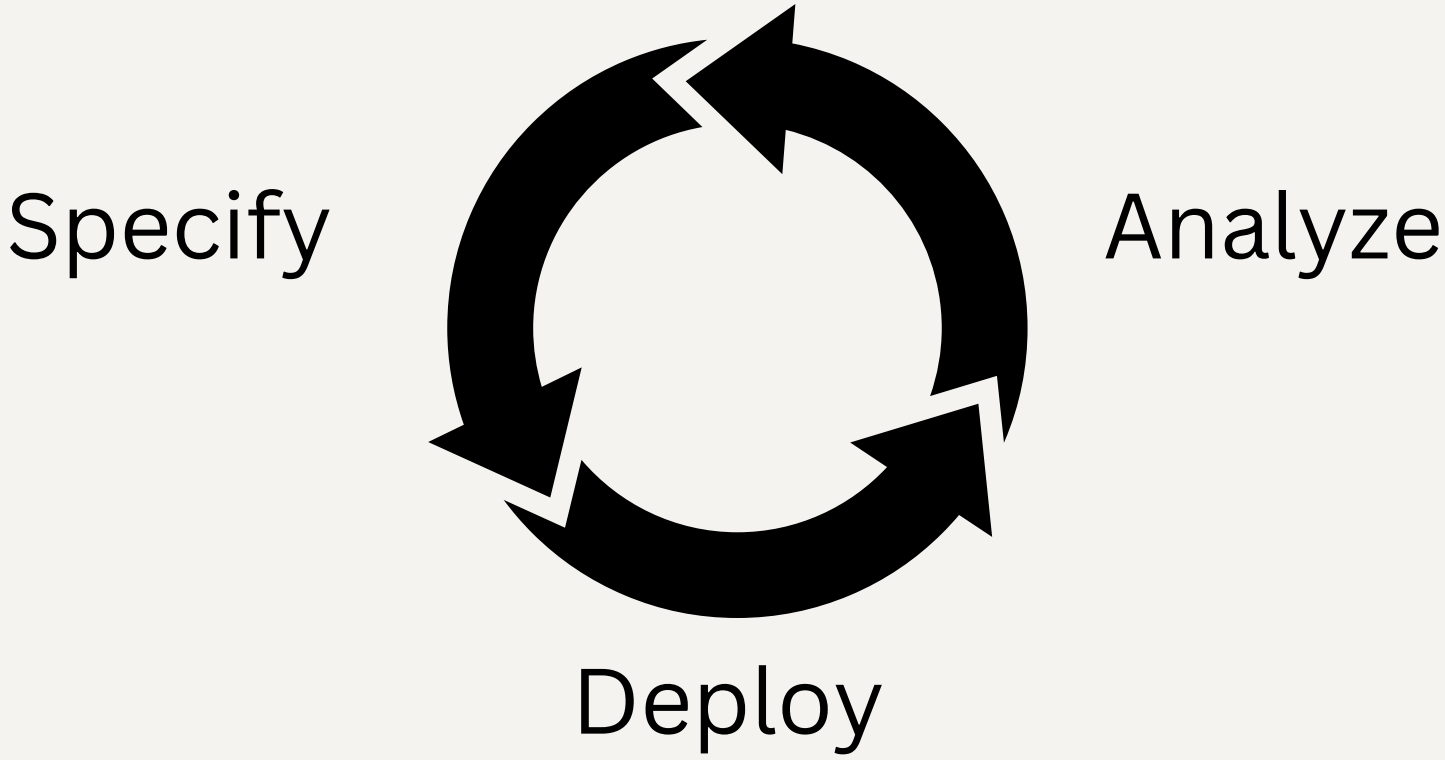
IETF 122

Nick Sullivan
nicholas.sullivan+ietf@gmail.com

WHAT WOULD YOU SAY
YOU DO HERE?

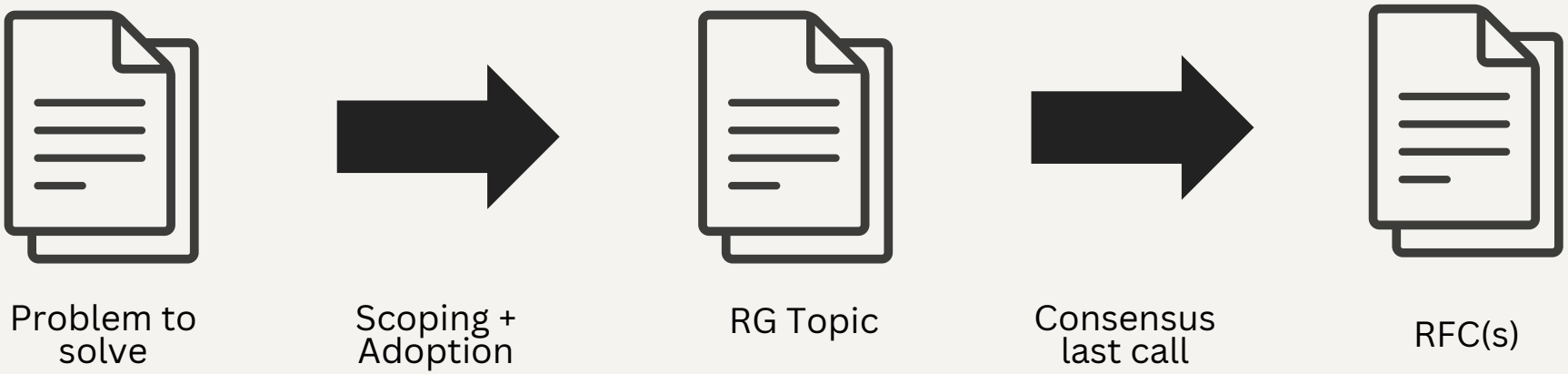

IETF®
Help!
We got you
IRTF

TYPICAL IETF WORKING GROUP (STANDARDS TRACK)

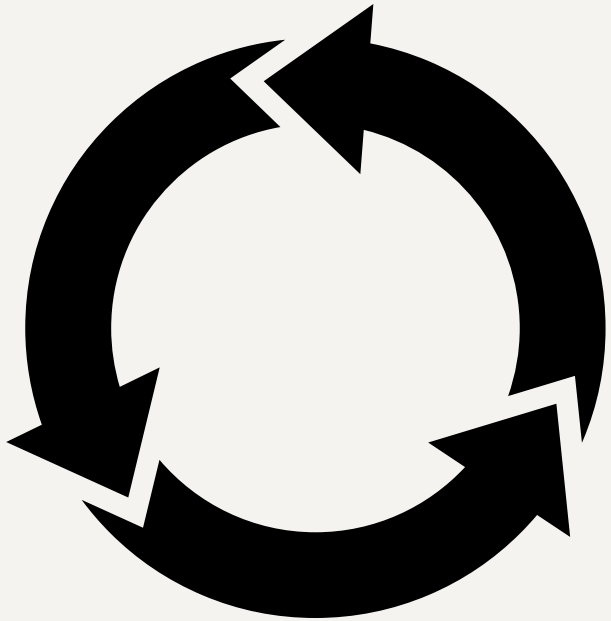


TYPICAL IRTF RESEARCH GROUP (INFORMATIONAL TRACK)

CRYPTO FORUM RESEARCH GROUP



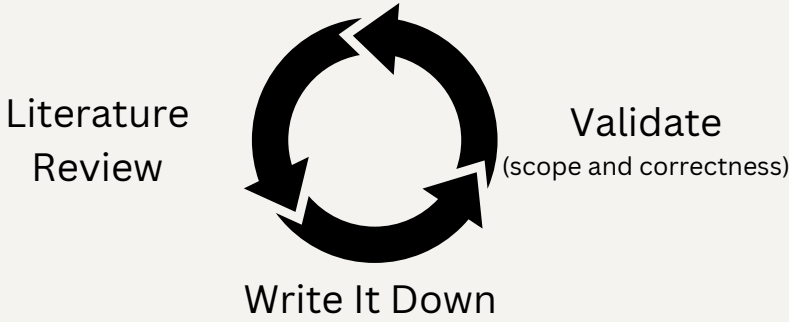
Literature Review



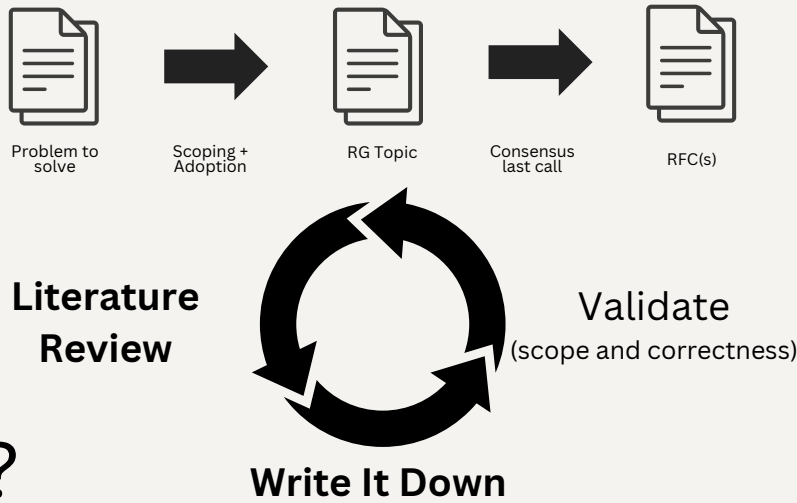
Validate
(scope and correctness)

Write It Down

SCOPING + ADOPTION



- How big is this problem?
- Which IETF groups need a solution?
- How many aspects of this problem need to be studied to avoid revisiting later?
- Do we have the expertise needed?
- Are there any practical requirements? (such as performance, size, security, etc.)

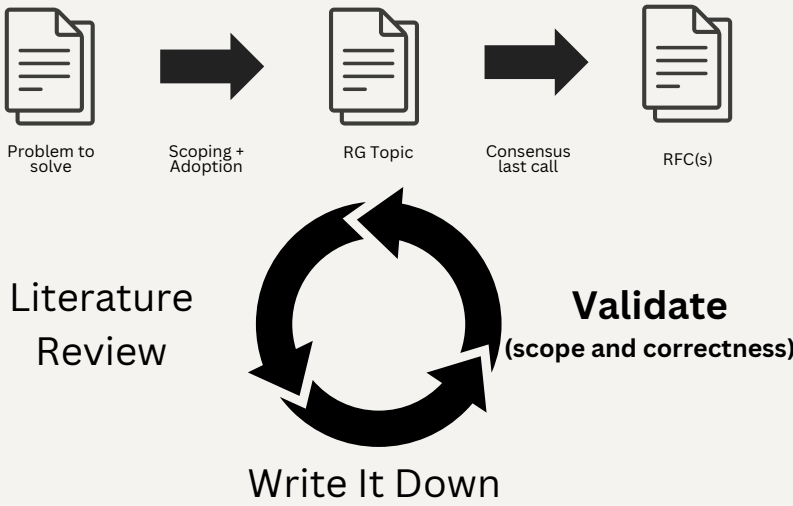


LITERATURE REVIEW

- Are there security proofs?
- Are there reference specs?

WRITE IT DOWN

- *Collaborative* writing process
- Editors chosen by chairs
- One or more documents
- Pseudocode and test vectors
- Validate against implementations

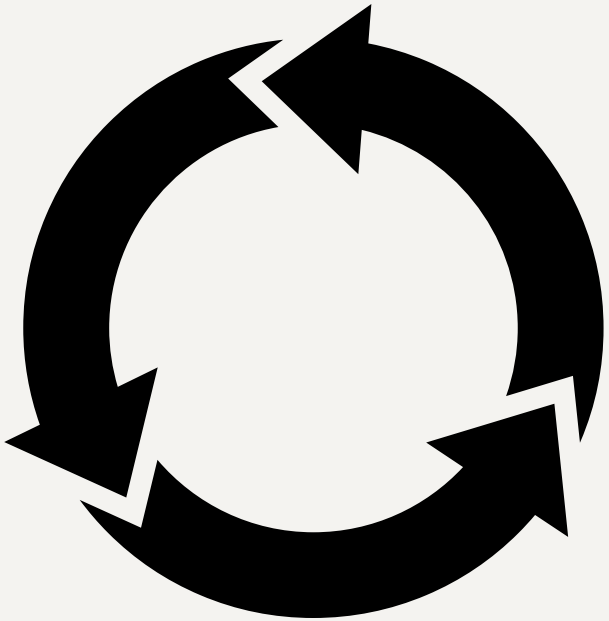


VALIDATE

- Community and crypto panel review
  - Do the documents match the scope?
  - Are the security proofs referenced valid?
- Is a scope change necessary?

PROBLEM: WE NEED MEMORY-HARD HASHING

Literature Review



Validate

(scope and correctness)

Write It Down

PROBLEM: WE NEED PAKES

Problem statement from IETF groups

Requirements document + Contest format

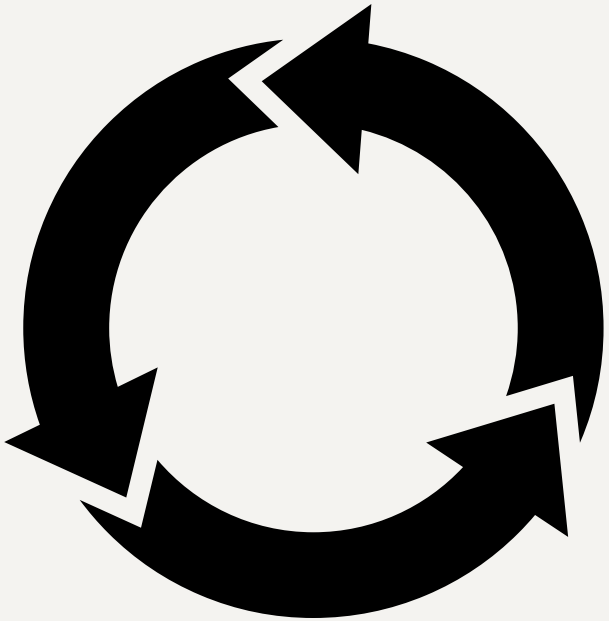
RG Topic

Consensus last call

RFC 8125 + CPace + OPAQUE

Literature Review

Candidate Draft Submissions



Validate

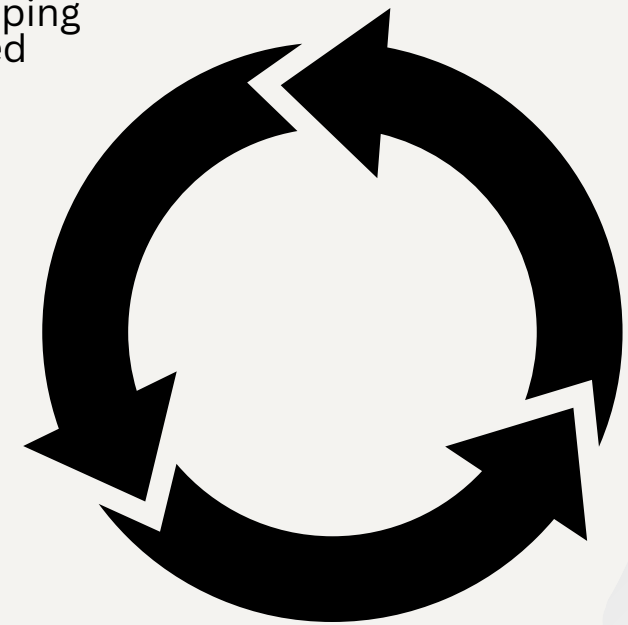
(scope and correctness)

Expert reviews
Results discussed on list
Chairs adopt CPace and OPAQUE

Write It Down

PROBLEM: WE NEED HYBRID KEMS

Literature Review



Validate

(scope and correctness)

Write It Down

QUESTIONS FOR THE GROUP

- Who has read the design team output/scoping text?
- Who has read *draft-irtf-cfrg-hybrid-kems-03*?
- Is the draft on the way to addressing the goals outlined in the scoping text?
- Is the velocity of this draft sufficient for the needs of the IETF groups that would benefit from this work?
- If not, who's willing to help in this collaborative writing process?

KEM COMBINERS PROCESS UPDATE

IETF 122

Nick Sullivan
nicholas.sullivan+ietf@gmail.com