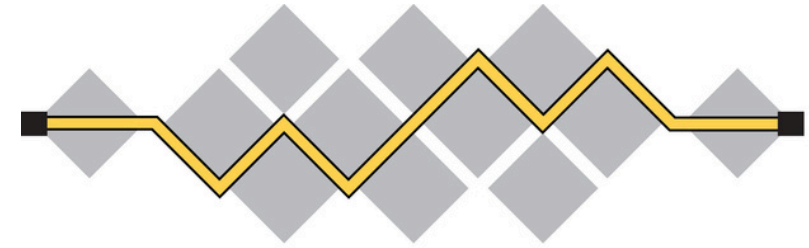
KEM COMBINERS PROCESS UPDATE

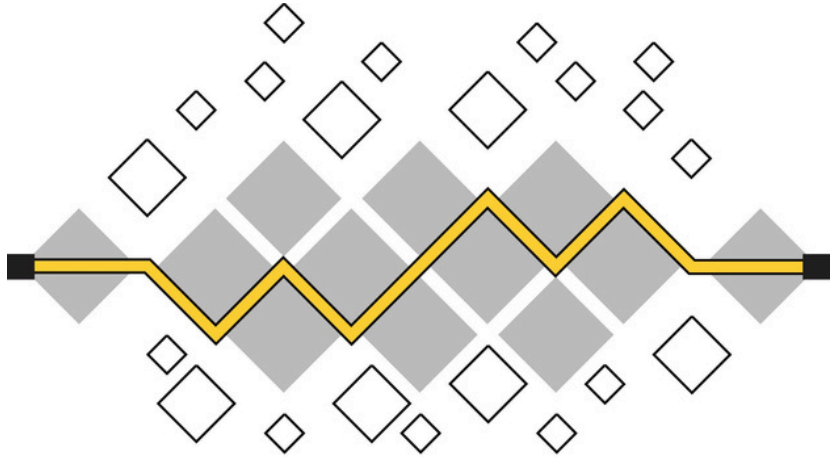
IETF 122

Nick Sullivan
nicholas.sullivan+ietf@gmail.com

WHAT WOULD YOU SAY YOU DO HERE?



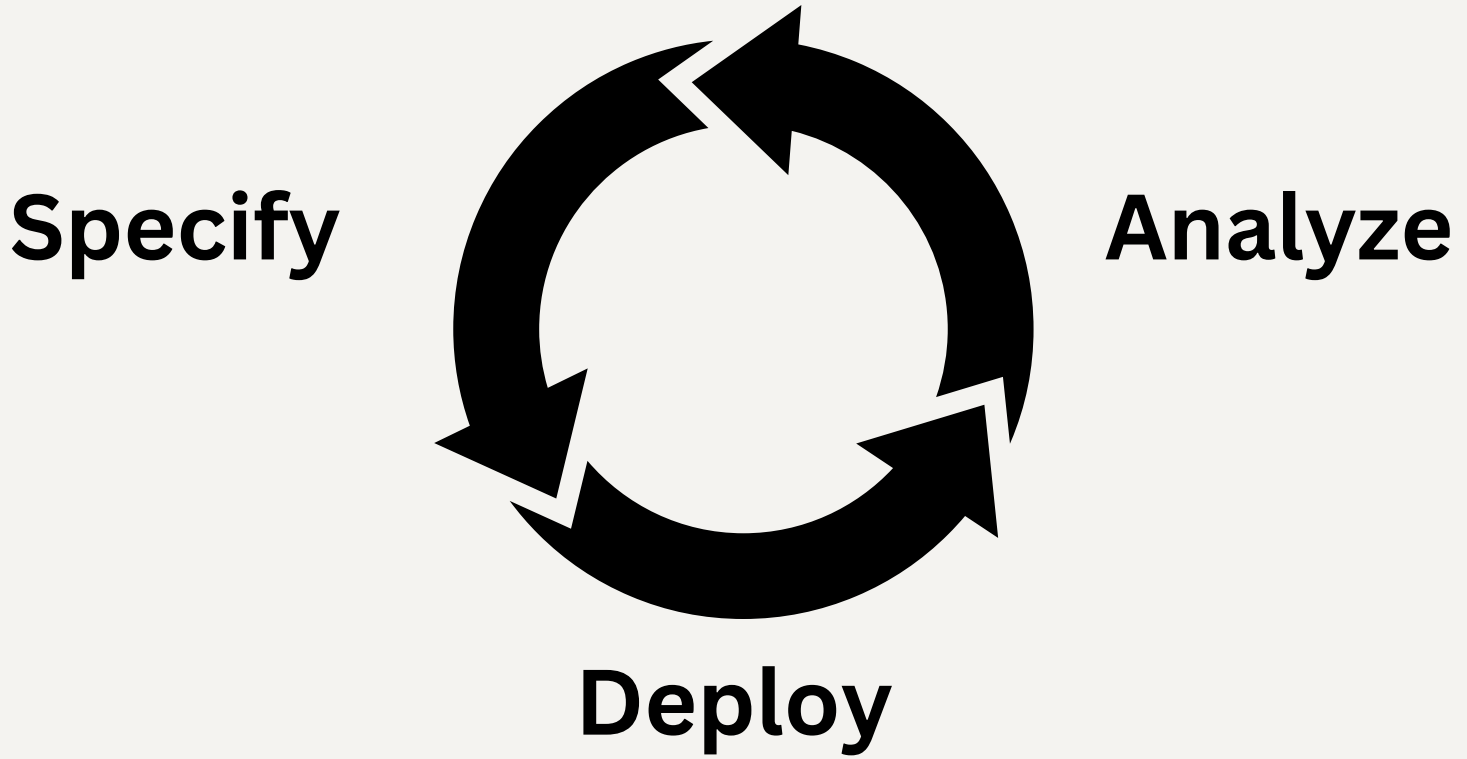
I E T F®



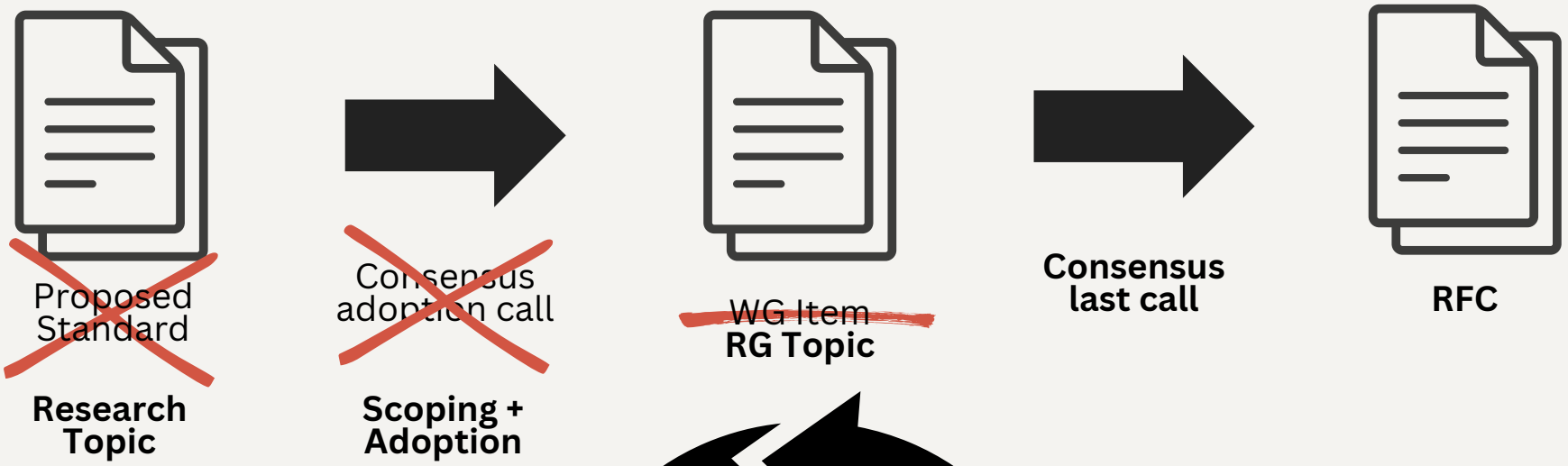
I R T F

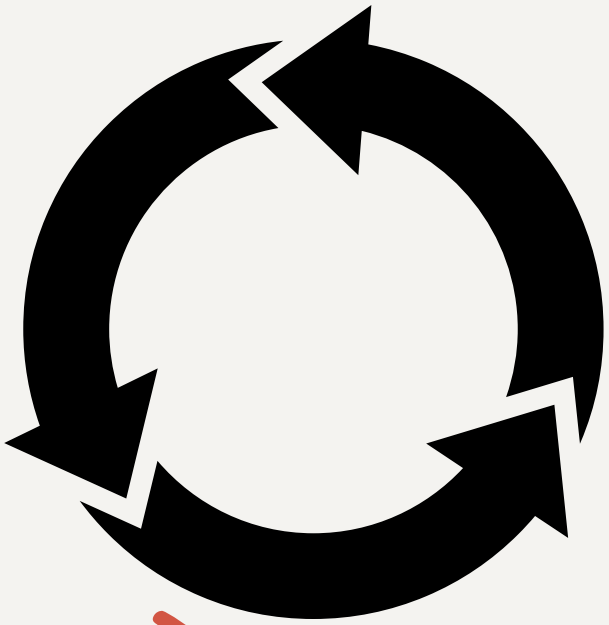
122nd IETF CFRG Research Group

TYPICAL IETF WORKING GROUP (STANDARDS TRACK)



TYPICAL IRTF RESEARCH GROUP (INFORMATIONAL TRACK)





Specify

Do Research

Analyze

Validate

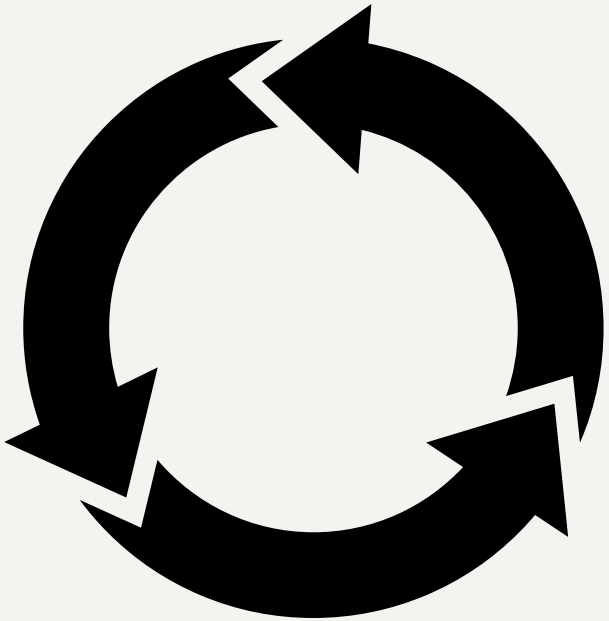
(scope and correctness)

Deploy

Write Report

CRYPTO FORUM RESEARCH GROUP

Literature Review



Validate
(scope and correctness)

Write It Down

SCOPING

- How big is this question?
- Which IETF groups need an answer?
- How many aspects of this problem need to be studied so we don’t have to revisit the question?
- Are there any practical requirements? (such as performance, size, security, etc.)

LITERATURE REVIEW

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

WRITE IT DOWN

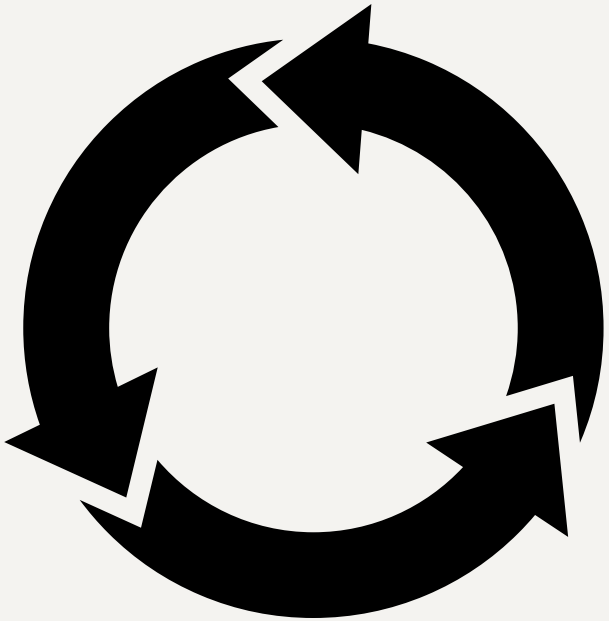
- *Collaborative* writing process
- Editors chosen by chairs
- One or more documents
- Pseudocode and test vectors
- Validate against implementations

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

Contest format + Requirements document

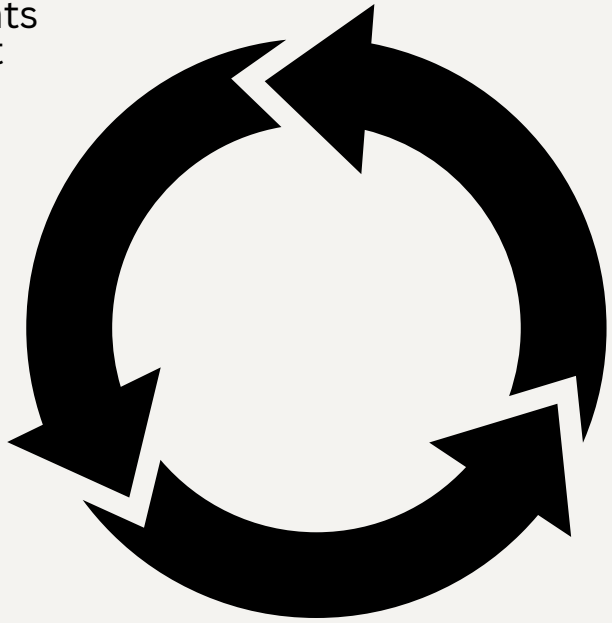
RG Topic

Consensus last call

RFC 8125 + CPace + OPAQUE

Literature Review

Candidate Draft Submissions



Validate

(scope and correctness)

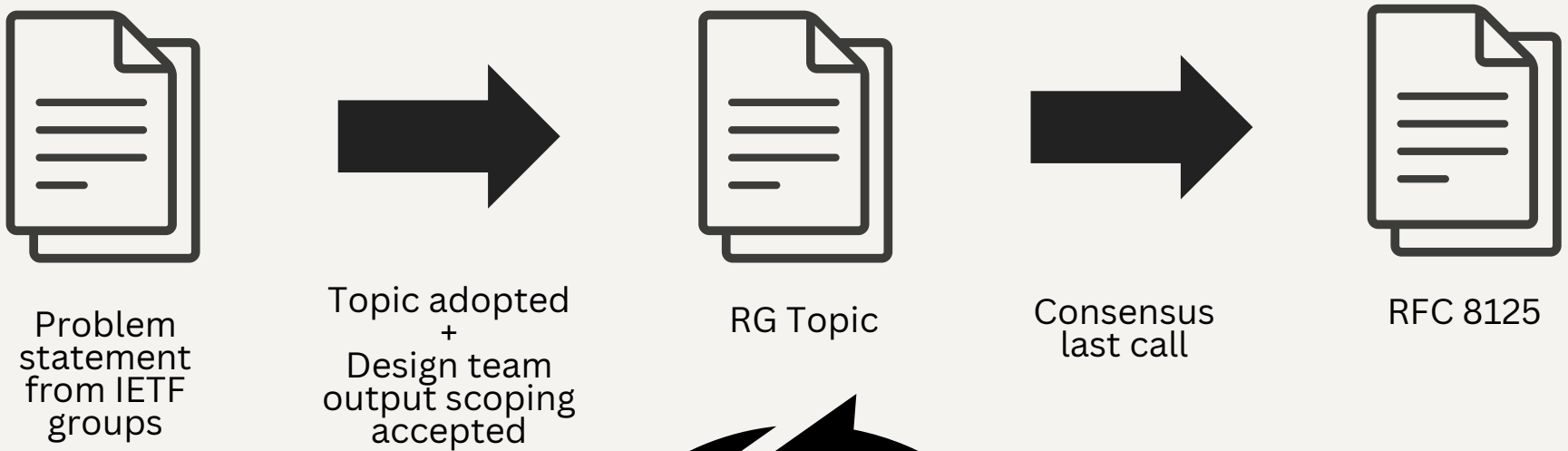
Expert reviews
Results discussed on list
Chairs adopt CPace and OPAQUE

Write It Down

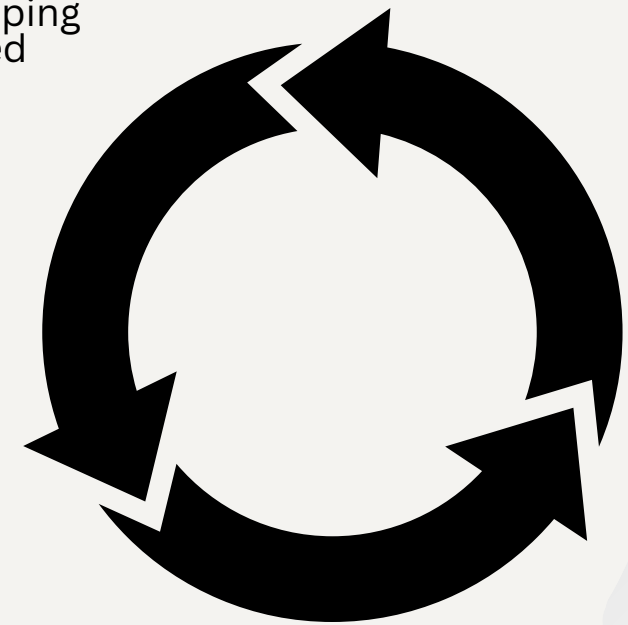
VELOCITY

- Overall complexity of the work
- Urgency (driven by IETF and other “network security in general”)
- Efficient editorial management of community feedback

PROBLEM: WE NEED HYBRID KEMS



Literature Review

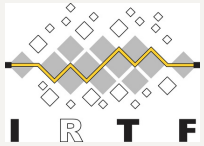


Validate

(scope and correctness)

Write It Down

QUESTIONS FOR THE GROUP



- Who has read the design team output/scoping?
- Who has read draft-irtf-cfrg-hybrid-kems-03?
- Does the draft match the scope laid out by the design team?
- The design team output was confirmed eight months ago; is the velocity of this draft sufficient?
- If not, who's willing to help this collaborative writing process?

- Given the urgency expressed by IETF groups needing a stable reference, is there a compelling reason to relitigate the scoping?

KEM COMBINERS PROCESS UPDATE

IETF 122

Nick Sullivan
nicholas.sullivan+ietf@gmail.com