

How do we standardize cryptography at the IETF?

—
A proposal for clearer publication pathways
between CFRG and IETF working groups

NICK SULLIVAN

LANE 1 / CFRG / IRTF STREAM

Cryptographic foundation

Mechanism spec or security considerations. No wire formats, no code points, no IANA registries.



LANE 2 / IETF WG / STANDARDS TRACK

Protocol profiles

Wire formats, code points, IANA registries. Normatively references Lane 1.
Where interoperability lives.

What is broken today

PROBLEM ONE

WGs use primitives without crypto panel review

Working groups use cryptographic primitives (KDFs, nonce schemes) that have not received review from the crypto panel on their use in protocols. The result ends up on the Standards Track without that guidance.

PROBLEM TWO

Crypto issues surface at Last Call

Protocol documents reach IETF Last Call or IESG review before anyone spots the crypto gaps. Fixing them at that stage adds months and forces design changes under time pressure.

Fixing design issues under time pressure forces compromises

Delays affect not just one WG but every downstream consumer

Review done at Last Call has no memory: the same gaps recur in the next WG

The two-lane model

LANE 1 / CFRG / IRTF STREAM

Cryptographic foundation

Mechanism spec or security considerations.
No wire formats, no code points, no IANA registries.

MECHANISM SPEC

SEC CONSIDERATIONS

IRTF STREAM

LANE 2 / IETF WG / STANDARDS TRACK

Protocol profiles

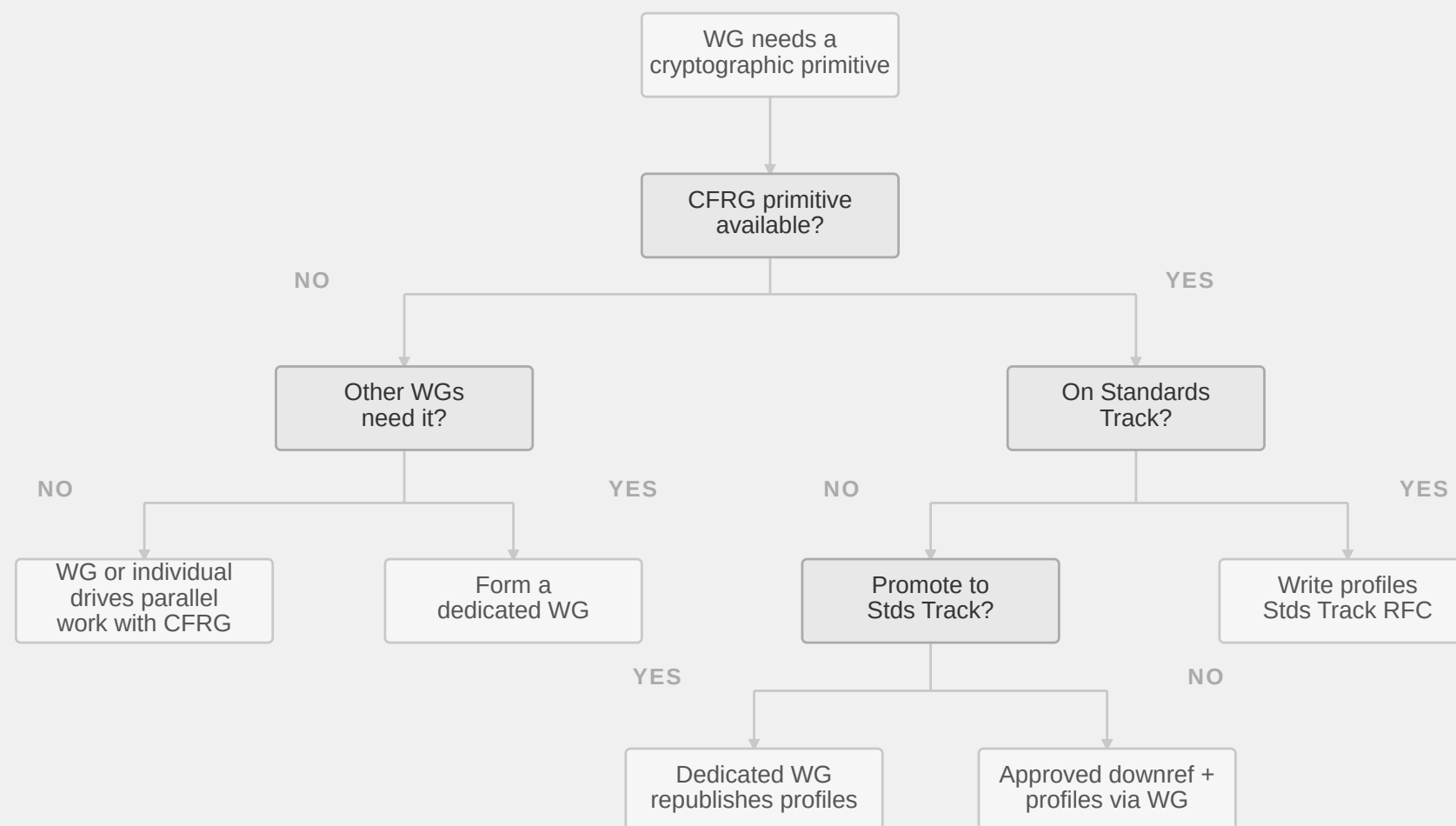
Wire formats, code points, IANA registries.
Normatively references Lane 1.

WIRE FORMATS

CODE POINTS

STDS TRACK

Also describes pathways for when no CFRG primitive exists yet, when a dedicated WG is needed, and when an approved downref suffices instead of promotion.



PATH TAKEN

Privacy Pass

VOPRF (RFC 9497) + Blinded RSA (RFC 9474) + Privacy Pass WG

1 CFRG primitive available? NO

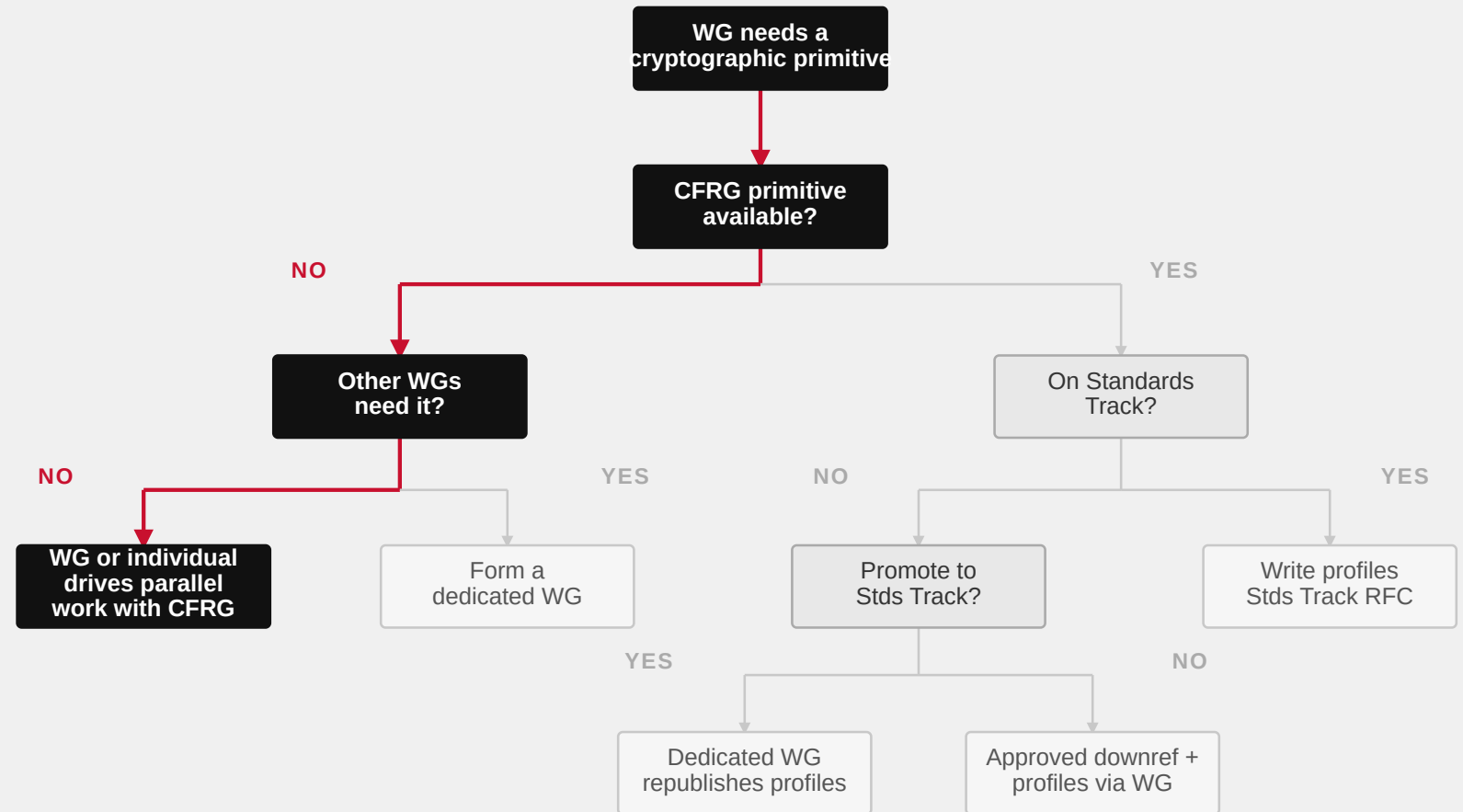
Neither VOPRF nor Blinded RSA existed yet; Privacy Pass WG needed both

2 Other WGs need it? NO

Only Privacy Pass required these primitives at that point

3 WG drives parallel work with CFRG

PP WG owned protocol and codepoints; CFRG standardized VOPRF and Blinded RSA in tandem

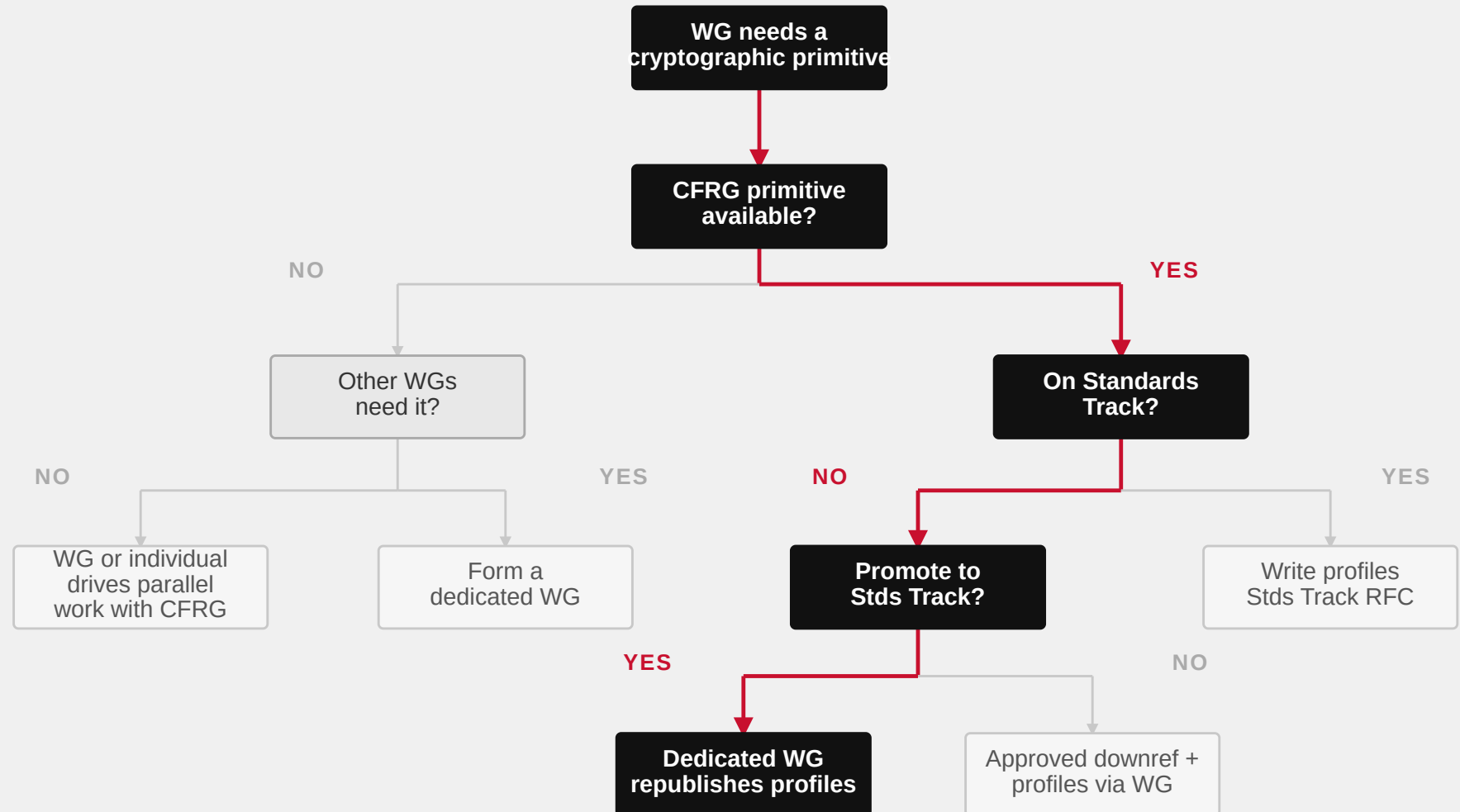


PATH TAKEN

HPKE

RFC 9180 (IRTF) + HPKE WG Standards Track RFC

- 1 CFRG primitive available? YES**
 HPKE (RFC 9180) published on IRTF stream
- 2 On Standards Track? NO**
 RFC 9180 is Informational; one-stage KDF design raised concerns for Standards Track use
- 3 Promote to Stds Track? YES**
 HPKE WG chartered to resolve KDF issues, add errata, and PQ ciphersuites (ML-KEM)
- 4 Dedicated WG republishes profiles**
 HPKE WG produces Standards Track RFC; protocol WGs reference it normatively

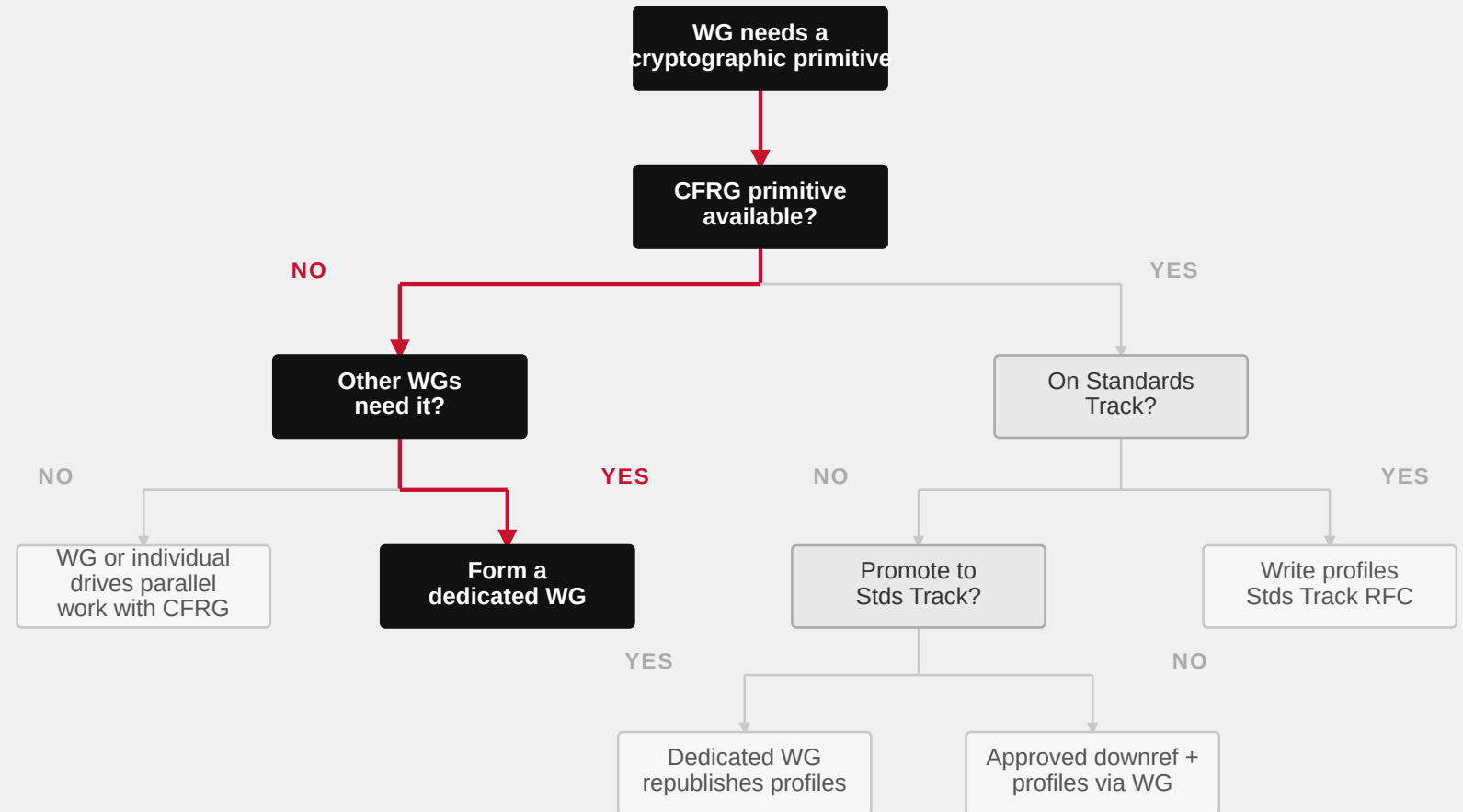


PROPOSED PATH

PQ Signatures(?)

Use of ML-DSA or other non-stateful signature algorithms

- 1 CFRG primitive available? NO**
 No CFRG document covers protocol use of ML-DSA; WGs proceeding without shared security guidance
- 2 Other WGs need it? YES**
 TLS (draft-ietf-tls-mldsa), LAMPS, CMS, JOSE, SSH all active; each defining codepoints independently
- 3 Form a dedicated WG**
 Security analysis and codepoint registry once; pre-empts fragmented assumptions and redundant review across every consumer WG



Discussion

01 Is Lane 1 a feasible way to motivate consistent, useful research documents from within CFRG?

02 Are there cases where the two-lane separation creates friction rather than clarity?

03 Should this become a BCP, or is informational guidance sufficient?