Network Working Group
Internet-Draft
Intended status: Best Current Practice
Expires: 3 September 2026

N. Sullivan
Cryptography Consulting LLC

2 March 2026

Two-Lane Publication Model for Cryptographic Mechanisms
draft-sullivan-crypto-publication-00

Abstract

This document describes a repeatable publication model for cryptographic work in the IETF. It separates cryptographic mechanism specifications requiring deep security justification from protocol-oriented specifications defining interoperability, wire formats, and registries. It describes a dedicated working group model for coordinating Standards Track deployment of CFRG mechanisms and recommends use of the CFRG Crypto Review Panel to help working groups strengthen their Security Considerations text.

About This Document

This note is to be removed before publishing as an RFC.

Status information for this document may be found at https://datatracker.ietf.org/doc/draft-sullivan-crypto-publication/.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 3 September 2026.

Copyright Notice

Table of Contents

1. Introduction

The CFRG and IETF have developed effective collaboration patterns for publishing cryptographic mechanisms in IETF protocols. MLS and HPKE, Privacy Pass and VOPRF, PPM and VDAF all follow a similar structure: the Crypto Forum Research Group (CFRG) publishes mechanism specifications on the IRTF stream as Informational RFCs, and IETF working groups publish Standards Track protocol integration that references those mechanisms.

This document articulates a structured model, informed by those collaborations, for managing the boundary between CFRG mechanism development and IETF Standards Track deployment. It describes three elements: a two-lane publication model (mechanism specification vs. protocol integration), a dedicated working group template for coordinating Standards Track deployment of CFRG mechanisms across multiple protocols, and use of the CFRG Crypto Review Panel to help working groups strengthen their Security Considerations text.

In 2025, the IETF chartered the HPKE Working Group [HPKE-CHARTER] to republish [RFC9180] on the Standards Track and define post-quantum extensions. This document generalizes the HPKE WG approach into a repeatable pattern available for future mechanisms.

These collaboration patterns work well when followed deliberately. Without deliberate coordination between lanes, two recurring problems arise.

1.1. Under-Justified Cryptographic Decisions

Protocol working groups sometimes duplicate or redefine cryptographic algorithm parameters, encodings, or constructions without CFRG-level analysis. This happens when a WG perceives CFRG engagement as too slow or out-of-scope, leading to cryptographic design decisions in Standards Track documents without security proofs, test vectors, or independent review. A WG that defines a custom key derivation construction or novel nonce generation scheme has made a cryptographic design decision that warrants CFRG scrutiny, regardless of how "straightforward" the construction appears.

1.2. Late-Stage Security Surprises

Protocol working groups sometimes discover at IETF Last Call or IESG review that a document needs CFRG review, when Security Considerations text is scrutinized and assumptions about threat models, key management, or algorithm properties diverge between cryptographic experts and protocol engineers. This applies across IETF areas, not just the Security Area: any working group using cryptographic mechanisms may encounter gaps between its protocol expertise and the cryptographic properties it depends on. A document that reaches IETF Last Call without crypto review may require Crypto Panel review late in the process, adding months to publication and forcing substantive design changes under time pressure.

Working groups, area directors, and the Independent Submissions Editor retain full discretion over adoption. The normative keywords in this document describe recommended practice for those adopting this model.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "NOT RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14 [RFC2119] [RFC8174] when, and only when, they appear in all capitals, as shown here.

1.3. Terminology

Mechanism agreement: The set of documents establishing that a cryptographic mechanism is suitable for IETF use. For CFRG-authored mechanisms, this is a mechanism specification (algorithm definition, security analysis, and test vectors) published on the IRTF stream. For externally specified mechanisms, this is the external specification plus a CFRG security considerations document validating the mechanism for IETF protocol contexts. See Section 2 for the full definition of Lane 1.

Protocol profile: A Standards Track document (also called "integration document") that defines wire formats, code points, and protocol-specific usage for a given mechanism. See Section 2 for the full definition of Lane 2.

2. Two-Lane Publication Model

The two-lane publication model separates cryptographic work into two tracks. This separation follows the principle of companion algorithm documents recommended in [RFC7696] (BCP 201): base protocol specifications reference separate algorithm documents, allowing either to evolve independently.

2.1. Lane 1: Mechanism Agreement

Lane 1 establishes that a cryptographic mechanism is suitable for IETF protocol use. Two paths through Lane 1 exist, depending on where the mechanism originates.

2.1.1. CFRG-Authored Specification

When CFRG develops a mechanism, it publishes a mechanism specification on the IRTF stream as an Informational RFC. This document defines the cryptographic algorithm, construction, or primitive. It includes algorithm definition with complete mathematical description, security rationale with proofs or references to security analyses, test vectors for all specified operations, and implementation guidance covering known pitfalls.

A mechanism specification does not include protocol wire formats or encodings, protocol-specific code point assignments (TLS SignatureScheme values, JOSE algorithm names, etc.), negotiation mechanisms, or integration with specific protocol frameworks. This boundary ensures the mechanism specification can serve multiple protocols without revision, and that protocol changes do not require cryptographic re-analysis.

Example: [RFC8032] defines EdDSA as a signature scheme over twisted Edwards curves. It includes the algorithm, security analysis, and test vectors. It does not define JOSE or PKIX encodings.

2.1.2. Externally Specified Mechanisms

When a mechanism is specified through an external open process with extensive public cryptanalysis (e.g., NIST post-quantum competitions), CFRG does not need to respecify the algorithm. The external specification provides the unambiguous definition; CFRG validates security properties for IETF use cases. Lane 2 work may proceed in parallel with CFRG validation (see Section 2.2.4).

Two validation paths exist, depending on how many instantiations are under consideration:

CFRG security considerations document: When multiple instantiations of a mechanism type are candidates for IETF use, CFRG may adopt the topic of that mechanism type's use in the requested setting. The resulting document studies the set of suitable instantiations, analyzing assumptions about key management, composition with other primitives, known limitations, and parameter guidance without duplicating the external specifications.

Crypto Panel review: When a single instantiation is under consideration, Crypto Panel review (Section 3) of the working group's profile document is sufficient. A full CFRG security considerations document is not required.

In some cases, CFRG adoption of the security considerations topic is sufficient for Lane 2 work to proceed; publication is not a prerequisite. Lane 2 authors coordinate with the evolving CFRG document on changes and test vectors.

2.1.3. Mechanism Registries

Mechanism specifications SHOULD NOT create IANA registries. Two categories of registries exist, with different ownership models:

Mechanism-level registries: Algorithm identifiers that must be consistent across all consuming protocols. Example: HPKE's KEM, KDF, and AEAD suite identifiers. These are unavoidable when the mechanism itself defines parameterized constructions.

Protocol-specific registries: Code points within a particular protocol's namespace. Example: TLS SignatureScheme values, JOSE algorithm names, COSE algorithm identifiers. These belong in protocol profile documents, not mechanism specifications.

When mechanism-level registries exist, a dedicated WG or consuming protocol provides the long-term maintenance path on the Standards Track. See Section 2.5 for guidance on registry ownership and errata resolution.

2.2. Lane 2: Protocol Profiles (IETF Stream)

Lane 2 produces Standards Track documents that make a mechanism usable in IETF protocols. The choice depends on scope and novelty:

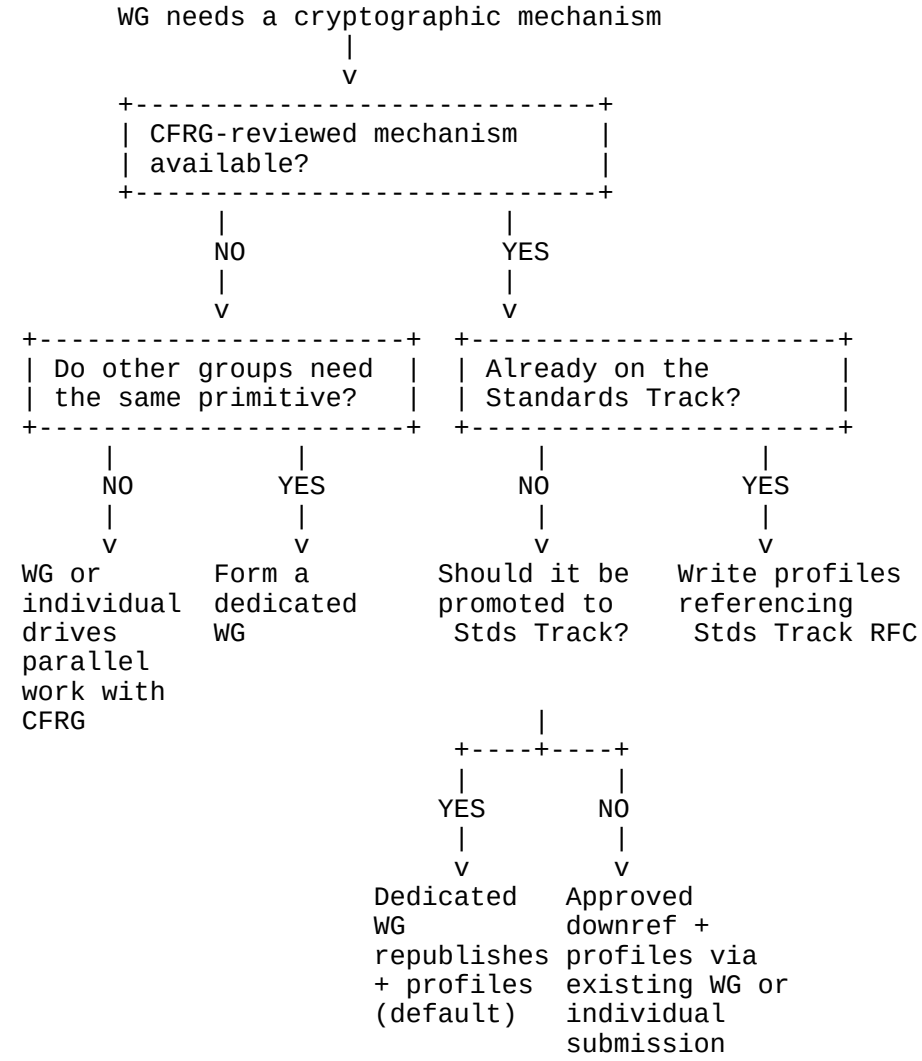

Figure 1: Lane 2 decision tree

"CFRG-reviewed" in Figure 1 includes both mechanisms that CFRG itself produced and externally specified algorithms that CFRG has validated for IETF use cases. For externally specified algorithms, CFRG validates security properties for IETF protocol contexts without respecifying the algorithm. See Section 2.1.2.

2.2.1. Existing WG Adoption

When an existing working group is the primary consumer of a mechanism and cross-area coordination is minimal, that WG may adopt both the mechanism republication and its protocol profile. The WG requests Crypto Panel review to cover cryptographic aspects outside its core expertise. This avoids creating a new WG while keeping work within established IETF process.

2.2.2. Individual Submission

When no existing working group covers the protocol domain, an individual submission produces a profile without forming a working group. Two paths exist depending on the target stream:

* AD-sponsored: The responsible AD sponsors a Standards Track profile through IESG review. The author requests CFRG Crypto Review Panel analysis.

* ISE: The Independent Submissions Editor sponsors an Informational profile on the Independent stream. This path is appropriate for regional or special-purpose profiles (e.g., regionally mandated algorithm suites) that do not target the Standards Track.

Independent submissions generally cannot create IANA registries; profiles on the Independent stream reference existing registry entries rather than creating new ones. This is the lightest-weight path for narrow-scope work.

2.2.3. Dedicated Working Groups

When multiple protocols across areas need the mechanism, a dedicated working group coordinates Standards Track integration. The WG republishes the mechanism on the Standards Track, incorporating errata and implementation experience, and coordinates per-protocol profile documents that allocate code points in protocol-specific registries.

A dedicated WG is typically warranted when three or more protocol domains need profiles (e.g., TLS, JOSE, COSE, PKIX), the scope is bounded with clear technical consensus, and cross-area coordination justifies a dedicated venue.

Proponents may propose charters through existing dispatch mechanisms ([RFC7957], secdispatch). A BoF [RFC5434] is not required if ADs and relevant WG chairs agree the work is uncontroversial and scope is well-defined. The responsible AD determines the appropriate path: a BoF for complex or controversial scope, dispatch through secdispatch, or direct charter sponsorship ([RFC3710]).

The charter MUST reference the specific mechanism specification being profiled and enumerate the protocol domains in scope (e.g., "TLS code points and PKIX encodings for X"). It MUST state explicit non-goals (e.g., "this WG will not redesign the cryptographic mechanism") and include a scope lock prohibiting expansion. The timeline SHOULD be aggressive: 12-18 months.

The WG exists to publish, not to redesign. The charter may permit targeted changes based on implementation experience: resolving errata, removing unused features, aligning with IETF formatting requirements.

The WG SHOULD maintain a registry of consuming WGs and their profile requirements to ensure complete coverage. The charter SHOULD include a sunset clause: the WG closes upon completing its enumerated deliverables.

2.2.3.1. Example: HPKE

The HPKE Working Group, chartered in 2025 [HPKE-CHARTER], serves as the first instance of this pattern. It was chartered without a BoF, with AD sponsorship, to republish [RFC9180] on the Standards Track and define post-quantum algorithm suites. The WG uses the consolidated approach: a single Standards Track document that is both the mechanism republication and the registry definition for consuming protocols. The charter explicitly constrained scope, excluding redesign of the HPKE mechanism itself.

See Appendix A for a sample charter template.

2.2.4. Timing Models

Regardless of which Lane 2 approach is used, two timing models exist for when profile work begins:

Post-publication: The mechanism RFC exists before profile work starts. This avoids coordination risk and leads to tighter alignment between CFRG and IETF milestones, resulting in more predictable timelines.

Parallel: Profile work begins while CFRG is still developing the

mechanism. This carries coordination risk: if the mechanism changes, profile work may need revision. ADs considering parallel work should assess mechanism stability with CFRG chairs before proceeding. Profiles cannot publish until the mechanism RFC exists (normative reference), but can reach IESG review shortly after.

2.2.5. Profile Document Contents

Regardless of which approach produces it, a protocol profile integrates the mechanism into a specific protocol context:

* Wire format definitions (byte layouts, ASN.1 modules, JSON structures)
* IANA code point assignments for that protocol's registries
* Negotiation and algorithm selection mechanisms
* Normative reference to the mechanism specification
* Protocol-specific security considerations

A protocol profile runs 5-15 pages. It normatively references the mechanism specification and focuses on interoperability within its protocol domain.

Examples: [RFC8037] defines JOSE encodings for EdDSA. [RFC8410] defines PKIX encodings. Both reference [RFC8032] and are Standards Track.

2.2.6. Entry Criteria

Two situations trigger this coordination path, depending on whether the mechanism already exists.

Republication of an existing CFRG mechanism: A published CFRG mechanism is a candidate for Standards Track promotion when it is referenced as a de facto standard by multiple IETF Standards Track protocols and has verified errata with security or functionality impact. When both conditions hold, Standards Track republication is warranted. When only the first holds, the Downref Registry may suffice. When only the second holds, a CFRG -bis revision may be more appropriate.

New mechanism requiring Standards Track integration: When CFRG has

adopted a mechanism topic and multiple protocols have expressed integration intent, the coordination path described here sequences parallel Lane 2 work. ADs considering parallel work should assess mechanism stability with CFRG chairs before proceeding.

2.2.7. Scope

Scope depends on the mechanism's condition:

Clean mechanism (no blocking errata, ready for deployment): The coor dination effort produces Standards Track profiles and optionally republishes the mechanism for status alignment. Republication eliminates downref requirements but is not mandatory if profiles can reference the Informational RFC directly.

Mechanism with accumulated technical debt (unresolved errata,

ambiguities, implementation divergence): The effort republishes the mechanism on the Standards Track with fixes, then produces updated profiles. The CFRG Crypto Review Panel validates that fixes preserve cryptographic properties. Consuming WGs coordinate reference updates.

Example: An EdDSA coordination effort could resolve [RFC8032]'s cofactor ambiguity, incorporate held errata, and produce a Standards Track specification that consuming protocols reference.

The scope MUST NOT permit new cryptographic modes or substantial algorithm modifications. Profile work may involve updating recommended code points in alignment with ongoing or completed CFRG work, or with Crypto Panel review. Protocol profiles may include design decisions specific to integration (parameter restrictions, serialization choices, negotiation strategies). These protocol-level design decisions are in scope; changes to the underlying cryptographic mechanism are not.

2.3. Coordination Between Lanes

The two-lane model requires a coordination point between CFRG (upstream mechanism owner) and the protocols that consume the mechanism (downstream integrators). For a dedicated working group, the WG fills this role. For existing WG adoption, that WG does. For an individual submission, the author and sponsoring AD coordinate directly.

Upstream coordination with CFRG: The coordination point is the

single contact for errata resolution, ambiguity clarification, and mechanism updates. CFRG addresses technical questions once rather than responding to N consuming protocols independently.

Downstream coordination with consumers: Protocols that need code points or profiles register those needs with the coordination point, which sequences work: mechanism republication first, then profiles in parallel. This aligns timelines so consumers can plan milestones around the mechanism's Standards Track availability rather than managing independent downref approvals.

Coordination mechanisms include cross-posted review requests, cross-area review discussions, and inviting chairs or designees of consuming WGs to participate.

The two-lane separation also raises practical questions about normative references, registry ownership, errata resolution, and change control. The following subsections address these.

2.4. Normative Reference Rules

Protocol profiles normatively reference mechanism specifications. When the mechanism specification is Informational or Experimental (IRTF stream), this creates a downward reference (downref) as defined in [RFC3967]. The IETF maintains a Downref Registry and established IESG procedures that handle individual downrefs adequately.

A side-effect of the two-lane model is reducing the number of downref exceptions. When a mechanism is republished on the Standards Track, subsequent protocol profiles reference the Standards Track version with no downref required. This is not a driving motivation for the model, but a measurable signal that it reduces coordination overhead.

Two resolution paths exist:

* Approved downref: The IESG approves the downref and adds it to the Downref Registry. This is appropriate when the mechanism is stable, widely reviewed, and referenced by few Standards Track documents.

* Standards Track republication: A dedicated WG (Section 2.2.6) republishes the mechanism on the Standards Track, eliminating the downref for all current and future consumers. This is appropriate when the mechanism is widely referenced as a de facto standard.

2.5. IANA Considerations Placement

2.5.1. Registry Ownership

While IRTF documents can create IANA registries, CFRG is not well-positioned for long-term document maintenance. CFRG's value is cryptographic analysis: security proofs, parameter validation, construction review. Registry administration is not.

Protocol-specific registries belong in profile documents, not mechanism specifications. Registry ownership depends on the publication approach. A dedicated WG may consolidate all registries (mechanism-level and protocol code points) in a single Standards Track document, or coordinate separate profile documents where each consuming protocol maintains its own registry allocations. When mechanism-level registries exist in CFRG documents, a dedicated WG or consuming protocol provides the maintenance path on the Standards Track. The mechanics of transferring registry ownership from an IRTF document to a Standards Track document should be confirmed with IANA; the HPKE WG [HPKE-CHARTER] provides an example. See Section 2.2.3 for charter guidance.

2.5.2. Errata and Maintenance

Informational RFCs accumulate errata marked "Hold for Document Update" [I-D.rpc-errata-process]. CFRG can publish -bis revisions as Informational to address these. The Standards Track path provides an alternative with additional benefits: clear document ownership, established IETF maintenance procedures, and elimination of downref requirements for consuming protocols.

The model provides a decision framework for when each path is appropriate. A mechanism that is referenced as a de facto standard by multiple IETF Standards Track protocols and has verified errata with security or functionality impact is a candidate for Standards Track promotion. See Section 2.2.6 for entry criteria.

[RFC9180] (HPKE) and [RFC8554] (LMS) are CFRG documents that created IANA registries. HPKE is now being retrofitted: the HPKE WG [HPKE-CHARTER] is republishing it on the Standards Track, taking over registry ownership and providing a clear home for code point allocation as post-quantum suites are added.

2.6. Change Control Boundaries

When a mechanism is republished on the Standards Track, the IETF owns the resulting document and any subsequent revisions. CFRG retains cryptographic review authority: substantive changes to the algorithm or security properties require CFRG Crypto Review Panel analysis before IETF publication. This division places document maintenance (errata resolution, bis revisions) within IETF process while ensuring cryptographic expertise guides substantive changes.

Protocol working groups own protocol profile evolution: code point assignments, wire format changes, and integration updates. Cryptographic expertise stays with CFRG. Protocol-specific details stay with domain experts.

3. CFRG Crypto Review Panel

The CFRG maintains a Crypto Review Panel [CFRG-PANEL] that provides expert cryptographic analysis for documents across the IETF and IRTF. The panel's members are primarily external cryptographic experts who bring independent analytical capability. While primarily used by Security Area working groups, the panel is available to any WG whose documents include cryptographic mechanisms.

To request review, an AD, WG chair, or author contacts the CFRG chairs, who assign a panel reviewer based on the document's cryptographic content. The ISE may also request review for independent submissions. Panel findings do not bind the WG or responsible AD, who decide how to address them. The responsible AD determines whether Crypto Panel review is needed before IESG approval, based on cryptographic complexity.

If the panel demonstrates consistent value under increased use, the community may explore further organizational support (such as published membership rosters, documented review procedures, or datatracker integration) to sustain review capacity.

3.1. What Is Reviewed

The panel focuses on cryptographic correctness and appropriateness, not general protocol design. Review areas include:

* Cryptographic justification for algorithm choices
* Security Considerations text covering algorithm-specific risks
* Correctness of algorithm usage (modes, parameters, contexts)

* Parameter choices (key sizes, nonce handling, iteration counts)

* Composition of primitives (KDF chains, AEAD usage, etc.)

* Externally specified algorithms proposed for IETF use: validating that security claims hold in IETF protocol contexts

The panel does not duplicate Security Area Directorate review. Working groups may request targeted reviews of specific cryptographic usage (e.g., "review our use of HKDF in this context") without requiring a full document review.

3.2. Requesting Review

Review is warranted when a draft defines cryptographic behavior beyond what existing CFRG specifications cover: novel constructions, non-standard parameter choices, or security claims that rely on unanalyzed cryptographic properties. Review is generally not needed when a draft uses CFRG-published mechanisms as specified, defining only wire formats, code points, or protocol integration.

Working groups SHOULD request review before WG Last Call, ideally when the Security Considerations section nears completion. The panel targets 2-4 weeks for review completion. WGs introducing novel cryptographic constructions should consult the panel during design, not after. Appendix B provides a complete pre-WG-Last-Call checklist.

The WG documents the disposition of each finding (accepted, rejected with rationale, or overtaken by design changes). The Crypto Panel may recommend routing a document through CFRG if the work involves novel mechanisms requiring deeper research community review.

4. National Cryptography

The two-lane model applies to all cryptographic mechanisms. This section addresses algorithms that have not undergone broad open international review and whose adoption is primarily driven by regulatory compliance.

4.1. Definition

This section uses the term "national cryptography" as shorthand for algorithms where:

* Public cryptanalysis and independent review are limited relative to algorithms selected through open international processes

* Adoption is driven by regulatory compliance in a specific jurisdiction rather than broad cryptographic community consensus

Algorithms that have undergone extensive public review enter IETF protocols through the main flowchart path (Figure 1). The guardrails below apply to algorithms that have not.

4.2. Risks and Challenges

Algorithms in this category create tension between regional regulatory compliance and global protocol interoperability. When a regulator mandates algorithm X for domestic deployments, the IETF must decide whether and how to accommodate X without fragmenting the global protocol baseline.

Incorporating such algorithms without sufficient safeguards produces four problems. First, regulatory mandates create compliance pressure that overrides global interoperability, fragmenting protocols into regional variants. Second, algorithms without extensive public cryptanalysis carry higher risk of undiscovered weaknesses. Third, algorithms with limited global deployment inflate IANA registries and increase implementation complexity for marginal benefit. Fourth, algorithms perceived as government-controlled raise concerns about backdoors regardless of technical merit.

These risks motivate the guardrails below.

4.3. Guardrails and Best Practices

The following practices manage the risks above while preserving regional extensibility. These guardrails are process-based: they apply to any algorithm that has not undergone broad open international review, regardless of origin. Algorithms that have undergone extensive public review enter through the main path (Figure 1). Algorithms without such review appear in separate optional profile documents that reference the algorithm’s authoritative specification (whether a national standard, an Informational RFC, or an independent submission). They do not modify core protocol specifications or base mechanism documents.

Optional profiles: Algorithms without broad international review SHOULD be specified in separate optional profile documents, not embedded in core protocol specifications. This preserves a globally interoperable baseline while allowing regional extensions. [RFC8998] is an example of this pattern for TLS 1.3 [RFC8446].

Recommendation marking: Where IANA registries include a

"Recommended" column, working groups MAY choose to only recommend algorithms that have CFRG approval. See [RFC9367] for an example.

Registry policy: Registries for cryptographic algorithms SHOULD maintain "RFC Required" or "Specification Required" [RFC8126] policies with designated expert review. Early allocation and private use ranges mitigate pressure for premature standardization.

Crypto Panel review required: Algorithms entering through this path MUST receive Crypto Panel review. Lack of public cryptanalysis is grounds for rejection or marking as Not Recommended.

Code point coordination: Algorithms appearing in multiple protocols SHOULD coordinate all registrations together to avoid redundant or conflicting identifiers.

4.4. Example: NIST Post-Quantum Algorithms

Algorithms selected through open international competitions with extensive public cryptanalysis illustrate the main-path model for well-reviewed external algorithms. Such algorithms enter IETF protocols through the main flowchart path (Figure 1): externally specified, CFRG-reviewed via security considerations documents, then working groups write protocol profiles. The guardrails in this section do not apply because these algorithms have undergone extensive public review.

4.5. Neutral Language

Documents involving algorithms in this category MUST use neutral, technical language focused on interoperability and security properties. Political or geopolitical framing is inappropriate. Factual statements about algorithm provenance, standardization body, and public analysis status are acceptable and encouraged for transparency.

5. Security Considerations

This document defines processes and best practices; it does not specify protocols or cryptographic algorithms directly.

The two-lane model is designed to improve security outcomes by routing cryptographic mechanisms through focused expert review in CFRG while protocol integration receives appropriate review in working groups. Separating these concerns is intended to reduce the risk of cryptographic errors during protocol design and provide a structured path for applying CFRG Crypto Review Panel expertise to documents across the IETF and IRTF.

Concentrating cryptographic review in a small panel creates process risks: reviewer availability can bottleneck publication, and a narrow reviewer pool may develop blind spots. Mitigations include maintaining diverse panel membership, publishing review criteria, and preserving AD discretion to proceed when panel review is unavailable or disputed.

6. IANA Considerations

This document has no IANA actions.

7. References

7.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, DOI 10.17487/RFC2119, March 1997, <https://www.rfc-editor.org/rfc/rfc2119>.

[RFC3967] Bush, R. and T. Narten, "Clarifying when Standards Track Documents may Refer Normatively to Documents at a Lower Level", BCP 97, RFC 3967, DOI 10.17487/RFC3967, December 2004, <https://www.rfc-editor.org/rfc/rfc3967>.

[RFC7696] Housley, R., "Guidelines for Cryptographic Algorithm Agility and Selecting Mandatory-to-Implement Algorithms", BCP 201, RFC 7696, DOI 10.17487/RFC7696, November 2015, <https://www.rfc-editor.org/rfc/rfc7696>.

[RFC8126] Cotton, M., Leiba, B., and T. Narten, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 8126, DOI 10.17487/RFC8126, June 2017, <https://www.rfc-editor.org/rfc/rfc8126>.

[RFC8174] Leiba, B., "Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words", BCP 14, RFC 8174, DOI 10.17487/RFC8174, May 2017, <https://www.rfc-editor.org/rfc/rfc8174>.

7.2. Informative References

[CFRG-PANEL]
"CFRG Crypto Review Panel", 2024,
<https://wiki.ietf.org/group/cfrg/CryptoPanel>.

[CHALKIAS] Chalkias, K., Garillot, F., and V. Nikolaenko, "Taming the many EdDSAs", 2020, <https://eprint.iacr.org/2020/1244>.

[HPKE-CHARTER]
"Hybrid Public Key Encryption (hpke) Charter", May 2025,
<https://datatracker.ietf.org/doc/charter-ietf-hpke/>.

[I-D.rpc-errata-process]
Russo, A. and J. Mahoney, "Current Process for Handling RFC Errata Reports", Work in Progress, Internet-Draft, draft-rpc-errata-process-04, 29 August 2025, <https://datatracker.ietf.org/doc/html/draft-rpc-errata-process-04>.

[RFC3710] Alvestrand, H., "An IESG charter", RFC 3710, DOI 10.17487/RFC3710, February 2004, <https://www.rfc-editor.org/rfc/rfc3710>.

[RFC5434] Narten, T., "Considerations for Having a Successful Birds-of-a-Feather (BOF) Session", RFC 5434, DOI 10.17487/RFC5434, February 2009, <https://www.rfc-editor.org/rfc/rfc5434>.

[RFC7748] Langley, A., Hamburg, M., and S. Turner, "Elliptic Curves for Security", RFC 7748, DOI 10.17487/RFC7748, January 2016, <https://www.rfc-editor.org/rfc/rfc7748>.

[RFC7957] Campbell, B., Ed., Cooper, A., and B. Leiba, "DISPATCH-Style Working Groups and the SIP Change Process", BCP 67, RFC 7957, DOI 10.17487/RFC7957, August 2016, <https://www.rfc-editor.org/rfc/rfc7957>.

[RFC8032] Josefsson, S. and I. Liusvaara, "Edwards-Curve Digital Signature Algorithm (EdDSA)", RFC 8032, DOI 10.17487/RFC8032, January 2017, <https://www.rfc-editor.org/rfc/rfc8032>.

[RFC8037] Liusvaara, I., "CFRG Elliptic Curve Diffie-Hellman (ECDH) and Signatures in JSON Object Signing and Encryption (JOSE)", RFC 8037, DOI 10.17487/RFC8037, January 2017, <https://www.rfc-editor.org/rfc/rfc8037>.

[RFC8410] Josefsson, S. and J. Schaad, "Algorithm Identifiers for Ed25519, Ed448, X25519, and X448 for Use in the Internet X.509 Public Key Infrastructure", RFC 8410, DOI 10.17487/RFC8410, August 2018, <https://www.rfc-editor.org/rfc/rfc8410>.

[RFC8446] Rescorla, E., "The Transport Layer Security (TLS) Protocol Version 1.3", RFC 8446, DOI 10.17487/RFC8446, August 2018, <https://www.rfc-editor.org/rfc/rfc8446>.

[RFC8554] McGrew, D., Curcio, M., and S. Fluhrer, "Leighton-Micali Hash-Based Signatures", RFC 8554, DOI 10.17487/RFC8554, April 2019, <https://www.rfc-editor.org/rfc/rfc8554>.

[RFC8998] Yang, P., "ShangMi (SM) Cipher Suites for TLS 1.3", RFC 8998, DOI 10.17487/RFC8998, March 2021, <https://www.rfc-editor.org/rfc/rfc8998>.

[RFC9180] Barnes, R., Bhargavan, K., Lipp, B., and C. Wood, "Hybrid Public Key Encryption", RFC 9180, DOI 10.17487/RFC9180, February 2022, <https://www.rfc-editor.org/rfc/rfc9180>.

[RFC9367] Smyshlyaev, S., Ed., Alekseev, E., Griboedova, E., Babueva, A., and L. Nikiforova, "GOST Cipher Suites for Transport Layer Security (TLS) Protocol Version 1.3", RFC 9367, DOI 10.17487/RFC9367, February 2023, <https://www.rfc-editor.org/rfc/rfc9367>.

Appendix A. Charter Template

The following sample template is provided for area directors chartering dedicated working groups that deploy CFRG cryptographic mechanisms. Text in brackets should be replaced with context-specific content.

[XYZ] Working Group Charter

Background and Motivation:

[For post-publication charters:]
The IETF Crypto Forum Research Group (CFRG) has published [RFC xxxx], which specifies [mechanism name], a [brief description].

[For parallel charters:]
The IETF Crypto Forum Research Group (CFRG) has adopted [draft-irtf-cfrg-xxx], which specifies [mechanism name], a [brief description]. CFRG expects to publish this mechanism as an RFC in [timeframe].

[Common text:]
This mechanism has applications in [list key use cases]. Multiple IETF working groups have expressed interest in integrating [mechanism name] into their protocols, including [WG1], [WG2], and [WG3].

To ensure consistent and secure integration across protocols, the [XYZ] working group will coordinate Standards Track specifications for [mechanism name] deployment in IETF protocols.

Scope:

The working group will produce the following deliverables:

1. Standards-Track Specification (optional):
   [For post-publication:] Produce a Standards Track version of the CFRG mechanism specification suitable for normative reference. This document owns any mechanism-level registries (e.g., algorithm identifiers used across protocols) and eliminates downref requirements for consuming protocols.
   [For parallel:] Protocol profiles are the primary deliverable. Mechanism republication is deferred until CFRG publishes and may be omitted if profiles can reference the CFRG RFC directly.

2. Protocol Profiles:
   Standards Track RFCs defining integration of [mechanism name] into:
   - [Protocol 1] ([target RFC, e.g., TLS 1.3, JOSE, etc.])
   - [Protocol 2]
   - [Protocol 3]
   Each profile will allocate code points in protocol-specific registries, define serialization formats and parameter restrictions, and specify protocol-specific security considerations.

3. Algorithm Updates and Extensions (optional):
   The WG may add new algorithm parameters using CFRG-approved primitives (e.g., post-quantum suites) and resolve errata or clarifications identified through implementation experience. Substantial changes to cryptographic constructions require CFRG review; the WG coordinates with CFRG for such changes.

Out of Scope:

- New cryptographic mechanism research (belongs in CFRG)
- Protocol redesign unrelated to [mechanism name] integration
- [Other specific exclusions]

Working Methods:

The working group will operate on an accelerated timeline with tight scope control. The WG will:

- Hold virtual interim meetings as needed for rapid iteration
- Coordinate with [relevant WGs] to avoid duplicate work
- Request CFRG Crypto Review Panel review of all profile documents
- Sunset after delivering chartered items (typically 12-18 months)

Milestones:

[For post-publication:]
- [Month Year]: WG formation, adopt mechanism spec (if needed)
- [Month Year]: Adopt protocol profile documents
- [Month Year]: WG Last Call on mechanism spec (if needed)
- [Month Year]: Submit mechanism spec to IESG (if needed)
- [Month Year]: WG Last Call on protocol profiles
- [Month Year]: Submit protocol profiles to IESG
- [Month Year]: WG closure

[For parallel:]
- [Month Year]: WG formation, adopt protocol profile documents
- [Month Year]: WG Last Call on protocol profiles
- [Month Year]: CFRG mechanism published (external dependency)
- [Month Year]: Adopt mechanism republication (if needed)
- [Month Year]: WG Last Call on mechanism republication (if needed)
- [Month Year]: Submit mechanism republication to IESG (if needed)
- [Month Year]: Submit protocol profiles to IESG
- [Month Year]: WG closure

Success Criteria:

The WG is successful if [mechanism name] can be deployed interoperably in [list key protocols] with consistent security properties and well-understood integration guidance. [Suggested: interoperability demonstrated by e.g. at least two independent implementations per protocol profile passing published test vectors.]

Appendix B. Pre-Last-Call Crypto Checklist

Working groups introducing cryptographic mechanisms should address these items before WG Last Call. This checklist complements formal review processes.

1. Stable algorithm specification exists: Does a published or imminent RFC specify the cryptographic mechanism in full detail, including security analysis? Or does this draft invent new cryptography?

2. Crypto Panel review completed: Has the CFRG Crypto Review Panel reviewed this document? If not, has a review request been filed with the CFRG chairs?

3. Security Considerations drafted: Does the Security Considerations section address algorithm- specific risks (key size, parameter choices, known attacks) in addition to protocol-level concerns?

4. IANA code points identified: Have algorithm identifiers, code points, or OIDs been requested in appropriate registries? Is the registration policy appropriate for cryptographic algorithms?

5. No duplicate work elsewhere: Have you confirmed that another WG or SDO is not standardizing the same algorithm integration? Check related WG charters and recent IETF Last Calls.

6. Backward compatibility considered: If extending an existing protocol, how do implementations negotiate the new algorithm? What happens when one peer does not support it?

7. Performance impact assessed: What is the computational cost compared to existing alternatives? Are there environments (IoT, constrained devices) where performance is prohibitive?

8. Recommended vs optional status decided: Should this algorithm be marked "Recommended" in IANA registries, or is it a special-purpose or regional algorithm? What is the justification?

9. Test vectors included or referenced: Are there test vectors for implementation validation? If in a separate mechanism spec, is that document normatively referenced?

10. Algorithm agility preserved: Does the design follow algorithm agility principles [RFC7696]? Can the algorithm be replaced or deprecated without redesigning the protocol?

Appendix C. Summary for ADs and Chairs

Three elements for IETF cryptographic standardization:

C.1. Two-Lane Model (Mechanism + Profiles)

Separate cryptographic mechanism specifications (CFRG Informational RFCs with full algorithm details and security analysis) from protocol profile specifications (Standards Track RFCs defining integration into specific protocols). Profiles normatively reference mechanism specs rather than duplicating algorithm text. This avoids duplication, ensures consistent security analysis, and lets one mechanism serve multiple protocols.

C.2. Coordination Path

A coordination model for moving CFRG mechanisms to the Standards Track, applicable to any Lane 2 vehicle: existing WG adoption, individual submission, or a dedicated working group. The model establishes a single coordination point between CFRG (upstream) and consuming protocols (downstream). Two timing models apply: post-publication (mechanism RFC exists) and parallel (work begins while CFRG is still developing the mechanism, with the AD assessing stability). When three or more protocol domains need profiles, a dedicated WG provides cross-area coordination. Scope prohibits new cryptographic modes or algorithm modifications, though profile work may update recommended code points in alignment with CFRG work or Crypto Panel review.

C.3. CFRG Crypto Review Panel

An optional resource to help working groups strengthen their Security Considerations text. To request review, an AD, WG chair, or author contacts the panel. This applies cryptographic expertise consistently, catches algorithm usage errors, and identifies when work should route to CFRG.

Appendix D. Example: EdDSA

The Edwards-curve Digital Signature Algorithm (EdDSA) predates this document. It did not follow the two-lane model deliberately, but its history illustrates both the accidental benefits of separation and the costs of insufficient CFRG vetting.

D.1. What Happened

CFRG published [RFC8032] (EdDSA) as an Informational RFC in January 2017. Three Standards Track profiles followed independently: [RFC8446] (TLS 1.3 code points), [RFC8037] (JOSE identifier), and [RFC8410] (PKIX OIDs). [RFC8032] served as a Lane 1 mechanism specification; the three Standards Track RFCs served as Lane 2 profiles, each normatively referencing [RFC8032] without duplicating

algorithm text.

D.2. What Went Wrong

[RFC8032]’s publication revealed gaps that additional structured review might have caught. These gaps illustrate why this document recommends more rigorous review for mechanism specifications. Consequences:

Cofactor ambiguity: [RFC8032] underspecifies validation of public key and signature components, causing implementation divergence in whether small-order elements are accepted. [CHALKIAS] documents this incompatibility across deployed implementations.

Errata backlog: Contributors filed multiple errata against [RFC8032]. Several are held for a document update that has no publication path: CFRG cannot publish Standards Track revisions and no IETF WG owns the document.

Missing security theorem: The document provides security discussion but no precise theorem statement or citation to the relevant Schnorr-family reduction. A mechanism specification under the two-lane model should cite or reproduce the formal security argument.

No coordinated profile timing: The JOSE profile ([RFC8037]) appeared simultaneously with [RFC8032] in January 2017, but the PKIX profile ([RFC8410]) took until August 2018. The Curve25519 key agreement function [RFC7748] predated [RFC8032] by a year, causing sequencing confusion about which curves were ready for which protocols.

D.3. How the Two-Lane Model Applies

Under the two-lane model, CFRG would resolve the cofactor ambiguity and produce formal security arguments before publication. A dedicated WG would then republish the vetted mechanism on the Standards Track, coordinate profile documents, and sequence work so consuming WGs can plan their milestones. The Crypto Review Panel would review profiles for correct algorithm usage: cofactor handling, context strings, cross-protocol attack prevention.

D.4. EdDSA as Pilot

The two-lane model also applies retroactively. EdDSA is a candidate for testing whether this coordination model is repeatable: it meets both decision criteria (de facto standard referenced by multiple Standards Track protocols; verified errata with security and functionality impact), it is well-understood, and it is not on the post-quantum transition hot path. A charter for EdDSA would illustrate the model without interfering with higher-priority work.

EdDSA remains widely deployed and its errata affect current implementations regardless of post-quantum timelines. Six confirmed errata, some highlighting deployment and interoperability hazards, warrant resolution independent of the post-quantum transition.

A charter might be scoped as follows:

Charter scope: Produce a Standards Track EdDSA specification that resolves the cofactor ambiguity by specifying explicit validation criteria for public keys and signature components. Incorporate held errata. Add a formal security theorem statement or normative citation to the Schnorr-family reduction. The resulting document supersedes [RFC8032] as the normative algorithm reference.

Profile updates: Coordinate with TLS, JOSE, and PKIX working groups to update their normative references from [RFC8032] to the new Standards Track document. Existing code points and wire formats remain unchanged; only the reference target changes.

Crypto Panel review: The Crypto Review Panel reviews the new specification’s resolution of the cofactor ambiguity, confirms the security argument is complete, and verifies that validation criteria produce consistent behavior across implementations.

Success or failure of this pilot informs how the model applies to higher-stakes mechanisms during the post-quantum transition.

Author’s Address

Nick Sullivan
Cryptography Consulting LLC
Email: nicholas.sullivan+ietf@gmail.com