Terminology for Post-Quantum Traditional Hybrid Schemes

draft-driscoll-pqt-hybrid-terminology

SECDISPATCH – IETF 114 – 26th July 2022
Context

• IETF protocols need to be updated to permit use of post-quantum asymmetric algorithms.

• During the algorithm transition period there may be a desire for protocols which use both post-quantum and traditional algorithms, so called “hybrids”.

• There is ongoing work to standardise these constructions in LAMPS, IPSECME and TLS.

• A draft on terminology was suggested at the LAMPS interim in April.
Language problems

• Hybrid = dual, multi-key, multi-algorithm, composite, non-composite...?

• There are multiple types of hybrid constructions, what do we call them?

• Hybrid schemes may aim to achieve different properties, how do we describe these?

• The word hybrid is already used in cryptography e.g. Hybrid Public Key Encryption (RFC 9180).
Proposal

• An informational draft to standardise a glossary for Post-Quantum Traditional Hybrids*.

• Aims to ensure consistency across different protocols, standards and organisations.

* This phrase is subject to change of course.
Why do we need a draft?

- To make it clear what security properties a particular hybrid construction claims.
- To enable easier comparison of solutions.
- To settle language discussions, and prevent them from derailing protocol development.
Dispatch options

• A new PQ migration group?

• CFRG?

• LAMPS?

• AD Sponsorship?
Thanks

florence.d@ncsc.gov.uk
https://datatracker.ietf.org/doc/draft-driscoll-pqt-hybrid-terminology/
Draft Content
(Bonus Slide)

• Primitives
  • Types of algorithm (traditional, post-quantum)
  • Abstract use of algorithms in schemes
  • Post-Quantum Traditional (PQT) Hybrid Schemes (KEM, PKE, Signature)

• Functionality
  • Hybrid Confidentiality
  • Hybrid Authentication

• Cryptographic Elements
  • Component and Composite Cryptographic Elements, Combiners

• Protocols
  • PQT Hybrid Protocol
  • Composite and Non-Composite PQT Hybrid Protocols

• Certificates
  • PQT Hybrid Certificates
Outstanding Work
(Bonus Slide)

• Agree or change terminology in draft -00.
• Add more to functionality section.
• Improve the definition of hybrid authentication.
• Add terminology for certificate chains and for algorithm specification.
• ...

9