

Terminology for Post- Quantum Traditional Hybrid Schemes

[draft-ietf-pquip-pqt-hybrid-terminology](#)

PQUIP – IETF 118 – 10th November 2023

Context

- An informational draft to standardise a glossary for Post-Quantum Traditional Hybrids.
- Aims:
 - Ensure consistency across different protocols, standards and organisations.
 - Make it clear what security properties a particular hybrid construction claims.
 - Enable easier comparison of solutions.
- Adopted by PQUIP following IETF 116.

Version -01

- Adding new definitions for properties of Post-Quantum Hybrid signature schemes.
- Adding alternative language for basic definitions.
- Updating references to refer to up-to-date drafts.
- Updating naming for Kyber and Dilithium to ML-KEM and ML-DSA.
- Removing Editor's Notes.

New Definitions

- Forwards Compatibility
- Backwards Compatibility
- Weak Non-Separability
- Strong Non-Separability
- Simultaneous Verification

See [draft-hale-pquip-hybrid-signature-spectrums](#) for more on these concepts

Removing the Editor's Notes

- EDNOTE 1: Should we distinguish between source authentication and identity authentication?
 - No comments made on this, and it's not something that's come up in the context of PQC so I decided to remove it.
- EDNOTE 2: Should we define more properties from a PQ/T Hybrid Scheme?
 - Done in version -01.
- EDNOTE 3: Do we want a definition of multi-cert authentication or similar?
 - Again no comments made on this topic, but it has been suggested we add definitions for "mixed certificate chain" and "multi-cert authentication".

What's next?

- A few edits to make based on feedback on -01
- Approaching WGLC?

Get involved!

- Contact me at flo.d@ncsc.gov.uk or on the pqc list.
- Contributions are very welcome.