RFC 9794: a new standard for post-quantum terminology

The NCSC's contribution to the Internet Engineering Task Force will help to make the internet more secure.

Michael P

Migration to Post-Quantum Cryptography (PQC) to protect against the threat posed by future developments in quantum computing is a global-scale and multi-year challenge.

As the UK's national technical authority for cyber security and cryptography, the NCSC is deeply invested in this process. We have published technical guidelines and timelines for migration and launched an assured consultancy scheme to support business and industry in their migration process. However, we are very aware that we cannot do this alone. We work closely with academia and industry to understand the state-of-the-art in cryptographic research and innovation, as well as what technical advice and guidance is needed to ensure the effectiveness of the transition.

Underpinning the migration to PQC are standards for algorithms, protocols and systems. These international standards are documents, agreed between a range of experts from governments, academia and industry, that define how things should work, or set out best practice. Standards ensure organisations can build interoperable products and solutions.

One of the key standards development organisations in this process is the Internet Engineering Task Force (IETF), which is responsible for designing and maintaining the protocols that – to use their own words – "make the internet work better". These protocols are documented as RFCs.

To contribute to the international effort to ensure a smooth and secure migration to PQC, the NCSC has taken an active role in the development of PQC standards. In June 2025, the IETF published RFC 9794, specifying 'Terminology for Post-Quantum/Traditional Hybrid Schemes'. This RFC defines foundational language for PQC standardisation in protocols, and was authored by the NCSC, partnering with Dr. Britta Hale from the Naval Postgraduate School. Consistent terminology across PQC ensures that technical proposals and discussions have clarity and consistency, and prevents misunderstandings that can lead to security issues.

Since 2016, the National Institute of Standards and Technology (NIST) has been running a process to standardise new cryptographic algorithms that are based on different mathematical problems to cryptography used today and specifically designed to be resistant against a cryptographically-relevant quantum computer (CRQC). The study of these mathematical problems and algorithms is known as post-quantum cryptography (PQC). In August 2024, NIST published algorithm standards for algorithms for key establishment and digital signatures, ML-KEM, ML-DSA and SLH-DSA, and continue work on alternative algorithms. Around the same time, the NCSC published guidance on Next steps in preparing for post-quantum cryptography.

Alongside this work, the IETF has been working on standards to define how to use these algorithms in internet protocols. The IETF is responsible for designing the most important security protocols on the internet, including TLS, SSH and IPSec. These protocols will need to be updated to use PQC algorithms to ensure their security against an attacker with access to a CRQC.

Within the IETF, each protocol is developed in a separate Working Group. However, the threat of a quantum computer and the introduction of PQC raises many cross-cutting issues, which are relevant for many protocols. Therefore, the IETF established a new Working Group named 'Post-Quantum Use In Protocols' (PQUIP) as a venue for discussion and guidance on PQC that is applicable across the IETF.

This Working Group, and the documents that it produces, is key in supporting the security of IETF protocols. The NCSC identified a vital part of improving security and mitigating the quantum threat was to ensure that IETF standards had a consistent terminology to rely upon, in particular on the topic of using Post Quantum and Traditional algorithms together - referred to as PQ/T hybrid schemes.

Inconsistent use of terminology is a potential security risk as it creates the possibility of either having multiple terms for the same concept or, more worryingly for security, having discussions about different concepts, with different security properties, whilst using the same wording, undermining the security analysis that takes place throughout the standards development process.

To address this risk, the NCSC published a *first draft* of an RFC to specify terminology for Post Quantum/Traditional (or PQ/T) Hybrid Schemes in July 2022. Standards in the IETF begin with an Internet-Draft and are developed by consensus, taking into account the views of experts who contribute in person and via mailing lists. The NCSC have worked with a range of partners to decide on the right terminology and concepts, incorporating expert comments and analysis for many different sources. Finally, in June 2025, having gained agreement from academics and industry professionals, the new standard was published as an RFC.

The RFC starts from first principles, specifying definitions related to cryptographic algorithms and building up to cryptographic artefacts, protocols and security properties, providing useful references for a range of use cases. Migration to PQC is complex and will require a range of stakeholders, with different levels of cryptographic expertise, so consistency and clarity in language is vital. Building this foundation will enable readers to work together to assess and compare to make the right decisions for the security of their systems.

General guidance about specific security considerations, migration timelines, and benefits and drawbacks of use of PQ/T hybrids (along with protocol-specific considerations) are out of scope of this document. However, the RFC provides terminology that enables accurate descriptions to be used in assessment of security and comparison of schemes, providing a foundation for future work.

Whilst some prefer alternative terms to those specified in the RFC, the document acknowledges and identifies these alternatives and captures them within the main definitions to ensure consistency of meaning during technical discussions.

The RFC is currently referenced by more than 20 technical draft RFCs within the IETF, as well as in academic papers, and in guidance from other standards development organisations. So it's safe to say that the NCSC's RFC will improve the security of technical proposals that will be relied upon long into the future.

The NCSC has been participating in the IETF for a number of years. RFC 9794 is the second RFC that the NCSC have written, following the publication of RFC 9424

('Indicators of Compromise (IoCs) and Their Role in Attack Defence'). Being able to contribute our cyber security and cryptographic expertise helps to make the internet, UK citizens and organisations who use it, more secure.

We would encourage others who are interested in the future of PQC technology to get involved with the IETF and contribute to the security of emerging technology standards.

Michael P
Senior Internet Standards Researcher

WRITTEN BY

Michael P
Senior Internet Standards Researcher

PUBLISHED

2 October 2025

WRITTEN FOR

Cyber security professionals

PART OF BLOG

NCSC publications