

Post-quantum updates to our TLS guidance

The NCSC publishes its recommendations for configuring post-quantum cryptography in TLS. Now is time to migrate.

Today we have published our updated [guidance on using TLS to protect data](#), to include recommended configurations for post-quantum cryptography (PQC). This follows the recent publication of [RFC 10024](#) (Post-quantum traditional hybrid key agreement mechanisms for TLS 1.3) by the IETF (Internet Engineering Task Force). These configurations are suitable for general use, and for protecting government OFFICIAL information.

The key points of the guidance are:

- We recommend both hybrid post-quantum/traditional and pure post-quantum cipher choices. The hybrid choices are the most widely deployed in commonly-used libraries, but we also recommend configurations that support a pure PQC future.
- Some procedural delays have meant that we are still awaiting publication of the final RFC (equivalent to a standard) for pure PQC options. However, stable pure PQC options exist in a number of major libraries, and are available for use.
- TLS 1.3 is the only version that supports PQC; earlier versions will not be upgraded. So, if you currently use TLS 1.2 or older versions, you should be moving to TLS 1.3 as soon as possible. As well as supporting quantum resilience, this will give you the much wider set of security benefits that TLS 1.3 offers.

The guidance supports migration to PQC in line with the [NCSC's published timelines](#), in which we recommend that **high priority migration activities should be carried out by 2031**. For many organisations, protecting the confidentiality of their data in transit will fall into this 'high priority' category, and the availability of standardised post-quantum TLS configurations together with implementations in well-studied libraries, means that **you should be aiming to make this move now**.

We will continue to provide updates to our technical guidance as PQC support is introduced into particular protocols and product types. In the coming months we plan to update our IPsec guidance as those RFCs are finalised, and to include post-quantum authentication recommendations for TLS.

Jeremy B

Principal Technical Director for Crypt and High Threat Technologies, NCSC

WRITTEN BY



Jeremy B

Principal Technical Director for Crypt and High Threat Technologies, NCSC

PUBLISHED

15 October 2026

WRITTEN FOR

Cyber security professionals

Large organisations

Public sector

PART OF BLOG

NCSC publications