NATIONELLT CYBERSÄKERHETSCENTER

Rekommendationer för övergången till kvantsäker kryptografi

Tidpunkter

I de flesta situationer ska övergången till kvantsäker kryptografi vara avklarad vid slutet av år 2035.

I situationer där kryptering är essentiell för att inte röja information på tio år eller längre ska övergången till kvantsäker kryptografi vara avklarad vid slutet av år 2030.

Algoritmer

Endast standardiserade algoritmer med implementationer som används internationellt av företag och myndigheter i omfattande skala ska användas. Exempel på sådana är: NIST FIPS 203 Module-Lattice-Based Key-Encapsulation Mechanism Standard, NIST FIPS 204 Module--Lattice-Based Digital Signature Standard och NIST FIPS 205 Stateless Hash-Based Digital Signature Standard.

Kvantsäker kryptografi i den Europeiska unionen

Den Europeiska kommissionen rekommenderade i april 2024 att en samordnad färdplan för genomförandet av övergången till kvantsäker kryptografi tas fram. Färdplanen kommer att publiceras i två delar, i maj 2025 och maj 2026. Den första delen innehåller konkreta råd kring aktiviteter som behöver vidtas på vägen av organisationer. Den andra delen innehåller bland annat mer detaljerade och utförliga rekommendationer på algoritmer. Publikationerna från EU och denna text har ingen bäring på nationell säkerhet som signalskydd.

Nationellt cybersäkerhetscenter, NCSC
2025-05-15
pqc@ncsc.se
www.ncsc.se