Post-Quantum Public-Key-Infrastrukturen

Transition to post-quantum Public Key Infrastructures

ECCC
EUROPEAN CYBERSECURITY COMPETENCE CENTRE

1

Für dieses Topic aus **Digitales Europa 2025** beträgt das Fördervolumen insgesamt **15 Mio. €** und wird vom **ECCC** verwaltet. Die vorgesehene Projektgröße umfasst 3 bis 4 Mio. Euro.

2

Förderquote: 50%

Laufzeit: ca. 3 Jahre

Ausschreibungsstart: 12. Juni 2025

Einreichungsfrist: 07. Oktober 2025

Projektpartner keine Angabe, generell von Vorteil

Zuwendungsberechtigt: Rechtsträger mit Sitz in der EU, weitere nur nach Einhaltung von Artikel 12(5) der DEP Regulierung 2021/694.

Ziele

Entwicklung und Integration quantensicherer Algorithmen in bestehende Public-Key-Infrastrukturen (PKI), unter Wahrung von Sicherheit, Interoperabilität und Geschäftskontinuität über verschiedene Anwendungsbereiche.

Maßnahmen

Entwurf und Test hybrider kryptografischer Verfahren, Migration bestehender Zertifikatsstrukturen (z. B. X.509), Entwicklung neuer Protokolle für Zertifikatsverwaltung und -transparenz, und Berücksichtigung sektorenspezifischer Anforderungen wie IoT oder E-Government.

Technische Umsetzung

Einsatz kombinierter Prä-/Post-Quantum-Methoden zur Gewährleistung von Rückwärtskompatibilität, Open-Source-Bibliotheken, neue PKI-Modelle, neue Zertifikatsformate (z. B. Auf Basis von Merkle-Bäumen oder dem GNU-Name-System), Tools zur Schlüsselverwaltung und Testspezifikationen für Sonderfälle.

Erwartete Ergebnisse

Combiner für PQC-Verfahren mit mind. 128 Bit Sicherheit, getestete Hybrid-Zertifikate, neue PKI-Protokolle, verbesserte Open-Source-Tools, sichere Schlüsselverwaltungsverfahren, Dokumentationen zu Tests und Übergangsstrategien, Schulungsmaßnahmen.

Sie haben Fragen? Nehmen Sie Kontakt mit uns auf:
www.nkcs.bund.de/de/kontakt