HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Originaltext auf Englisch finden Sie in folgendem Dokument:

“Digital Europe Cybersecurity Work Programme 2025-2027“
Version 1, März 2025 herausgegeben vom ECCC

https://cybersecurity-centre.europa.eu/document/8af166e1-69c5-4ccd-b38f-5a3ffe43ad73_en

Förderbereich:	New technologies, AI & post-quantum transition
Förderthema:	2.3 Deployment of a European testing infrastructure for the transition to PQC in different usage domains
Seiten:	25-27

Deutsche Übersetzung des Förderthemas durch das NKCS/ NCC-DE als unterstützendes Informationsangebot erstellt:

2.3 Aufbau einer europäischen Testinfrastruktur für den Übergang zu PQC in verschiedenen Anwendungsbereichen

2.3.1 Ziele

Dieses Thema unterstützt die Schaffung einer europäischen globalen Benchmark-Testing-Infrastruktur für den Übergang zu PQC, die für verschiedene Arten von Akteuren zugänglich ist, um realistische Tests durchzuführen und die Herausforderungen bei der Einführung von PQC-Systemen zu ermitteln, wobei der Schwerpunkt auf Konnektivität, Interoperabilität und Flexibilität liegt. Auch Sicherheitstests sollten in Betracht gezogen werden, aufbauend auf den Ergebnissen anderer EU-finanzierter Projekte und Aktivitäten, die bereits laufen. Die Testinfrastruktur sollte europäischen KMU, Start-ups, Anbietern und Akademikern offen stehen, um die Konzeption von Tests und die Bewertung der Ergebnisse besser zu unterstützen, sowie öffentlichen Organisationen und großer europäischer Industrieverbände, um den Austausch mit den Akteuren zu erleichtern, die bereits mit ihren Tests begonnen haben. Dieses Thema soll den Übergang öffentlicher und privater Einrichtungen zu PQC unterstützen und das Entstehen eines europäischen Marktes für PQC-Produkte, -Werkzeuge und -Dienstleistungen erleichtern.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

2.3.2 Umfang (oder Anwendungsbereich)

Es werden Vorschläge für die Schaffung und Pflege einer europäischen PQC-Prüfungsinfrastruktur erwartet. Die Testinfrastruktur sollte einen physischen Raum für Vor-Ort-Tests bieten, der möglicherweise zentralisiert oder an verschiedenen Orten in verteilt ist. Dies schließt die Möglichkeit ein, Ferntests für verschiedene europäische Interessengruppen im öffentlichen und privaten Sektor durchzuführen, um reale Tests durchzuführen und Herausforderungen zu identifizieren, wobei der Schwerpunkt auf Konnektivität, Interoperabilität, Agilität und Sicherheitstests liegt. Die Vorschläge sollten auf den Ergebnissen laufender Aktivitäten in der EU aufbauen.

Die PQC-Testinfrastruktur sollte die notwendigen Einrichtungen und die Verfügbarkeit von Werkzeugen auf dem neuesten Stand der Technik gewährleisten, damit die europäischen Nutzer PQC-Einführungen in einer vertrauenswürdigen Umgebung testen können, und sie sollte den Zugang der europäischen Industrie erleichtern und unterstützen, wobei ein besonderes Augenmerk auf

Schwerpunkt auf KMU. Die Infrastruktur-Governance sollte einen fairen Zugang zu den Einrichtungen für verschiedene Nutzer und Praktiken der Datenverwaltung gewährleisten.

Eine große Herausforderung, die es zu bewältigen gilt, ist die Aufrechterhaltung der Konnektivität und Interoperabilität zwischen Organisationen und Einrichtungen sowie zwischen Produkten verschiedener Anbieter während des Übergangs zu quantenresistenten Algorithmen.

Die Maßnahme sollte die Entwicklung modularer und anpassungsfähiger Lösungen fördern, die zeigen, wie Normen und bewährte Verfahren unter Verwendung handelsüblicher Technologien angewendet werden können.

Die Aktivitäten können auch die Erprobung innovativer Lösungen vorsehen, wie z. B. die Kombination von qualitativ hochwertigen Quanten-Zufallszahlengeneratoren (QRNGs) und PQC, was die erfolgreiche Markteinführung solcher Lösungen erleichtert.

Die Entwicklung von Lösungen für den digitalen Zwilling, die ein bestimmtes Verhalten kritischer Infrastrukturen nachahmen, könnte ebenfalls ins Auge gefasst werden, um für den Übergang zu schulen und Folgenabschätzungen durchzuführen.

Die Aktivitäten sollten Folgendes umfassen:

- Einrichtung eines physischen Raums für In-situ-Tests mit der Möglichkeit von Ferntests, einschließlich des Kaufs der erforderlichen Werkzeuge, neuer Produkte und Dienstleistungen.
- Entwurf und Durchführung von Praxistests mit Schwerpunkt auf Konnektivität, Interoperabilität und Agilität, um ein Verständnis für die Betriebsbedingungen der Protokolle für die Anwendungen und für die

Einschränkungen zu entwickeln, die sich auf die Nutzung der Produkte auswirken können.

- Identifizierung des Bedarfs an Ersatz/Aktualisierung von Hardware, Software und Diensten, die PQC nutzen.
- Entwicklung eines wirksamen Governance-Mechanismus, der die Prioritäten des angebotenen Dienstes und ein transparentes Verwaltungsverfahren für die Gewährung des Zugangs an die Nutzer festlegt.
- Entwicklung oder Anpassung der erforderlichen Software/Hardware und Validierung der Lösungen, einschließlich quelloffener Bibliotheken mit hybriden Lösungen, die sowohl die Kombination von Prä-Quantum- und Post-Quantum-Verfahren aus Sicherheitsgründen als auch die Abwärtskompatibilität mit ihren Prä-Quantum-Versionen unterstützen.
- Definition der Zugangsbedingungen, Entwicklung eines Testkatalogs und von Diensten, einschließlich Bemühungen zur Automatisierung von Konformitäts- und Sicherheitstests.
- Entwicklung und Einsatz von Instrumenten, die die Umsetzung des europäischen PQC- Übergangsfahrplans unterstützen können, entweder für öffentliche Verwaltungen oder andere spezifische Sektoren; die Instrumente sollten gegen mögliche Abhängigkeiten und Schwachstellen in der Cybersicherheit geschützt werden, um ausländischer Einflussnahme und Kontrolle vorzubeugen.

Vorschläge können von Konsortien eingereicht werden, die sich aus Akteuren der europäischen Industrie zusammensetzen und an denen sich möglicherweise auch öffentliche Einrichtungen und Forschende aus dem Bereich der angewandten Kryptografie beteiligen.

Die Teilnahme von Nicht-EU-Stellen birgt das Risiko, dass hochsensible Informationen über Sicherheitsinfrastrukturen, Risiken und Vorfälle Gegenstand von Rechtsvorschriften oder Druck sind, die diese Nicht-EU-Stellen dazu zwingen, diese Informationen an Nicht-EU-Regierungen weiterzugeben, was ein unvorhersehbares Sicherheitsrisiko darstellt. Daher fällt dieses Thema unter Artikel 12 Absatz 5 der Verordnung (EU) 2021/694.

2.3.3 Zu erbringende Leistungen

- Eine vertrauenswürdige, weltweite PQC-Testinfrastruktur mit den erforderlichen Einrichtungen und der Verfügbarkeit modernster Werkzeuge, die es den Nutzern der Infrastruktur ermöglichen, alle Aspekte im Zusammenhang mit vertrauenswürdigen PQC-Einsätzen umfassend zu testen.
- Eine Reihe von Integrationstests und End-to-End-Tests sowie eine Reihe automatisierter Tests, um problematische Funktionsweisen von PQC-Produkten frühzeitig zu erkennen und Abhilfemaßnahmen vorzuschlagen.

- Ein Portfolio von Tools, die Konnektivitäts- und Interoperabilitätstests unterstützen können.
- Ein Rahmen mit einem Modus Operandi, der es ermöglicht, PQC für eine Vielzahl von Kontexten und Anwendungsbereichen zu testen und Abhängigkeiten zwischen Problemen im Zusammenhang mit Hardware, Bibliotheken, Protokollen und Anwendungen zu identifizieren.
- Automatisierte Sicherheitsevaluierungen von Software auf Korrektheit und Widerstandsfähigkeit gegen Angriffe über entfernte Seitenkanäle sowie Testkataloge zur Bewertung der Sicherheit gegen lokale Implementierungsangriffe.
- Benutzerfreundliche Tools, Open-Source-Bibliotheken und sichere Hardware-Implementierungen für PQC.
- Einsatz von kryptoagilen Ansätzen in den vorgeschlagenen Lösungen.
- Erweiterung und Konsolidierung der Fähigkeiten zur Einführung von PQC in verschiedenen Bereichen.
- Regelmäßige Veröffentlichung von Berichten über die Ergebnisse, einschließlich erfolgreicher und fehlgeschlagener Interoperabilitätstests, sowie über festgestellte Probleme und Herausforderungen.
- Ergebnisse der Erprobung innovativer Lösungen, die verschiedene Technologien kombinieren, z. B. neue Quantenzufallszahlengeneratoren (QRNG) und PQC.

Art der Maßnahme	Simple grant
Vorläufiges Budget	*45 Mio. EUR*
Vorläufige Ausschreibungsplanung	2025, 2026, 2027
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Technologieanbieter, Betreiber von Cyber-Hubs, Forschung und Hochschulen, Cybersicherheits-einrichtungen, öffentlicher Sektor, von der NIS-2-Richtlinie betroffene Einrichtungen, Privatsektor, andere einschlägige Akteure, die die Einführung sicherer KI-Lösungen im Internet unterstützen
Sicherheit	Die Einreichung von Anträgen und die Auftragsvergabe sind gemäß Artikel 12 Absatz 5 der Verordnung (EU) 2021/694 beschränkt.

HINWEIS: Frei übersetzt aus dem Englischen. Wir empfehlen als Referenz bei der Bewerbung den englischen Text zu nutzen.

Das **Nationale Koordinierungszentrum für Cybersicherheit (NKCS/ NCC-DE)**

berät zu **EU-Fördermöglichkeiten in der Cybersicherheit**

und hilft bei der **Vernetzung mit EU-Partnern**.

Sie erreichen uns unter **nkcs@bsi.bund.de**