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:	2.4 Transition to post-quantum Public Key Infrastructures
Seiten:	28-30

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

2.4 Übergang zu Post-Quantum Public-Key-Infrastrukturen

2.4.1 Ziele

Das übergeordnete Ziel dieser Aufforderung ist es, die Herausforderungen einer effektiven Integration von PQC-Algorithmen in Public-Key-Infrastrukturen (PKI) zu bewältigen, die effiziente Migrationsstrategien und starke Garantien für die Geschäftskontinuität bietet.

Die Aufforderung richtet sich an die verschiedenen Akteure des PKI-Ökosystems und der Liefer- und Wertschöpfungsketten, die alle eine Reihe unterschiedlicher Bedürfnisse und Abhängigkeiten haben, wie z. B. Zertifizierungsstellen (CAs), zwischengeschaltete CAs, Forscher, Endnutzer in verschiedenen Bereichen und Anbieter.

2.4.2 Umfang (oder Anwendungsbereich)

Die Vorschläge müssen Aktivitäten zu den folgenden Themen betreffen:

- Entwurf von Kombinatoren für digitale Signaturen und von Kombinatoren für Schlüsselkapselungsmechanismen.
- die Prüfung des Einsatzes von Zertifikaten in Protokollen, die diese Zertifikate verwenden.
- die Entwicklung neuartiger Protokolle um Zertifikate automatisiert zu verwalten bzw. zu widerrufen und neuartiger Protokolle für (datenschutzfreundliche) Zertifikatstransparenz

- die Entwicklung von Methoden und Werkzeugen, die von Experten in verschiedenen PKI-Bereichen verwendet werden können, einschließlich aller Aspekte der Schlüsselverwaltung asymmetrischer Systeme.

Die Vorschläge sollten die Anforderungen und Einschränkungen wie Sicherheitsniveau, Leistung und Geschäftskontinuität in einem breiten Spektrum von Anwendungen berücksichtigen, die für kritische gesellschaftliche Sektoren und Prozesse relevant sind (z. B. Behördendienste, Telekommunikation, Bankwesen, intelligente Häuser, elektronische Gesundheitsdienste, Automobilindustrie und andere Sektoren).

Die Vorschläge sollten sich auf Funktionen wie die Schlüssel-Einrichtung, digitale Signaturen und sichere Kommunikationsprotokolle beziehen, die eine sorgfältige Anpassung an Post-Quantum-Pendants erfordern, um die Widerstandsfähigkeit gegen Bedrohungen durch quantenfähige Gegner zu gewährleisten.

Die Vorschläge sollten die Kompatibilität mit bestehenden Altsystemen gewährleisten. Um dies zu erreichen, sollte ein Übergang zu PKI, die sowohl die Prä-Quantum- als auch die Post-Quantum-Kryptografie unterstützen, in Betracht gezogen werden. Die vorgeschlagenen Systeme sollten in der Lage sein, nahtlos mit Altsystemen zu interagieren, indem sie die Post-Quantum-Komponente bei Bedarf deaktivieren und gleichzeitig Downgrade-Angriffe verhindern. Sich in dieser Übergangsphase ausschließlich auf PQC-Lösungen zu verlassen, könnte Sicherheitsrisiken mit sich bringen, da die Sicherheitsanalyse der Kryptosysteme und ihrer Implementierungen noch nicht so ausgereift ist wie bei ihren Prä-Quantum-Pendants. Vorschläge sollten daher Kombinationen aus PQC-Lösungen und etablierten Prä-Quantum-Lösungen verwenden, hierbei jedoch sicherstellen, dass die Sicherheit der jeweils stärksten Komponente bereitgestellt wird, sodass das System so lange sicher ist, wie mindestens eine der Komponenten der Kombination sicher ist.

Bei Zertifikaten für Protokolle, die eine Verhandlung unterstützen, wie z. B. X.509-Zertifikate für die Transportschicht (TLS), wurde die Verwendung des Post-Quantum-Schlüsselaustauschs bereits demonstriert und kann auf dezentrale Weise umgesetzt werden. Viele andere Protokolle hingegen müssen noch migriert werden, und dieser Prozess wird komplexer sein, wenn alte und neue Konfigurationen koexistieren. Zudem könnte es sein, dass die Migrationsstrategien, die für die Kernaufgaben des X.509 Protokolls definiert wurden, bei Anwendungen für IoT, Smartcards, Ausweisdokumenten und anderen Bereichen nicht funktionieren.

In den Vorschlägen sollten klare Prozesse entwickelt werden, um die verschiedenen an PKI beteiligten Akteure in den verschiedenen Anwendungsbereichen wirksam durch den Übergangsprozess zu führen.

Wirksame Konsortien sollten ein breites Spektrum von Akteuren entlang der gesamten PKI-Kette umfassen, die über Fachwissen in Bereichen wie Softwareentwicklung, Hardware-Implementierung, kryptografische Forschung, Normung, Politik und Anwendungsimplementierung sowie Organisationen einbeziehen, die Anwender-Fallstudien und reale Anwendungen liefern können.

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

Die Aktivitäten sollten einige oder alle der folgenden Punkte umfassen:

- Identifizierung der Anforderungen, die für die Einführung von Hybridzertifikaten erforderlich sind.
- Entwicklung von Ansätzen und Techniken zur Konstruktion von kryptographischen Kombinatoren für verschiedene Protokolle.
- Prüfung der Kombinatoren für die Ausstellung neuer Zertifikate für die verschiedenen Anwendungen unter Berücksichtigung der Notwendigkeit, das Wachstum von Schlüssel-, Signatur- und Chiffretextgrößen auszugleichen, was zu Kompatibilitätsproblemen mit Standards wie PKI-Zertifikaten, Widerrufsmechanismen, (datenschutzfreundlichen) Zertifikatstransparenzmechanismen, der Verwendung verschiedener kryptografischer Protokolle über Zertifikatsketten hinweg, Anforderungen der Anwendungen wie Sicherheitsniveau, Zeitbeschränkungen bei Signier- und Überprüfungsschritten, Kommunikations-/Rechen- und Speicheraufwand sowie Hardware-Optimierungsanforderungen führen kann.
- Entwicklung und/oder weitere Verbesserung von Open-Source-Bibliotheken.
- Entwicklung neuartiger Protokolle für die automatische Verwaltung und den Widerruf von Zertifikaten und neuartiger Protokolle für (datenschutzfreundliche) Zertifikatstransparenz. Unterstützung von Standardisierungsaktivitäten.
- Entwicklung von Leitfäden für die Konzeption und den Einsatz der neuen PKI, mit Analysen, die von den einzelnen Komponenten einer bestimmten PKI abhängen.
- Tests zu speziellen Verwendungszwecken von X.509-Zertifikaten, die nicht zu den Kernfällen der Verwendung von TLS gehören, wie z. B. Vertrauenswurzeln, Geräteintegrität, Firmware-Signierung und andere.
- Entwurf, Verbesserung und Erprobung von X.509-Alternativen, wie z.B Merkle-Baumleitern, das GNU Name System, ältere Vorschläge wie SPKI und SDSI und die Verwendung von Schlüsselkapselungsmechanismen für die Authentifizierung auf Anfrage anstelle von Signaturen.
- Sensibilisierungs- und Schulungsmaßnahmen für Beteiligte mit unterschiedlichen Profilen, die die gegenseitigen Abhängigkeiten bei der Umstellung hervorheben und ein breiteres Verständnis der technischen Standards unter den PKI-Nutzern fördern.
- Die Mitwirkung von nicht-EU-Entitäten beinhaltet das Risiko, äußerst sensible Daten über Sicherheitsinfrastruktur, Risiken und Vorfälle einer Gesetzgebung oder anderen Zwängen zu unterwerfen, die diese nicht-EU-Entitäten verpflichtet oder zwingt, diese Informationen für nicht-EU-Regierungen zugänglich zu machen - mit unvorhersehbaren

Sicherheitsrisiken. Aus den dargelegten Sicherheitsgründen unterliegt dieses Thema daher Artikel 12 Absatz 5 der Verordnung (EU) 2021/694.

2.4.3 Zu erbringende Leistungen

- Neue Kombinatoren, die sicherstellen, dass kryptografische Verfahren mindestens 128 Bit Sicherheit gegen Quantengegner bieten.
- Bewertung hybrider Zertifikate auf experimenteller Basis in mehreren Standardprotokollen, die diese Zertifikate verwenden, wobei auch Optionen für verschiedene kryptografische Algorithmen auf der Ebene der Stammzertifizierungsstelle und auf den anderen Ebenen im Hinblick auf Sicherheit, Leistung und Rückwärtskompatibilität berücksichtigt werden. Die Auswirkungen solcher Zertifikate in Protokollen sollten über Open-Source-Bibliotheken getestet werden.
- Neue und/oder verbesserte Open-Source-Bibliotheken für Zertifikatsanforderung, -ausstellung, -validierung, -widerruf und (datenschutzfreundliche) Zertifikatstransparenz.
- Klare Verfahren, die alle Aspekte der Schlüsselverwaltung berücksichtigen:
    - Anforderungen an die Signaturgenerierung, sowohl in Bezug auf die zur Signaturerstellung verwendete Soft- und Hardware als auch auf sichere Speicherung und die Handhabung privater Schlüssel, um deren Authentizität und Vertraulichkeit sicherzustellen
    - Signaturvalidierung inklusive Benennung der für die Verifizierung erforderlichen Daten und Darlegung der zu erfüllenden Bedingungen für einen erfolgreichen Signaturprüfungsprozess.
    - Lebenszyklusprozess der Signaturen
    - Gültigkeitsstatus der Signaturen
- Prüfung und Bewertung von Verwendungsarten von X.509-Zertifikaten, die nicht zum Kerngeschäft gehören.
- Tests und Bewertung von Alternativen zu X.509-Zertifikaten.
- Sensibilisierungsmaßnahmen und Schulungskurse.

Art der Maßnahme	Simple grant
Vorläufiges Budget	*15 Mill. EUR*
Vorläufige Ausschreibungsplanung	2025
Vorläufige Projektdauer	3 Jahre
Implementierung	ECCC
Zielgruppe	Alle Akteure in PKI-Kette
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**