# Transizione verso infrastrutture a chiave pubblica post-quantistica

## Transition to post quantum Public Key Infrastructures

**TOPIC ID**:
DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PUBLICPQC

**Ente finanziatore:**
Commissione europea
Programma Europa digitale (DIGITAL)

**Obiettivi ed impatto attesi:**
Risultato atteso:

- Nuovi combinatori che garantiscono che gli schemi crittografici forniscano una sicurezza di almeno 128 bit contro gli avversari quantistici.
- Valutazione sperimentale su certificati ibridi in diversi protocolli standard che utilizzano tali certificati, considerando anche le opzioni per diversi algoritmi crittografici a livello di Certification Authority di root e agli altri livelli, in termini di sicurezza, prestazioni e retrocompatibilità. L'impatto di tali certificati nei protocolli dovrebbe essere testato tramite librerie open source.
- Librerie open source nuove e/o migliorate per la richiesta di certificati, l'emissione, la convalida, la revoca e la trasparenza dei certificati (rispettosa della privacy).
- Procedure chiare che tengono conto di tutti gli aspetti della gestione delle chiavi: requisiti per la generazione delle firme, in termini di software e hardware utilizzati per creare le firme, nonché l'archiviazione e la gestione sicure delle chiavi private per mantenerne l'autenticità e la riservatezza, convalida delle firme, con la specificazione dei dati necessari per la verifica delle firme e la definizione delle condizioni necessarie per un processo di verifica delle firme di successo, processo del ciclo di vita delle firme e stato di validità delle firme.
- Test e valutazione degli usi dei certificati X.509 diversi dai loro usi principali.
- Test e valutazione di alternative ai certificati X.509.
- Attività di sensibilizzazione e corsi di formazione.

Obiettivo:
L'obiettivo generale di questo invito è quello di affrontare le sfide di un'integrazione efficace degli algoritmi PQC nelle infrastrutture a chiave pubblica (PKI), che offra strategie di migrazione efficienti e solide garanzie di continuità operativa.
L'invito si rivolge ai diversi attori coinvolti negli ecosistemi PKI e nelle catene di approvvigionamento e del valore, che hanno tutti un insieme unico di esigenze e interdipendenze diverse, come le autorità di certificazione (CA), le CA intermedie, i ricercatori, gli utenti finali in diversi domini e i fornitori.
Portata:
Le proposte riguardano le seguenti tematiche:

- Progettazione di combinatori di firme digitali e combinatori di meccanismi di incapsulamento delle chiavi.

- il test della distribuzione dei certificati nei protocolli che utilizzano tali certificati.
- lo sviluppo di nuovi protocolli per la gestione automatica e la revoca dei certificati e di nuovi protocolli per la trasparenza dei certificati (rispettosa della privacy).
- lo sviluppo di metodi e strumenti che possono essere utilizzati da esperti in vari domini PKI, compresi tutti gli aspetti della gestione chiave dei sistemi asimmetrici.

Le proposte dovrebbero considerare attentamente i requisiti e i vincoli, quali il livello di sicurezza, le prestazioni e la continuità operativa, in un'ampia gamma di applicazioni pertinenti per settori e processi sociali critici (come i servizi governativi, le telecomunicazioni, le banche, le case intelligenti, l'e-health, l'automotive e altri settori).
Le proposte dovrebbero riguardare funzioni quali l'istituzione delle chiavi, le firme digitali e i protocolli di comunicazione sicuri che richiedono un attento adattamento con le controparti post-quantistiche per garantire la resilienza contro le minacce poste da avversari con capacità quantistica.
Le proposte dovrebbero salvaguardare la compatibilità con i sistemi preesistenti esistenti. A tal fine, è necessario prendere in considerazione una transizione verso PKI che supportino sia la crittografia pre-quantistica che post-quantistica. I sistemi proposti dovrebbero essere in grado di interagire senza problemi con i sistemi legacy disabilitando il componente post-quantistico secondo necessità, prevenendo al contempo gli attacchi di downgrade. Affidarsi esclusivamente a soluzioni PQC in questa fase intermedia di transizione potrebbe introdurre rischi per la sicurezza, dato che l'analisi della sicurezza dei criptosistemi e delle loro implementazioni non è così matura come per le loro controparti pre-quantistiche. Le proposte dovrebbero pertanto utilizzare combinazioni di soluzioni PQC e soluzioni pre-quantistiche consolidate, assicurandosi di fornire la massima sicurezza del collegamento, il che significa che il sistema rimane sicuro finché almeno uno dei componenti della combinazione è sicuro.
Per i certificati per i protocolli che supportano la negoziazione, ad esempio i certificati X.509 per il livello di trasporto (TLS), l'uso dello scambio di chiavi post-quantistico è già stato dimostrato e può essere implementato in modo decentralizzato. È necessario eseguire la migrazione di molti altri protocolli e questo processo sarà più complesso quando le configurazioni vecchie e nuove devono coesistere. Inoltre, per le applicazioni in IoT, smartcard, documenti di identità e altro, le strategie di migrazione definite per i casi d'uso principali di X.509 potrebbero non funzionare.
Le proposte dovrebbero sviluppare procedure chiare per guidare efficacemente le varie parti interessate coinvolte nelle PKI in diversi domini di utilizzo attraverso il processo di transizione.
I consorzi efficaci dovrebbero comprendere una gamma diversificata di attori lungo l'intera catena PKI, comprendendo competenze in settori quali lo sviluppo di software, l'implementazione di hardware, la ricerca crittografica, la standardizzazione, le politiche e l'implementazione di applicazioni, nonché organizzazioni in grado di fornire studi di casi di utenti e applicazioni nel mondo reale.
Le attività dovrebbero includere alcuni o tutti i seguenti elementi:

- Identificazione dei requisiti necessari per implementare i certificati ibridi.
- Sviluppo di approcci e tecniche per la costruzione di combinatori crittografici per diversi protocolli.
- Test dei combinatori per l'emissione di nuovi certificati per le diverse applicazioni, tenendo in considerazione la necessità di bilanciare l'aumento delle dimensioni della chiave, della firma e del testo cifrato, che può portare a problemi di compatibilità con gli standard, come i certificati PKI, i meccanismi

di revoca, i meccanismi di trasparenza dei certificati (rispettosi della privacy), l'uso di diversi protocolli crittografici tra le catene di certificati, i requisiti delle applicazioni, come il livello di sicurezza, i vincoli di tempo nelle fasi di firma e verifica, il sovraccarico di comunicazione/calcolo e archiviazione e i requisiti di ottimizzazione dell'hardware.

- Sviluppo e/o ulteriore miglioramento di librerie open source.
- Sviluppo di nuovi protocolli per la gestione e la revoca automatica dei certificati e di nuovi protocolli per la trasparenza dei certificati (rispettosa della privacy). Supporto alle attività di normazione.
- Sviluppo di ricette per la progettazione e l'implementazione delle nuove PKI, con analisi che dipendono da ogni componente di una data PKI. • Test su usi specializzati dei certificati X.509 diversi dai casi principali che utilizzano TLS, come le radici di attendibilità, l'integrità del dispositivo, la firma del firmware e altri.
- Progettazione, miglioramento e test di alternative X.509, come, tra le altre, le scale ad albero di Merkle, il GNU Name System, proposte più vecchie come SPKI e SDSI e l'uso di meccanismi di incapsulamento delle chiavi per l'autenticazione su richiesta al posto delle firme.
- Attività di sensibilizzazione e formazione per le parti interessate con profili diversi, sottolineando le interdipendenze nella transizione e facilitando una più ampia comprensione delle norme tecniche tra gli utenti PKI.

La partecipazione di soggetti di paesi terzi comporta il rischio che informazioni altamente sensibili relative alle infrastrutture di sicurezza, ai rischi e agli incidenti siano oggetto di una legislazione o di una pressione che obblighi tali soggetti di paesi terzi a divulgare tali informazioni a governi di paesi terzi, con un rischio imprevedibile per la sicurezza. Pertanto, sulla base dei motivi di sicurezza delineati, questo tema è soggetto all'articolo 12, paragrafo 5, del regolamento (UE) 2021/694.

**Criteri di eleggibilità:**

Per essere ammissibili, i richiedenti (beneficiari ed entità affiliate) devono:
− essere persone giuridiche (enti pubblici o privati)
− essere stabiliti in uno dei paesi ammissibili, ovvero:
− Stati membri dell'UE (compresi i paesi e territori d'oltremare (PTOM))
− paesi SEE (Norvegia, Islanda, Liechtenstein)

I beneficiari e le entità affiliate devono registrarsi nel registro dei partecipanti — prima di presentare la proposta — e dovranno essere convalidati dal servizio centrale di convalida (REA Convalida).
Per la convalida, verrà richiesto di caricare documenti che dimostrino lo status legale e l'origine. Altri soggetti possono partecipare ad altri ruoli del consorzio, quali partner associati, subappaltatori, terzi che forniscono contributi in natura, ecc. (cfr. sezione 13).
Si prega di notare tuttavia che tutti gli argomenti di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto le entità non devono essere controllate direttamente o indirettamente da un paese che non è un paese ammissibile. Tutti i soggetti dovranno compilare e presentare una dichiarazione sulla proprietà e il controllo.
Inoltre:
− la partecipazione a qualsiasi titolo (in qualità di beneficiario, entità affiliata, partner associato,

subappaltatore o destinatario di sostegno finanziario a terzi) è limitata a entità stabilite e controllate da paesi ammissibili
− le attività del progetto (compreso il lavoro in subappalto) devono svolgersi in paesi ammissibili (cfr. sezione Ubicazione geografica e sezione 10)
− la Convenzione di sovvenzione può prevedere restrizioni in materia di diritti di proprietà intellettuale (cfr. sezione 10).

**Contributo finanziario:**
Il bilancio stimato disponibile è di 15 000 000 EUR.

I parametri della sovvenzione (importo massimo della sovvenzione, tasso di finanziamento, costi totali ammissibili, ecc.) saranno fissati nella Convenzione di sovvenzione (Scheda tecnica, punto 3 e art 5). Budget del progetto (importo del contributo richiesto): − per i temi DIGITAL-ECCC-2025-DEPLOY-CYBER-08-PublicPQC: indicativamente tra i 3 e i 4 milioni di euro per progetto ma non sono esclusi altri importi, se debitamente giustificati. La sovvenzione concessa può essere inferiore all'importo richiesto. Il budget minimo per ogni argomento, come elencato sopra, è fortemente raccomandato.

Dopo la firma della sovvenzione, di norma si riceve un prefinanziamento per iniziare a lavorare al progetto (flottante di norma pari all'80% dell'importo massimo della sovvenzione; eccezionalmente un prefinanziamento inferiore o nullo). Il prefinanziamento sarà versato 30 giorni dopo l'entrata in vigore/10 giorni prima della data di inizio/garanzia finanziaria (se richiesta), se posteriore. Sono previsti uno o più pagamenti intermedi (con rendicontazione dei costi attraverso il report sull'utilizzo delle risorse).

**Scadenza:**
07 ottobre 2025 17:00:00 ora di Bruxelles

**Ulteriori informazioni:**
**Bando di concorso DIGITAL-ECCC-2025-DEPLOY-CYBER-08 - bando | Centro e rete europei di competenza sulla cibersicurezza**