Standardizzazione e consapevolezza della transizione europea alla crittografia post-quantum

Standardisation and awareness of the European transition to post-quantum cryptography

TOPIC ID:
DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD

Ente finanziatore:
Commissione europea
Programma Europa digitale

Obiettivi ed impatto attesi:
Risultati e risultati
• Contributi a norme e regolamenti europei e internazionali in materia di PQC
• Workshop, white paper e altre attività per sostenere le sinergie tra i diversi settori in transizione verso la PQC
• Una tabella di marcia europea per la migrazione di PQC, che può essere la base per le tabelle di marcia specifiche del settore.
• Azioni a sostegno della comunità europea PQC
• Sviluppo di standard per sistemi crittografici ibridi (sistemi di crittografia pre- e post-quantistica) per la crittografia, i meccanismi di incapsulamento delle chiavi, le firme digitali, ecc. e per l'integrazione del PQC nell'infrastruttura digitale esistente.
• Sostegno alla partecipazione di esperti europei pertinenti agli organismi di standardizzazione trasversali europei e internazionali, al fine di integrare il PQC ogni volta che vengono sviluppati nuovi standard crittografici o vengono aggiornati quelli esistenti, in particolare per i settori critici come l'energia, i trasporti, la salute e la finanza.
Obiettivo:
Le proposte devono mirare a rafforzare gli sforzi dell'Europa nella transizione verso la PQC, sostenendo le attività di standardizzazione europee e internazionali, fornendo una tabella di marcia completa per la migrazione industriale PQC in Europa e sensibilizzando l'opinione pubblica sugli sforzi della PQC. Questo obiettivo dovrebbe essere raggiunto in particolare attraverso le seguenti azioni strategiche:
• Organizzazione di eventi, workshop, consultazioni con le parti interessate e produzione di libri bianchi per promuovere lo sviluppo di standard armonizzati sulla PQC.
• Sostegno alla partecipazione di esperti europei pertinenti ai forum di standardizzazione europei e internazionali relativi alla PQC.
• Tabella di marcia per la migrazione dei PQC su base comunitaria: Promuovere un processo collaborativo che coinvolga le parti interessate della ricerca e dell'industria per formulare una solida tabella di marcia europea per la migrazione dei PQC, che possa essere la base per le tabelle di marcia specifiche del settore.
• Diffusione dei risultati della PQC: Promuovere un'ampia consapevolezza e comprensione dei risultati della PQC europea attraverso un'ampia opera di divulgazione su varie piattaforme, compresi i social media. Ciò include eventi di sensibilizzazione e dialoghi strutturati con il pubblico in generale, che esplorano le dimensioni etiche e sociali della PQC, soprattutto in termini di privacy, sicurezza, fiducia del pubblico e accettazione.

• Servizi di divulgazione della ricerca: Fornire servizi di divulgazione specializzati rivolti alle comunità interessate, come i fornitori e gli utenti europei di cibersicurezza, condividendo efficacemente le intuizioni della ricerca.
• Identificare le esigenze di formazione e infrastruttura: Identificare i requisiti fondamentali per la formazione, l'istruzione e le infrastrutture per far progredire lo sviluppo di PQC.
Ambito di applicazione:
Le proposte devono impegnarsi in iniziative concrete di standardizzazione all'interno di forum di standardizzazione europei e internazionali, dove la PQC svolgerà un ruolo centrale nel prossimo futuro e dove i progressi nella standardizzazione aumenteranno le capacità di cybersecurity esistenti e creeranno un vantaggio competitivo per l'Europa. Inoltre, in linea con i progetti derivanti dal tema "Transition to Quantum-Resistant Cryptography" (bando HORIZON-CL3-2022-CS-01-03) e con il tema Deployment of Post-Quantum Cryptography (PQC) systems in industrial sectors (in questo programma di lavoro), le proposte includeranno strategie pratiche per coordinare e sinergizzare gli sforzi europei di ricerca e innovazione con le iniziative di standardizzazione della PQC.
A tal fine, le proposte dovrebbero stabilire una presenza proattiva e assumere ruoli di leadership nell'orchestrazione e nella definizione di standard e regolamenti internazionali per la PQC. Ciò può avvenire all'interno di attività e organismi di standardizzazione esistenti o, se del caso, contribuendo alla creazione di nuove attività di standardizzazione in gruppi già esistenti e/o alla creazione di nuovi gruppi.
Le proposte devono coltivare una comunità europea PQC coesa, promuovendo la collaborazione tra le parti interessate del mondo accademico e industriale, e impegnarsi in un dialogo strutturato in varie sedi. Ciò comporterà l'armonizzazione delle attività tra i programmi e i progetti europei, nazionali e regionali, e aprirà la strada a sforzi sinergici di innovazione in PQC per contribuire a sbloccare casi d'uso per applicazioni pratiche di sicurezza informatica in Europa.
Le proposte devono riunire i principali stakeholder dell'intera catena del valore PQC. Questo approccio olistico dovrebbe comprendere ricercatori, esperti di standardizzazione e rappresentanti dei settori industriali. Nella proposta deve essere fornito uno schema completo che illustri le parti interessate da coinvolgere e le metodologie per coordinare in modo efficiente i loro sforzi a livello europeo, al fine di ottenere risultati d'impatto che promuovano efficacemente gli interessi europei nella standardizzazione della PQC.
Inoltre, le proposte si sforzeranno di stabilire dialoghi costruttivi con i programmi PQC internazionali e di promuovere attività di cooperazione internazionale. L'accento dovrebbe essere posto sugli scambi di collaborazione tra i principali partecipanti internazionali, tra cui l'UE e paesi come gli USA, sfruttando i punti di forza e le sfide complementari e promuovendo risultati reciprocamente vantaggiosi negli sforzi di standardizzazione.
Questa azione mira a supportare le parti interessate che si occupano di tecnologie che saranno utilizzate per proteggere la sicurezza informatica degli asset industriali critici con un nuovo paradigma che è destinato a cambiare le carte in tavola nel campo della crittografia. Il controllo di tali strumenti è di estrema importanza sia per i governi che per l'industria, in quanto potrebbero essere sfruttati da attori malintenzionati. Per questo motivo, devono essere protetti da possibili dipendenze e vulnerabilità nella sicurezza informatica per prevenire l'influenza e il controllo stranieri. La partecipazione di entità extra-UE comporta il rischio che informazioni altamente sensibili su infrastrutture di sicurezza, rischi e incidenti siano soggette a legislazioni o pressioni che obbligano tali entità extra-UE a divulgare tali informazioni a governi extra-UE, con un rischio di sicurezza imprevedibile. Pertanto, in base alle ragioni di sicurezza

esposte, le azioni relative a queste tecnologie sono soggette all'articolo 12, paragrafo 5, del Regolamento (UE) 2021/694.

Criteri di eleggibilità:
Le domande saranno considerate ammissibili solo se il loro contenuto corrisponde interamente (o almeno in parte) alla descrizione del tema per cui sono state presentate. Partecipanti ammissibili (Paesi ammissibili)
Per essere ammissibili, i richiedenti (beneficiari ed enti affiliati) devono:
- essere persone giuridiche (enti pubblici o privati)
- essere stabilito in uno dei paesi ammissibili, ossia:
- Stati membri dell'UE (compresi i paesi e territori d'oltremare (PTOM))
- Paesi SEE (Norvegia, Islanda, Liechtenstein)
I beneficiari e gli enti affiliati devono iscriversi al Registro dei Partecipanti - prima di presentare la proposta - e dovranno essere convalidati dal Servizio Centrale di Convalida (REA Validation).
Per la convalida, sarà richiesto loro di caricare documenti che dimostrino lo status giuridico e l'origine.
Altre entità possono partecipare in altri ruoli del consorzio, come partner associati, subappaltatori, terze parti che forniscono contributi in natura, ecc.
Si ricorda che tutti i temi di questo bando sono soggetti a restrizioni per motivi di sicurezza, pertanto i soggetti non devono essere controllati direttamente o indirettamente da un Paese che non sia un Paese ammissibile. Tutti i soggetti5 dovranno compilare e presentare una dichiarazione sulla proprietà e sul controllo.
Inoltre:
- la partecipazione a qualsiasi titolo (come beneficiario, entità affiliata, partner associato, subappaltatore o destinatario di sostegno finanziario a terzi) è limitata alle entità dei paesi ammissibili
- le attività del progetto (compreso il lavoro in subappalto) devono svolgersi nei paesi ammissibili
- la Convenzione di sovvenzione può prevedere restrizioni sui DPI
Composizione del consorzio - nessuna restrizione
Per l'argomento DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD Standardizzazione e sensibilizzazione della transizione europea alla crittografia post-quantistica la durata indicativa dell'azione è fino a 36 mesi, ma non si escludono altre durate.

Contributo finanziario:
Tipo di azione e tasso di finanziamento Sovvenzione per azioni di coordinamento e sostegno - tasso di finanziamento del 100%.
- Per il tema DIGITAL-ECCC-2024-DEPLOY-CYBER-06-PQCSTANDARD Standardizzazione e consapevolezza della transizione europea alla crittografia post-quantistica: 1 milione di euro per progetto.
Bilancio complessivo per questo invito 1.000.000 EUR

Scadenza:
26 marzo 2024 17:00:00 ora di Bruxelles

Ulteriori informazioni:
call-fiche_digital-eccc-2024-deploy-cyber-06_en.pdf (europa.eu)