Transizione della crittografia post-quantum
Post-quantum cryptography transition

TOPIC ID:
HORIZON-MSCA-2023-DN-01-01

Ente finanziatore:
Commissione europea
Horizon Europe program

Obiettivi ed impatto attesi:
I risultati dei progetti dovrebbero contribuire ad alcuni o a tutti i seguenti risultati:
- Aumento della maturità degli attuali algoritmi crittografici post-quantistici e contributo a un'ulteriore standardizzazione;
- Strumenti di facile utilizzo per l'implementazione su larga scala di algoritmi di crittografia post-quantistica, basati su standard all'avanguardia;
- transizione sicura ed efficiente dalla crittografia pre-quantistica a quella post-quantistica attraverso strumenti che implementano un approccio ibrido che combina algoritmi a chiave pubblica pre-quantistica riconosciuti e algoritmi post-quantistici aggiuntivi; - introduzione graduale di algoritmi o protocolli post-quantistici in applicazioni nuove o esistenti;
- Dimostratori e implementazioni di buone pratiche di algoritmi crittografici post-quantistici su diverse piattaforme hardware e software;
- Raccomandazioni orientate all'applicazione per l'implementazione diffusa della crittografia post-quantistica in tutta l'UE.

Ambito di applicazione: L'avvento dei computer quantistici su larga scala comprometterà gran parte della crittografia moderna, che è fondamentale per garantire la sicurezza informatica e la privacy della transizione digitale. Qualsiasi primitiva crittografica basata sulla fattorizzazione degli interi e/o sui problemi di logaritmo discreto sarà vulnerabile ad attacchi su larga scala basati sulla tecnologia quantistica. I dati/prodotti/sistemi digitali che derivano la loro sicurezza dalle primitive sopra citate saranno compromessi e dovranno essere aggiornati - compresa la loro sostituzione, se necessaria - con una crittografia resistente ai quanti.

L'enorme portata di questo aggiornamento previsto dimostra che è necessario prepararsi oggi per poter implementare ampiamente le relative mitigazioni in futuro. Molte aziende e governi non possono permettersi che le loro comunicazioni/dati protetti vengano decriptati in futuro, anche se questo futuro sembra ancora lontano. È necessario avanzare rapidamente nella transizione verso una crittografia resistente ai quanti. Gli algoritmi di crittografia post-quantistica dovrebbero essere implementabili in modo dinamico per reagire rapidamente ai nuovi sviluppi dei computer quantistici. Le raccomandazioni per la crittografia post-quantistica sono già state pubblicate, ma devono essere mantenute aggiornate.

Le proposte ricevute nell'ambito di questo argomento devono contribuire a sviluppare raccomandazioni europee coordinate per la transizione alla crittografia post-quantistica in tutta l'UE. Si incoraggia l'identificazione e l'analisi di potenziali aspetti normativi e barriere per le tecnologie/soluzioni sviluppate, se pertinenti.

Criteri di eleggibilità:
Qualsiasi soggetto giuridico, indipendentemente dal suo luogo di stabilimento, compresi i soggetti giuridici di Paesi terzi non associati o di organizzazioni internazionali (comprese le organizzazioni internazionali di ricerca europee) può partecipare (indipendentemente dal fatto che sia idoneo o meno al finanziamento), a condizione che siano state soddisfatte le condizioni stabilite dal regolamento Horizon Europe e qualsiasi altra condizione stabilita nel tema specifico del bando. Per "soggetto giuridico" si intende qualsiasi persona fisica o giuridica costituita e riconosciuta come tale ai sensi del diritto nazionale, del diritto dell'UE o del diritto internazionale, dotata di personalità giuridica e che può, agendo in nome proprio, esercitare diritti ed essere soggetta a obblighi, oppure un soggetto privo di personalità giuridica.
I beneficiari e gli enti affiliati devono registrarsi nel Registro dei Partecipanti prima di presentare la domanda, per ottenere un codice di identificazione del partecipante (PIC) ed essere convalidati dal Servizio Centrale di Convalida prima di firmare la convenzione di sovvenzione. Per la convalida, durante la fase di preparazione della sovvenzione, verrà chiesto loro di caricare i documenti necessari che dimostrino il loro status giuridico e la loro origine. Un PIC convalidato non è un prerequisito per presentare una domanda.

Al fine di conseguire i risultati attesi e salvaguardare le risorse strategiche, gli interessi, l'autonomia e la sicurezza dell'Unione, la partecipazione a questo tema è limitata ai soggetti giuridici stabiliti negli Stati membri, nei paesi associati e nei paesi dell'OCSE. Le proposte che includono soggetti giuridici che non sono stabiliti in questi paesi non saranno ammissibili. Si applicano le seguenti eccezioni: fatte salve le restrizioni per la protezione delle reti di comunicazione europee.

Contributo finanziario:
Contributo UE previsto per progetto La Commissione ritiene che un contributo UE tra i 4 e i 6 milioni di euro consentirebbe di affrontare adeguatamente questi risultati. Tuttavia, ciò non preclude la presentazione e la selezione di una proposta che richieda importi diversi. Budget indicativo Il budget totale indicativo per il tema è di 23,40 milioni di euro.
Tipo di azione Azioni di ricerca e innovazione

Scadenza:
20 novembre 2024 17:00:00 ora di Bruxelles

Ulteriori informazioni:
wp-6-civil-security-for-society_horizon-2023-2024_en.pdf (europa.eu)