PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 27 - numero 5843 di Mercoledì 07 maggio 2025

La crittografia quantistica diventa sempre più accessibile

Tutti gli esperti di sicurezza informatica sanno che ormai il futuro criptografico è affidato alle applicazioni quantistiche. La costante opera normativa di ETSI offre un prezioso contributo ad un utilizzo allargato di questi applicativi criptografici.

ETSI ha annunciato, il 25 marzo 2025, il lancio del suo standard di sicurezza post-quantistico, in grado di garantire la protezione dei dati e delle comunicazioni critiche, in futuro.

La specifica "Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies" (ETSI TS 104 015) è stata sviluppata per migliorare i meccanismi di sicurezza in essere, garantendo che solo gli utenti autorizzati, con le autorizzazioni appropriate, possano accedere ai dati sensibili per decriptografarli.
La nuova specifica ETSI definisce uno schema per i meccanismi di incapsulamento delle chiavi (KEM) con controllo degli accessi (KEMAC), chiamato Covercrypt, che garantisce la sicurezza sia pre-quantistica, sia post-quantistica, attraverso l'ibridazione.

Ciò significa che la criptografia risulta protetta sia contro le minacce attuali, sia contro le future capacità di calcolo quantistico, offrendo una transizione senza soluzione di continuità verso un panorama criptografico più avanzato. In pratica, le chiavi di sessione risultano bloccate, in base agli attributi dell'utente e mantenute anonime; solo gli utenti, con attributi che soddisfino la politica di incapsulamento, saranno in grado di recuperare le chiavi di sessione, mentre coloro che non sono autorizzati non saranno in grado di farlo.

Ad esempio, mentre un reparto IT può definire chi accede alle applicazioni, lo standard ETSI KEMAC aiuta a determinare chi può decrittografare i dati all'interno di tali applicazioni, attraverso una specifica politica di accesso.

Questa nuova soluzione rappresenta una vera e propria svolta in termini di efficienza: bastano poche centinaia di microsecondi per incapsulare e de-capsulare le chiavi di sessione.

"L'ultima specifica di ETSI segna una pietra miliare significativa nella transizione verso la crittografia post-quantistica", ha dichiarato Matt Campagna, presidente del gruppo di lavoro ETSI QSC (Quantum Safe Cryptography). "Questo standard è fondamentale per il futuro quantistico, in quanto oggi siamo in grado di consentire alle organizzazioni di salvaguardare i propri

dati sensibili, sia per oggi, sia per i decenni a venire. Il lavoro che abbiamo svolto nel gruppo di lavoro Cyber QSC sottolinea il nostro impegno a fornire soluzioni sicure ed a prova di futuro, in grado di resistere alle minacce emergenti, contribuendo al contempo a costruire un ecosistema industriale sano ed un'economia sostenibile".

Ricordiamo ai lettori che le organizzazioni che guardano al futuro debbono sin da oggi iniziare a utilizzare la criptografia quantistica, per

- rendere la sicurezza dei dati a prova di futuro,
- salvaguardare le informazioni sensibili da attacchi di malintenzionati e
- garantire la conformità agli standard in evoluzione.

La soluzione di crittografia ETSI Covercrypt è progettata per proteggere dalle minacce emergenti, poste dall'informatica quantistica, e offre un sistema di crittografia ibrido ad alte prestazioni, che può essere facilmente e prontamente integrato nei prodotti di sicurezza commerciali esistenti.
Ad esempio, una azienda del settore sta già lanciando la sua nuova soluzione di criptografia, basata appunto su questo standard ETSI.

Ricordiamo ai lettori che ETSI fornisce ai membri un ambiente aperto e inclusivo per supportare lo sviluppo, la ratifica e la sperimentazione tempestivi di standard applicabili a livello globale per sistemi, applicazioni e servizi abilitati alle ITC in tutti i settori dell'industria e della società. È un ente senza scopo di lucro, con più di 900 organizzazioni associate in tutto il mondo, provenienti da oltre 60 paesi e cinque continenti. I membri comprendono un pool diversificato di grandi e piccole aziende private, enti di ricerca, università, governi e organizzazioni pubbliche. L'ETSI è uno dei soli tre organismi ufficialmente riconosciuti dall'UE come European Standards Organization (ESO), oltre a CEN e CENELEC

ETSI TS 104 015 V1.1.1 (2025-02) - Cyber Security (CYBER); Quantum-Safe Cryptography (QSC); Efficient Quantum-Safe Hybrid Key Exchanges with Hidden Access Policies

Adalberto Biasiotti