MINISTERO DELLA DIFESA
AGENZIA INDUSTRIE DIFESA
DIREZIONE GENERALE

Piazza della Marina, 4 - 00196 ROMA
E-mail: aid@aid.difesa.it - PEC: aid@postacert.difesa.it

Allegato A

CARATTERISTICHE TECNICHE

1. Una piattaforma di comunicazione sicura, decentralizzata, in tempo reale, distribuita non rintracciabile anonima e crittografata post-quantum caratterizzata da:
   - Crittografia sicura PQC end-to-end [NIST Module-Lattice-Based Key-Encapsulation Mechanism (ML-KEM) compatibile con FIPS 203];
   - Software-Defined Network (SDN) brevettato e progettato per interrompere la raccolta e l'analisi dei Pattern of Life (POL), garantendo una connessione sicura e resiliente tra infrastrutture, endpoint, server e servizi;
   - Messaggi vocali e di testo/chat, video, videoconferenze (anche di gruppo), condivisione di file (di tipo eterogene, in transito e a riposo), mimetizzati e blindati;
   - Distribuzione Flessibile e Universale: cloud o on-prem, virtuale o "bare metal";
   - Al 99,999% resistente agli attacchi cibernetici grazie al server virtuale dissimulato crittografato (SDQC);
   - Protezione dalla raccolta e dall'analisi dei "pattern of life";
   - Controllo Completo o Servizio Gestito;
   - Comunicazioni segmentate;
   - Nessun scraping o registrazione delle informazioni di contatto del dispositivo, dei dati o delle informazioni sulle attività.
   - Perfettamente compatibile con il router mobile 5G da viaggio con WiFi e Telefono cifrato;
   - Nessuna terza parte ha accesso ai dati;
   - Nascosta ed Installabile su qualsiasi computer;
   - Supporta casi d'uso unici con implementazioni decentralizzate, bridge di reti e persino reti private o chiuse autonome (ad es. reti Mesh Ad hoc, cellulari private, ecc.).

2. Soluzioni di comunicazione portatile: kit di soluzioni mobili con un telefono cifrato, una chiave cifrata, un tablet o un computer portatile appositamente configurato e un router da viaggio Mobile 5G WiFi; da utilizzare con la piattaforma di comunicazione.

   - Router da viaggio Mobile 5G senza attribuzione:

   - Soluzione internet globale 5G anonima;
   - Velocità fino a 10 volte superiore a quella del 4G;
   - Wi-Fi 6E abilitato, fino a 32 dispositivi;
   - Connettività a batteria per tutto il giorno;
   - Crittografia post-quantistica end-to-end;
   - Accesso globale a Internet;

- Rete di punti di accesso (APN) fornita dal carrier o rete privata opzionale Quantum Ket Access Point Network (APN) per offuscare, criptare PQC dual-layer e instradare privatamente i dati cellulari tramite Quantum Ket Encrypted Network (QEN);

- Telefono Cifrato: Smartphone resistenti agli attacchi cibernetici. Servizi Cyber VOIPper numeri selezionabili da oltre 30 paesi;

- Chiave Cifrata: unità miniaturizzata, bootable, crittografata d'avanguardia per un ambiente di calcolo completo e senza tracce.

- Supporta Windows, Ubuntu, MacOS e Kali Linux; suite Microsoft Office, chat sicure ed e-mail crittografate;
- PQC Mercury VPN Client;
- protezione dei dati in transito e a riposo;

3. Rete decentralizzata resistente ad attacchi cibernetici:
   L'SDN con crittografia post-quantistica con una rete distribuita e sicura che nasconde, collega e protegge qualsiasi end point, server, servizio o infrastruttura da qualsiasi luogo, deve prevedere almeno la configurazione di 5 server e (scala infinita) l'SDN criptato con le seguenti caratteristiche:
   - Non conserva alcun contenuto;
   - Piattaforma crittografata completamente decentralizzata e multilivello;
   - Offusca i percorsi di trasporto con una randomizzazione complessa, non proxy o il protocollo Onion Router dipendente;
   - La firma digitale riguarda solo il traffico web HTTPS;
   - Nessuna porta aperta standard predefinita e nessun servizio predefinito;
   - Sistema di rilevamento delle intrusioni abilitato;
   - Nessun accesso root e nessun privilegio di console;
   - IPv6 disabilitato (opzionale);
   - Distribuzione flessibile, virtuale o fisica (ad esempio, VPS, "bare-metal", hypervisor)
   - Console molto sicura: Chiave privata a 4096 bit e porta randomizzata;

4. Protezione degli utenti e dell'infrastruttura distribuita:
   Disponibile anche come Virtual Private Server (VPS) anonimo e con protezione post-quantum con un numero di connessioni da 1 a 100;

5. Sincronizzazione dello storage distribuito;

6. Archiviazione dei dati con crittografia post-quantistica – (Quantum Data Server – QDS):
   QDS è un server di archiviazione dati privato e criptato con crittografia post-quantistica che protegge sia i dati a riposo che quelli messi in movimento in scrittura o ad accesso distribuito. Le opzioni di dimensionamento dello storage sono 16 TB, 24 TB, 32 TB, 64 TB e fino a 100 TB;

7. Mimetizzazione e protezione di server, servizi ed e-mail: SDQC:

Proteggere i server, i siti web e i servizi pubblici rivolti a internet.
Quantum Ket impiega tecniche avanzate basate sull'offuscamento per camuffare e proteggere l'infrastruttura di server e servizi critici, indipendentemente da dove risiedono. Un server virtuale dissimulato crittografato (SDQC) si installa davanti a un server pubblico rivolto a Internet instradando tutto il traffico attraverso la Rete Crittografata Quantum Ket (QEN) nascondendo l'indirizzo reale del proprio server e i punti di accesso. Altre opzioni includono high-fidelity decoys e caratteristiche di progettazione per il depistaggio.
Per le esigenze di isolamento della rete o del sistema Quantum Ket offre un rete privata virtuale indipendente (VPN) Server con crittografia avanzata, sicurezza solida e anonimato assoluto.

8. Hosting e-mail privato criptato PQC.

Il RUP

_____