



Strictly Private & Confidential

# Summary



- ✓ **True Randomness<sup>(1)</sup>**
- ✓ **Customizable Encryption Options<sup>(2)</sup>**
- ✓ **Robust Multi-Layer Security Protocol<sup>(3)</sup>**
- ✓ **Flexible Deployment Architecture<sup>(4)</sup>**
- ✓ **Optional Master-Key<sup>(5)</sup>**

## Notes

- (1) Leveraging proprietary Single Photon Quantum Random Number Generator which adhere to the stringent standards set by the NIST (SP 800-90B) and has received certification from METAS. Competitors like Telegram and Signal rely on Pseudo Generated Random Numbers which are inherently less secure due to their predictable
- (2) AES-256 or advanced Post-Quantum algorithms such as ML-KEM (Kyber KEM), ML-DSA (Dilithium) with E2EE (End-to-End Encryption) and PFS (Perfect Forward Secrecy)
- (3) Security is further underscored by a three-tier security protocol: (A) TLS 1.3 : Establishes a secure connection to prevent eavesdropping and tampering, (B) Channel encryption: Secures the communication channels, safeguarding data in transit, and (C) Message encryption: Ensures that the content of your messages remains private and accessible only to intended recipients
- (4) Cloud-Hosted Service (GCP) or On-Premise for heightened security and complete autonomy over the data environment
- (5) System can be deployed with or without Master-Key. If deployed with Master-Key, the dedicated, own Master-Key can be used for regulatory, audit trail, and/or monitoring/ control purposes