LUSNA | QUANTUM SECURITY PLATFORM

Q-Day

In the near future, quantum computers will break the encryption algorithms that we rely upon in email, cloud, banking, and other critical communication systems — this date we call Q-Day.

Keeping your company's information private is crucial in order to stay in the game. Information such as sensitive clientele data, corporate decision-making processes, internal communications, future strategies, etc, are at **risk of being retroactively decrypted.**

6 000 hours

THE LUSNA TEAM HAS SPENT TIME ASSEMBLING THE NEXT-GENERATION **POST-QUANTUM COMMUNICATIONS PLATFORM** FOR DEVELOPERS TO BE USED BY INDIVIDUALS, INDUSTRY, AND GOVERNMENT

THE LONGER WE WAIT, THE MORE DAMAGE INCURRED. ALL DATA THAT HAS EVER BEEN CAPTURED IS AT IMMINENT RISK OF BEING RETROACTIVELY DECRYPTED AFTER Q-DAY

NIST National Institute of Standards and Technology

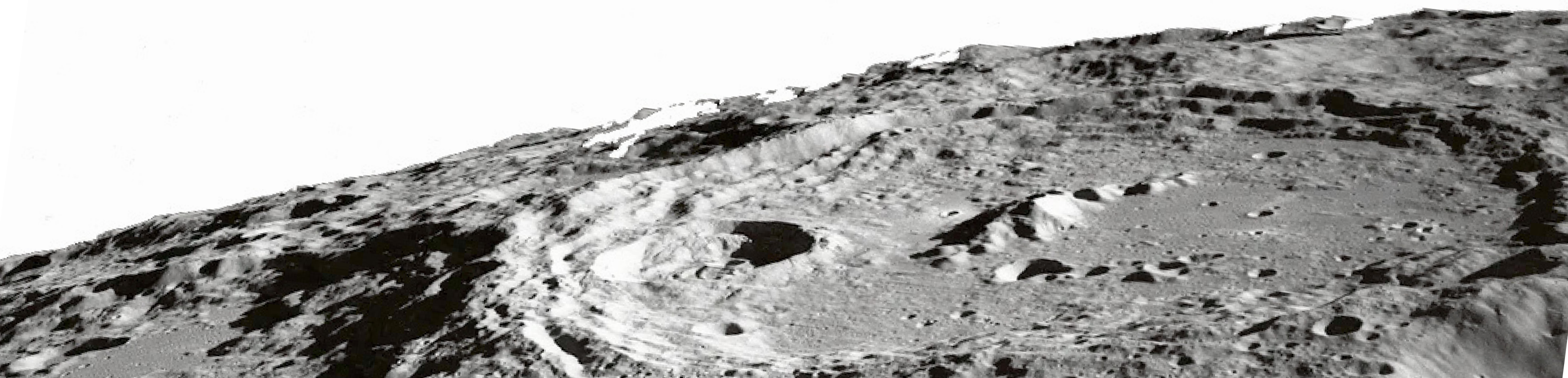
Lusna uses the most sophisticated post-quantum cryptographic mechanisms from the NIST competition

Post-Quantum Cryptography Standardization is a program and competition by the NIST to update the world's encryption standards to include post-quantum cryptography.

LUSNA IS ON THE FRONTIER OF DEVELOPING APPLIED PROTECTION AGAINST THE QUANTUM THREAT AND OFFERING A RANGE OF UNIQUE **COMMERCIAL** AND **GOVERNMENT SOLUTIONS**

What do we have today?

- The cloud encryption platform is in the beta stage after more than 6000 hours of development
- Extensive testing has been done
- The Messenger/File-sharing app is in the MVP stage



LUSNA | QUANTUM SECURITY PLATFORM

WHO NEEDS LUSNA?

PRIVATE

P2P messaging protocols, secure communication platforms

Q-safe calling, video chat

Q-safe File-sharing

Q-safe SDK for App development

Secure crypto currency wallet infrastructure

ENTERPRISE

Enterprise-private communications

Customer onboarding workflow, secure Know Your Customer (KYC) checks

Cloud communications

Platform for secure P2P applications

Database APIs

GOVERNMENT

Military communications

City/Public-Work Communications

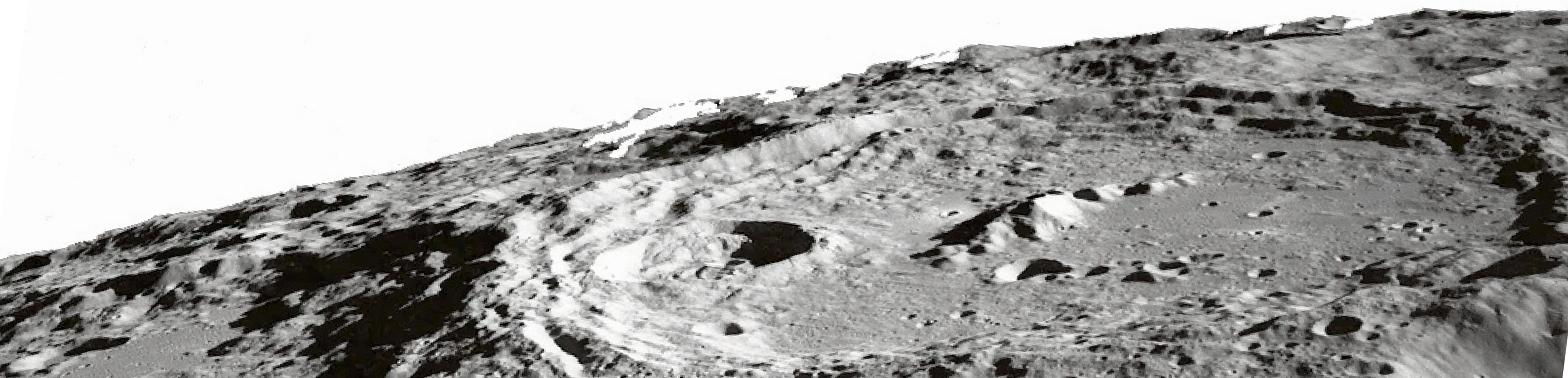
Voting systems

Secure GIS systems

Critical Infrastructure

WHY LUSNA?

Features	wickr	Signal	LUSNA	**Lusna additional information**
Programming language	C (last-gen.)	C/Java (soon Rust)	Rust	Rust is inherently **memory-safe** and high-performance
Encryption Algorithm	AES-256	AES-256	AES-256-GCM-SIV	Or: Xchacha20poly1305
Endpoint-to-endpoint Encryption	✓	✓	✓	Separate peer/server and p2p keys
Perfect Forward Secrecy	✓	✓	✓	Using extended double-ratchet algorithm
File transfer support	✓	✓	✓	Tests show Lusna up to **50% faster** than SCP
File Transfer Scrambling	✗	✗	✓	Scramble key is independent to data encryption key
User-based Authentication	✓	✗	✓	Argon2id-hashed password is **more secure than Wickr's**
Device-dependent Authentication	✗	✓	✓	Additional security measure
Post-Quantum Key Exchange	✗	✗	✓	Firesaber, NIST post-quantum finalist
Custom Central Nodes	enterprise only	advanced setup	all versions	Built-in peer-discovery enables **p2p connections**
Variable security levels	✗	✗	✓	**Multi-layered encryption**, 256 possible security levels
Passive background re-keying	✗	✗	✓	The re-keying frequency is determined by the security level
Single-threaded/multi-threaded mode	✗	✗	✓	Single = **lower latency**. Multi = **higher throughput**
Built-in Google FCM Compatibility	✗	✓	✓	Quantum security maintained through Google servers



LUSNA | QUANTUM SECURITY PLATFORM

WE ALREADY HAVE THE TECNOLOGY BUILT

WE SEEK FUNDING

FOR

- **GETTING LEGAL ON BOARD**
- **DEVELOP MARKETING**
- **BUILD SALES DEPARTMENT**

You can participate in the next big thing in the field of cybersecurity

Investment in our company will open doors for us that remain closed for others at an opportune and necessary time in cyber history