qanapi

WHITEPAPER

KARST_ECHO

Beyond QKD

How Decentralized Key Management Overcomes the 5 limitations the NSA Identified with Quantum Key Distribution

PREPARED BY

Paul Bockelman

Chief Technology Officer & VP Product Engineering

Qanapi Group, Inc.

RESTON | WASHINGTON, DC | SYDNEY

Originally Published: February 2026

Revised: June 2026

CONTENTS

Table of Contents

Executive Summary

The National Security Agency's advisory on Quantum Key Distribution (QKD) and Quantum Cryptography (QC) identifies five specific technical limitations that prevent the agency from recommending QKD for securing National Security Systems. These aren't minor caveats as they represent fundamental architectural constraints that prevent QKD from operating at the scale, flexibility, and assurance level modern defense operations demand.

Yet the underlying operational need QKD was designed to address, secure, resilient cryptographic key distribution across contested, distributed environments, remains one of the most pressing challenges in national defense. The 2026 National Defense Strategy makes this explicit, mandating modernized key management that operates across distributed networks. The Q-BID Critical Technology Area adds requirements for assured communications in contested electromagnetic environments.

Qanapi's Karst_Echo is a decentralized key management service that approaches this problem from a fundamentally different direction. Rather than relying on quantum physics to secure key transmission, Karst_Echo uses Verifiable Concealed Shares (VCS). VCS is a patent-pending approach built on threshold cryptography with a goal to eliminate the need for secure point-to-point key transmission entirely. The result is a system that achieves the security objectives QKD promises while avoiding every limitation the NSA has identified.

Here is how Karst_Echo addresses each one.

Limitation 1: QKD Is Only a Partial Solution

NSA POSITION

> *"QKD generates keying material for an encryption algorithm that provides confidentiality. [It] does not provide a means to authenticate the QKD transmission source. Therefore, source authentication requires the use of asymmetric cryptography or preplaced keys."*

KARST_ECHO RESPONSE

QKD addresses only one dimension of the cryptographic problem: confidentiality of key material in transit. It cannot authenticate the source of a key exchange, which means organizations still need conventional asymmetric cryptography layered alongside QKD negating much of the theoretical benefit.

Karst_Echo is architected as a complete key lifecycle management system, not merely a key transport mechanism. The platform covers creation, distribution, rotation, versioning, policy enforcement, and destruction of key material through a unified API. Source authentication is handled natively through the Access and Authorization Director (AAD), which enforces Role and Attribute-Based Access Control (R/ABAC) at every distribution point. Identity verification, classification, clearance, and mission context are all evaluated before any key share is released.

The hierarchical key structure includes Master Encryption Keys generating Key Encryption Keys, which in turn protect Data Encryption Keys thus providing fine-grained access control at the individual data-object level. This is a complete cryptographic management architecture, not a partial solution requiring supplemental systems.

Limitation 2: QKD Requires Special Purpose Equipment

NSA POSITION

> *"QKD is based on physical properties, and its security derives from unique physical layer communications. This requires users to lease dedicated fiber connections or physically manage free-space transmitters. It cannot be implemented in software or as a service on a network."*

KARST_ECHO RESPONSE

This may be the most operationally disqualifying limitation of QKD. Requiring dedicated fiber optic connections or line-of-sight transmitters is incompatible with how modern defense operations actually work and forces deploy rapidly, operate across global distances, and rely on whatever communications infrastructure is available.

Karst_Echo is entirely software-defined. It operates as a containerized service deployable on commodity hardware across six operational tiers: from hyperscale cloud providers (AWS GovCloud, Azure Government, GCP) down to micro-devices like NVIDIA Jetson and tactical radios. There is no specialized hardware. No dedicated fiber. No free-space optical links.

Because Karst_Echo is API-driven, it integrates into existing network infrastructure rather than demanding parallel physical systems. The hybrid HTTP/UDP transport protocol enables key distribution across any available channel be it satellite, HF radio, tactical mesh networks, commercial cellular, or standard IP networks. This protocol-agnostic approach means Karst_Echo adapts to operational reality rather than constraining it.

Equally critical: because it's software, Karst_Echo can be patched, upgraded, and reconfigured without hardware replacement. This is a significant capability QKD's hardware-bound architecture fundamentally cannot match.

Limitation 3: QKD Increases Infrastructure Costs and Insider Threat Risks

NSA POSITION

> *"QKD networks frequently necessitate the use of trusted relays, entailing additional cost for secure facilities and additional security risk from insider threats. This eliminates many use cases from consideration."*

KARST_ECHO RESPONSE

QKD's distance limitations force the use of trusted relay nodes as physical facilities where quantum keys are decrypted, re-encrypted, and forwarded. Each relay is a point of vulnerability: it must be physically secured, staffed, and trusted. This creates both a cost problem and, as the NSA explicitly notes, an insider threat vector.

Karst_Echo eliminates trusted relays entirely. The Verifiable Concealed Shares architecture means no single node ever holds complete key material. Shares are distributed across multiple independent endpoints, and VCS-secured threshold cryptography ensures that compromising any individual relay, node, or insider yields zero cryptographic value. An adversary or a malicious insider would need to simultaneously breach multiple, geographically and logically separated systems to reconstruct a key.

The infrastructure cost model is also inverted. QKD requires dedicated facilities, specialized equipment, and fiber leases. Karst_Echo operates on an OPEX model using existing infrastructure. It scales elastically from a single containerized instance to a globally distributed deployment with flexible pricing and no capital expenditure for dedicated cryptographic hardware.

Limitation 4: Securing and Validating QKD Is a Significant Challenge

NSA POSITION

> *"The actual security provided by a QKD system is not the theoretical unconditional security from the laws of physics... but rather the more limited security that can be achieved by hardware and engineering designs. The specific hardware used to perform QKD can introduce vulnerabilities."*

KARST_ECHO RESPONSE

This is a particularly damaging finding. QKD's marketing promise *"security guaranteed by the laws of physics"* collapses when theory meets implementation. Real QKD hardware introduces side channels, timing vulnerabilities, and engineering tolerances that have been exploited in multiple published attacks. The gap between theoretical and implemented security is wide, and validating QKD systems to cryptographic standards is, as the NSA notes, extraordinarily difficult.

Karst_Echo builds on proven, well-understood mathematical foundations. The Verifiable Concealed Shares mechanism is rooted in threshold cryptography, a field with decades of peer review, formal security proofs, and operational deployment history. The underlying cryptographic algorithms (AES-256, Kyber, Dilithium, SHA-3) are NIST-standardized and FIPS 140-3 validated, with well-characterized security properties and known attack surfaces.

Because Karst_Echo is software-defined, it benefits from established validation methodologies: code audits, penetration testing, formal verification, and continuous security monitoring. When vulnerabilities are discovered, they can be patched through software updates without replacing physical hardware or re-engineering optical systems. The result is a system with a well-understood, validatable risk profile rather than one dependent on manufacturing tolerances of quantum optical components.

Limitation 5: QKD Increases the Risk of Denial of Service

NSA POSITION

> *"The sensitivity to an eavesdropper as the theoretical basis for QKD security claims also shows that denial of service is a significant risk for QKD."*

KARST_ECHO RESPONSE

This is perhaps QKD's cruelest irony. The very mechanism that provides its theoretical security advantage, the ability to detect eavesdropping through quantum state disturbance, creates an inherent denial-of-service vulnerability. Any interference with the quantum channel, whether from an adversary, environmental noise, or equipment malfunction, halts key distribution. In contested electromagnetic environments, this makes QKD fundamentally unsuitable.

Karst_Echo is designed from the ground up for Denied, Disrupted, Intermittent, and Limited bandwidth (DDIL) environments precisely the conditions where QKD fails. The threshold-based VCS architecture provides multiple layers of resilience.

Pre-positioned Command and Control at forward operating locations enable local key reconstruction without reach-back to any central infrastructure. The N-of-M threshold configuration (for example, requiring 7 of 10 shares to reconstruct a key) means operations continue even when a significant portion of nodes are unreachable due to jamming, destruction, or network degradation. If some distribution paths are denied, shares route across whichever channels remain available whether satellite, HF, mesh, or commercial cellular.

In the adversary capture scenario, Karst_Echo actually strengthens security posture: the captured device's shares become cryptographically useless because mere possession of partial shares is insufficient for reconstruction. Remaining force elements can reconstitute a key without the compromised endpoint as long as the share threshold is met. The mission continues.

The Architectural Difference

The contrast between QKD and Karst_Echo isn't incremental, it's architectural. They approach the same problem from opposite directions: QKD attempts to make key *transmission* secure through physics; Karst_Echo eliminates the need for secure transmission by distributing key *fragments* that are individually worthless and temporal constrained.

DIMENSION	QKD LIMITATION	KARST_ECHO APPROACH
Scope	Key transport only; requires supplemental authentication	Full lifecycle: create, distribute, rotate, enforce, destroy
Infrastructure	Dedicated fiber or free-space optics; hardware-bound	Software-defined; any network, any hardware
Cost Model	High CAPEX; dedicated facilities; trusted relays	OPEX; elastic scaling; no dedicated hardware
Insider Threat	Trusted relays create exposure points	No node holds complete key material
Validation	Hardware-dependent; difficult to validate against theory	Software-based; FIPS 140-3 validated; patchable
Denial of Service	Eavesdropper detection = inherent DoS vulnerability	DDIL-native; threshold tolerance; multi-path distribution
Quantum Readiness	Requires dedicated quantum channel	Crypto-agile; NIST PQC algorithms with hot-swap
Upgradability	Hardware replacement required	Library-level software update

Aligned with NSA's Recommended Path Forward

The NSA's advisory doesn't just identify QKD's limitations, it points toward a solution direction. The agency explicitly states that it views quantum-resistant (post-quantum) cryptography as a more cost-effective and easily maintained solution than quantum key distribution, and references NIST's post-quantum cryptography standardization effort as the path forward.

Karst_Echo is built directly on this guidance. The system provides native support for NIST Post-Quantum Cryptography finalists, including Kyber for key encapsulation and Dilithium for digital signatures, while maintaining FIPS 140-3 validation. The library-agnostic, crypto-agile architecture means that as NIST finalizes additional standards or as the cryptographic landscape evolves, Karst_Echo adapts through library-level updates rather than infrastructure replacement.

This crypto-agility isn't a future roadmap item, it's a core architectural principle. Karst_Echo was designed with the explicit expectation that cryptographic standards will continue to evolve, and that any system locked to a single algorithm or hardware implementation will become a liability rather than an asset.

KEY TAKEAWAY

QKD and Karst_Echo both address the challenge of secure key distribution in adversarial environments. But where QKD constrains operations to match its physical requirements including dedicated channels, specialized hardware, and trusted relays. Karst_Echo is a composable architecture that deploys in the shape of the mission. One architecture. Six deployment tiers. Every mission profile from hyperscale cloud to a tactical radio on a dismounted operator.

From Theory to Operations

The 2026 National Defense Strategy and Q-BID Critical Technology Area have established the operational requirements clearly: key management must be net-centric, contested-environment-ready, coalition-capable, quantum-resistant, mission-integrated, and spectrum-agile. QKD, as the NSA has assessed, cannot meet these requirements in its current form.

Karst_Echo demonstrates full alignment across all six integrated requirement categories. It does so not by attempting to solve the key distribution problem through physics, but by rendering the problem architecturally irrelevant. When key shares are individually worthless, the security of the transmission channel becomes a secondary concern. When reconstruction is threshold-based, denial of any single path doesn't deny the capability. When the entire system is software-defined and API-driven, it meets the force where the force operates… not where the infrastructure allows.

The quantum threat to current cryptographic systems is real and will eventually materialize. But the solution isn't to build an entirely parallel physical infrastructure vulnerable to the operational realities of contested environments. The solution is to build key management that works with the networks, hardware, and operational conditions that exist today while being cryptographically prepared for the threats of tomorrow.

That is what Karst_Echo was designed to do.

END OF DOCUMENT

About Qanapi Group

Qanapi is revolutionizing cybersecurity through it's API-driven data protection platform called Karst. Its core mission is to provide state-of-the-art support for post-quantum encryption and data protection that integrates directly at the data level. The platform's foundational principle is a Zero Trust framework applied to the data itself, ensuring that security context, identity, and policy remain with the data object regardless of the infrastructure, network, or application it traverses.

CONTACT INFORMATION

Qanapi Group, Inc.

info@qanapi.com

www.qanapi.com

Reston | Washington, DC | Sydney

DOCUMENT CLASSIFICATION

UNCLASSIFIED

VERSION

1.3 - June 2026
