Next-Generation Secure Communications:

Qwyit as a Standalone Solution and as a Security Enhancement

Summary Introduction

Imagine you are sending a message, making a phone call, or transmitting data from a device such as a medical monitor, autonomous vehicle, or industrial sensor. Right now, most communication systems, whether apps, phone networks, or embedded devices, use a kind of digital lock to keep information private. These locks are strong against today's hackers, but they rely on complex mathematical problems that super-powerful future computers, called quantum computers, could easily solve and break open. Once those computers exist, the digital locks used by many secure systems, from messaging applications to Internet of Things (IoT) devices, would no longer be reliable.

Qwyit is a new kind of digital lock that does not depend on these vulnerable mathematical problems. Instead, it uses a fundamentally different approach: a fast and efficient encryption method where every tiny piece of data is protected with its own unique key, combined with a system that continuously verifies the identity of the communicating parties or devices. This makes encryption virtually impossible to crack, even with quantum computers. Qwyit can operate on its own as a fully secure platform for messaging, voice calls, video, and data transmission, or it can be integrated into existing systems, whether communication applications, IoT devices, enterprise software, or operating systems, like a stronger protective layer that enhances whatever security those systems already have.

The versatility of Qwyit extends beyond traditional communications to a wide range of applications, including securing data streams from wearable medical devices, protecting command and control links for drones and autonomous vehicles, safeguarding file systems and network traffic, and providing continuous protection within operating systems. By using Qwyit, whether as a standalone solution or as an enhancement to existing products, companies and developers can ensure that their communications and data transmissions, across mobile applications, embedded devices, enterprise environments, and beyond,

remain reliably private and secure, even in the face of the most advanced future threats, including quantum computing attacks.

Technical Overview and Value Proposition

Qwyit represents a fundamentally new approach to secure communications, offering two primary deployment models: a standalone communication platform and an integration layer for enhancing existing systems. In both cases, Qwyit's core technologies, QCy™, a lightweight stream cipher that applies a unique key to every bit of data, and QwyitKey™, a continuous multi-channel authentication mechanism, provide capabilities that surpass the limitations of current cryptographic protocols.

Current secure communication platforms, such as Signal, WhatsApp, and FaceTime, rely primarily on symmetric ciphers like AES-256 combined with public-key mechanisms such as Elliptic Curve Diffie-Hellman (ECDH). While these systems provide effective protection against classical computing threats, they are inherently vulnerable to quantum attacks, specifically Shor's algorithm, which efficiently solves the discrete logarithm and factoring problems underlying ECDH and other elliptic curve cryptosystems. Additionally, these platforms perform authentication only at session initiation, leaving them susceptible to undetected compromise during an active session.

Qwyit addresses these limitations without dependence on discrete-logarithm-based mathematics. Its architecture ensures that no cryptographic primitive is vulnerable to quantum speedup, while introducing per-event authentication that verifies the ongoing integrity of participating devices. This combination enables two distinct product offerings:

1. **Standalone Communication Platform**
   Qwyit can be deployed as a complete, self-contained application for messaging, voice, video, and IoT communications. Operating independently of existing infrastructure, it eliminates reliance on centralized key servers or traditional public key infrastructure (PKI). Communications are secured with bit-level unique keys and continuously authenticated across multiple independent channels, providing forward secrecy, post-compromise security, and resistance to impersonation without exposing metadata through server-mediated routing.

2. **Security Enhancement Layer**
   Qwyit can be integrated into existing platforms as a drop-in cryptographic layer, replacing or augmenting vulnerable components while preserving compatibility with current application architectures. This modular approach allows platform owners to incrementally upgrade their security profile without redesigning their entire system.

Integration and Improvement Potential for Communications

The following outlines how Qwyit, whether as a standalone solution or an enhancement layer, addresses the key limitations of major communication platforms:

- Key Differentiators: Unlike existing systems, Qwyit provides continuous authentication throughout a communication session, detecting and preventing compromise even after initial verification. Its stream cipher operates with per-bit key uniqueness, ensuring that partial decryption of captured traffic reveals no usable information, and it requires significantly lower computational resources than AES-based systems with equivalent security margins.

Deployment Flexibility: Qwyit's software development kit (SDK) enables straightforward integration at the application layer. For standalone use, the full protocol stack—including encryption, authentication, and routing obfuscation—can be implemented independently. As an enhancement layer, targeted components such as key agreement, encryption primitives, and identity verification can be selectively replaced.

Commercial and Strategic Advantages

Deploying Qwyit, either as a standalone platform or as an enhancement layer, enables communication providers to achieve a decisive security advantage. As a standalone product, Qwyit offers a complete, future-proof communication solution that does not inherit the architectural constraints of legacy systems. As an enhancement layer, it allows existing platforms to neutralize their primary vulnerabilities, quantum susceptibility, discontinuous authentication, and centralized trust dependencies, without requiring a wholesale system replacement.

This dual-model approach provides unparalleled flexibility: organizations seeking a clean-slate secure communication platform can adopt Qwyit independently, while those with established user bases can integrate its components to incrementally achieve quantum-safe, compromise-resistant communications. In both scenarios, the result is a system that maintains confidentiality even under advanced persistent threats, including quantum computation, device compromise, and metadata analysis.

Comparative Security Benefits

The table summarizes the security properties of major platforms and the improvements achievable with Qwyit:

Platform	Current End-to-End Encryption	Quantum Resistance	Continuous Authentication	Metadata Exposure	Potential with Qwyit Integration/Deployment
Qwyit	Yes	Yes	Yes	Minimal	Baseline: Fully realized capabilities
Signal	Yes	No	No	Medium	Quantum resistance, continuous authentication, reduced server trust
WhatsApp	Yes	No	No	Very High	Quantum resistance, secure backups, protection against account compromise
Facebook Messenger	Partial	No	No	Extremely High	Universal end-to-end encryption, continuous authentication, reduced metadata leakage
SMS	No	No	No	Extremely High	Full encryption and authentication over existing channels
Phone Calls	No	No	No	High	End-to-end encryption with verified identities
FaceTime	Yes	No	No	Medium	Quantum resistance, continuous device verification, reduced infrastructure dependency

Truly Lightweight Communications Solution

Qwyit provides the foundation for secure communications that are simultaneously lightweight, quantum-resistant, and resilient to compromise. Whether implemented as a standalone application that redefines secure messaging and real-time communication, or as a cryptographic enhancement layer that fortifies existing platforms, Qwyit delivers capabilities that are absent from all currently deployed systems. By eliminating reliance on quantum-vulnerable public-key cryptography, enforcing continuous mutual authentication, and ensuring unique key usage at the finest granularity, Qwyit enables the creation of communication platforms that are demonstrably superior in security, efficiency, and futureproofing. This positions Qwyit as both a viable independent solution and a strategic upgrade path for any communication service seeking to establish and maintain leadership in secure communications.

Qwyit for Internet of Things Applications

The unique architectural properties of Qwyit make it exceptionally well-suited for deployment in resource-constrained Internet of Things (IoT) environments, including autonomous vehicles, drones, industrial sensors, smart infrastructure, and other embedded systems. Unlike traditional cryptographic protocols that rely on computationally intensive public-key operations—such as elliptic curve Diffie-Hellman key exchanges—Qwyit's design is inherently lightweight, enabling secure communications without imposing significant performance, power, or memory overheads.

Key Advantages for IoT Deployment

Qwyit's core components, the QCy™ stream cipher and QwyitKey™ continuous authentication mechanism, are specifically engineered to address the operational constraints inherent to IoT devices:

- **Computational Efficiency:** The QCy™ cipher operates as a high-speed stream cipher that applies unique per-bit keys, eliminating the need for resource-intensive block cipher modes, key derivation functions, or repeated public-key operations. Unlike AES-based systems, which require padding, mode-specific processing, and substantial memory for intermediate state management, QCy™ encryption and decryption impose minimal computational burden. This efficiency is particularly beneficial for devices with limited processing capabilities, such as microcontrollers, where traditional cryptographic primitives can exceed available cycle budgets or cause unacceptable latency.
- **Low Memory Footprint:** Qwyit requires no persistent key storage, certificate management, or revocation lists, as it does not depend on traditional public key

infrastructure (PKI). The absence of large key rings, ephemeral key generation, or certificate validation processes significantly reduces both static and dynamic memory requirements, making it feasible to implement fully secure communications on devices with kilobytes rather than megabytes of available RAM.

- **Power Efficiency:** By avoiding the high computational costs associated with public-key cryptography and minimizing the frequency and complexity of cryptographic operations, Qwyit enables secure communication without substantially increasing power consumption. This is a critical requirement for battery-powered or energy-harvesting IoT devices, where traditional secure communication protocols can rapidly deplete available energy reserves.

Specific Applications in High-Value IoT Domains

Qwyit's capabilities are particularly valuable in mission-critical IoT applications where secure, verifiable, and continuous communication is essential for operational integrity and safety:

- **Autonomous Vehicles:** In vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), and vehicle-to-everything (V2X) communication systems, Qwyit provides secure messaging with continuous mutual authentication. Traditional V2X protocols, which rely on certificate-based authentication and periodic public-key operations, are vulnerable to both quantum attacks and delayed detection of compromised devices. Qwyit's event-level authentication ensures that participating vehicles and infrastructure continuously verify each other's integrity throughout a communication session, immediately detecting and isolating devices that have been compromised—whether through physical tampering, remote exploitation, or supply chain attacks. Additionally, the lightweight nature of QCy™ encryption supports the high-throughput, low-latency requirements of real-time situational awareness data exchanges without overloading vehicle onboard processors.
- **Unmanned Aerial Systems (Drones):** Drone operations, whether for commercial package delivery, infrastructure inspection, or defense applications, require robust protection against interception, spoofing, and unauthorized command insertion. Qwyit enables secure command-and-control links, telemetry transmission, and swarm coordination by providing tamper-evident, continuously authenticated communications. The per-bit key uniqueness of QCy™ ensures that even partial interception of high-bandwidth video feeds or sensor data yields no recoverable information, while continuous authentication prevents an attacker from injecting

malicious commands into an ongoing session, even if they successfully impersonate a legitimate operator at session initiation.

- **Medical Devices and Other Health Care Applications:** Qwyit's cryptographic architecture is particularly well-suited for securing wearable medical devices and other health-related applications, where continuous, reliable, and highly assured communication is essential for both patient safety and regulatory compliance. Devices such as continuous glucose monitors, implantable cardiac rhythm management systems, insulin pumps, and remote patient monitoring wearables transmit highly sensitive physiological data that must remain confidential and authentically sourced, even in the presence of persistent adversaries.

  Traditional cryptographic approaches, which depend on computationally expensive public-key operations and periodic re-authentication, are impractical for these devices due to their severe constraints on processing power, memory, and battery life, often resulting in infrequent or unreliable security mechanisms. In contrast, Qwyit's lightweight QCy™ stream cipher enables efficient, per-bit encryption of continuous data streams, such as real-time biometric telemetry, without the overhead of block cipher modes or ephemeral key exchanges, thereby preserving limited device resources while ensuring that intercepted data remains entirely undecipherable. Complementing this, the QwyitKey™ continuous authentication mechanism provides ongoing verification of the identity and operational integrity of both the transmitting device and receiving endpoint, such as a clinician's workstation or hospital data aggregation platform, allowing immediate detection of device compromise, tampering, or substitution. This capability is critical for medical devices, where unauthorized data manipulation, delayed compromise detection, or failure to authenticate the receiving endpoint could have life-threatening consequences.

  Furthermore, Qwyit's independence from centralized key management infrastructure eliminates single points of failure and simplifies deployment across large-scale deployments of heterogeneous medical devices, ensuring secure communication even in environments with intermittent connectivity. By providing robust, resource-efficient encryption and uninterrupted mutual authentication, Qwyit enables wearable medical devices and health monitoring systems to maintain an unbroken chain of trust for their sensitive data streams, satisfying stringent security requirements such as those mandated by HIPAA, FDA cybersecurity guidelines, and emerging standards for wireless medical device

security, while preserving the operational longevity and performance of these critical, resource-constrained platforms.

- **Other IoT Use Cases:** Qwyit is equally applicable to a broad range of embedded systems, including industrial control systems (ICS), supervisory control and data acquisition (SCADA) networks, and distributed sensor networks. In these environments, where devices often operate unattended for extended periods and are primary targets for disruption, Qwyit's independence from centralized trust authorities eliminates single points of failure associated with certificate authorities or key management servers. The ability to establish secure, authenticated communications without reliance on external infrastructure ensures operational resilience in environments with intermittent or unreliable network connectivity.

Deployment Considerations for IoT

Qwyit can be integrated into IoT ecosystems through a compact software development kit (SDK) that supports a wide range of embedded platforms, including those without an underlying operating system. Optional hardware acceleration, via dedicated QCy™ cipher cores implemented in FPGA or ASIC, further reduces the performance footprint for high-volume or ultra-low-latency applications. Because Qwyit does not require global key synchronization, time synchronization, or external revocation mechanisms, it simplifies deployment across heterogeneous device fleets, including legacy systems that lack the resources for full PKI management.

Furthermore, the multi-channel authentication model inherent to QwyitKey™ allows device authenticity to be corroborated across diverse communication pathways—such as radio frequency, satellite links, and wired backhaul—providing layered assurance against sophisticated attacks that attempt to manipulate individual communication channels.

High-Volume, Large-Market Applications

Several significant market opportunities exist where Qwyit's unique combination of lightweight, continuous authentication and per-bit encryption provides substantial value:

1. **Enterprise Endpoint Security and Device Protection:** Qwyit can serve as a foundational security layer within operating systems and endpoint protection platforms. Rather than relying solely on periodic credential validation followed by extended trust periods, Qwyit enables continuous, low-overhead verification of system integrity throughout active sessions. This capability is particularly valuable for preventing lateral movement attacks, where a compromised user credential is used to access multiple systems without subsequent verification. Applications

include privileged access management, secure remote working environments, and defense against advanced persistent threats.

2. **File System and Storage Encryption:** Qwyit's stream cipher architecture is exceptionally well-suited for continuous, inline encryption of file systems, network-attached storage, and cloud storage environments. Unlike traditional file-level encryption schemes that apply a single key per file—creating significant risk if that key is compromised—Qwyit's per-bit keying ensures that even if an attacker obtains partial access to an encryption key, the vast majority of file contents remain completely inaccessible. This provides a fundamentally stronger security margin for data at rest across enterprise storage systems, backup repositories, and consumer storage solutions.
3. **Secure Virtual Private Network (VPN) and Remote Access Solutions:** Qwyit can replace or augment existing VPN encryption protocols, providing continuous mutual authentication between client and network endpoints throughout extended connection sessions. This eliminates the vulnerability window that exists between initial connection establishment and subsequent compromise detection, preventing session hijacking and unauthorized network traversal even after initial authentication. The lightweight nature of the cipher also enables more efficient, lower-latency encrypted tunnels compared to protocols requiring frequent key renegotiation.
4. **Software Supply Chain and Code Signing Protection:** Qwyit's continuous authentication model can be applied to verify the provenance and integrity of software components throughout their deployment lifecycle. Rather than relying solely on static signatures validated only at installation, Qwyit enables ongoing verification that deployed software components remain unmodified and originate from authorized sources, providing defense against supply chain compromise, delayed payload activation, and runtime tampering.

Integration within Operating Systems

Qwyit can be implemented as a continuous cryptographic service within an operating system, functioning as a system-wide security substrate rather than a discrete application-layer component. Several implementation approaches are feasible:

- **Kernel-Level Cryptographic Service:** Qwyit can be integrated as a native cryptographic primitive within the operating system kernel, providing system-wide access to its stream cipher and continuous authentication capabilities. This would enable all file system operations, network communications, process execution, and

inter-process communication to benefit from per-bit encryption and continuous integrity verification without requiring explicit invocation by individual applications.

- **Security Subsystem Architecture:** Qwyit can operate as a privileged security subsystem that provides cryptographic services to applications through well-defined application programming interfaces (APIs). This approach maintains the separation between user-space applications and cryptographic operations while enabling seamless, transparent access to Qwyit's capabilities across the entire system.
- **Continuous Integrity Monitoring:** Within an operating system context, Qwyit's multi-channel authentication mechanisms can support continuous verification of critical system components—including kernel modules, device drivers, system binaries, and running processes. This creates a layered defense that detects and responds to unauthorized modifications in real time, rather than relying on periodic integrity checks that leave significant compromise windows.

The primary advantages of operating system-level integration include the ability to provide comprehensive, continuous protection across all system activities without requiring explicit security management from individual applications. Because Qwyit does not depend on computationally expensive public-key operations, its continuous operation imposes minimal performance overhead, making it feasible to maintain cryptographic verification across all system activities without compromising responsiveness.

Market Significance

The potential market applications outlined above represent substantial addressable markets, including enterprise endpoint security (approximately $16 billion annually), data storage encryption solutions, VPN and secure remote access platforms, and emerging software supply chain security requirements. By providing a cryptographic foundation that supports continuous authentication and protection without the limitations of traditional periodic verification models, Qwyit addresses fundamental limitations in existing security architectures.

Operating system-level integration, in particular, represents a strategic opportunity to establish Qwyit as a foundational security capability rather than a discrete product. This approach enables broad, systemic deployment where cryptographic protection becomes a native property of all system operations, rather than an application-specific or network-bound capability. Such comprehensive integration would position Qwyit to serve as the underlying security infrastructure for entire computing platforms, providing continuous

protection across diverse workloads and eliminating the vulnerabilities inherent in discrete, session-scoped security mechanisms.

ABOUT HST GLOBAL, INC.

HST Global, Inc. (OTC: HSTC) is a diversified development-stage company focused on regenerative medicine, biotechnology, secure communications, and transportation. Through subsidiaries such as Fractional. Travel, Amnion® and Qwyit™, HST is building a platform that combines clinical innovation with advanced encryption to advance both human and digital health. The company's mission is to accelerate the convergence of life sciences and secure data, creating solutions that protect human wellness and information integrity alike.

FORWARD-LOOKING STATEMENTS

This press release contains forward-looking statements within the meaning of the Private Securities Litigation Reform Act of 1995. These statements may include, but are not limited to, statements regarding the Company's business strategy, operations, and financial performance. Forward-looking statements are subject to risks and uncertainties that could cause actual results to differ materially from those expressed or implied. Readers are cautioned not to place undue reliance on these statements, which speak only as of the date hereof. HST Global, Inc. undertakes no obligation to update or revise any forward-looking statements to reflect subsequent events or circumstances.

CONTACT:

Investor Relations
HST Global, Inc.
509 Old Great Neck Road Suite 105
Virginia Beach, VA 23454
info@hstglobal.com
www.hstglobal.com