BLUESKYTEC

Keyspace Technology for Secure Open Architecture Exchange

Submitted by Blueskytec America Inc. | Clinton Groves, CEO

Nontraditional Defense Contractor (NDC) | Small Business Concern (SBC) | U.S. Owned

1. EXECUTIVE SUMMARY

The Keyspace Technology (KST) ecosystem provides a hardware foundation of assured integrity for the Department of War.

KST is a modular deterministic trust sub-kit that uniquely authenticates each command signal at the physical layer, at wire speed, without human intervention. Operating beneath conventional cyber, KST ensures that any platform, facility or mobile/autonomous solution acts only on verified inputs. KST is a hardware-based root-of-trust system constructed using a quantum-derived One-Time-Key / One-Time-Pad architecture. It implements zero-trust principles protected by advanced anti-tamper features to deliver permanent, maintenance-free and proactive protection to any system, across any domain, with no maintenance or network dependence. KST answers a question once thought impossible to address. This is no theory, it is proven.

KST is TRL6+/7 and has been validated under a three-year Navy OTA (MSTIC 22-02-A-002, NSWCPD HM&E) where it successfully demonstrated all claims. The pathway to TRL8/9 is focused solely on field integration refinement. As a signal type and protocol agnostic solution, KST enables the Department of War's open-architecture vision by providing a unified verifiable trust layer for legacy and new systems. It enables autonomy, sensing, and control environments to operate securely and predictably at scale.

2. CHALLENGE & SOLUTION

Modern warfighter systems operate in environments that are uncertain, intermittently disconnected, and often contested. Whether fixed or mobile, intelligence or weapon, their effectiveness depends on trust. Every action must be verifiable, every signal authentic.

The Department of War faces an inflection point. This risk is not hypothetical or future-facing. Modern assets operate under the constraint of unverifiable trust. Increasing levels of automation and autonomy expand this threat by accelerating machine action beyond human oversight. As these, or any new systems, move from controlled environments into contested operations, provable trust must be a prerequisite for safety and mission success.

Most existing trust frameworks and security solutions rely on layered software, cloud synchronization, and certificate management. They depend on detecting abnormal behavior or correcting flaws after exploitation. They were built for data environments, not operational, and as such they collapse when connectivity, power, or time are inhibited. Modern warfighter systems require rejection, not reaction. Rejection of untrusted input, non-compliant behavior, and ambiguity about what is allowed.

These same assets require trust under isolation. The ability to verify and protect system behavior without reliance on software, behavioral analysis, oversight and external networks. Without this capability, even advanced systems remain brittle.

This is the gap KST addresses.

KST delivers absolute certainty via provable trust at the signal layer. It is not software. It is not a firewall or a filter. It is a hardware-based adjudicator that operates in line with the physical signal, authenticating machine-to-machine communication before any command is executed. Rather than assuming compromise and responding after the fact, KST prevents compromise from beginning.

Figure - KST CN2 Protector

KST delivers trust beneath conventional cyber, verifying every interaction and enforcing deterministic control behavior in real time at the edge. It does not depend on network access, continuous maintenance, or rekeying. Trust is embedded permanently in silicon as part of the platform itself.

Operationally, KST enables secure integration of mixed-protocol systems, isolation of critical functions from unauthorized and malformed signals. It provides deterministic control signal validation with line-speed authentication and obfuscation. Permitting the secure operation of any new, and the rapid conversion of any legacy, asset into trustworthy systems under any domain condition.

The requirement is clear. Systems whose behavior and integrity can be verified and sustained without human intervention. KST provides this foundation of trust.

3. WARFIGHTER IMPACT

Today’s warfighters operate systems that can act faster than humans can intervene, yet they remain fully accountable for the outcome. Once a command executes, loss of control is irreversible.

Until KST, this risk was unavoidable as no solution existed that could prevent the corruption of command traffic in real-time beneath the software stack. The risk could be managed, mitigated, and responded to, but it could not be prevented.

KST changes this reality. It ensures that systems act only on explicitly authorized commands and prevents malicious actions before they occur. If a command is not authentic and allowed, it does not execute. With KST in place, warfighters and systems authorities are no longer forced to compensate for either known and unknown cyber and control risks through procedure, redundancy, or restraint. Systems behave predictably under stress, restoring confidence that equipment will not act against intent or place personnel in danger due to unseen manipulation.

Most critically, KST aligns accountability. System authorities, once forced to approve use of solutions they knew to have vulnerabilities they could not prevent, can now remove the threat. Warfighters, exposed to risks they cannot see or stop, can now take stock in the equipment they rely on. What was previously accepted as an unavoidable condition of modern warfare, now becomes a preventable risk.

KST allows warfighters to focus on the mission, knowing that when they give an order, their assets will be available, execute exactly that order and nothing else.