WHITE PAPER

Agentic AI Security | Department of War Applications

ZipIPS™

Quantum-Secure IoT Authentication with NanoTimestamp Power

Securing Autonomous Military AI: Quantum-Secure Authentication for Department of War Agentic Systems

Helene E. Schmidt, Inventor | Creative Synergies LLC

synergies.com | US10171465B2 | US10348729B2

April 2026

Executive Summary

The Department of War is deploying Agentic AI across its most consequential operations — command and control, autonomous weapons systems, intelligence analysis, logistics, and cyber operations. These systems act autonomously, at machine speed, without a human in the loop at every decision point. That is their advantage. It is also their vulnerability.

When an autonomous system receives a command — to engage a target, redirect a mission, execute a logistics action, or respond to a cyber threat — how does it know the command is genuine? Not assumed genuine. Actually verified, right now, before execution. A fraudulent command in a combat environment is not a data breach. It is a mission failure, or worse.

ZipIPS™ provides quantum-secure authentication for exactly this problem. Every command issued to an autonomous military system can be challenged with a fresh timestamp before execution. The commanding source must respond with a credential derived from pre-shared tables that never cross the network. An impersonator — human or AI — cannot produce what it doesn't have. The command does not execute. The attempt is permanently logged.

The Department of War also faces a hard deadline. The National Security Agency's Commercial National Security Algorithm Suite 2.0 (CNSA 2.0) requires all new National Security Systems to be quantum-safe by January 2027. Agentic AI systems being deployed today must meet that requirement. ZipIPS™ is quantum-secure by architecture — not by algorithm selection, not as a retrofit, but as a structural property of how it works.

Grok 4 (xAI) first determined that ZipIPS™ exceeds current NIST post-quantum and lightweight cryptography standards in both security level and credential efficiency. Claude (Anthropic) subsequently reached the same conclusions independently — two separate analyses, the same result. ZipIPS™ is available for licensing. Creative Synergies LLC welcomes inquiries.

1. The Authentication Problem in Military Agentic AI

1.1 What Agentic AI Means in a Military Context

Military Agentic AI is not a future scenario. It is operational today across the Department of War in forms that range from autonomous logistics optimization to AI-assisted targeting, from signals intelligence processing to autonomous cyber defense. In each case, an AI system is making decisions and issuing instructions without waiting for human approval at every step.

The authentication problem this creates is simple and serious: every instruction an autonomous military system receives must be verified as genuine before it is executed. A spoofed targeting instruction, a fraudulent mission abort, a hijacked logistics command, a compromised cyber defense agent — each of these represents a different kind of mission failure. All of them share the same root cause: the receiving system trusted an instruction it should have challenged.

1.2 Why Legacy Authentication Fails in Combat Environments

Legacy authentication was designed for peacetime networks, human-scale interactions, and the assumption that the attacker is outside the perimeter. Military Agentic AI operates in environments where none of those assumptions hold:

- Adversarial environment: Nation-state adversaries actively attempt to intercept, spoof, and inject commands into military communication channels. The attacker is not outside the perimeter — in a contested environment, the perimeter may not exist.
- Machine speed: Autonomous systems make decisions and issue commands faster than any human can verify. Session-level authentication is not sufficient — by the time a session is reviewed, the command has already executed.
- Quantum threat: The cryptographic foundations of most military communication — RSA, ECC, Diffie-Hellman — are vulnerable to quantum computing. Adversaries with quantum computing capabilities can break these systems. The CNSA 2.0 mandate exists precisely because this threat is real and near.
- Contested communications: In a degraded or jammed communications environment, authentication systems that depend on continuous network connectivity, clock synchronization, or certificate revocation checking fail exactly when they are needed most.
- AI-enabled adversaries: An adversary using AI to conduct attacks can probe authentication systems at machine speed, identify weaknesses, and exploit them faster than human analysts can respond.

A military AI system that can be commanded by an adversary is not an asset. It is a liability. The authentication architecture is the difference between the two.

1.3 The CNSA 2.0 Mandate

The National Security Agency's CNSA 2.0 requires all new National Security Systems to use quantum-safe cryptography by January 2027. This is not a recommendation — it is a requirement for systems operating at the classification levels that Department of War Agentic AI systems occupy.

Most current military authentication relies on algorithms that CNSA 2.0 is designed to replace. Agentic AI systems being deployed today under legacy authentication are non-compliant with the approaching mandate and vulnerable to quantum attack before that mandate is even enforced.

ZipIPS™ does not rely on any algorithm that CNSA 2.0 identifies for replacement. It is quantum-secure by architecture — no transition required, no migration project, no compliance gap.

2. How ZipIPS™ Addresses Military Agentic AI Authentication

2.1 Command-Level Verification

The most important property of ZipIPS™ for military applications is command-level verification. Every instruction an autonomous system receives — every targeting data update, every mission parameter change, every logistics directive, every cyber response command — can be challenged before execution.

The receiving system generates a fresh timestamp and sends it as a challenge to the commanding source. The commanding source must respond with a credential derived from pre-shared tables — tables that were provisioned before the operation began and never cross the network during operation. The receiving system independently derives the expected credential from its own copy of the same tables and compares. If they match, the command executes. If they don't, the command is blocked and the attempt is logged.

There is no window, no range, no second chance. Each credential is tied to a single, unrepeatable and unpredictable timestamp. A captured credential is immediately worthless. An impersonator without the pre-shared tables cannot pass the challenge regardless of computational resources — including quantum computing resources.

2.2 Operation Without Continuous Connectivity

Legacy authentication systems were designed for connected environments — ones where a certificate authority is reachable, a time server is available, and the network is functioning as intended. In peacetime enterprise environments, these assumptions are reasonable. In military operations, they are not.

Modern contested environments deliberately target communications infrastructure. GPS jamming, radio frequency denial, network interdiction, and electronic warfare are standard tools of near-peer adversaries. An authentication system that fails when the network is degraded fails precisely when the stakes are highest — when autonomous systems are operating in the most dangerous conditions, executing the most consequential commands.

ZipIPS™ requires none of the infrastructure that contested environments destroy. There is no certificate authority to reach, no time server to consult, no revocation list to check, no clock synchronization between devices. Each platform uses its own internal clock, and the commanding source sends its timestamp as part of the challenge. The receiving platform derives the expected credential from its own pre-shared tables — loaded before the operation began, requiring no network connection to use.

This means ZipIPS™ authentication functions in any environment in which the command itself can be transmitted. Jamming the authentication infrastructure is not possible — there is no authentication infrastructure to jam. The security is carried by the platform, not by the network.

For autonomous systems operating beyond communications range — unmanned platforms executing pre-authorized mission profiles, edge sensors in denied areas, forward-deployed logistics nodes — this property is not a convenience. It is a requirement.

2.3 The Double Two-Way Handshake

Authentication works in both directions. The commanding source verifies the receiving system, and the receiving system verifies the commanding source. Neither side trusts a single exchange. Both must pass before the command executes.

For military applications, this bidirectional verification is critical. A system receiving commands from what appears to be an authorized controller can independently verify that controller before executing. A substituted or spoofed controller — one that has been inserted between the legitimate command authority and the receiving system — cannot pass the independent verification. The command does not execute. The substitution is detected.

Property	Military Significance
No static credential	Static keys and session tokens are high-value targets for adversarial collection. ZipIPS™ generates a fresh credential at every command exchange — there is no persistent secret to collect, compromise, or replay.
No transmitted sequence	The sequence ordering that makes each credential unique is never transmitted. An adversary who intercepts command traffic captures credentials that are already expired and sequence orderings they cannot derive without the pre-shared tables.
No clock synchronization	Operates without synchronized clocks — functional in degraded, denied, and contested communications environments where time synchronization infrastructure may be unavailable or compromised.
Command-level challenge	Every command is independently verified before execution — not just the session. A compromised or spoofed commanding agent cannot issue executable commands without the pre-shared tables.
Quantum-secure by construction	No mathematical structure for quantum algorithms to attack. CNSA 2.0 compliant by architecture. Systems deployed today remain secure as adversary quantum capabilities mature.
Permanent audit log	Every authentication attempt — successful or failed — is permanently logged with a precise timestamp. Post-mission analysis has a complete, tamper-evident record of every command exchange.
On-demand generation only	No background process, no idle computation. Critical for power-constrained platforms — unmanned systems, sensors, and edge devices operating on limited power budgets.

3. Department of War Agentic AI Applications

3.1 Command and Control (C2) AI

AI systems supporting command and control operations manage the flow of orders, situational awareness data, and coordination instructions across military units and platforms. A compromised C2 AI — one receiving fraudulent instructions from a spoofed command authority — can redirect assets, abort missions, or create coordination failures that degrade combat effectiveness without a single shot fired.

ZipIPS™ authenticates every C2 instruction at the command level. Before an autonomous C2 system executes a directive — redirecting a unit, updating rules of engagement, coordinating fires — it challenges the commanding source with a fresh timestamp. A spoofed command authority cannot pass the challenge. The directive does not execute. The attempt is logged for immediate analysis.

3.2 Autonomous Weapons Systems

Autonomous weapons systems — loitering munitions, unmanned aerial vehicles, unmanned surface and undersea vehicles — receive targeting, engagement, and mission instructions from AI agents operating in the command chain. The consequences of a fraudulent command in this context require no elaboration.

ZipIPS™ provides command-level authentication for autonomous weapons systems. Every engagement instruction, every target update, every mission abort command is challenged before execution. A spoofed or hijacked commanding agent cannot produce the pre-shared table credential. The system does not engage on fraudulent instructions. The on-demand generation property is particularly relevant for power-constrained unmanned platforms — authentication imposes no background computational load, consuming resources only when a command challenge occurs.

3.3 Intelligence Analysis AI

AI agent chains processing signals intelligence, imagery, open source data, and multi-source fusion operate at speeds and volumes that no human analyst can match. A compromised agent in an intelligence pipeline — one receiving or injecting fraudulent data — can corrupt analysis at machine speed, producing assessments that drive decisions based on manipulated inputs.

ZipIPS™ authenticates the command and data flow between intelligence AI agents. An agent receiving analysis inputs from an upstream agent can verify the source before incorporating those inputs. A substituted or compromised upstream agent cannot pass the command-level challenge. The corrupted data does not enter the analytical pipeline.

3.4 Autonomous Logistics and Supply Chain AI

Military logistics AI manages resupply, maintenance scheduling, fuel management, and materiel positioning across distributed operations. Fraudulent logistics commands — misdirected resupply, manipulated maintenance schedules, corrupted positioning data — degrade operational readiness without direct engagement. An adversary who can command a logistics AI has found a way to degrade combat power without firing a weapon.

ZipIPS™ authenticates every logistics directive. Before an autonomous logistics system executes a resupply routing, a maintenance dispatch, or a materiel positioning order, it challenges the commanding source. A fraudulent logistics command cannot pass the timestamp challenge. The system continues operating on verified instructions only.

3.5 Cyber Operations AI

AI agents conducting defensive cyber operations — identifying threats, isolating compromised systems, responding to intrusions — operate autonomously in contested network environments. A defensive cyber AI that has been hijacked or is receiving fraudulent commands from a compromised orchestrator becomes an offensive tool. It isolates the wrong systems, misidentifies threats, or creates vulnerabilities it was designed to close.

ZipIPS™ authenticates the command chain for cyber operations AI. Every directive to an autonomous cyber agent — isolate this system, block this traffic, respond to this threat — is challenged before execution. A compromised orchestrating agent cannot issue executable commands. The cyber defense AI continues operating on verified instructions only, maintaining the integrity of the defensive posture it was designed to protect.

3.6 Multi-Domain Operations AI

Multi-domain operations require AI systems across land, sea, air, space, and cyber to coordinate in real time, sharing situational awareness and executing synchronized actions. The coordination commands flowing between domain AI systems are authentication events — each one an opportunity for an adversary to inject, intercept, or corrupt.

ZipIPS™ provides a common authentication architecture across domain boundaries. The same patented method and system — timestamp-derived credentials, pre-shared tables, double two-way handshake — applies whether the authentication event is between a ground C2 system and an airborne platform, a space-based sensor and a naval fire control system, or a cyber operations center and an edge defensive agent. One architecture, every domain.

4. Threat Scenarios and ZipIPS™ Response

Threat Scenario	Attack Method	ZipIPS™ Response
Spoofed command authority	Adversary impersonates a legitimate command authority, issuing fraudulent mission instructions to autonomous systems.	Receiving system challenges the commanding source with a fresh timestamp. Spoofed authority without pre-shared tables cannot respond correctly. Command does not execute. Attempt logged.
Man-in-the-Middle insertion	Adversary inserts a fraudulent relay between legitimate command authority and autonomous systems, intercepting and modifying commands in transit.	Double two-way handshake detects the substitution. The inserted relay cannot independently produce credentials for both the upstream and downstream challenge. The insertion is detected and logged.
Replay attack	Adversary captures a valid command credential and attempts to reuse it to issue fraudulent instructions.	Every credential is tied to a single, unrepeatable timestamp. A captured credential is immediately expired. There is nothing to replay.
Quantum cryptanalysis	Adversary with quantum computing capability breaks the cryptographic foundation of legacy authentication, gaining the ability to forge credentials.	ZipIPS™ has no mathematical structure for quantum algorithms to attack. No factoring problem, no discrete logarithm, no elliptic curve. Quantum computing provides no advantage against pre-shared table architecture.
AI-enabled probing	Adversary deploys AI to probe authentication systems at machine speed, seeking patterns or vulnerabilities to exploit.	Each failed authentication attempt permanently blocks that timestamp. No iterative search is possible — every attempt requires a new timestamp producing a completely different credential. There is no pattern to exploit.
Compromised orchestrator	Top-level command AI is compromised. Downstream autonomous systems receive fraudulent instructions from what appears to be a legitimate authority.	Downstream systems challenge the orchestrator before executing each instruction. Table rotation policy determines how quickly a compromised orchestrator loses the ability to pass challenges. Table rotation is the primary governance control.

5. Security Performance

ZipIPS™ is a licensable architecture. Implementing organizations configure the system for their specific environment and security requirements. The following illustrative entropy levels represent what the architecture can achieve. There is no upper limit — entropy can be increased by adding character sets, time units, or any real-time data the implementing system can generate.

Implementation	Entropy	Payload	Characteristics
ms original	381 bits	95 bytes	Millisecond-resolution timestamps. Alphanumeric character strings. Eight time units. Suitable for high-frequency logistics and coordination authentication on resource-constrained platforms.
ns standard	476 bits	117 bytes	Nanosecond-resolution timestamps. Alphanumeric character strings. Ten time units. Appropriate for C2 systems, intelligence pipelines, and cyber operations command authentication.
ns+ high security	735 bits	157 bytes	Maximum time-unit depth with non-control special characters from the extended ASCII character set. Designed for autonomous weapons systems, sensitive intelligence operations, and highest-consequence command channels.

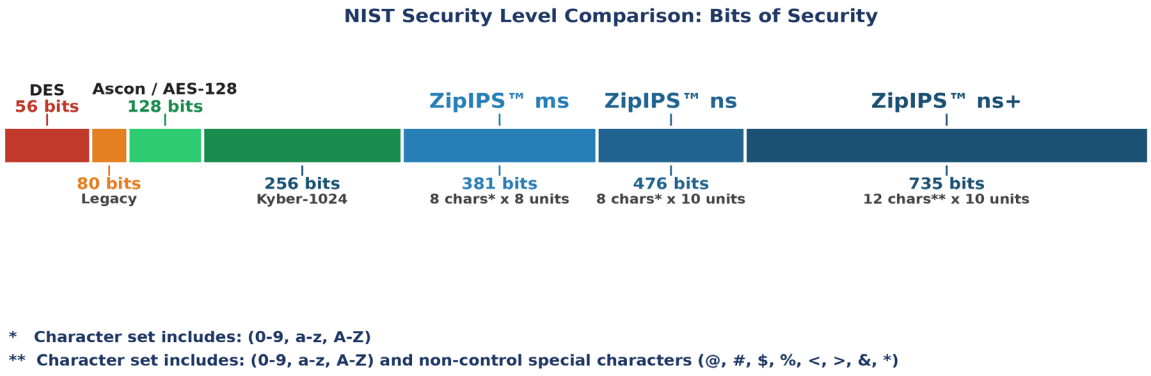

Figure 1: NIST Security Level Comparison — ZipIPS™ illustrative implementations vs. reference points

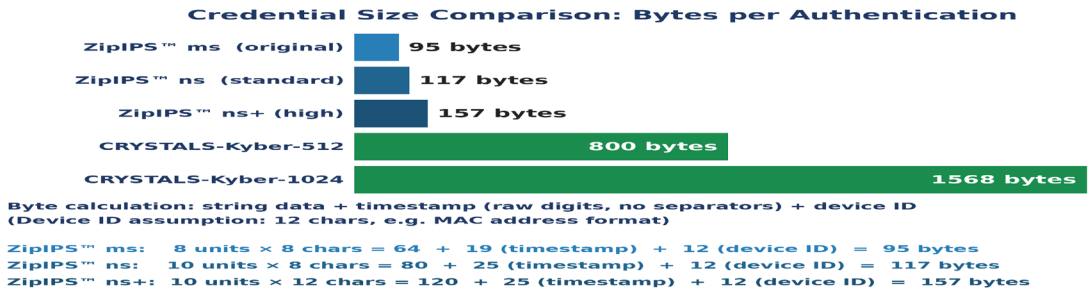

Figure 2: Credential Size Comparison — ZipIPS™ illustrative implementations vs. CRYSTALS-Kyber

ZipIPS™ ns+ generates 735-bit credentials in a 157-byte payload — nearly three times the entropy of AES-256, one-tenth the size of CRYSTALS-Kyber-1024, quantum-secure by construction. For power-constrained autonomous platforms, the credential is generated on demand only — no background process, no idle computation, no power budget impact between authentication events.

6. Regulatory and Standards Alignment

Requirement	Mandate	ZipIPS™ Alignment
CNSA 2.0 (NSA)	All new National Security Systems must use quantum-safe cryptography by January 2027	ZipIPS™ is quantum-secure by architecture. No transition required. Systems authenticated with ZipIPS™ meet the quantum-safe requirement from day one of deployment.
SP 800-207 (Zero Trust)	Never trust, always verify — no system is implicitly trusted based on prior session or network position	ZipIPS™ implements Zero Trust at the command level. Every instruction is independently challenged before execution. No session-level trust assumption. No implicit trust based on network location.
FIPS 203/204/205 (PQC Standards)	Transition away from cryptographic algorithms vulnerable to quantum computing	ZipIPS™ does not use RSA, ECC, or any algorithm NIST identifies for replacement. Authentication security derives from timestamp resolution and table complexity — no quantum-vulnerable mathematical structure.
SP 800-213A (IoT Authentication)	IoT device authentication — the ability of a device to verify its identity with other system elements	ZipIPS™ provides device-level mutual authentication as its core function. Both devices independently verify each other through the double two-way handshake — applicable to any networked device including autonomous military platforms.
EO 14028 (Cybersecurity)	Federal agencies to improve cybersecurity, including adoption of Zero Trust architecture	ZipIPS™ directly implements Zero Trust authentication at the device and command level, consistent with EO 14028 objectives applied to Department of War autonomous systems.

Note: These alignments are architectural observations, not certifications. ZipIPS™ has not been submitted to NSA, NIST, or any Department of War agency for evaluation or endorsement. Prospective licensees should conduct their own evaluation of compliance applicability.

7. Implementation Considerations

ZipIPS™ is a licensable architecture — not a product. Implementing organizations write their own code, configured for their specific platform, communications environment, and security requirements. For Department of War applications, two implementation decisions are especially critical:

- Command-level challenge integration: The most effective implementation builds the timestamp challenge into the platform's command-processing logic — every received instruction is challenged before execution. This is a design decision that determines whether protection operates at session initiation (insufficient for military applications) or at the command level (the appropriate level for autonomous military systems).

- Table provisioning and rotation: Pre-shared tables are loaded before operations begin. Table rotation — replacing tables on a defined schedule or following a compromise event — is the primary governance control for a compromised or captured platform. A platform whose tables have been rotated can no longer authenticate with old credentials. Rotation policy is an operational security decision for the implementing organization.

Implementation requirements will vary by platform, communications architecture, and operational environment. These are the licensee's responsibility to evaluate. Creative Synergies LLC makes no representation regarding specific integration requirements for any particular Department of War system or platform.

8. Patent Foundation

ZipIPS™ is protected by two issued United States patents, both assigned to Helene E. Schmidt of Creative Synergies LLC.

Patent	Issued	Scope
US10171465B2	Jan. 1, 2019	Method patent covering the authentication process: timestamp generation, character string retrieval and sequencing, initiating string construction and transmission, host-side verification, second timestamp generation, client-side verification, and the on-demand re-verification loop. Applicable to any networked device pair, including autonomous military platforms receiving commands from AI agent systems.
US10348729B2	Jul. 9, 2019	System patent covering the authentication architecture: host device with sequence tables and string tables at variable security levels, client device with mirrored table architecture, device identifier, and the system configuration for the complete double two-way handshake with on-demand re-verification. Continuation of US10171465B2.

Both patents establish broad protection for timestamp-based authentication using independently-derived, never-transmitted sequence ordering across device pairs with mirrored table structures. The architecture applies to any networked device pair — including AI agent-to-platform command channels in military autonomous systems. Prospective licensees are encouraged to review the patents directly and consult qualified patent counsel regarding scope and applicability to specific Department of War programs.

9. Licensing

Creative Synergies LLC welcomes inquiries from qualified organizations interested in exploring licensing opportunities. No terms are presented in this White Paper — the right licensing structure is best arrived at through direct dialogue between technically and legally informed parties.

ZipIPS™ is available for licensing. Please visit synergies.com and Contact Us if you have any questions. Helene E. Schmidt, Inventor Creative Synergies LLC synergies.com | zipips@synergies.com