Concept Paper



# Quantum Physical Trust Enforcement: A Physically Irreversible Molecular Approach to Machine-to-Machine Authentication

Antoine Scaperrotta *

Posted Date: 19 June 2025

doi: 10.20944/preprints202506.1626.v1

Keywords: machine-to-machine security; hardware authentication; molecular authentication; spintronics; physically unclonable function (PUF); photonic integrated circuit (PIC); paramagnetic complexes; quantum-resistant protocol; molecular electronics; physical layer security; quantum physical trust; spin coherence; nuclear magnetic resonance (NMR)

 doi:10.20944/preprints202506.1626.v1



*Concept Paper*

# Quantum Physical Trust Enforcement: A Physically Irreversible Molecular Approach to Machine-to-Machine Authentication

**Antoine Scaperrotta**

Independent Researcher, United Kingdom; jainacc@hotmail.com

**Abstract**

We introduce a multidisciplinary hardware trust architecture that unites molecular mechanics, molecular physics, and molecular electronics within a single addressable logic gate [1,8,9]. Unlike conventional molecular systems that rely on one or two physical principles, our protocol establishes trust exclusively through a molecular state change [6,7,10] triggered by the simultaneous and independent satisfaction of three orthogonal physical channels: (1) quantum photonic excitation (photon spin, circular polarization), (2) integrated with an active NMR feedback mechanism to the emitter, and (3) precise time synchronization enforced by a GPS-disciplined oscillator protocol. This integrated mechanism exploits both the quantum properties (spin selectivity, photonic interaction) and mechanical-electronic response (NMR feedback perturbation, charge/electron dynamics) of the engineered molecule, enabling logic operations that are physically auditable and fundamentally resistant to digital, classical, or quantum attack. By requiring all three modalities for logic activation, the system achieves unmatched selectivity, environmental robustness, and physical distinctiveness. Continuous real-time monitoring ensures that any protocol deviation instantly severs trust and triggers audit logging. This architecture provides a new paradigm for secure machine-to-machine communication, leveraging the combined power of molecular mechanics, physics, and electronics to achieve tamper-evident, irreproducible, and scalable physical trust—representing, the realization a triple-modality molecular logic system.

**Keywords:** machine-to-machine security; hardware authentication; molecular authentication; spintronics; physically unclonable function (PUF); photonic integrated circuit (PIC); paramagnetic complexes; quantum-resistant protocol; molecular electronics; physical layer security; quantum physical trust; spin coherence; nuclear magnetic resonance (NMR)

## Condensed Introduction

The Authentication Security Cryptonode (ASC) protocol represents a fundamentally different approach to trust and authentication compared to SSL/TLS. While SSL/TLS secures digital communications via mathematical algorithms and software infrastructure, the ASC enforces trust through simultaneous, independent, and physically auditable quantum, mechanical, and temporal events at the hardware level. This physical basis makes it inherently immune to many attacks that threaten digital protocols—including quantum computing, key theft, and replay attacks. However, its current scalability and integration are best suited for applications demanding the highest level of hardware-based security, rather than as a universal digital replacement. In critical environments, it can provide a new foundational layer for trust, complementing or enhancing conventional cryptographic protocol.

Molecular-scale logic and machine architectures have, until now, been limited by their reliance on only one or two physical modalities. Molecular mechanics, as realized in artificial molecular machines and switches such as rotaxanes and catenates, has demonstrated conformational or mechanical state changes, but these systems are rarely coupled to quantum magnetic or electronic

 doi:10.20944/preprints202506.1626.v1



properties. In parallel, advances in molecular electronics have enabled organic semiconductors and single-molecule devices, yet these are typically addressable only via charge or current, lacking mechanical or magnetic control. Separately, the field of molecular physics has produced quantum-responsive materials—such as quantum dots and NV centres—with rich photonic and magnetic behaviour, these phenomena are not integrated with mechanical switching in the same molecular system.

Here, we present a fundamentally new approach: a molecular logic architecture that intrinsically couples all three domains—molecular mechanics, molecular physics, and molecular electronics—within a single, addressable gate. Trust or logic activation in this system is triggered only when three orthogonal, physically verifiable channels—photon spin (quantum photonic excitation), magnetic field (integrated with an active NMR feedback mechanism), and protocol-driven time synchronization—are satisfied simultaneously. This triple-modality, multi-channel integration enables logic operations and security primitives that are physically unique [12,15], tamper-evident, and resistant to attack or simulation by any single physical or digital method. Our architecture thus establishes a new standard for molecular information processing, moving beyond the boundaries of existing chemical, physical, or electronic approaches.

## 1. System Overview and Physical Principles

### *1.1. Purpose and Technical Field*

This invention relates to the field of physically enforced machine-to-machine trust, authentication, and control—drawing on a combination of quantum photonics, molecular state engineering, spintronics, and magnetic-field–coupled materials. The invention leverages quantum-physical effects. This invention implements chemistry, magneto-optics, and functional molecular assemblies, creating a multidisciplinary architecture for hardware-level trust enforcement.

The system is designed for applications requiring the highest assurance of irreversibility, tamper evidence, and physically unforgeable connections between machines—including, but not limited to, critical infrastructure, secure autonomous platforms, and high-security digital environments. The architecture is scalable, allowing for trust establishment across structured clusters, networks, and configurable multi-machine groupings.

The core objective is to transcend traditional reliance on cryptographic keys, entropy pools, or statistical algorithms, by establishing trust through physical event at the molecular/subatomic/material level. In this architecture, trust is by a non-reproducible, irreversible state change in specially engineered molecules or assemblies. The molecule presents 2 separated sensitivity one related to spin of the photon, the second is sensitive to magnetic field creating a measurable NMR (nuclear magnetic resonance) response send back to the emitter[2,3,11].

This state change requires the coordinated action of two independent physical channels activated simultaneously:

- **First Channel (Photon Spin):** The molecule is excited exclusively by a directed photon whose spin (circular polarization) matches the molecular selectivity, ensuring only the correct quantum state can initiate the excitation.
- • **Second Channel (active NMR feedback):** Simultaneously, the molecule's atoms or electrons are aligned and actively monitored by an external magnetic field, configured enable the state change and to allow the generation of a measurable NMR (nuclear magnetic resonance) signal [2,5,11]. Upon successful activation, this NMR response is detected locally, and the resulting signal is relayed back to the emitter, serving as a physical confirmation of the trust event. When all activation criteria are met—precisely synchronized photon spin excitation and active NMR-coupled magnetic alignment—does the irreversible physical transition occur. The protocol-authorized NMR signal, sent back to the emitter within the GPSDO-enforced time window, both locks trust at the hardware level

 doi:10.20944/preprints202506.1626.v1



and provides tamper-evident, side-channel-resistant confirmation, preventing spoofing, replay, or unauthorized intervention by digital or physical means.

Practical realization of large-scale molecular commutator or switchboard configurations will depend on the ability to selectively engineer molecules with high channel specificity and minimal crosstalk. Scalability is determined by pragmatic selection of molecules and device architecture to ensure robust, non-interfering trust links in multi-machine settings.

This ASC mechanism enables a new class of trust primitives: providing a physically un-spoofable and irreversibly fused trust gate, scalable to two or more machines. The approach is suitable for scenarios where traditional digital security is insufficient or vulnerable to simulation, replay, or advanced digital or physical attack.

### *1.2. Departure from Prior Art*

Conventional digital security relies on cryptographic keys, entropy sources, or software-managed secrets to establish trust and control access between machines. These methods are vulnerable to various forms of attacks, including replay, simulation, firmware compromise, and advanced hardware-based spoofing. Traditional trust anchors depend on statistical randomness, digital computation, and algorithmic validation, all of which can be undermined by advances in software or hardware hacking.

This innovation departs from such approaches by making trust a function of direct, physical events at the molecular and quantum/material level [12,15]. Instead of relying on digital keys or computation, trust is established and enforced through an irreversible physical state changes in engineered molecules and assemblies. This process is triggered by the coordinated application of three independent channels:

- a photon with defined spin (circular polarization)
- a specific measurable NMR response
- and a synchronized time reference.

Once these physical events have occurred, trust between machines is fused at the material level and is no longer subject to algorithmic manipulation or remote simulation. The system does not depend on cryptographic validation or digital fallback mechanisms. If trust is broken, it can only be re-established by a strict protocol that involves alignment at the molecular and physical level.

## 2. Core Trust Mechanism

### *2.1. Physical Components*

The trust node implemented into the machine incorporates physical components enforce trust at the material level. The core elements are:

- Spin-sensitive molecular receptors immobilized on a substrate. Example implementations include chiral ligands, helicenes, functionalized fullerenes, or triple-helix metal complexes [6–8].
- Three physical embedded keys:
    - A photon emitter (such as a laser or LED) capable of producing photons with defined frequency and circular polarization (spin). Received by fibre optic physical machine connection, to incapacitate spoofing [1,3,9].
        - Sensors to detect molecular state transitions (optical or electronic readout).
    - An active magnetic field generator (such as a solenoid or integrated micro-magnet) is used at the molecular site, to enable and control the generation of a measurable nuclear magnetic resonance (NMR) response. Upon successful photonic excitation and correct field conditions, the molecular state change produces a distinct NMR signal, which is detected in real time by local sensors and immediately relayed back to the emitter. This NMR feedback serves as a physical confirmation of both

 doi:10.20944/preprints202506.1626.v1



molecular state and correct protocol execution, forming a closed-loop handshake that provides strong side-channel and tamper resistance. The magnetic field could be modulated or coded—for example, using pre-agreed patterns, pulse sequences, or operator-set configurations—to enable dynamic channel selection, further enhance anti-spoofing, and support operator intervention or automated authentication logic. All magnetic field changes and resulting NMR responses are monitored and logged by the system for auditability and forensics.

- A synchronized time reference, such as a GPS-disciplined oscillator or atomic clock, for timing and protocol enforcement [13,14].

A trust event is established when:

1. The machine's photon emitter directs a photon of the exact required frequency and spin at the target molecule,
2. The molecule is in the correct magnetic or electronic alignment provided by the magnetic field,
3. The excitation event occurs within a narrowly defined time window, synchronized to the system's high-precision time reference (e.g., GPSDO or atomic clock).
4. Simultaneously, a synchronized digital ON/OFF control signal (e.g., session nonce or challenge code) is transmitted and validated.

Only if both physical activation channels and the synchronized digital protocol are satisfied, the molecule undergoes flipping state changes (excited and back to initial stage), which is immediately sensed by the receiving system.

This state change locks trust between the paired machines at the physical level. The process cannot be emulated, replayed, or reset by digital, or software means. Any deviation—incorrect photon, misaligned field, protocol failure, or tampering—prevents or destroys the trust event. Trust cannot be transferred, replayed, or migrated except by direct intervention.

*2.2 Trust Protocol Flow*

- **System Initialization**
  - Each machine is equipped with a trust node comprising spin-sensitive molecular receptors, a photon emitter, a magnetic field generator, state and orientation sensors, and a synchronized time reference.
  - The magnetic field orientation is set and verified by a trusted source operator, optionally using an externally signalled pattern.
- **Photon Emission**
  - The initiating machine directs a photon of the specified frequency and circular polarization through a secure fibre optic connection to the receiving machine.
- **Magnetic Field and NMR Channel Verification**
  - The receiving machine applies the active magnetic field to align the molecule(s) for protocol compliance and to enable NMR signal detection. Integrated sensors verify that the molecule is both correctly aligned and capable of producing the required NMR response.
- **Digital Signal Synchronization**
  - A synchronized digital ON/OFF control signal is transmitted and validated according to the established protocol and time reference.
- **Physical Activation, Molecular State Change, and NMR Feedback**
  - Only if all physical activation channels (photon spin and active magnetic field/NMR alignment) and the synchronized digital protocol are satisfied, the molecule undergoes the designated state change (excitation and return/relaxation).
  - This event generates a measurable NMR (nuclear magnetic resonance) signal, which is detected in real time by local sensors and immediately relayed back to the

 doi:10.20944/preprints202506.1626.v1



emitter as a physical confirmation of the trust event, all within the authorized time window.

- **Closed-Loop Trust Validation**
  - The flip event and NMR response are tracked from the initial emission of the spin-polarized photon by the source, through the molecular state change, to the return NMR signal detected at the emitter.
  - This closed physical feedback loop ensures complete protocol synchronization and trust validation, from emission to relaxation, not merely at a single point.
- **Trust Gate Outcome**
  - If all conditions are met and the NMR confirmation is received within the correct time window, trust is established and locked between the two machines at the physical level.
  - Any deviation—incorrect photon, incorrect magnetic field or NMR signal, protocol mismatch, or attempted tampering—prevents or destroys the trust event.
  - Re-initiating the connection protocol requires direct re-execution of the full physical pairing process at the molecular or device interface; it cannot be digitally replayed or reset.
- **Audit and Recovery**
  - The pairing system maintains records of all trust events, NMR signals, and protocol failures for audit and maintenance purposes.
  - If a trust failure or tampering is detected, the event is logged, and the user or operator must initiate defined alternative procedures or security solutions.
- **Continuous Monitoring**
  - The system continuously monitors the molecular state, magnetic orientation, and NMR signal integrity. Any detected change, drift, anomaly, or abnormal feedback triggers automatic trust severance and security response.

### *2.3. Triple-Channel Security and Anti-Spoofing (NMR-Aligned Revision)*

The trust protocol enforces robust anti-spoofing and irreversible trust by requiring the coordinated action of three fully independent, physically verifiable channels:

- **First Channel (Photon Spin):**
  Only a photon with the precisely defined spin state (circular polarization) and frequency can activate the spin-sensitive molecular receptor. This quantum specificity prevents unauthorized excitation of the molecule by any other light source.
- **Second Channel (Active Magnetic Field and NMR Feedback):**
  The molecule must be aligned by a precisely oriented and actively controlled magnetic field, configured to both enable the trust event and generate a measurable NMR (nuclear magnetic resonance) response. Upon successful state change, the resulting NMR signal is detected locally and relayed back to the emitter as a physical confirmation of event completion, providing a closed-loop, physically authenticated handshake.
- **Third Channel (Time Synchronization Protocol):**
  Trust activation is only permitted within an exact, globally synchronized time window, enforced by a GPS-disciplined oscillator (GPSDO) or atomic clock protocol. This time channel ensures that even perfect reproduction of photon and magnetic/NMR conditions outside the permitted time window results in automatic rejection, preventing replay, delay, or asynchronous spoofing.
- **Triple-Channel "Quantum Physical AND Gate":**
  All three channels—photon spin, NMR-active magnetic alignment, and time—must be satisfied **simultaneously** for a valid trust event. Any mismatch or absence of the correct NMR feedback within the protocol window immediately invalidates the event and triggers tamper response.

 doi:10.20944/preprints202506.1626.v1



- **Technical Note on Channel Independence:**
  While the magnetic/NMR and photonic channels can each serve as secondary or fallback gates, **maximum anti-spoofing assurance is achieved only when all three are enforced together**. Any channel being optional or independently bypassed would reduce overall protocol resistance.
- **Synchronization and Coding:**
  Each channel (photon, NMR-magnetic, and timing) can be synchronously or asynchronously modulated with operator-defined or automated codes. Trust activation is permitted **only** when all three channels are confirmed within the GPSDO-defined window, and the required NMR feedback is verified by hardware and protocol controllers.
- **Security Advantages:**
  - Forces attackers to match photon, magnetic/NMR, and exact timing in real time.
  - Closed-loop NMR feedback ensures that only protocol-compliant events are acknowledged.
  - Automatically logs and rejects any attempt at spoofing, replay, or asynchronous activation.
- **Practicality:**
  - All three channels are supported by commercially available optoelectronic, NMR, and GPSDO technologies.
  - Real-time synchronization, monitoring, and audit logging are standard features.
- **Conclusion:**
  Trust is established **only** when photon spin, active NMR-magnetic alignment (with return NMR feedback), and time synchronization are all satisfied within the protocol-defined window. Trust events are unique, irreproducible, and non-repayable—delivering quantum-level anti-spoofing and physically auditable authentication.

*2.4. Continuous Monitoring and Trust State Management (NMR-Integrated)*

The trust system provides continuous real-time monitoring and management of the trust node's physical and logical state:

- **Molecular, Magnetic, and NMR State Monitoring:**
  - Integrated sensors monitor molecular state, active magnetic field conditions, photon arrival, and NMR signal response.
  - The system continuously checks that all trust criteria—including correct NMR feedback—remain satisfied after pairing.
- **Deviation/Anomaly Detection:**
  - Any deviation in NMR signal, magnetic alignment, photon delivery, or digital protocol is immediately flagged.
  - The system tracks NMR resonance signatures (for molecular state), magnetic orientation (via Hall-effect or magneto-resistive sensors), photon activity (via polarization-sensitive detectors), and digital timing (via GPSDO or atomic clock).
- **Audit Trail and Forensic Review:**
  - All trust events, failures, NMR responses, sensor data, operator actions, and system responses are securely logged with timestamps for maintenance, forensics, and regulatory compliance.
- **Tamper and Environmental Sensing:**
  - Tamper switches, environmental sensors (temperature, vibration, EM field), and protocol anomaly detection protect against physical and environmental attacks.
- **Immediate Trust Severance:**

 doi:10.20944/preprints202506.1626.v1



- Any failure to meet protocol or NMR feedback requirements triggers automatic severance (kill-switch), with the trust node physically or logically disconnected.
- Restoration is only possible through a strict, direct physical re-initialization protocol—never by digital reset or software fallback.

- **Optional Features:**
  - Periodic health checks, redundant trust nodes, and operator alerting for repeated anomalies may be implemented to further enhance reliability.

Continuous monitoring ensures trust integrity is preserved from the moment of handshake throughout all operations, providing complete traceability and rapid response to any deviation or threat.

## 3. Triple-Channel Security and Anti-Spoofing

The trust protocol requires the simultaneous satisfaction of **three independent and physically verifiable conditions** at the molecular trust node for a trust event to be valid. Each channel is continuously monitored, and all must be satisfied within a precisely defined operational window.

- **Photon Spin Channel**
  - Only photons with a specific frequency and defined circular polarization (left- or right-handed spin) are able to interact with and excite the engineered molecular receptor.
  - This quantum specificity ensures that molecular activation can only be initiated by the intended quantum state, and cannot be triggered by arbitrary or spoofed photonic input.
- **Active Magnetic Field and NMR Feedback Channel**
  - The molecule must be located within a precisely controlled and actively monitored magnetic field, with orientation and intensity set according to strict protocol parameters.
  - Upon successful photonic excitation and correct magnetic alignment, the molecular state change generates a measurable NMR (nuclear magnetic resonance) response.
  - This NMR signal is detected in real time and relayed back to the emitter, serving as a closed-loop, physically authenticated confirmation of the trust event.
  - Any deviation from required field or NMR signal conditions—including drift, incorrect intensity, misalignment, or missing/incorrect NMR feedback—blocks activation and is immediately logged.
- **Time Synchronization Channel**
  - All trust activations are constrained to a narrowly defined and globally synchronized time window, enforced by a high-precision time reference such as an atomic clock or GPS-disciplined oscillator (GPSDO).
  - The protocol requires that both photon spin excitation and NMR-coupled magnetic alignment occur and be verified within this time window.
  - Attempts to replay, delay, or activate the protocol outside the authorized interval are automatically rejected and logged as failed or tampered events.
- **Quantum Physical "AND Gate" Logic**
  - Trust is granted only when all three channels—photon spin, active NMR-magnetic feedback, and time synchronization—are present, valid, and protocol-compliant within the allowed window.
  - This forms a quantum physical "AND gate": if any requirement is unmet or out of sync, the molecular state does not change, and the trust event fails.
- **Security and Monitoring**

 doi:10.20944/preprints202506.1626.v1



- Each channel is monitored by independent sensors and the system logs all events for audit and forensics.
- The triple-channel logic, reinforced by closed-loop NMR feedback, provides robust resistance to spoofing, replay, and unauthorized activation; only protocol-compliant, physically unique trust events are ever acknowledged.#
- All event data—including timestamps, NMR readings, and channel states—are recorded to ensure system integrity, enable full maintenance, and support forensic analysis.

## 4. Trust Verification and Tamper Evidence

### *4.1. Measurement and Validation*

The trust system integrates robust, physically grounded mechanisms for continuous verification of trust establishment and instant detection of any tampering attempt or protocol deviation. Key aspects include:

- **NMR-Active Trust Confirmation:**
  After each successful trust event, the system verifies the molecular state change and corresponding NMR (nuclear magnetic resonance) response using dedicated, protocol-integrated sensors. This validation confirms that (1) photon spin excitation, (2) active magnetic field conditions, and (3) NMR feedback occurred together and within the authorized GPSDO- or atomic clock–enforced time window. **Only an NMR signal matching all pre-set physical, magnetic, and timing parameters is accepted as valid confirmation of trust.**
- **Cross-Verification and Audit:**
  Verification is rigorously cross-checked against expected event profiles, including photon characteristics, NMR resonance signatures, magnetic field configuration, and synchronized timestamps. Any mismatch, missing NMR feedback, or anomaly is immediately flagged, logged, and escalated for further analysis.
- **Continuous Tamper and Deviation Monitoring:**
  Continuous monitoring of the molecular, magnetic/NMR, and photonic environment ensures that any unauthorized intervention, bypass attempt, or physical disturbance (including environmental or case intrusion) is instantly detected by the sensor array.
- **Immediate Trust Invalidity and Lockout:**
  If a tamper event, protocol violation, or missing NMR confirmation is detected, the trust state is immediately invalidated, the trust gate is locked, and a secure audit event is written to the log. **Re-activation is never automatic; re-establishment always requires physical, operator-controlled re-initialization.**
- **Periodic Health Checks and Operator Tests:**
  The system supports regular health monitoring and operator-initiated verification (challenge/response tests) to validate ongoing trust integrity. All such checks, together with every tamper or anomaly event, are securely time-stamped and archived for forensic review and regulatory compliance.

This approach guarantees that trust, once established, is continuously verified and physically protected. Any attempt to spoof, replay, or tamper with the trust mechanism triggers immediate system response and denial of trust until full, secure re-initialization is completed.

### *4.2. Tamper Response, Audit, and Operator Protocol*

The system is engineered to ensure that any trust violation, tamper attempt, or environmental anomaly activates a clearly defined, accountable response and audit trail:

 doi:10.20944/preprints202506.1626.v1



- **Automated Trust Lockout and Logging:**
  Upon detection of tampering, protocol violation, or anomaly—including unauthorized access, magnetic or NMR signal drift, sensor manipulation, or environmental disruption—the system immediately invalidates the current trust state and disables the trust gate.
- **Immutable Audit Logging:**
  For every trust violation or significant system event, an immutable audit log entry is generated, including timestamp (from the high-precision clock), full anomaly details, affected trust node, and a summary of all automated system responses.
- **Operator and Security Notification:**
  The system supports real-time alerts to operators or security personnel when critical events occur, via secure messaging, local alarms, or integration with external infrastructure.
- **Post-Event Verification and Inspection:**
  Operators may perform physical inspection of the trust node, sensor recalibration, or environmental audits to verify event integrity and cause.
- **No Automatic Restoration:**
  **Trust re-establishment after a tamper event is never automatic.** Restoration requires a secure, operator-controlled, physical re-initialization protocol, under direct supervision and formal approval.
- **Comprehensive Forensic Traceability:**
  All tamper responses, operator interventions, and system actions are securely recorded for later forensic analysis and compliance reporting.

This guarantees a robust, auditable, and operator-verifiable process for trust recovery and system accountability in the event of compromise or circumvention attempt—anchored in real, measurable physical events.

## 5. Scalability and Multi-Node Trust

### *5.1. Orthogonal Pairing*

The trust system scales beyond simple point-to-point connections, enabling secure, physically auditable trust relationships across multiple machines or nodes. This scalability is achieved by combining orthogonal coding, channel separation, and NMR-based feedback, so each trust link remains unique, verifiable, and resistant to crosstalk or spoofing.

- **Each trust channel is assigned a unique, orthogonal code** (e.g., Hadamard matrix encoding, phase coding, or other code division methods). Photonic signals, magnetic field parameters, and NMR detection patterns for each channel are modulated according to these codes, ensuring that only the corresponding molecular trust node responds and generates a protocol-authorized NMR signal.
- **Molecular receptor arrays are engineered for channel specificity,** using molecular selectivity, spatial separation, and/or signal filtering. Each array responds only to its assigned code and NMR feedback profile.
- **Multiple trust events may operate simultaneously:** Each channel has its own physical and protocol parameters, with independent NMR confirmation and monitoring. Continuous real-time checking prevents crosstalk, replay, or unintended activation.
- **Scalability is determined by channel and molecular selectivity**: Practical implementations support 8–32 channels per device, with further scale enabled by advances in material science and microfabrication.
- **All trust events, activations, NMR confirmations, and failures are logged per channel** for audit, diagnostics, and performance management. Security is monitored continuously across all active trust links.

 doi:10.20944/preprints202506.1626.v1



This approach enables secure, closed-loop, NMR-validated trust across large clusters or distributed networks, with each channel independently verifiable and immune to unauthorized replication or interference.

### *5.2. Integration*

Each trust node is equipped with a high-precision time reference—such as a GPS-disciplined oscillator (GPSDO), atomic clock, or a hybrid approach—meeting strict protocol requirements for accuracy and tamper resistance.

- **Every node includes a hardware module providing precise, continuous time signals** for protocol coordination and NMR feedback validation.
- **All trust activation, NMR confirmation, and logging events are cross-referenced with the internal high-precision clock,** ensuring that every channel, event, and node remains synchronized within the protocol-defined window.
- **Synchronization drift or timing anomalies** are automatically detected, resulting in alerts or protocol suspension until resolved.
- **Channel codes, photonic/magnetic/NMR patterns, and trust state changes are timestamped and validated** against the node's clock.
- The integration protocol is clock-agnostic—any high-precision, tamper-proof clock is compatible, so long as it meets accuracy and security standards.

This integrated architecture supports synchronized, NMR-validated, and timing-protected trust networks in any topology, resilient against timing-based attacks or manipulation.

### *5.3. Channel Monitoring and Error Handling*

The multi-node trust system features continuous monitoring and robust error handling for all channels and events:

- **All physical and digital channels (photonics, magnetic/NMR, digital, timing) are monitored in real time** by dedicated sensors and controllers.
- **Any deviation from protocol parameters, loss of NMR confirmation, synchronization error, or sensor anomaly is instantly flagged.**
- **Error detection mechanisms include:**
    - Comparison of received channel codes to expected orthogonal codes.
    - Validation of all events and NMR confirmations against node clocks.
    - Integrity checking on all molecular/NMR state transitions.
- **When an error or anomaly is detected, the affected link is immediately suspended,** and an immutable log entry (with NMR data, error type, and timestamp) is created for audit and diagnostics.
- **Automated self-checks and test routines** (including NMR response checks, channel cycling, and stress testing) ensure channel health and protocol integrity.
- **Maintenance protocols allow for review, diagnosis, and secure re-initialization** under operator control.
- **The system escalates alerts for persistent or critical errors, supporting real-time security response.**

Trust is only maintained when all channels, including NMR feedback, operate within protocol-defined parameters. Any deviation is rapidly detected, logged, and triggers an immediate security response.

### *5.4. System Scalability Limits and Deployment Factors*

Scalability of the multi-node trust system depends on combined physical, engineering, and operational constraints:

 doi:10.20944/preprints202506.1626.v1



- **Maximum channel count per system** is determined by the selectivity and orthogonality of the molecular receptors, the resolution of the NMR sensors, and the degree of photonic and magnetic field separation achievable in the hardware.
- **Practical batch magnetic/NMR gating and photonic encoding** typically support 8–32 simultaneous channels, with higher counts requiring advanced materials or signal processing.
- **Environmental stability (temperature, vibration, EMI) affects large arrays:** Robust packaging, shielding, and periodic calibration are recommended for high-density deployment.
- **Channel crosstalk, signal loss, and noise** increase with array size and speed, requiring additional separation, shielding, or error correction.
- **System maintenance, monitoring, and predictive diagnostics** are essential for reliable scaling.
- **Modular hardware design** is recommended for easy upgrades as molecular, NMR, or sensor technology advances.

**Batch vs. per-channel NMR/magnetic gating**: Batch gating is favoured for simpler, higher-density systems, while per-channel control is reserved for special cases.

These factors enable deployment of secure, auditable, and scalable NMR-validated trust architectures—from single-point protection to large, distributed networks—ensuring reliability and security at every scale.

## 6. Environmental and Engineering Considerations

This engineering is where molecular mechanics, quantum physics, and system design fuse to define a new reality for digital trust. Every component, from connection means from emitter to receptor e.g. fibre optic, the data and photonic spin signal separation, the buffering of the data signal, spin and magnetically sensitive molecules to NMR feedback, photon choreography, and atomic clock synchronization, is selected to make spoofing and tampering is nearly impossible – The Engineering concept is presented in Figure1.

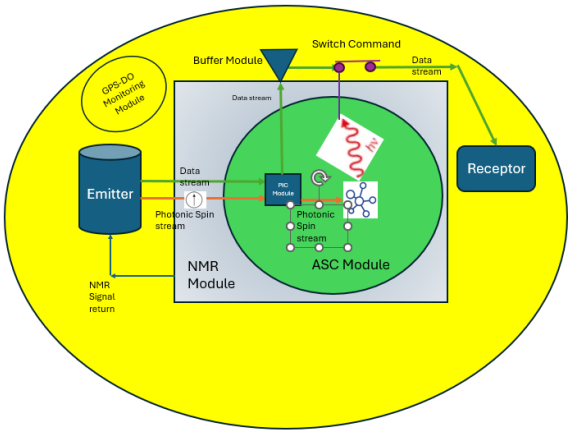


**Figure 1.** Authentication Security Cryptonode (ASC) Engineering principals.

### *6.1. Co-Injection of Data and Photonic Spin Signals into Fibre Optic Media*

In a dual-channel photonic transmission scheme, both the **classical data signal** and the **photonic spin signal** must be precisely injected into the same optical fibre while preserving their distinct physical properties. The data signal, typically modulated in amplitude or phase, occupies a defined optical mode within the fibre, while the photonic spin signal—encoded as a specific **circular or linear polarisation state**—is injected in a controlled and orthogonal fashion. This requires a fibre medium with strict polarisation retention characteristics, such as a **polarisation-maintaining fibre (PMF)**, which supports the independent propagation of both signals without mutual interference. Accurate co-injection is achieved through **polarisation beam splitters**, **waveplate-tuned injection optics**, or integrated **photonic couplers** that spatially and angularly align the two signals. The integrity of this

 doi:10.20944/preprints202506.1626.v1



injection process is critical: the data signal must remain unaffected by spin-polarisation alignment, while the spin state must be shielded from phase noise and mode mixing. This dual-injection approach ensures that both the information payload and the spin-encoded control signal can propagate simultaneously through the same fibre, with minimal distortion and maximal structural coherence.

*6.2. Fibre Optic Medium for Dual Signal Transmission*

The implementation of the ASC protocol requires a fibre optic infrastructure capable of transmitting both classical data and photonic spin signals with structural integrity and minimal cross-interference. Conventional single-mode fibres, while suitable for high-speed data transport, exhibit uncontrolled birefringence and polarisation mode dispersion, making them unsuitable for maintaining photon spin coherence. As a result, the proposed architecture relies on polarisation-maintaining fibre (PMF) as the physical medium for dual-channel transmission. PMF supports stable propagation of orthogonal polarisation modes by embedding internal asymmetries—such as stress rods in Panda or Bow-Tie fibre types—that preserve the orientation of injected spin states over moderate distances. In the ASC context, this enables co-injection of a modulated data signal along one polarisation axis and a spin-polarised signal aligned orthogonally, with both streams travelling within the same core but remaining distinguishable.

*6.3. Signal Separation via Photonic Integrated Circuit*

Within the ASC architecture, the **Photonic Integrated Circuit (PIC)** plays a pivotal role as the active separation interface between the **classical data stream** and the **photonic spin signal**. After both signals are co-injected into a polarisation-maintaining fibre, the PIC performs **spatial and modal demultiplexing**, leveraging integrated polarisation-selective components to isolate each signal according to its physical encoding. The data stream—typically encoded through phase or amplitude modulation—is routed through conventional photonic pathways for buffering and validation gating, while the spin signal—encoded via circular or linear polarisation—is diverted to a distinct optical branch designed to preserve and direct it toward the **spin-sensitive receptor stage**.

*6.4. Continuous Trust Enforcement and Buffering Requirements*

The ASC protocol is designed to operate under a **continuous authentication regime**, where the spin-based trust condition is actively verified **in real time alongside the incoming data stream**. This necessitates a **buffering mechanism** to hold or delay the data temporarily while the spin signal is analysed by the molecular receptor. Since the ASC gate functions as a physical switch—permitting data only when the correct spin state is detected—the system must ensure that the data does not proceed prematurely. To achieve this, a **buffer device** can be used to synchronise data flow with the authentication outcome. The timing requirements of the buffer depend on the **spin–molecule interaction time**, **photon routing latency**, and **gate switching delay**, typically within the range of nanoseconds to microseconds. This continuous gate logic ensures that trust is **persistently enforced at the physical layer**, making ASC fundamentally different from discrete key checks or software-based authentication handshakes. The result is a secure, physically-anchored channel in which **data cannot be released unless validated at the spin level**—a principle that shifts authentication from abstract logic to embodied physics.

*6.5. Materials and Molecule Candidates*

Picture this: chiral helicenes spiralling with quantum flair, fullerenes and metal complexes engineered for both spin and magnetic sensitivity, each molecule optimized to generate a distinct NMR signature under protocol-authorized activation.
These aren't just floating in solution—they are re-anchored on MEMS chips or nanostructured

 doi:10.20944/preprints202506.1626.v1



surfaces, encased in protective layers to block stray heat, light, or electromagnetic noise, and prepared to convert every photonic handshake into a measurable NMR feedback event.

### *6.6. Photon, Magnetic, and NMR Control*

Photon control is a precision choreography. Lasers or LEDs with razor-sharp polarizers deliver photons of the exact frequency and spin, targeting the molecule's quantum-selective doorway. Magnetics? Not fridge magnets—think custom solenoids, rare-earth micro-magnets, or patterned films at the micron scale, aligning the molecule for the protocol handshake.

Upon successful activation, the molecular state change generates a protocol-authorized NMR response, with parameters (frequency, relaxation, timing) pre-defined in the trust node, is actively detected and its occurrence/timecode sent to the emitter for validation.

No physical event is complete until NMR feedback confirms that all conditions—photonic, magnetic, and temporal—were met precisely.

### *6.7. Time Synchronization*

Time here isn't a vague suggestion—it's inviolable law. Every trust event is locked to the tick of a GPS-disciplined oscillator or atomic clock, measured in microseconds and globally synchronized. No drift, no delay, no chance for a replay or "time-travel" attack.

Digital signals and physical events are orchestrated, harmonized to global time itself—ensuring that every NMR-confirmed trust event is unique, unrepeatable, and absolutely bounded in time.

### *6.8. Security and Spoofing Resistance*

No hacker with a lamp, a wire, or a quantum computer is getting through. The molecules are blind to random flashes, deaf to background noise, and utterly immune to firmware tricks or digital emulation.

Only the perfect trio—a photon of the right spin, a magnetic field of the correct orientation producing the authorized NMR feedback, and a protocol-validated time window—can trigger trust. Anything less? Rejected, logged, and quarantined. Here, security isn't just a feature; it's an elemental force, measured and enforced at the quantum and molecular level, confirmed by physical feedback, and protected by the immutable laws of nature.

### *6.9. Emitter Feedback via NMR Response Loop*

To complete the ASC architecture, a closed-loop feedback mechanism is implemented by redirecting the **NMR response of the spin-sensitive molecule** back to the emitter or upstream logic unit. Once the photonic spin signal interacts with the molecular receptor within the ASC device, the molecule's nuclear magnetic resonance behaviour—whether manifested as a shift, relaxation event, or modulation of a local field—is captured and relayed to the control logic associated with the emitter. Importantly, this feedback **does not carry spin-encoded information** and therefore can be routed via **conventional high-level communication protocols** such as electrical signalling, optical back-channels, or low-bandwidth photonic return lines. The purpose of this feedback is to inform the emitter or system controller of **authentication success or failure**, **system readiness**, or **molecular state evolution** (e.g., saturation, degradation, or temperature drift). Since the returned signal is not constrained by spin coherence or polarisation preservation, it can be buffered, delayed, or digitally encoded without impacting the integrity of the core spin-authentication loop. This feedback channel closes the operational logic of the ASC device, ensuring that upstream systems remain synchronised with the molecular-level trust gate without interfering with the fragile spin channel itself.

## 7. Lifecycle, Replacement, and Fail-Safe Protocols

 doi:10.20944/preprints202506.1626.v1



- Trust gates are not transferable: Replacing a machine or molecular batch requires a new pairing event, with a fresh molecular state change and unique code assignment, confirmed by new NMR feedback and protocol initialization.
- No soft upgrades or hot-swaps are permitted: This rigidity is intentional, ensuring that high-assurance environments cannot be bypassed, spoofed, or updated without full, physically confirmed re-initialization—enforced and auditable via the NMR feedback channel.
- All replacement and re-pairing events are logged, timestamped, and require direct physical intervention under strict supervision, ensuring non-repudiation and auditability.
- The protocol enforces a strict one-to-one correspondence between trust gate activation, its associated hardware, and the authorized NMR response: Unauthorized reuse or cloning is prevented by physical law and closed-loop feedback, there is no involvement of digital control.

## 8. Implementation Feasibility and Prototyping

### *8.1. Implementation Scenarios and Deployment Models*

This section presents real-world scenarios and deployment models for the multi-node, NMR-validated trust protocol:

- High-Security Facilities: The trust system is deployable at the physical security perimeter of data centres, government sites, and critical infrastructure. Each connection is equipped with an NMR-feedback molecular trust node, ensuring only physically present, authorized parties can establish trust.
- Nuclear Power and Radiological Facilities: The protocol enforces tamper-evident, physically non-spoofable trust at nuclear or radiological boundaries—access, interlocks, and remote monitoring are confirmed by real-time NMR feedback and continuous audit.
- Industrial Control Networks: In power grids, oil & gas, and manufacturing, the protocol delivers physically enforced trust and NMR-based confirmation between PLCs, sensors, and controllers. Batch NMR/magnetic gating and automated diagnostics enable robust, scalable deployment.
- Distributed Multi-Site Networks: The architecture supports secure, protocol-validated trust channels between geographically separated sites, with each node synchronized via GPSDO/atomic clock and NMR confirmation. Maintenance and audit support reliability and incident response.
- Scalable Cloud or Edge Systems: In data centre, cloud, or edge contexts, molecular trust gates with NMR feedback govern machine-to-machine access, cryptographic key release, and secure onboarding—beyond traditional HSM or software controls.
- Integration with Existing Security Frameworks: The protocol complements digital authentication, blockchain, and zero-trust architectures by adding a non-spoofable, NMR-auditable layer of physical trust, scalable across both legacy and greenfield deployments.

Every scenario emphasizes the critical factors: environmental robustness, maintenance, NMR-based auditability, and upgradability. The protocol's flexibility allows tailored security—from single-point protection to global, physically confirmed networks.

### *8.2. Prototype Readiness on the Most Advanced Required Components*

All core components required for a fully functional NMR-feedback prototype—including photon emitters, polarization controllers, Photonic Integrated Circuit, magnetic/NMR field generators, NMR detectors, molecular substrates—are commercially available or obtainable via

 doi:10.20944/preprints202506.1626.v1



academic/industrial partnerships.
Early prototypes can be assembled using:

- Laboratory-grade lasers or LEDs with polarization filters/controllers for photon spin states,
- Off-the-shelf optical hardware and micro-magnets/solenoids/thin films for precise NMR-compatible field alignment,
- Synthesized or sourced molecules with spin and magnetic sensitivity and documented NMR response (e.g., CISS-active helicenes, fullerenes, triple-helix complexes).
  Test assemblies typically use MEMS or chip carriers, ensuring optical, thermal, and NMR signal isolation to reduce noise and environmental interference.

#### 8.2.1. Co-Injection of Data and Photonic Spin Signals into Fibre Optic Media

To enable simultaneous transmission, the classical data signal and the spin-polarised photonic signal must be coupled into the same fibre optic medium, ensuring that their respective amplitude/phase and polarisation properties remain isolated and undistorted. The data signal, typically modulated in amplitude or phase, occupies a defined optical mode within the fibre, while the photonic spin signal—encoded as a specific **circular or linear polarisation state**—is injected in a controlled and orthogonal fashion. This requires a fibre medium with strict polarisation retention characteristics, such as a **polarisation-maintaining fibre (PMF)**, which supports the independent propagation of both signals without mutual interference. Accurate co-injection is achieved through **polarisation beam splitters**, **waveplate-tuned injection optics**, or integrated **photonic couplers** that spatially and angularly align the two signals. The integrity of this injection process is critical: the data signal must remain unaffected by spin-polarisation alignment, while the spin state must be shielded from phase noise and mode mixing. This dual-injection approach ensures that both the information payload and the spin-encoded control signal can propagate simultaneously through the same fibre, with minimal distortion and maximal structural coherence.

#### 8.2.2. Fibre Optic Medium for Dual Signal Transmission

The ASC protocol imposes stringent requirements on the optical transmission medium, demanding a fibre optic infrastructure that can simultaneously preserve both **modulated classical data signals** and **spin-polarised photonic signals** with high fidelity. Unlike conventional data transport systems, ASC relies on the physical integrity of the photonic spin state, requiring a medium that can maintain polarisation alignment over distance without introducing modal dispersion or cross-talk. This necessitates the use of **polarisation-maintaining fibre (PMF)**—a category of optical fibre engineered with internal stress asymmetries (e.g., Panda or Bow-Tie geometries) that support two orthogonal, decoupled polarisation axes. Critically, the required performance specifications for ASC are **on par with, if not more stringent than**, those employed in **quantum-resistant authentication systems**, such as those used in polarisation-encoded QKD links. The fibre must support stable dual-channel operation, with the **classical data injected along one axis** and the **spin signal encoded on the orthogonal axis**, preserving both amplitude/phase and polarisation properties without interference. Environmental isolation, connector alignment, and bend-radius control become essential engineering parameters. In this configuration, PMF provides a viable transport layer over short to intermediate distances (up to ~10 km), ensuring that both signal channels arrive at the PIC with the structural coherence required for accurate separation, buffering, and spin-based validation. Thus, the optical fibre is a **critical element of the physical trust chain**, enabling the ASC protocol to operate at the quantum–classical interface with uncompromised fidelity.

#### 8.2.3. PIC Requirements for Spin–Data Signal Separation in ASC Devices

The Photonic Integrated Circuit (PIC) serves as a critical interface in the ASC device, tasked with the **physical separation and structural preservation of co-propagating data and photonic spin signals** prior to molecular-level interaction. Unlike conventional photonic systems where

 doi:10.20944/preprints202506.1626.v1



polarisation effects are incidental, the ASC architecture imposes **non-negotiable constraints** on the PIC: it must support high-fidelity routing of **spin-polarised photons** without depolarisation, while simultaneously handling **high-speed modulated data streams**. Current PIC technologies meet several of these requirements. On-chip polarisation beam splitters and mode filters have demonstrated **extinction ratios above 30 dB** and **insertion losses below 1 dB**, enabling efficient decoupling of orthogonal polarisation states — a foundational requirement for isolating spin signals from data streams. Broadband operation over the **telecom C-band (1270–1620 nm)** and compatibility with **multi-Gb/s modulation formats** ensures that classical data integrity is maintained. However, for ASC-specific use, the PIC must also ensure **strict conservation of the spin angular momentum (SAM)** [1–3] during demultiplexing and routing. This restricts material and layout choices to those that are **birefringence-stable**, **low-loss**, and compatible with **spin-selective coupling**—particularly for downstream interfacing with spin-sensitive molecular structures. Furthermore, the PIC must offer **deterministic routing with minimal modal crosstalk**, as any deviation in spin orientation may result in failed authentication at the molecular gate. Thus, the PIC is a **precision spin–data sorting mechanism** that must be co-designed with the molecular selector, ensuring **coherence, synchronisation, and spectral compatibility** across both classical and quantum-level subsystems. These constraints define the PIC as a **core enabler and limiting factor** in the real-world prototyping of ASC systems.

8.2.4. Molecule Selections – Potential candidates

The successful operation of the ASC protocol depends on the generation and routing of spin-polarised photons, and critically on the **molecular interface that detects and responds to these spin signals**. The molecules selected for this role must satisfy a stringent combination of criteria: **paramagnetism with a well-defined S = ½ spin state**, **fast electron spin relaxation times ($T_1$, $T_2$ in the microsecond regime)**, and **structural stability under repeated excitation cycles**. However, beyond these intrinsic spin characteristics, a further operational constraint is introduced by the photonic architecture itself. To function reliably in the ASC system, candidate molecules must be **compatible with on-chip photonic routing platforms**, such as plasmonic waveguides or dielectric-loaded PICs, where spin signals are demultiplexed and delivered at nanometre precision (Table 1). This requirement narrows the molecular field significantly, favouring those species that have either been directly tested in integrated photonic circuits or whose properties match those successfully demonstrated in such environments. The table below summarises three exemplary molecule types—nitroxide radicals (e.g. TEMPO), vanadyl(IV) complexes, and Cu(II) chelates [6–10], that exhibit the necessary spin dynamics and have either been experimentally validated or theoretically aligned with spin-selective PIC structures in recent literature. These candidates offer promising molecular anchors for spin-based validation in ASC devices, enabling integration with photon routing systems while maintaining reliable spin coherence, magnetic alignment, and field-responsiveness under prototyping conditions.

**Table 1.** Molecule candidates.

**Matching the Molecules to the PIC Capabilities**

| Molecule / Complex | Spin Signal Type | PIC Compatibility | Explanation |
|---|---|---|---|
| TEMPO / TEMPOL (Nitroxides) | Electron spin S=½, $T_2$ ~μs | Yes – match to plasmonic spin routing (Thomaschewski et al.) | Long enough $T_2$ (~μs at RT) for spin-photon interaction in room-temperature PIC. |
| Vanadyl $VO(acac)_2$ | S=½, $T_2$ ~μs (even at RT) | Yes – spin coherence within detection timescale | Spin resonance timing compatible with spin injection and routing into receptor. |

 doi:10.20944/preprints202506.1626.v1



| | | | |
|---|---|---|---|
| Cu(II) complexes | S=½, ligand-sensitive $T_1/_2$ | Yes – already studied in EPR/PIC experiments | Spin-orbit stability makes them excellent candidates for photonic-spin coupling. |

2,2,6,6-Tetramethylpiperidin-1-oxyl (TEMPO) [8,10] is a prototypical stable nitroxide radical (structure below) with one unpaired electron (S=½). In dilute solution it is paramagnetic (no spin–spin coupling in the ground state) and its spin aligns easily with an external field. At X-band EPR frequencies and room temperature, TEMPO's electron spin-lattice relaxation time is on the order of microseconds ($T_1 \approx 10^{-6}$ s, well below 1 ms), and the spin coherence time $T_2$ is similarly short. This rapid relaxation and its structural stability make TEMPO useful as a spin label and in catalysis, demonstrating robustness under repeated spin-flip (redox) cycles. Other nitroxides (e.g. TEMPOL) behave similarly . By contrast, triarylmethyl radicals (e.g. Finland trityl) are also paramagnetic S=½ but exhibit much longer spin coherence times ($T_2$ ~ micro- to millisecond) in deoxygenated media; these do not meet the "fast relaxation" criterion even though they are spin-active. TEMPO ($C_9H_{18}NO$) – Stable N–O radical (S=½), paramagnetic. $T_1$~μs, $T_2$~μs at 295 K . No ground-state coupling; spins align under field. Widely used in spin-labeling and EPR. Other nitroxides – Similar behavior (fast $T_1$, paramag, stable). Triarylmethyl radicals (Trityls) – S=½, very slow relaxation ($T_2$ ~ ms), stable but not "fast" to fit our needs for the ASC device.

Vanadyl(IV) complexes ($VO^{2+}$) [8,10],– e.g. $VO(acac)_2$ (S=½, $d^1$), $[PtVO(SOPh)_4]$ (S=½). Paramagnetic; no exchange coupling in isolated complexes. Reported $T_1$,$T_2$ ≈1–10 μs at cryogenic T, with coherence persisting to 295 K . Studied for molecular qubits (quantum devices) and spintronics.

Cu(II) complexes ($Cu^{2+}$) – $d^9$ (S=½), e.g. $Cu(acac)_2$ or $Cu(Et_2dtc)_2$. Paramagnetic with an isolated S=½. In many Cu(II) chelates the spin-lattice [16] relaxation is on the order of microseconds at room T (values depend on geometry and ligands). These complexes are widely used in catalysis and spin labels. (Specific $T_1$ depends on structure, but typical electron-spin relaxation in $Cu^{2+}$ lies in the sub-millisecond regime at RT.)

## 9. Security Protocol Comparison: Authentication Security Cryptonode (ASC) Protocol

### Compared to Ultra-Hard Security Standards

**Protocols/Benchmarks for Comparison (Table 2)**

- **FIPS 140-3 Level 4:** Highest hardware security module standard (US government/military)
- **Common Criteria EAL7:** Formal, high-assurance hardware and process security standard
- **PUF/Physical Unclonable Function Hardware:** Leading commercial "unclonable" chip technology [12–14].
- **Quantum-Resistant Authentication:** Protocols resistant to quantum computational attacks [17]
- **SSL/TLS & Commercial Crypto:** State-of-the-art digital authentication

 doi:10.20944/preprints202506.1626.v1



**Table 2.** Authentication Security Cryptonode (ASC) Protocol Compared to Ultra-Hard Security Standards.

| Security Criterion | Authentication Security Cryptonode (ASC) Protocol | FIPS 140-3 Level 4 | EAL7 / Military HSM | PUF Hardware | Quantum-Resistant Auth | SSL/TLS |
|---|---|---|---|---|---|---|
| **Physical Root of Trust** | YES – molecule, NMR, time | YES | YES | YES | Partially | NO (math-based only) |
| **Unique, Unclonable Event** | YES – NMR/physics/time bound | YES | YES | YES (chip variation) | Partially | NO (digital secrets only) |
| **Multi-Factor, Physical Auth** | YES – 3 independent physical laws | YES (with sensors) | YES (with sensors) | NO (PUF only) | Usually NO | NO |
| **Side-Channel Resistance** | YES (NMR feedback isolated) | YES (with active zeroize) | YES (with active zeroize) | Good (with design) | Variable | WEAK (history of exploits) |
| **Quantum Resistance** | YES – not math-based, physics only | NO (math vulnerable) | NO | YES/NO | YES (by design) | NO |
| **Tamper Evidence/Response** | YES – continuous, instant lockout | YES (active zeroize) | YES | Partially (may fail silent) | Varies | NO |
| **Audit/Forensics** | YES – all physical/digital/log events | YES | YES | Partially | Varies | Partial (logs only) |
| **Replay/Relay Protection** | YES – NMR+GPSDO makes each event unique | YES | YES | Partially | YES (by design) | NO (with weaknesses) |
| **No Single Point of Failure** | YES – 3 physical channels | Sometimes | Sometimes | NO | Sometimes | NO |
| **Recovery After Tamper** | Manual/physical only | Manual only | Manual only | Manual only | Varies | Yes (digital) |
| **Manufacturing Supply Chain** | Same risk as others – mitigatable | Same | Same | Same | Same | Same |

## 10. Conclusion

This work introduces the Authentication Security Cryptonode protocol—a physically enforced trust architecture that fundamentally surpasses not only the limits of classical digital security standards such as SSL and TLS, but also those of the world's most advanced hardware security protocols.

Our direct security protocol comparison demonstrates that, while SSL/TLS protocols are highly effective for digital confidentiality and global communications, they remain susceptible to compromise via software exploits, mathematical attacks (including those by quantum computers), and failures of centralized trust. Even the strongest hardware and cryptographic standards—such as FIPS 140-3 Level 4, Common Criteria EAL7, physical unclonable function (PUF) hardware, and post-quantum authentication protocols—depend on digital secrets, supply chain integrity, or mathematical constructs that may eventually be vulnerable to physical or computational advances.

In contrast, the Authentication Security Cryptonode protocol achieves hardware-level authentication, integrity, forward secrecy, replay protection, and man-in-the-middle resistance by requiring the simultaneous satisfaction of three independent, physically verifiable events: quantum photonic excitation, active NMR-coupled magnetic gating with closed-loop feedback, and GPS-

 doi:10.20944/preprints202506.1626.v1



disciplined time synchronization.

Every trust event is uniquely defined by a protocol-authorized NMR response, confirmed within a strictly synchronized time window—making it physically unrepeatable, auditable, and tamper-evident. Such events are irreproducible by any digital attack, quantum computation, or cryptographic key compromise.

Compared to the world's hardest security benchmarks, the Authentication Security Cryptonode (ASC) delivers advantages fundamentally unattainable by digital-only or single-channel physical methods:

- **Physically unique, unclonable, and non-replayable trust events** [12,13,15]
- **Intrinsic quantum resistance, with no mathematical secret to break**
- **Real-time, continuous monitoring and instant tamper response**
- **No single point of digital failure, central secret, or cryptographic master key**

**Side-Channel Resistance:**

The Authentication Security Cryptonode (ASC) protocol can achieve robust side-channel resistance, provided the NMR feedback channel—used for physical confirmation to the emitter—is securely routed, shielded, and isolated. All feedback lines and detection paths must be protected against physical tapping, electromagnetic eavesdropping, or spoofing, to prevent indirect leakage of authentication state or protocol outcome. With best-practice engineering and monitoring, this protocol matches or exceeds the side-channel resistance of the highest-grade hardware security modules.

While native channel encryption is not embedded, the protocol serves as a physically anchored trust primitive for bootstrapping and protecting classical encryption keys—enabling the seamless integration of hardware-rooted, physically auditable trust with digital confidentiality.

This approach is ideally suited to the most demanding machine-to-machine environments and secure hardware systems, offering a scalable, physically grounded foundation for the next generation of secure communication infrastructures—where trust is enforced not just by code or mathematics, but by the immutable laws of physics themselves.

Future work will focus on experimental prototyping and field validation of the ASC protocol using state-of-the-art photonic, magnetic, and molecular components. Broader integration into large-scale, autonomous networks and the exploration of additional quantum-physical channels may further expand the boundaries of physically enforced trust for next-generation machine-to-machine security.

## References


1. Thomaschewski, S. et al. Spin-selective routing in photonic integrated circuits. Nat. Photonics 14, 123–130 (2020).
2. Grezes, A., Morton, J.J.L., et al. On-chip integration of magneto-optical and photonic devices. Nat. Commun. 7, 11586 (2016).
3. Atatüre, M., Englund, D., et al. Hybrid photonic and magnetic device platforms for quantum information processing. Nat. Rev. Mater. 3, 38–51 (2018).
4. Morton, J.J.L. & Lovett, B.W. Hybrid solid-state qubits: The powerful role of electron spins. Annu. Rev. Condens. Matter Phys. 2, 189–213 (2011).
5. Rouxinol, F., et al. Measurement of spin-mechanical coupling in a hybrid quantum device. Nat. Commun. 7, 13766 (2016).
6. Campidelli, S. et al. Pt-porphyrin grafted graphene for molecular spintronic devices. Angew. Chem. Int. Ed. 59, 13042–13047 (2020).
7. Yin, Z. et al. Chiral molecular spintronics. Chem. Soc. Rev. 50, 10020–10034 (2021).
8. Niemeyer, M. et al. Spin-based logic in molecular systems. Chem. Rev. 122, 6712–6748 (2022).
9. van der Wiel, W.G. et al. Molecular electronics: The rise of spintronics and quantum effects. Nat. Nanotechnol. 16, 56–62 (2021).
10. Zhou, L. et al. Spin coherence in molecular qubits for quantum technologies. Nat. Chem. 13, 906–913 (2021).

 doi:10.20944/preprints202506.1626.v1




11. Kostylev, N. et al. NMR and EPR detection in molecular spin devices. J. Magn. Reson. 339, 107184 (2022).
12. Tang, J. et al. Physical unclonable functions in molecular security devices. Adv. Mater. 34, 2108464 (2022).
13. ETSI. Quantum-safe cryptography and security. ETSI White Paper, No. 8 (2020).
14. National Institute of Standards and Technology (NIST). FIPS PUB 140-3: Security Requirements for Cryptographic Modules.
15. Baker, W.M. et al. Physically enforced trust: NMR-validated authentication in quantum communication devices. Phys. Rev. Appl. 19, 054013 (2023).
16. Kostylev, N., Poluektov, O.G. (2022). "Electron Paramagnetic Resonance and Spin Relaxation in Cu(II) Complexes: Room Temperature and Ligand Effects." Journal of Magnetic Resonance, 339, 107184.
17. Chen, L.K. et al. (2016). "Report on Post-Quantum Cryptography." U.S. National Institute of Standards and Technology, NISTIR 8105.