Reducing Trust-Establishment Latency in Distributed Sensing Architectures

Acquisition-Derived Authenticity Evidence for Time-Critical Decision Systems

Technical White Paper

Prepared for technical, defense, aerospace, sensing, cyber-physical, and signal-processing audiences

Executive Summary

Modern sensing, communications, and cyber-physical systems increasingly depend upon the ability to establish trust in information quickly enough to support operational decisions. In many environments, information may be acquired and transported with low latency, yet confidence in that information may not be established until after downstream verification, authentication, provenance analysis, correlation, or sensor-fusion processes have been completed. As sensing architectures become more distributed and decision timelines continue to compress, trust-establishment latency itself can become a limiting factor.

This white paper describes a latency-reduced authenticity-sensing acquisition architecture in which authenticity-related information is generated during acquisition rather than solely after acquisition. The approach leverages physical acquisition-process behavior as a source of authenticity evidence. Observable characteristics such as transfer-function behavior, latency-reduction behavior, phase-slope behavior, group-delay behavior, gain coherence, distortion signatures, residual behavior, stability characteristics, and environmental response may be characterized during acquisition and transformed into authenticity-related information.

The resulting acquisition-derived authenticity evidence may be represented as Temporal Authenticity Signals (TASs), which preserve timing relationships and authenticity observables associated with the acquisition event. By generating authenticity information during acquisition-associated operation, trust-informed interpretation, prioritization, fusion, and decision support may begin earlier than in conventional trust-establishment workflows.

The architecture is positioned within the context of prior Signal Advance and negative-group-delay research, physical-layer authentication methodologies, trusted-computing architectures, provenance-management frameworks, and distributed sensing systems. Particular attention is given to applications involving distributed sensor networks, missile-warning and missile-defense architectures, space-domain awareness systems, cyber-physical infrastructure, industrial monitoring, autonomous systems, and other environments in which the timing of trust establishment may be operationally significant.

The central objective is earlier availability of acquisition-derived authenticity evidence, enabling trust-informed operations to begin sooner within the overall sensing workflow.

Technology Basis and Scope

This white paper describes a patent-pending acquisition architecture for generating authenticity-related evidence during signal acquisition. It is written as a standalone technical article, not as a claim interpretation, not as a limitation of patent scope, and not as a statement that the architecture has been deployed in any named defense, space, medical, industrial, or communication program. References to missile defense, space sensing, Golden Dome, SDA architectures, physiological monitoring, and autonomous systems are application contexts that illustrate why earlier trust formation can matter.

The central technical thesis is narrow and important: authenticity evidence can be generated from the physical behavior of the acquisition process itself, and latency-reduction acquisition can make that evidence available earlier than corresponding post-acquisition trust workflows.

Contents

1. Why Trust-Establishment Latency Matters

Latency is usually discussed as a transport or processing problem: how quickly a signal is acquired, digitized, moved, decoded, filtered, classified, or fused. In time-critical systems, however, a second form of latency can be just as important: trust-establishment latency. Trust-establishment latency is the interval between acquisition of information and availability of sufficient authenticity-related evidence to use that information in a trust-informed operation.

In conventional architectures, a sensor or receiver typically acquires information first and evaluates trust later. The workflow often resembles the following sequence:

- acquire the signal or data;
- buffer, condition, digitize, transmit, or decode it;
- perform verification, correlation, authentication, provenance checks, or fusion;
- produce a confidence or trust assessment; and
- use the result for prioritization, decision support, control, or response.

That sequence may be adequate for slow-moving administrative or archival contexts, but it becomes limiting when the operational value of information decays rapidly.

Missile warning, space-domain awareness, electronic warfare, autonomous vehicles, industrial protection, grid control, high-frequency cyber-physical monitoring, and physiological event detection all share the same practical constraint: information that cannot be trusted quickly may not remain useful, even if it is eventually correct [9-14].

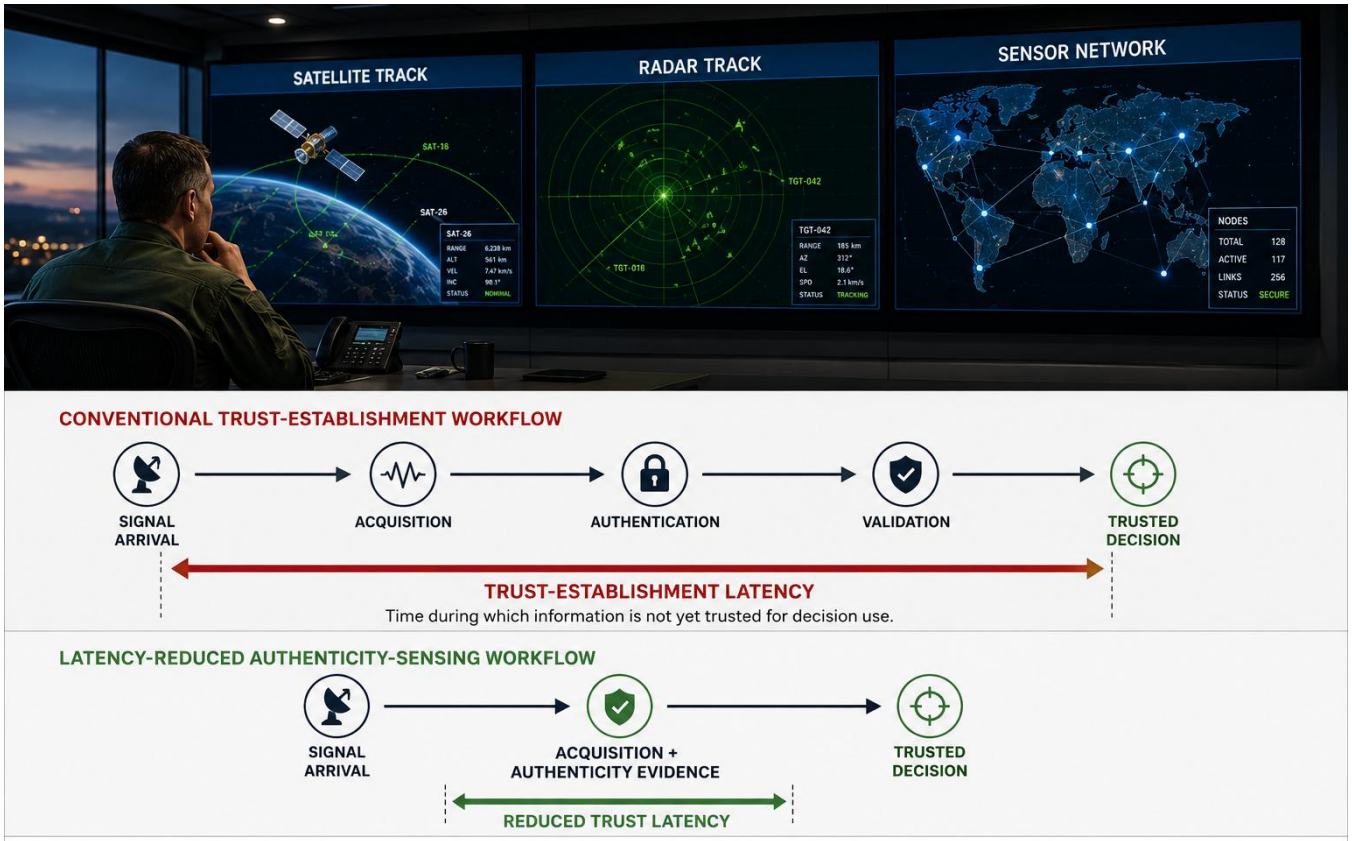

Figure 1. *Trust-establishment latency can become a limiting factor in time-critical sensing systems even when acquisition and communications latency are low.*

Modern missile-defense, space-domain awareness, and distributed sensing architectures increasingly depend on heterogeneous sensors operating across multiple domains and geographic regions, while conventional trust-establishment approaches often rely on cryptographic validation, provenance verification, attestation, or related trust infrastructure [9-14], [15-20].

This creates a design target that differs from ordinary low-latency communications: reducing the time required to establish confidence in acquired information.

Figure 1 illustrates the trust-establishment latency problem. In a conventional workflow, trust-related information often becomes available only after multiple downstream processing and verification stages. A latency-reduced authenticity-sensing architecture seeks to make authenticity-related evidence available earlier, even where communications and processing latency are already low.

2. From Faster Data to Earlier Trust Evidence

The architecture described here shifts authenticity assessment closer to the front end. Instead of treating acquisition hardware as a passive source of data and downstream software as the first meaningful trust layer, the acquisition stage becomes an evidence-generating element. It acquires the observed signal while simultaneously producing measurable acquisition-process behavior. That behavior is then characterized and transformed into authenticity observables.

As illustrated in **Figure 2**, the objective is not merely to accelerate acquisition. Rather, the acquisition stage itself becomes a source of authenticity-related information. Acquisition-derived observables may become available while the signal is being acquired, allowing trust formation to begin before completion of a conventional post-acquisition trust workflow. The figure emphasizes the key distinction that authenticity evidence is generated concurrently with acquisition rather than being deferred until later verification stages.

This is a different design philosophy. Conventional systems usually ask: "What does the received signal say, and can I authenticate the source or payload after the fact?" The architecture described here asks a different question: "What did the acquisition process physically do while acquiring this signal, and is that behavior consistent with authentic, contemporaneous acquisition?" Existing trust architectures frequently depend upon certificate validation, provenance verification, remote attestation, trusted execution environments, or similar post-acquisition trust mechanisms [15-17].

This distinction matters because acquisition-process behavior can remain informative even when signal content is encrypted, compressed, encoded, corrupted, transformed, partially unavailable, or semantically uninterpretable. A trust layer that depends only on payload interpretation is blind until the content is decoded or verified. A trust layer that derives observables from acquisition behavior can operate earlier and may operate even when content remains unavailable.

The timing relationship can be summarized as:

$$T_A \leq T_C < T_V$$

where T_A is the start of acquisition, T_C is the time at which acquisition-derived authenticity evidence becomes available, and T_V is the time at which a conventional post-acquisition trust workflow produces sufficient trust-related information. The value proposition is the interval between T_C and T_V: authenticity-related information may become available before conventional trust workflows based on cryptographic, provenance, attestation, or downstream verification mechanisms have completed [9-14], [15-17].

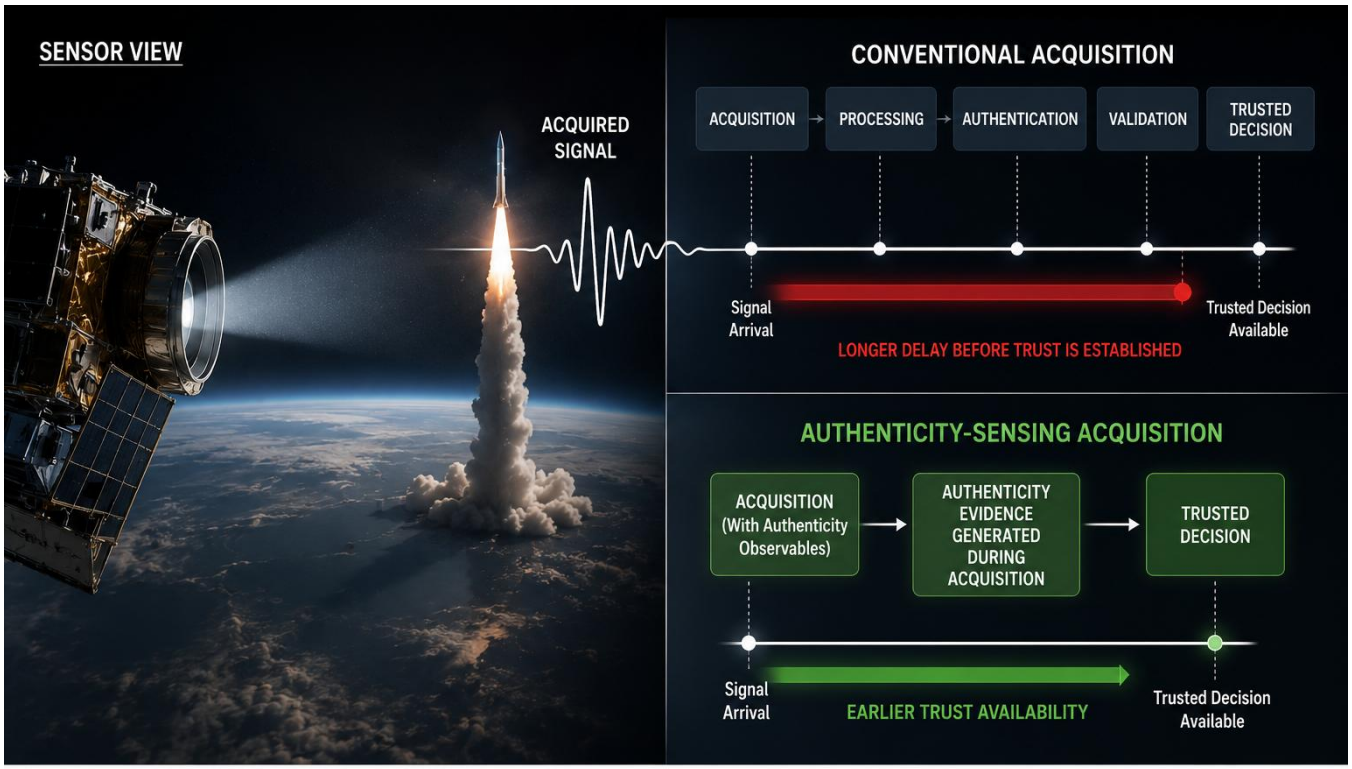

Figure 2. *Acquisition-derived authenticity evidence becomes available during acquisition rather than after completion of conventional trust-establishment workflows.*

3. Negative Group Delay and Signal Advance Context

Latency-reduced acquisition may be implemented using several approaches, including negative group delay (NGD), Signal Advance circuitry, resonant transfer-function shaping, predictive filtering, adaptive filtering, mixed-signal front ends, or software-assisted processing. Among these, Signal Advance and NGD deserve careful explanation because they are easily misunderstood.

The IEEE Circuits and Systems Magazine review on Temporally Advanced Signal Detection should be treated as the primary Signal Advance reference for this article [2]. It explains the relationship among group velocity, signal velocity, front velocity, phase behavior, causality, circuit implementation, filtering/conditioning, cascade and parallel circuit arrangements, ECG demonstrations, distortion analysis, and applications. It is especially useful because it translates NGD-related concepts into an engineering discussion rather than treating them only as optical or theoretical phenomena [2].

Independent NGD literature is also important. Mitchell and Chiao demonstrated negative group delay in a simple bandpass amplifier and emphasized that the effect does not conflict with causality [3]. Kitano et al. later presented an electronic-circuit implementation of negative group delay for band-limited signals [4]. Voss subsequently analyzed delayed-feedback NGD filters and practical implementation constraints [5].

These references support the engineering point that matters here: NGD is not time travel, not supernatural prediction, and not extraction of information before it physically exists. For properly constrained signal classes, an NGD or Signal Advance stage can reshape phase and amplitude relationships among signal components already present within a relevant bandwidth so that a waveform feature becomes detectable earlier than it would through a conventional positive-delay path.

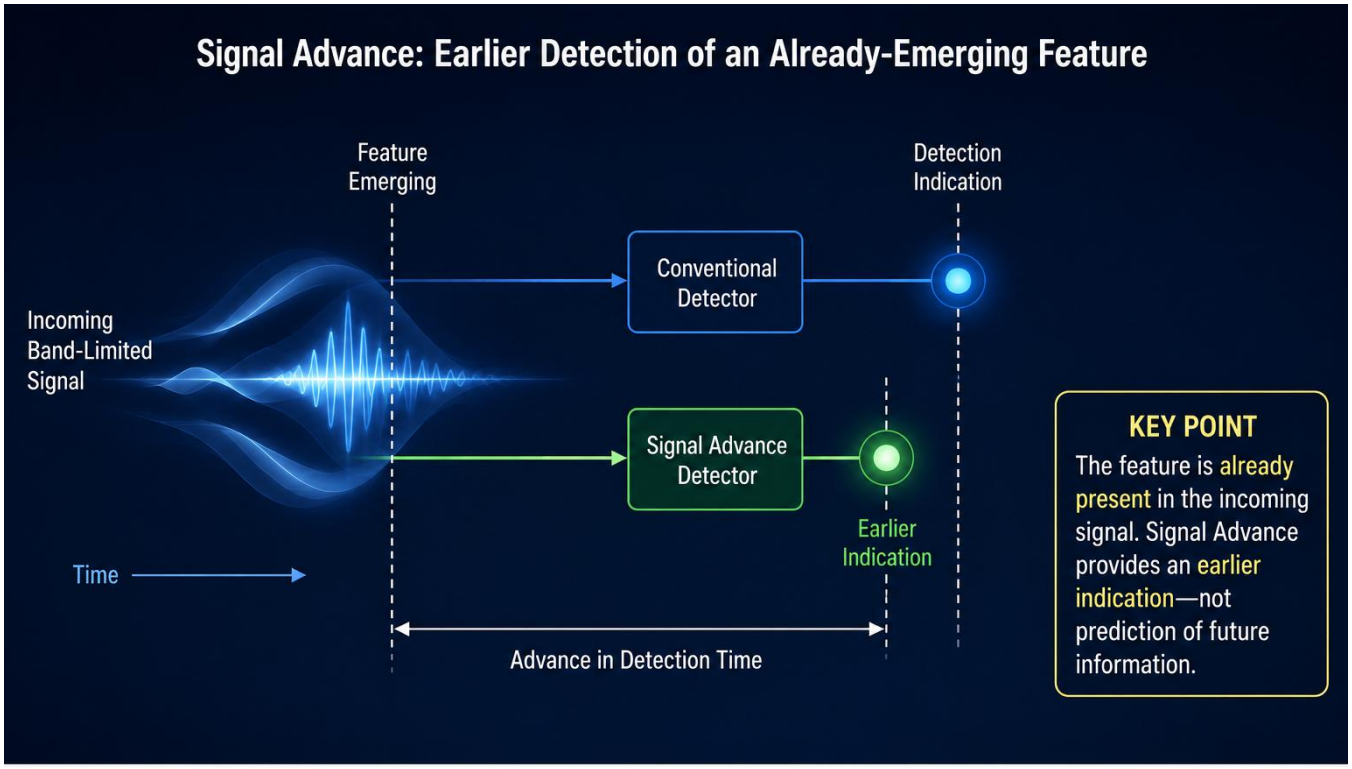

Figure 3. *Signal Advance techniques can provide earlier indication of already-emerging band-limited waveform features without violating causality.*

This distinction is central to the proposed authenticity architecture. The system does not need to predict unknown future information. It can derive authenticity evidence from how a latency-reduction acquisition stage behaves while responding to an already-emerging, band-limited waveform feature.

Figure 3 conceptually illustrates the Signal Advance principle. An already-emerging band-limited waveform feature may become detectable earlier through a latency-reduction acquisition path than through a conventional positive-delay acquisition path. The figure is intended only to illustrate earlier feature recognition and should not be interpreted as implying prediction of unknown future information or violation of causality.

3.1 What NGD Can and Cannot Do

A technically defensible NGD discussion should include the following constraints:

- **Band-limited feature requirement:** The useful advance applies to signal components already represented within the operating bandwidth. Abrupt fronts, unlimited-bandwidth discontinuities, and genuinely unknown future events are not advanced in a causality-violating manner.
- **Feature-bearing bandwidth:** The feature of interest may be an envelope change, modulation sideband, slope change, transient onset, phase transition, frequency drift, or threshold-crossing condition. The circuit must be designed for the relevant feature bandwidth, not merely the carrier frequency.
- **Distortion and noise limits:** The advance is useful only if the feature survives transfer-function shaping with acceptable distortion and signal-to-noise ratio.
- **Calibration dependence:** Gain, phase, group delay, coherence, distortion, component aging, and environmental response should be characterized and monitored.
- **No universal advance:** NGD circuits are not general-purpose future predictors. They are engineered transfer-function systems with finite bandwidth, stability, gain, and noise constraints.

4. Acquisition-Derived Authenticity Evidence

As illustrated in Figure 4, acquisition-process behavior may be transformed into authenticity-related information through extraction of representative observables. These observables may include timing, phase, gain, coherence, distortion, residual, and environmental-response characteristics, and may ultimately contribute to acquisition-derived authenticity evidence.

Acquisition-derived authenticity evidence is information about authenticity, temporal integrity, liveness, continuity, provenance consistency, or trustworthiness that is generated from the behavior of the acquisition process rather than solely from the informational content of the signal. Related physical-layer authentication research has shown that physical signal characteristics can carry security-relevant evidence, but those approaches typically emphasize transmitter fingerprints, channel state, or device identity rather than acquisition-stage behavior [6-8], [21-22].

Representative acquisition-process behaviors include:

- advance-duration behavior;
- group-delay and phase-slope behavior;
- gain-profile behavior;
- coherence behavior;
- distortion signature behavior;
- frequency-response behavior;
- stability and drift behavior;
- prediction-residual behavior;
- environmental-response behavior;
- nonlinear-response behavior;
- feature-arrival-time behavior; and
- early-threshold-crossing behavior.

These behaviors are not merely diagnostic artifacts. In the proposed architecture, they are transformed into authenticity observables. A latency-reduction acquisition path that consistently advances a given class of waveform feature by a calibrated amount may produce one kind of

authenticity evidence. A path whose gain profile, phase continuity, distortion signature, or environmental response deviates unexpectedly may produce a different kind of authenticity evidence. The evidence is not a binary declaration. It can be a confidence measure, residual, anomaly measure, fingerprint component, probability, ranking, or uncertainty representation.

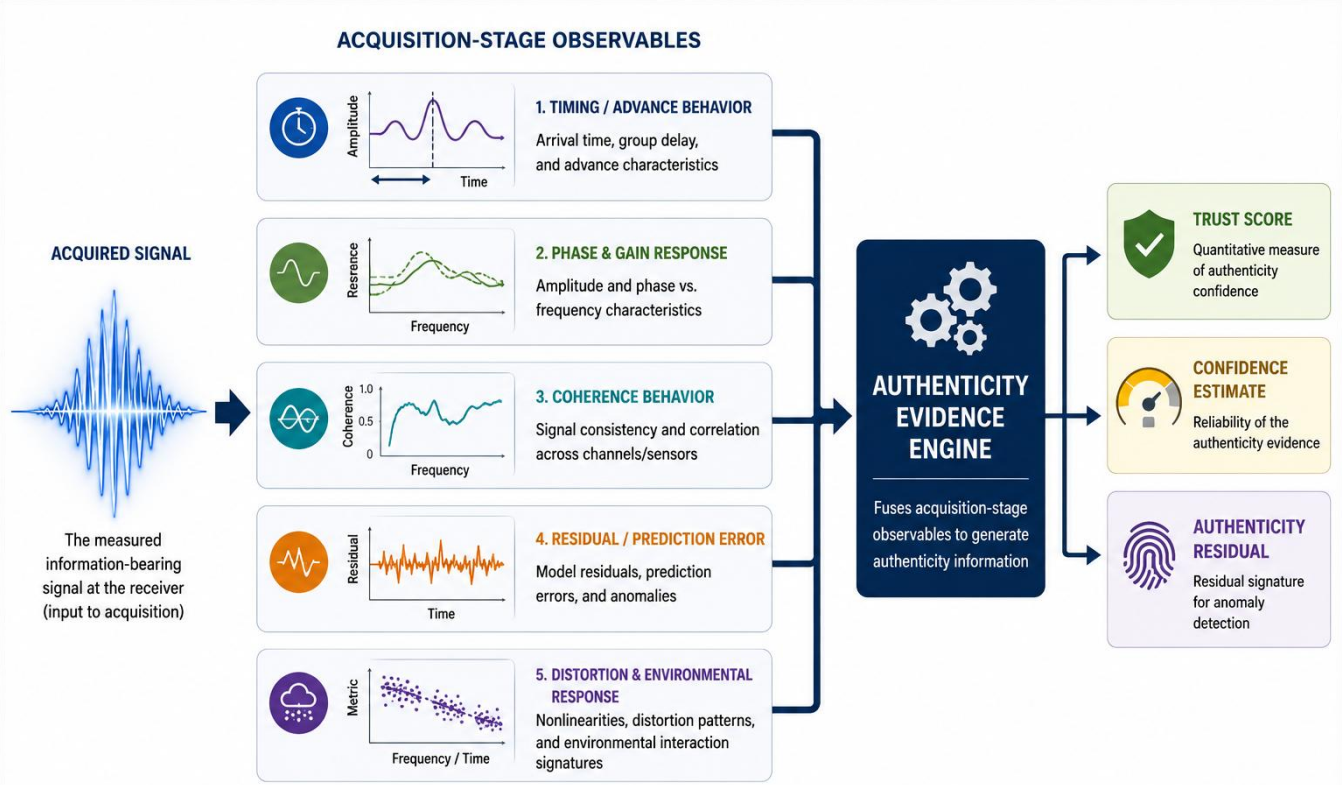

Figure 4. *Multiple acquisition-process observables may be combined to generate authenticity-related information.*

Unlike transmitter fingerprinting, channel-state authentication, or device-identification approaches, the present architecture derives authenticity evidence from behavior occurring within the acquisition architecture itself [6-8].

Observable class	What it characterizes	Why it matters for authenticity
Advance Duration Consistency	Consistency, repeatability, drift, or deviation in apparent feature advance.	Unexpected changes may indicate replay, delay, injected content, altered acquisition state, calibration drift, or environmental perturbation.
Feature-Arrival-Time Residual	Timing relationship between early feature detection and reference-path or expected detection.	Supports evaluation of whether earlier recognition is consistent with authentic acquisition behavior.
Gain Profile Coherence	Correspondence between observed gain behavior and enrolled, historical, modeled, or contextual gain behavior.	Helps distinguish expected hardware behavior from anomalous acquisition-path behavior.

Phase Continuity Indicator	Continuity or deviation in phase response, phase slope, group delay, or phase transitions.	Can reveal timing discontinuities, replay artifacts, relayed signals, or acquisition-state changes.
Distortion Signature Profile	Harmonic, intermodulation, amplitude-dependent, transient, or nonlinear distortion behavior.	Provides a hardware-behavior fingerprint that may be difficult to replicate exactly.
Environmental Response Signature	Change in acquisition behavior with temperature, vibration, radiation, impedance, motion, or interference.	Helps separate authentic environmental variation from authenticity-relevant anomalies.
Prediction-Residual Behavior	Residual error between expected and observed latency-reduction or predictive response.	Supports confidence and uncertainty estimates without relying solely on payload content.

The key point is that authenticity evidence can be generated from the physical acquisition event itself. The acquired data and the acquisition-derived evidence can then travel together, allowing downstream systems to evaluate not only what was observed but also how the observation was acquired.

5. Temporal Authenticity Signals

A Temporal Authenticity Signal (TAS) is a representation of authenticity-related information derived from acquisition-process behavior. A TAS may be implemented as a scalar, vector, waveform, metadata structure, statistical representation, probabilistic representation, learned feature representation, signed record, packet, frame, database entry, or trust-attested object. Its form is less important than its role: it carries evidence generated during acquisition.

As illustrated in Figure 5, a representative Temporal Authenticity Signal preserves the relationship between acquired information and acquisition-derived authenticity evidence. Timing information, confidence information, provenance-related metadata, and acquisition-process observables remain associated with the acquisition event from which they were derived.

TAS records should be understood as acquisition-derived evidence carriers rather than ordinary provenance records. Provenance-management and trust-preservation systems pursue related evidentiary-continuity objectives, but generally focus on content provenance, chain-of-custody information, or platform integrity rather than physical acquisition-process behavior [15], [18-19].

A representative TAS may include:

- timestamp or acquisition-event timing information;
- source or acquisition-stage identifier;
- latency-reduction state information;
- transfer-function state information;
- observable vector values;
- confidence, uncertainty, or residual information;

- calibration and context state;
- fingerprint or enrollment correspondence information;
- derivation history; and
- provenance or protected-domain information.

A simple representative vector may be expressed as:

$$TAS\_Vector = [ADC, FAT, GPC, PCI, DSP, ERS, ARM, AFC]$$

where ADC is Advance Duration Consistency, FAT is Feature-Arrival-Time residual or correspondence, GPC is Gain Profile Coherence, PCI is Phase Continuity Indicator, DSP is Distortion Signature Profile, ERS is Environmental Response Signature, ARM is an Authenticity Residual Metric, and AFC is an Authenticity Fingerprint Component. The specific observables are implementation-dependent. The broader concept is that the TAS captures the physical and timing behavior of the acquisition stage as trust-relevant evidence.

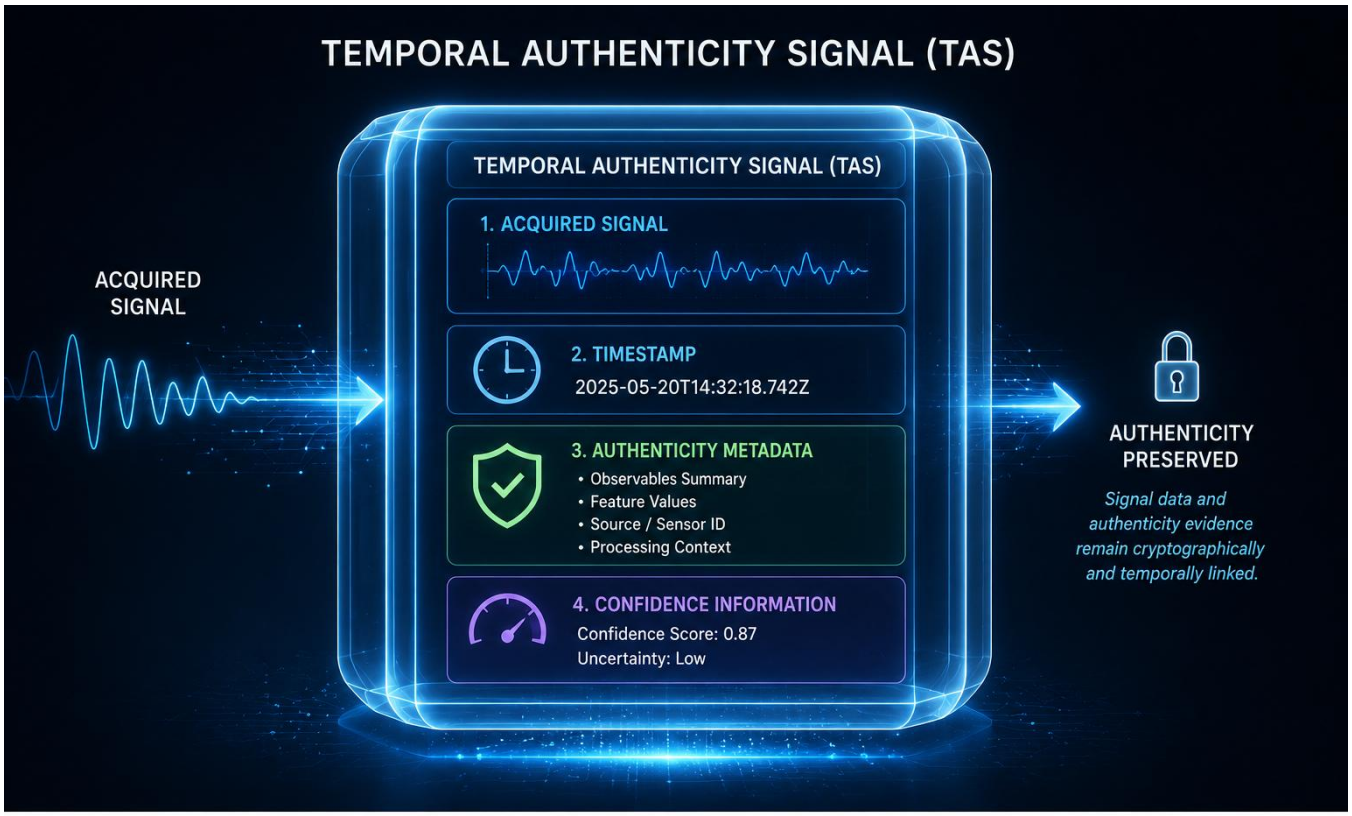

Figure 5. *A Temporal Authenticity Signal couples acquired information with acquisition-derived authenticity evidence.*

A TAS should also preserve derivation context. For high-value operations, it is not enough to state that a confidence score was produced. The system should retain enough context to know what acquisition behavior was measured, how it was transformed, what calibration or environmental state applied, and how the authenticity assessment was generated. Preservation of derivation context becomes increasingly important when authenticity evidence is retained, shared, fused, or used in downstream trust decisions.6. Conventional Authentication and Trust Approaches

Modern sensing, communications, and cyber-physical systems use several mechanisms to establish confidence in information, including cryptographic authentication, provenance management, trusted-computing architectures, physical-layer authentication, and distributed trust-assessment frameworks [6-8], [21-22]. Each addresses a different part of the trust problem.

These approaches are relevant but not identical to acquisition-derived authenticity evidence. Cryptographic and provenance systems generally authenticate content, credentials, or custody records; trusted-computing systems generally attest platform state; RF fingerprinting and channel-state authentication generally evaluate transmitter or propagation characteristics. The architecture described here asks a different question: did the acquisition process itself behave consistently with authentic, contemporaneous acquisition?

Table 1 summarizes representative distinctions between conventional trust approaches and acquisition-derived authenticity sensing.

Conventional Approach	**Primary Trust Source**	**Typical Availability of Trust Information**	**Representative References**
Cryptographic Authentication	Keys, certificates, signatures, message authentication codes	After cryptographic verification	[16-17]
Provenance / Chain of Custody	Origin records, signed metadata, edit history, custody records	After provenance verification	[15], [18-19]
Trusted Computing / Attestation	Platform measurements, secure enclaves, hardware roots of trust	After attestation and verification	[16-17]
RF Fingerprinting	Transmitter-specific RF characteristics	After signal analysis	[6-8]
Channel-State Authentication	Channel-state information and propagation characteristics	After channel analysis	[7-8]
Distributed Trust Frameworks	Trust scores, provenance information, node reputation, corroborating observations	After fusion and trust evaluation	[18-20]
Acquisition-Derived Authenticity Sensing	Physical acquisition-process behavior of latency-reduction acquisition hardware	During acquisition-associated operation	[1]

Acquisition-derived authenticity sensing is not intended to replace cryptography, provenance systems, attestation frameworks, or distributed trust architectures. It may complement those approaches by providing an additional source of authenticity-related information that becomes available earlier in the trust-establishment process. The resulting authenticity information may subsequently be incorporated into trust-attested outputs, distributed authenticity assessments, provenance structures, protected trust domains, or higher-level decision-support systems [1], [15-22].

Figure 6 summarizes this distinction. Conventional architectures typically perform trust generation after acquisition, whereas acquisition-derived authenticity architectures generate trust-relevant information during acquisition itself. This shifts trust formation toward the front end of the sensing workflow.

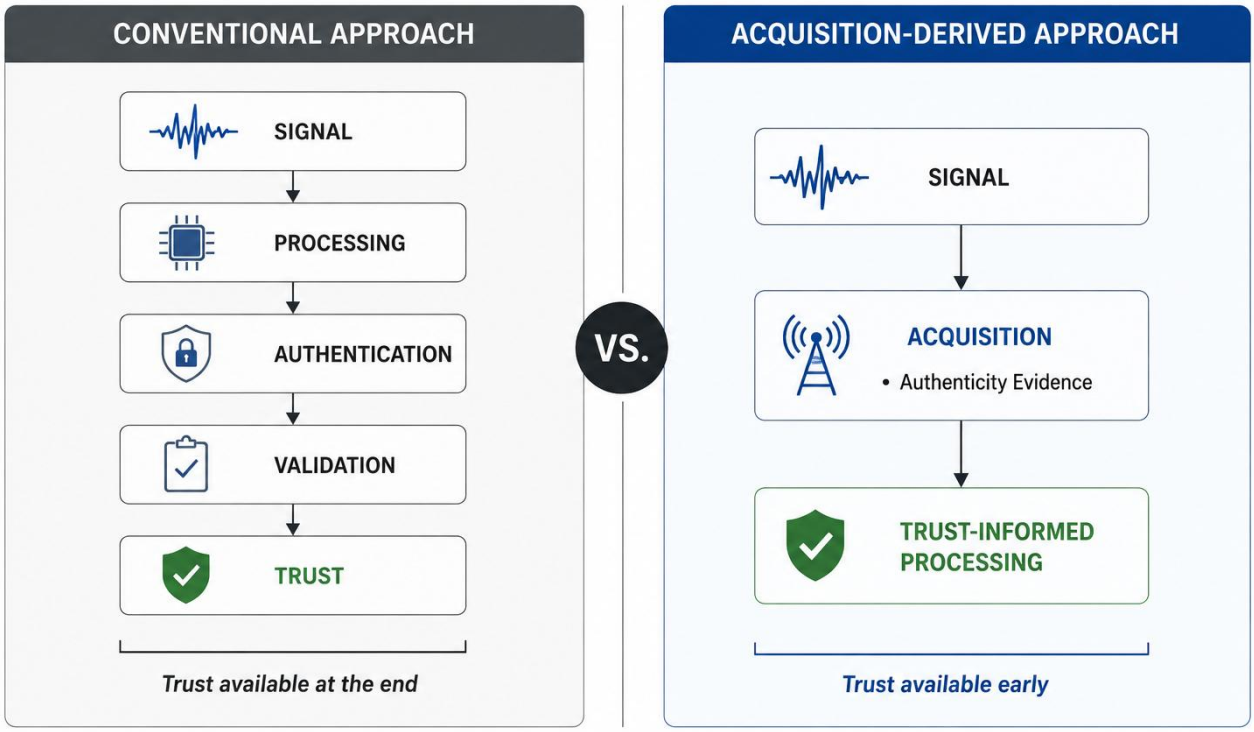

Figure 6. *Acquisition-derived authenticity evidence shifts trust generation toward the front end of the sensing workflow.*

7. Distributed Sensing and Space-Defense Relevance

The need for earlier trust evidence is especially clear in distributed sensing architectures. Space-based, airborne, terrestrial, maritime, autonomous, and cyber-physical sensors may each produce partial observations. A fusion system must decide which observations to prioritize, how to weight them, which inconsistencies matter, and when the evidence is sufficient for action. In such settings, trust-establishment latency is a system-level constraint.

Current missile-defense and space-sensing architectures illustrate the problem. The White House Executive Order titled "The Iron Dome for America" directed development of a next-generation missile defense shield against aerial attacks, including ballistic, hypersonic, and cruise-missile threats [9]. The Department of Defense later stated that Golden Dome would include space-based interceptors and sensors and would require seamless integration of system components [10]. SDA materials for the Proliferated Warfighter Space Architecture emphasize low-latency data connectivity, direct data to tactical elements, and missile warning and tracking for conventional missiles and hypersonic glide vehicles [11]. SDA also described its Tracking

Layer as a proliferated LEO constellation of infrared missile-warning and missile-tracking satellites integrated with the Transport Layer's low-latency mesh communications network [12].

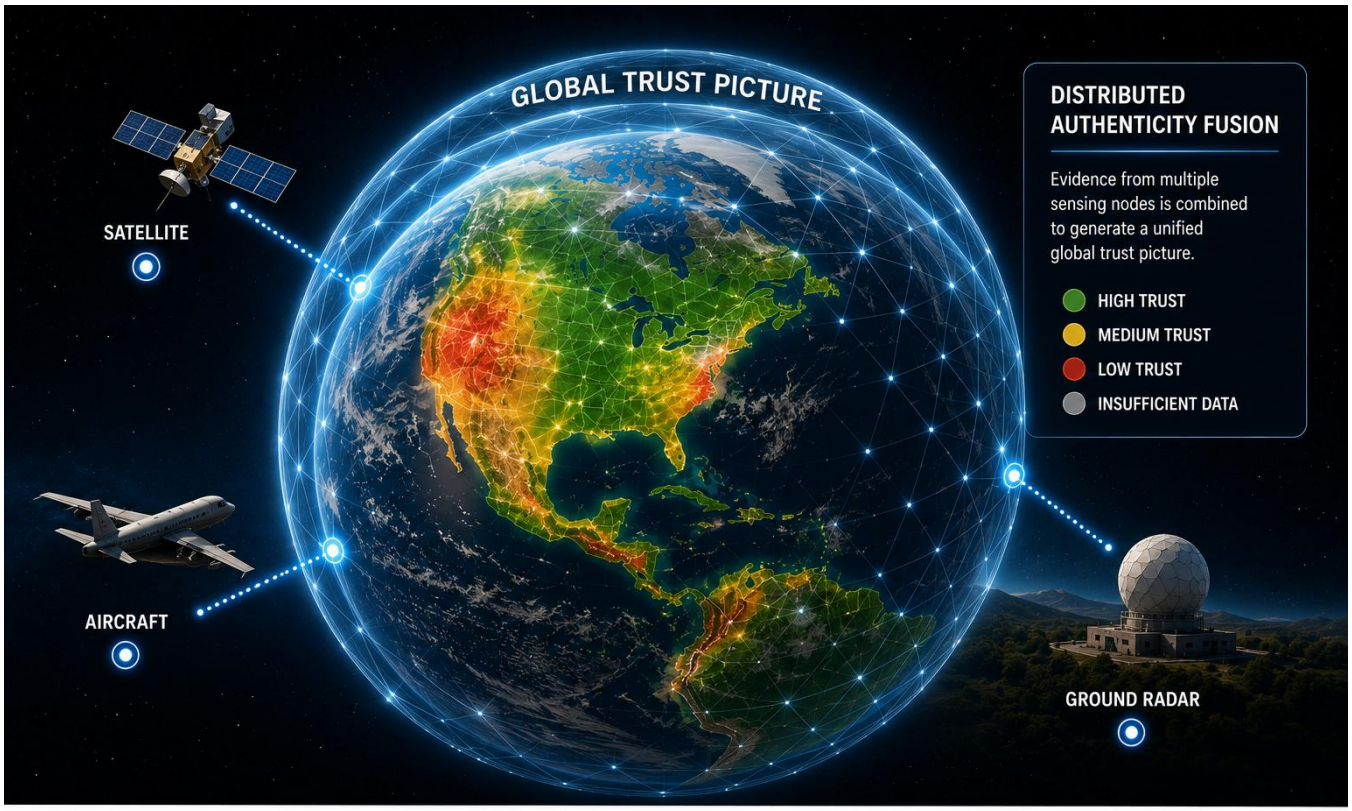

Figure 7. *Distributed authenticity fusion combines evidence generated across multiple sensing nodes.*

Figure 7 illustrates a representative distributed authenticity-fusion architecture. Multiple sensing nodes generate local authenticity evidence that can be combined into a broader trust picture. As shown in Figure 7, authenticity evidence generated at individual sensing nodes may contribute to a unified trust picture without requiring completion of every downstream verification process. The figure is intended to illustrate a conceptual fusion framework and not a specific implementation associated with any particular defense or space program.

Distributed trust assessment and sensor-fusion frameworks have been investigated in aerospace, cyber-physical, and wireless sensor-network environments [18-20]. Those public references are not evidence that any acquisition-derived authenticity technology is part of Golden Dome, SDA, or other programs; they show the broader architectural trend toward distributed, time-critical, space-integrated sensing and low-latency trustworthy fusion.

Technical reviews of missile-defense sensing architectures emphasize the challenges associated with detection, tracking, discrimination, and custody maintenance across layered radar and space-based sensing systems [13]. GAO has reported that SDA is developing space- and ground-based systems to detect and track missile threats in low Earth orbit while facing delivery, readiness, and lifecycle risks [14]. Existing distributed trust systems generally combine sensor outputs, trust scores, or provenance information rather than acquisition-process behavior itself

[18-20]. In such environments, a trust pipeline that waits for post-acquisition verification may consume operational time that cannot be recovered.

8. Representative Implementation Architecture

A practical implementation can be organized into seven functional layers. These layers may be implemented using analog circuitry, mixed-signal circuitry, digital signal processors, FPGA logic, ASIC resources, embedded processors, software-assisted processing, secure enclaves, edge-computing systems, cloud systems, or combinations of these technologies.

1. Latency-reduction acquisition stage: acquires the observed signal and produces a latency-reduced or temporally advanced representation of a feature-bearing signal component.
2. Transfer-function characterization stage: measures or estimates acquisition-process behavior, including gain, phase, group delay, phase slope, distortion, stability, coherence, and environmental response.
3. Observable-extraction stage: converts characterized behavior into authenticity observables such as ADC, GPC, PCI, DSP, feature-arrival-time residuals, and environmental-response signatures.
4. Temporal Authenticity Signal construction stage: packages the observables into a TAS together with timing, calibration, context, uncertainty, confidence, and derivation information.
5. Authenticity-evaluation stage: applies rules, thresholds, statistical models, Bayesian models, residual analysis, fingerprint comparison, or machine-learning models to generate authenticity assessments.
6. Protected trust domain: preserves the evidentiary relationship among acquired information, acquisition behavior, observables, TAS records, and assessments.
7. Trust-attested output stage: emits acquired information together with authenticity-related evidence for downstream fusion, prioritization, control, audit, or decision support.

This architecture does not require that every stage be physically separate. In compact embedded systems, several stages may be implemented in a shared mixed-signal front end or FPGA. In distributed systems, acquisition-derived TAS records may be generated at the edge, then fused at regional or central processing nodes.

8.1 Protected Trust Domains and Evidentiary Continuity

The value of acquisition-derived evidence depends on whether downstream systems can trust its relationship to the acquisition event. A TAS that can be modified without trace, detached from its originating observation, or reattached to unrelated data loses evidentiary value. A protected trust domain should therefore preserve derivation relationships, timing relationships, calibration state, transformation history, and the association between acquired information and the authenticity observables.

Protected trust domains may use secure processors, trusted execution environments, hardware security modules, secure elements, FPGA isolation, authenticated buffers, cryptographic hashes, digital signatures, secure logs, authenticated channels, or tamper-resistant hardware. Trusted-

computing technologies have long addressed secure roots of trust through attestation, measured boot, secure execution, and protected storage mechanisms [16-17]. The point is not that every implementation must use the same security mechanism; the point is that acquisition-derived evidence must remain meaningfully bound to the acquisition event it describes.

Unlike conventional attestation systems that primarily preserve platform integrity measurements, the present architecture preserves acquisition-derived authenticity evidence and associated derivation relationships [16-17].

9. Use Cases

9.1 RF, Radar and Missile Defense Sensing

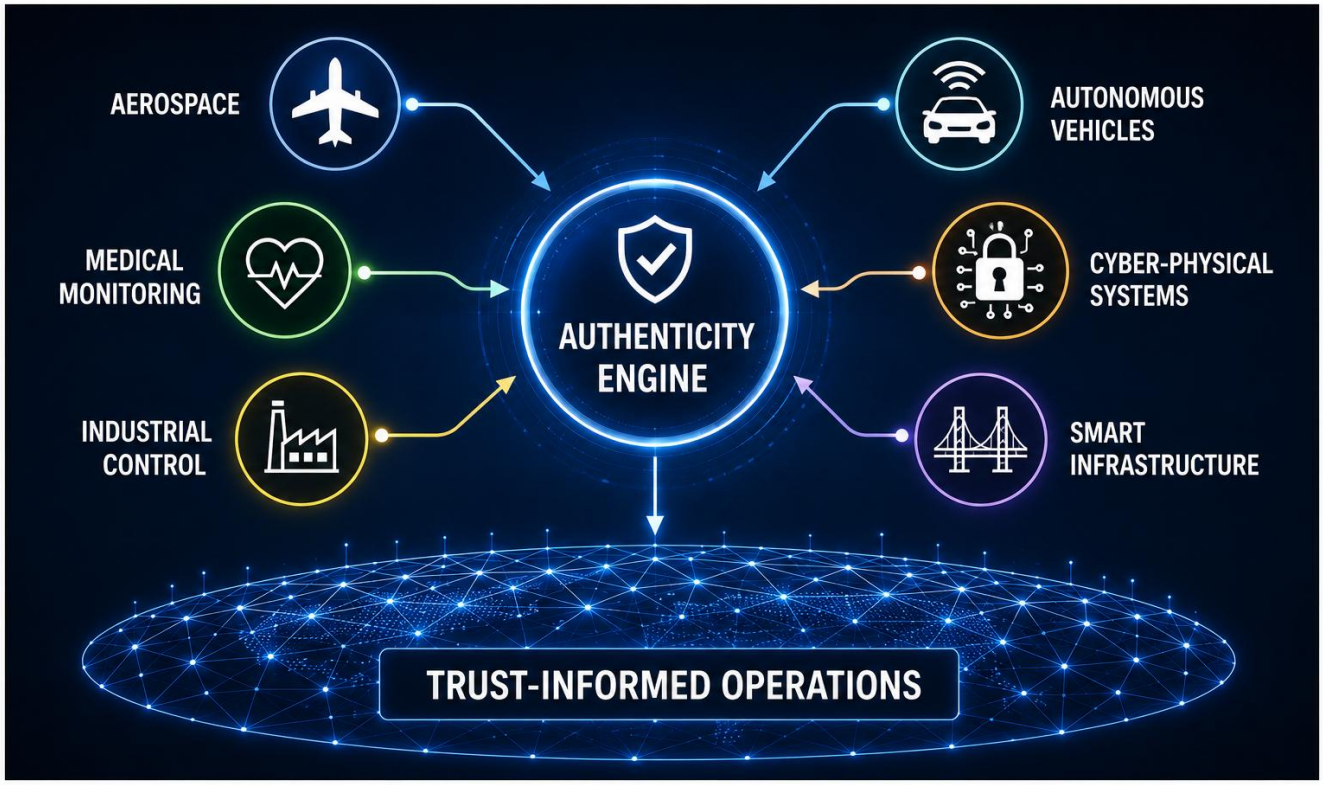

Figure 8. *Acquisition-derived authenticity evidence is applicable across diverse sensing domains.*

In RF and radar systems, the feature of interest may be a pulse onset, envelope rise, Doppler-related component, phase transition, chirp feature, reflected-signal feature, or threshold-crossing condition. A latency-reduction acquisition stage may produce earlier detection of a feature-bearing portion of the waveform. The transfer-function behavior of that stage can then generate observables such as feature-arrival-time residuals, phase-continuity indicators, gain-profile coherence, and distortion-signature profiles.

Similar authentication challenges have been studied within physical-layer authentication, RF fingerprinting, and transmitter-identification research [6-8].

Figure 8 illustrates the broad applicability of acquisition-derived authenticity evidence across multiple sensing domains. Although implementation details may differ among aerospace, medical, industrial, autonomous, and cyber-physical environments, the underlying principle remains the same: acquisition-process behavior can be transformed into trust-relevant information that supports trust-informed operations.

These observables can inform whether a radar return, RF emission, or sensor track is consistent with contemporaneous acquisition or whether it exhibits timing, phase, distortion, or residual behavior suggestive of delay, replay, relay, synthesis, manipulation, acquisition-path anomaly, or environmental disturbance. The resulting TAS can be fused with conventional radar signal processing, track correlation, identity information, and command-and-control data.

9.2 Space-Based Sensor Fusion

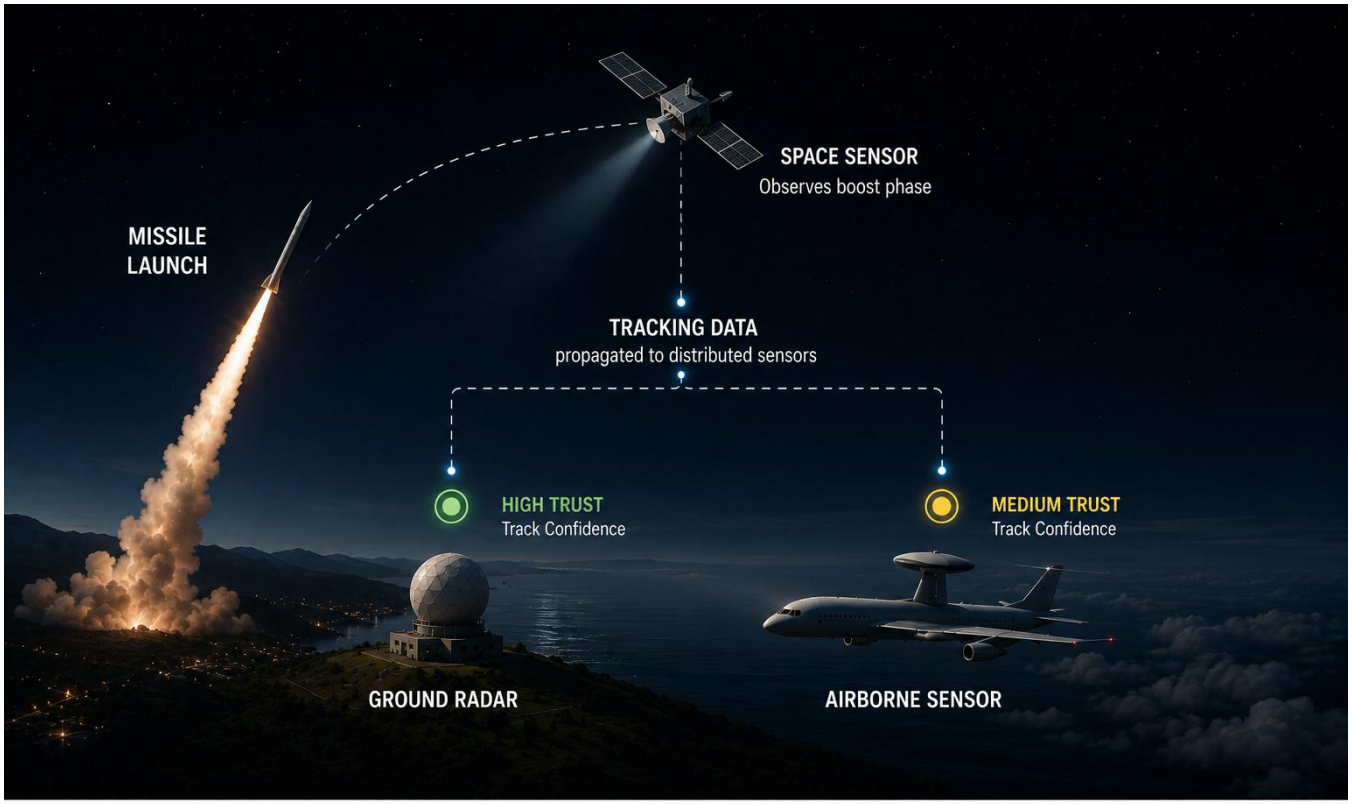

Figure 9. *Earlier authenticity evidence may improve confidence formation in distributed missile-warning and tracking architectures.*

Figure 9 provides a representative missile-warning and tracking example. The illustration emphasizes that confidence indicators may be generated concurrently with tracking operations rather than being deferred until completion of downstream verification processes. As shown in Figure 9, trust formation and track formation can occur simultaneously, allowing confidence information to accompany observations as they propagate through the sensing architecture.

A distributed space-sensing architecture may include many satellites and ground nodes, each observing different portions of an event. Each node can generate local acquisition-derived

authenticity evidence. Distributed trust assessment and provenance-aware fusion have previously been investigated for wireless sensor networks and cyber-physical systems [18-20].

A fusion node can compare TAS records across sensors and evaluate whether timing relationships, latency windows, phase continuity, environmental-response signatures, or residual trajectories are mutually consistent. The fusion system can then weight observations, flag inconsistencies, request additional acquisition, escalate anomalous tracks, or modify resource allocation.

This is particularly relevant for proliferated architectures, where no single sensor necessarily provides complete certainty. Acquisition-derived authenticity evidence becomes another dimension of fusion: not just what was observed, but how confidently and consistently it was acquired. The present architecture differs by evaluating relationships among acquisition-process behaviors and associated authenticity observables generated at individual sensing nodes [18-20].

9.3 Physiological Monitoring

The Signal Advance literature includes electrophysiological applications, including ECG waveform demonstrations [2]. In physiological systems, the authenticity problem is not usually adversarial in the same way as defense sensing, but temporal integrity still matters. A monitoring system may need confidence that an ECG, EEG, EMG, respiratory, hemodynamic, or photoplethysmographic signal corresponds to a current physiological condition rather than a delayed, corrupted, substituted, replayed, or artifact-dominated observation.

Acquisition-derived observables may characterize electrode-interface behavior, motion-induced distortion, contact impedance changes, environmental interference, feature-preservation residuals, and advance-duration consistency. These observables can support confidence measures, false-trigger reduction, anomaly detection, and supervisory review in continuous monitoring systems.

9.4 Industrial and Autonomous Systems

Industrial control and autonomous systems operate under constraints similar to defense sensing: events can evolve faster than conventional confidence workflows. A control system may need to determine whether a vibration signature, pressure transient, voltage anomaly, RF emission, thermal trend, or sensor threshold event is authentic, current, and relevant. Acquisition-derived authenticity evidence can help prioritize events, distinguish sensor artifacts from physical events, and support trust-informed control before a slower verification workflow completes.

9.5 Encrypted or Semantically Unavailable Content

One of the strongest advantages of acquisition-derived evidence is that it can operate when semantic content is unavailable. If a signal is encrypted, compressed, encoded, corrupted, or intentionally opaque, the payload may not be available for immediate interpretation. The acquisition process still has physical behavior. Transfer-function observables, timing relationships, latency-state information, distortion signatures, and residuals may remain measurable. A TAS can therefore provide early confidence information without decrypting or semantically interpreting the payload.

Conventional authenticity systems often depend upon access to content, metadata, provenance information, certificates, signatures, or platform-attestation information [15-17]. By contrast, authenticity-related information may be generated from acquisition-process behavior without requiring semantic interpretation of the informational content itself [6-8], [21-22].

10. Limits, Validation, and Engineering Discipline

The architecture should be presented with engineering discipline. It is not a universal detector, not a replacement for cryptography, and not a guarantee of authenticity. It is an evidence-generating front-end architecture. Its value depends on calibration, signal class, bandwidth, signal-to-noise ratio, stability, environmental characterization, secure association of evidence with data, and the quality of the evaluation model.

A credible validation program should include:

- comparison between latency-reduction and conventional positive-delay acquisition paths;
- measurement of feature-detection time, threshold-crossing time, and confidence-threshold time;
- characterization of group delay, phase slope, gain, coherence, and distortion across operating bands;
- testing across temperature, vibration, component aging, power-supply variation, electromagnetic interference, and calibration drift;
- false-positive and false-negative analysis for early feature detection;
- evaluation under replayed, delayed, relayed, injected, synthetic, corrupted, and semantically unavailable signal conditions;
- measurement of how much earlier TAS information becomes available relative to conventional trust workflows;
- fusion tests across multiple acquisition nodes;
- security testing of TAS preservation and protected-domain binding; and
- comparison against baseline cryptographic, RF fingerprinting, channel-state, and provenance-only approaches.

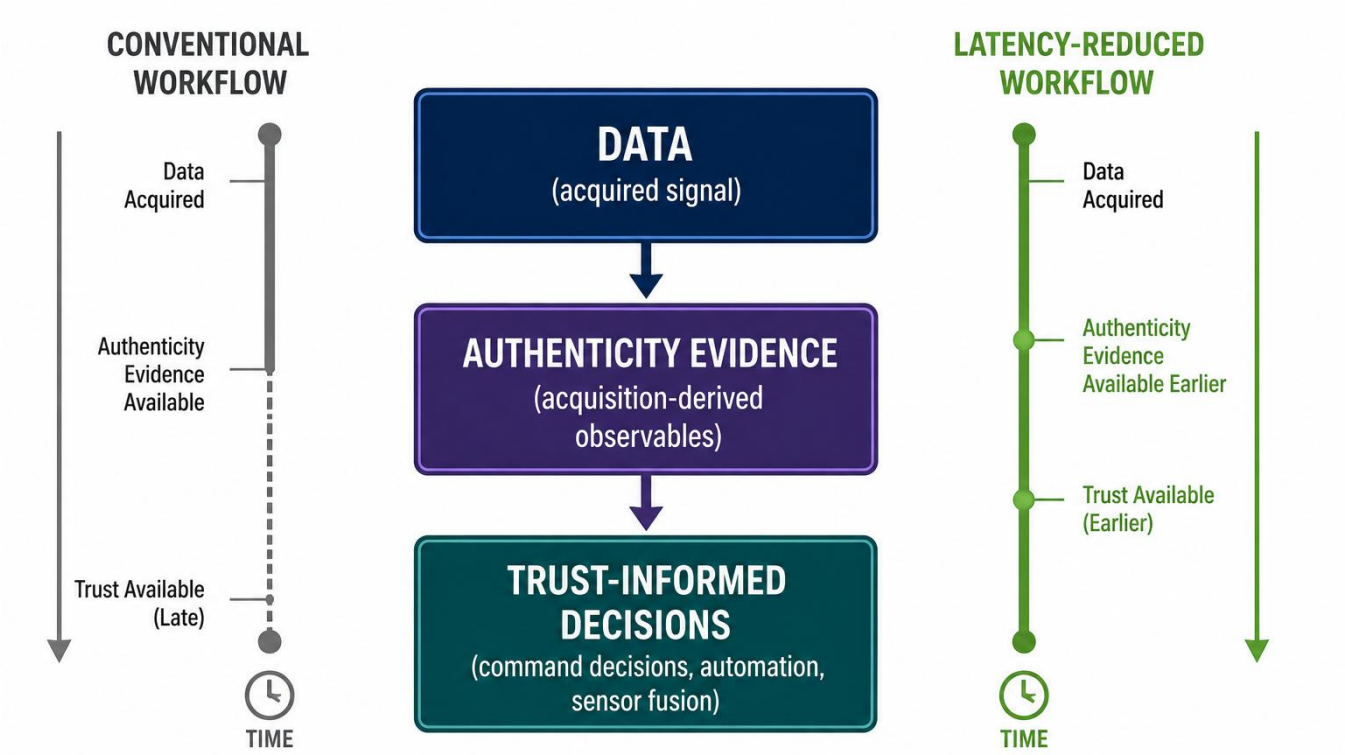

Figure 10. *The central objective is not merely faster acquisition, but earlier availability of acquisition-derived authenticity evidence.*

Figure 10 summarizes the central objective of the architecture. The goal is not merely to reduce acquisition latency. The goal is to make authenticity-related information available earlier in the information lifecycle so that trust-informed decisions can be initiated sooner than would be possible using conventional trust-establishment workflows.

Comparative evaluation against physical-layer authentication, RF fingerprinting, channel-state authentication, provenance, challenge-response, and trusted-computing baselines would further clarify the distinction between acquisition-derived authenticity sensing and existing trust-establishment approaches [6-8], [15-22].

The most important validation metric is not simply waveform advance. The more relevant metric is earlier availability of reliable authenticity evidence. A system that advances a waveform but does not produce trustworthy authenticity observables is merely a latency-reduction front end. A system that generates acquisition-derived observables but cannot preserve their relationship to the acquired data is merely a diagnostic subsystem. Accordingly, validation should evaluate both the generation of authenticity observables and preservation of their evidentiary relationship to acquired information.

11. Conclusion

The next generation of distributed sensing systems will not be judged only by how quickly they move data. They will be judged by how quickly they can form useful confidence in data. That is the gap addressed by latency-reduced authenticity-sensing acquisition.

As summarized in Figure 10, the central objective is not merely faster acquisition, but earlier availability of acquisition-derived authenticity evidence that supports earlier trust-informed decisions. The architecture therefore seeks to reduce trust-establishment latency rather than focusing exclusively on communications or processing latency.

Signal Advance and NGD literature provides a technical foundation for earlier recognition of suitable band-limited waveform features without violating causality. Physical-layer authentication literature shows that physical behavior can carry security-relevant evidence, but conventional approaches generally focus on transmitter identity, channel state, or device fingerprints. Modern missile-defense and space-sensing programs illustrate the system-level need for low-latency data movement and rapid multi-sensor integration. The architecture described here joins these threads into a specific front-end concept: generate authenticity evidence during acquisition from the physical behavior of the acquisition process itself.

The resulting architecture enables acquisition-derived authenticity evidence to accompany information throughout subsequent trust-establishment, fusion, and decision-support processes. That evidence can be transformed into Temporal Authenticity Signals, preserved in trust-attested structures, fused across distributed nodes, and used to support earlier prioritization, anomaly detection, sensor fusion, decision support, and operational response. In time-critical systems, the difference between data arriving early and trusted data becoming useful early may be decisive.

References

[1] C. M. Hymel, "Systems and Methods for Latency-Reduced Authenticity-Sensing Acquisition," patent-pending technical disclosure, 2026. Source architecture for ASAA, TAS, acquisition-derived authenticity observables, trust-attested outputs, and distributed authenticity fusion.

[2] C. M. Hymel, M. H. Skolnick, R. A. Stubbers, and M. E. Brandt, "Temporally Advanced Signal Detection: A Review of the Technology and Potential Applications," IEEE Circuits and Systems Magazine, vol. 11, no. 3, pp. 10-25, 2011. DOI: 10.1109/MCAS.2011.941076.

[3] M. W. Mitchell and R. Y. Chiao, "Causality and negative group delays in a simple bandpass amplifier," American Journal of Physics, vol. 66, no. 1, pp. 14-19, 1998. DOI: 10.1119/1.18813.

[4] M. Kitano, T. Nakanishi, and K. Sugiyama, "Negative group delay and superluminal propagation: An electronic circuit approach," IEEE Journal of Selected Topics in Quantum Electronics, vol. 9, no. 1, pp. 43-51, 2003. DOI: 10.1109/JSTQE.2002.807979.

[5] H. U. Voss, "A universal negative group delay filter for the prediction of band-limited signals," arXiv:1706.07326, 2017; see also "A delayed-feedback filter with negative group delay," Chaos, vol. 28, 113113, 2018.

[6] J. Zhang, F. Ardizzon, M. Piana, G. Shen, and S. Tomasin, "Physical Layer-Based Device Fingerprinting for Wireless Security: From Theory to Practice," arXiv:2506.09807, 2025.

[7] K. St. Germain and F. Kragh, "Physical-Layer Authentication Using Channel State Information and Machine Learning," arXiv:2006.03695, 2020.

[8] B. He, X. Zhou, and T. D. Abhayapala, "Wireless Physical Layer Security with Imperfect Channel State Information: A Survey," arXiv:1307.4146, 2013.

[9] The White House, "The Iron Dome for America," Executive Order, Jan. 27, 2025.

[10] U.S. Department of Defense, "Secretary of Defense Pete Hegseth Statement on Golden Dome for America," May 20, 2025.

[11] Space Development Agency, "Proliferated Warfighter Space Architecture - Tranche 1," Fact Sheet, June 10, 2024.

[12] Space Development Agency, "Space Development Agency Makes Awards to Build 72 Tracking Layer Satellites for Tranche 3," Dec. 19, 2025.

[13] S. Fontana, C. Lauro, A. Di Simone, et al., "An Overview of Sensors for Long Range Missile Defense," Sensors, vol. 22, no. 24, 9871, 2022.

[14] U.S. Government Accountability Office, "Missile Warning Satellites: Space Development Agency Should Improve Readiness to Support Operations," GAO-26-107085, Jan. 28, 2026.

[15] Coalition for Content Provenance and Authenticity (C2PA), *C2PA Technical Specification*, Version 2.4, 2025.

[16] Trusted Computing Group, *Overview of TCG Technologies for Device Identification and Attestation*, Version 1.0, Rev. 1.37, Feb. 2024.

[17] Trusted Computing Group, *Device Identifier Composition Engine (DICE) Architecture and Requirements*, 2024.

[18] Y. Lim, E. Bertino, and S. Moon, "Provenance-Based Trustworthiness Assessment in Sensor Networks," Proceedings of the VLDB Workshop on Data Management for Sensor Networks (DMSN), 2010.

[19] J. Wang, "Provenance for Wireless Sensor Networks: A Survey," Journal of Network and Computer Applications, vol. 78, pp. 115-129, 2017.

[20] M. Senel, M. Yuksel, and T. K. Capin, "Multi-Sensor Data Fusion for Real-Time Multi-Object Tracking," Processes, vol. 11, no. 2, 501, 2023.

[21] S. Zhang, K. Ren, C. Xing, and X. Du, "Physical Challenge-Response Authentication for Active Sensors Under Spoofing Attacks (PyCRA)," Proceedings of the ACM Conference on Computer and Communications Security (CCS), 2015.

[22] X. Du, M. Guizani, Y. Xiao, and H. H. Chen, "Physical Layer Challenge-Response Authentication in Wireless Networks with Relay," IEEE INFOCOM, 2014.

Appendix: Reference Relevance Matrix

The following matrix summarizes why each reference category was included. The purpose is reader comprehension, not claim construction.

Reference category	Representative references	Why it enhances the article
Signal Advance / TASD	[2]	Provides the primary engineering explanation of temporally advanced signal detection, including causality, circuit implementation, ECG demonstrations, distortion analysis, and application domains.
Independent NGD / causality literature	[3] - [5]	Shows that negative group delay is a recognized, causality-consistent phenomenon with practical bandwidth, stability, and distortion limits.
Physical-layer authentication and fingerprinting	[6]-[8], [21]-[22]	Provides context for how physical phenomena are used for authentication while clarifying that acquisition-derived authenticity evidence differs from transmitter, device, channel, or challenge-response authentication.
Golden Dome / missile-defense policy context	[9]-[10]	Shows the current operational emphasis on layered, integrated missile-defense architectures without implying deployment of the described technology.
SDA / proliferated space sensing	[11]-[12], [14]	Supports the need for low-latency, distributed sensing and integrated missile-warning/tracking data flows.
Missile-defense sensor literature	[13]	Provides technical background on radar, infrared, and space-sensor roles in long-range missile defense.
Digital provenance and content authenticity	[15], [18]-[19]	Provides context for provenance, content credentials, and sensor-data lineage while distinguishing acquisition-derived evidence from content or custody metadata.
Protected trust domains and attestation	[16]-[17]	Supports the discussion of trusted computing, attestation, secure roots of trust, and preservation of evidentiary relationships.
Distributed trust and sensor fusion	[18]-[20]	Supports the discussion of multi-node fusion, distributed trust, and cyber-physical system security while distinguishing fusion of acquisition-process behavior from fusion of sensor outputs or trust scores.