AffixIO Technical Paper · WP-028
June 2026
affix-io.com

AFFIXIO WHITE PAPER · WP-028

Supply Chain Provenance: Zero-Knowledge Attestations for IoT Device Authenticity and Critical Infrastructure Compliance

NIS2 and DORA require proof that the devices in your critical infrastructure are genuine. Here is how to provide it without revealing your supply chain to your competitors.

AffixIO | United Kingdom | affix-io.com | June 2026

ABSTRACT

Critical infrastructure operators deploying IoT devices face an intractable problem: regulators demand proof that devices are genuine, firmware-intact, and from verified supply chains, yet manufacturers regard component sourcing and manufacturing process details as commercially sensitive trade secrets. Zero-knowledge (ZK) attestation resolves this tension. A manufacturer can generate cryptographic proof that a device satisfies specified security criteria without disclosing which components it uses, where they were sourced, or what firmware version is running. AffixIO's attestation API converts manufacturer compliance data into ZK certificates anchored in a SHA-256 Merkle

tree and signed with ML-DSA-65 post-quantum signatures. The resulting attestation records satisfy NIS2 Article 21, DORA Article 28, and Cyber Resilience Act conformity requirements, and remain cryptographically secure throughout the 15-to-20-year operational lifetimes typical of critical infrastructure deployments.

CONTENTS

SECTION 1

Introduction: Why Device Provenance Is Now a Regulatory Requirement

Critical infrastructure runs on connected devices. Energy grids, water treatment facilities, financial market systems, and hospital networks all depend on IoT sensors, controllers, gateways, and communications equipment whose security properties directly determine the resilience of the services they underpin. The assumption that underlying hardware can be

trusted is so fundamental that it is often not articulated explicitly in security frameworks, yet it is precisely this assumption that a sophisticated adversary will seek to undermine.

The security of critical systems depends not just on software but on the physical integrity of the devices themselves. A counterfeit device, a device with substituted firmware, or a device manufactured under the oversight of an untrusted party can introduce vulnerabilities that are extremely difficult to detect through software-level testing. Unlike software vulnerabilities, which can often be patched after discovery, hardware-level compromises may require physical replacement of deployed infrastructure, an expensive and operationally disruptive remedy.

The EU's regulatory framework for critical infrastructure and digital resilience now addresses this directly. NIS2 (Directive (EU) 2022/2555, the Network and Information Security Directive), DORA (Regulation (EU) 2022/2554, the Digital Operational Resilience Act), and the Cyber Resilience Act all require organisations to manage supply chain security risk, including the security of the hardware they procure and deploy. Supply chain security is no longer a voluntary best practice; it is a legal obligation with enforcement consequences.

The challenge is structural. Verifying device authenticity in any rigorous sense requires access to the manufacturer's supply chain records: component sourcing, manufacturing process controls, firmware build provenance, and security testing results. Most manufacturers regard these as commercially sensitive and are unwilling to share them with customers. The result is a trust gap that conventional procurement and inspection processes cannot close: the operator needs to verify authenticity but cannot access the information needed to do so without the manufacturer exposing trade secrets.

Zero-knowledge attestation closes this gap. A manufacturer can prove, to a mathematically verifiable standard, that a device meets specified security criteria without revealing the underlying supply chain details that constitute the evidence for those claims. The operator receives a cryptographic certificate that a regulator can inspect and verify; the manufacturer retains

the confidentiality of its supply chain. This paper documents how that architecture works in practice, what it can and cannot prove, and how it integrates with existing device identity and audit infrastructure.

SECTION 2

The Counterfeiting and Substitution Risk

Counterfeit electronic components are a significant and growing problem in global supply chains. The US Department of Commerce has estimated that counterfeit electronics cause billions in annual losses; industry bodies including the Semiconductor Industry Association and ERAI (formerly the Electronic Resellers Association International) track thousands of reported incidents each year. In safety-critical applications, the consequences of deploying counterfeit components extend beyond financial loss to potential endangerment of life and critical service continuity.

Counterfeiting takes several distinct forms, each with different risk profiles. Fake devices that do not function as specified are dangerous in safety-critical applications where device behaviour is assumed rather than continually verified. Devices with substituted components may function normally in standard tests but include undisclosed radio modules, additional processors, or data-exfiltration capabilities that operate outside the device's documented functionality. Devices with modified firmware include backdoors that permit remote access or command injection by adversaries who know the modification. Cloned devices pass visual inspection and even initial functional testing but use inferior components, frequently salvaged or downgraded silicon, that fail under stress conditions or at end-of-rated-life.

The risk is particularly acute in critical infrastructure contexts. A counterfeit sensor in an energy management system may report incorrect readings that cause inappropriate control responses. A cloned controller in a water treatment facility may fail to respond correctly to exception conditions. A compromised networking device in a financial institution's data centre may forward traffic to an adversary while maintaining the appearance of normal

operation. These are not hypothetical scenarios; government advisories from CISA, the UK NCSC, and ENISA have all documented hardware supply chain threats to critical infrastructure.

Supply chain attacks targeting hardware represent a qualitatively different threat from software supply chain attacks. Software supply chain compromises, such as the insertion of malicious code into build pipelines, are detectable through code review, binary analysis, and reproducible build practices. Hardware-level modifications are substantially harder to detect: they may not be visible in firmware analysis, may be designed to activate only under specific conditions, and may be concealed within components that appear identical to genuine parts under standard inspection techniques. The asymmetry between the cost of executing a hardware supply chain attack and the cost of detecting one favours the attacker.

This asymmetry is precisely why cryptographic attestation at the point of manufacture is preferable to inspection at the point of deployment. If the device's compliance status is attested by the manufacturer at production time and bound to the device's hardware identity, any subsequent modification or substitution will be detectable as a mismatch between the physical device and its attestation record.

SECTION 3

NIS2 and DORA: Supply Chain Security Obligations

NIS2 (Directive (EU) 2022/2555) applies to essential and important entities operating in sectors including energy, transport, banking, financial market infrastructure, health, water, digital infrastructure, and managed services. It requires the implementation of appropriate and proportionate technical and organisational measures to manage cybersecurity risks. Article 21 specifies that these measures must include supply chain security, explicitly addressing "security-related aspects concerning the relationships between each entity

and its direct suppliers or service providers." Member States were required to transpose NIS2 into national law by October 2024, and enforcement regimes are now active across the EU.

The NIS2 supply chain obligation is not limited to software dependencies. Hardware suppliers are part of the supply chain, and devices deployed in critical infrastructure systems are subject to the same supply chain risk management requirements as software components. An operator of an energy management system who cannot demonstrate that the devices in that system come from verified, security-assessed sources is exposed to supervisory action under NIS2. The directive does not prescribe specific technical means for demonstrating supply chain security; it requires that the measures adopted are appropriate to the risk. Cryptographic attestation is among the most robust technical means available.

DORA (Regulation (EU) 2022/2554) applies to financial entities and their ICT third-party service providers. It establishes a comprehensive ICT risk management framework that includes specific requirements for managing third-party risk. Article 28 requires financial entities to identify, classify, and document ICT third-party service providers, and to assess the risks they introduce. For financial institutions operating critical ICT infrastructure, this extends to hardware suppliers whose components form part of that infrastructure. DORA entered into force in January 2025 and is subject to enforcement by national competent authorities across EU member states.

Both directives share a common analytical structure: organisations must identify the components of their critical systems, assess the risks introduced by each component's supply chain, and implement measures proportionate to those risks. Neither directive specifies how supply chain risk should be demonstrated technically, but both create an implicit demand for verifiable evidence. An operator who relies solely on supplier assurances, without any cryptographic verification mechanism, is in a significantly weaker position than one who can present auditable attestation records to a supervisor.

The common thread across the EU regulatory framework is that organisations must be able to demonstrate that the devices they use in critical systems meet specified security standards and come from verified supply chains. Demonstration requires evidence. Evidence, to be credible to a regulator,

must be tamper-resistant and independently verifiable. ZK attestation with Merkle-anchored records satisfies these requirements; commercial assurances in procurement contracts do not, at least not on their own.

REGULATION	SCOPE	RELEVANT ARTICLE	SUPPLY CHAIN OBLIGATION
NIS2 (Directive (EU) 2022/2555)	Essential and important entities in critical sectors	Article 21	Supply chain security including direct supplier relationships; hardware included
DORA (Regulation (EU) 2022/2554)	Financial entities and ICT third-party providers	Article 28	ICT third-party risk management; hardware suppliers for critical ICT infrastructure
Cyber Resilience Act	Manufacturers and importers of products with digital elements	Articles 13, 20, 23	Security by design; mandatory SBOM; conformity assessment for critical products

SECTION 4

The Cyber Resilience Act: Device Security by Design

The EU Cyber Resilience Act (CRA), entering into full force in 2027, creates mandatory security requirements for all products with digital elements sold in the EU. Unlike NIS2 and DORA, which impose obligations on the operators of critical systems, the CRA places obligations directly on manufacturers and importers: the security of a device is no longer solely the responsibility of the organisation that deploys it. A manufacturer that places an insecure product on the EU market can be held liable under the CRA regardless of any contractual arrangements with the customer.

The CRA establishes a two-tier product classification. Default products can demonstrate conformity through self-assessment. Critical products, a category that includes industrial automation systems, smart metering infrastructure, industrial IoT gateways, network switches for critical infrastructure, and similar components, require third-party conformity assessment. The conformity assessment process requires the manufacturer to demonstrate that the product meets the essential cybersecurity requirements set out in Annex I of the regulation, covering secure default configurations, least-privilege architecture, data protection, integrity verification, and vulnerability handling obligations.

For manufacturers of critical products, third-party conformity assessment creates a new challenge: the assessor needs access to sufficient technical detail to verify the product's security properties, but the manufacturer may not wish to expose firmware source code, component specifications, or manufacturing process details to an external assessor. ZK attestation from the manufacturer can provide the conformity assessment body with cryptographic evidence that specified security criteria are satisfied without requiring full disclosure of those technical details. The assessor can verify the ZK certificate and confirm that the device meets the criteria, without the manufacturer having to share the underlying evidence.

The mandatory SBOM requirement under the CRA is an area where ZK attestation adds particular value. An SBOM, as typically implemented, is a list of software components included in a product. For a security-critical IoT device, the SBOM entries may themselves be sensitive: knowing which open-source libraries a device uses, or which third-party firmware modules it incorporates, can inform an adversary's search for exploitable vulnerabilities. ZK attestation can accompany each SBOM entry with a proof that the component meets specified security standards, without revealing the component's version or supplier, where those details carry security or commercial sensitivity.

The CRA also establishes reporting obligations for actively exploited vulnerabilities and significant incidents. A manufacturer who has issued ZK attestation certificates for devices that are later found to be affected by a vulnerability will need to revoke or update those certificates as part of their incident response. The architecture described in this paper supports

certificate revocation through re-attestation with a new compliance record that reflects the updated compliance status, anchored in the Merkle audit tree with a timestamp that makes the revocation verifiable.

> **CRA Critical Product Classes:** Industrial automation and control systems, smart metering infrastructure, industrial IoT gateways, network switches targeting critical infrastructure, general-purpose operating systems, and firewalls for industrial use are among the product classes subject to mandatory third-party conformity assessment under the Cyber Resilience Act.

SECTION 5

What Proof of Authenticity Actually Requires

Proving that a device is authentic involves several distinct claims, each of which requires different technical mechanisms. Conflating these claims leads to attestation architectures that appear comprehensive but leave significant gaps. The claims are: the device was manufactured by the stated manufacturer; the device uses the components stated in its specification; the firmware running on the device is the version stated by the manufacturer and has not been modified after release; the device has not been physically tampered with since manufacture; and the device has not been cloned or copied.

Conventional approaches address these claims with varying degrees of success. Physical security seals provide visual evidence of tamper-absence but can be copied by sophisticated adversaries. Cryptographic device certificates issued at manufacture prove the device's identity against a certificate authority but do not prove component integrity, because the certificate is issued based on the device identity key rather than on any measurement of the device's components. Manual inspection by trained engineers is reliable but does not scale to the volume of devices deployed in large critical infrastructure installations, and cannot detect firmware-level compromises without invasive testing.

A more complete approach requires a hardware root of trust: an immutable identity embedded in the device at manufacture, using technologies such as TPM (Trusted Platform Module), DICE (Device Identity Composition Engine), or PUF (Physical Unclonable Function) circuits. The hardware root of trust provides a foundation that is difficult to clone or modify without destroying the device. It enables firmware measurement: a cryptographic hash of the firmware image can be stored in the hardware root of trust at boot time, providing evidence that the device is running a specific firmware image that has not been modified.

A chain of custody record links the device to its manufacturing process, establishing provenance from the point at which the hardware identity was instantiated. This record captures the sequence of manufacturing steps, quality controls, and security tests that the device passed before leaving the factory. In conventional supply chain systems, this record is held by the manufacturer and is typically not shared with the customer.

ZK attestation adds the privacy layer that makes this architecture practical. The device can prove, for example, that its firmware hash matches one of the manufacturer's certified release hashes without revealing which specific firmware release it is running, information that might indicate to an adversary exactly which vulnerabilities are present. The verifier learns only that the device is running certified firmware; they do not learn the specific version. This separation of the compliance claim from the underlying evidence is the core contribution of ZK techniques to device attestation.

AUTHENTICITY CLAIM	CONVENTIONAL MECHANISM	LIMITATION	ZK APPROACH
Manufacturer identity	Device certificate (PKI)	Proves identity, not component or firmware integrity	ZK certificate bound to hardware identity key
Component integrity	Manual inspection; BOM audit	Not scalable; exposes BOM to competitor	ZK proof of compliance flags without revealing component list
Firmware authenticity	Code-signing certificate	Reveals firmware version; adversary maps vulnerabilities	ZK membership proof: firmware hash in certified set
Tamper-absence post-manufacture	Physical seal; TPM PCR measurements	Seals can be copied; PCR values reveal configuration	ZK proof of PCR values against known-good set
Anti-cloning	PUF; DICE-based identity	Depends on hardware capability	ZK certificate bound to physically unclonable identity

SECTION 6

ZK Device Attestation Architecture

The attestation architecture comprises three distinct layers, each building on the one below it. The layers correspond to the three phases of a device's life cycle that are most relevant to supply chain security: manufacture, certification at end of production, and field deployment. Each layer produces verifiable artefacts that can be inspected by relying parties without requiring access to the layers below.

Layer 1: Hardware Identity

At manufacture, each device receives a unique identity rooted in its hardware. The mechanism depends on the device's security capability. Devices implementing DICE (Device Identity Composition Engine, as specified by the IETF RATS working group and the TCG DICE architecture) derive a unique device identity from a secret key stored in a one-time-programmable memory region during manufacture, combined with a measurement of the device's first-stage boot firmware. The resulting identity is bound to both the hardware and the firmware loaded at manufacture time. Devices using TPM-based identity anchor their identity in the TPM's Endorsement Key, which is injected by the TPM manufacturer and cannot be extracted from the TPM without destroying it. Devices incorporating PUF circuits derive their identity from physical variations in the silicon that are inherent to the manufacturing process and are not reproducible in any other physical device.

The output of Layer 1 is a hardware identity key pair, specifically a public key that represents the device's identity and a private key that is bound to the hardware and cannot be extracted. All subsequent attestation operations reference this public key as the device identifier.

Layer 2: Manufacturing Attestation

At the conclusion of the manufacturing process, once all quality controls, security tests, and firmware signing procedures have been completed, the manufacturer generates an attestation record for the device. This record consists of a set of binary compliance flags representing the outcomes of the manufacturing process, combined with the device's public hardware identity key. Typical flags include: `uses_certified_components`, `firmware_signed`, `security_tested`, `no_known_vulnerabilities_at_release`, and `manufacturing_site_certified`. The flags are set based on the manufacturer's internal records; those records are retained by the manufacturer and are not shared with AffixIO or with the end customer.

AffixIO's attestation API processes the compliance flags and the device identity key to produce a ZK attestation certificate. The certificate is a cryptographic proof that the device identified by this public key satisfies the stated compliance criteria. The certificate does not contain component part numbers, firmware version identifiers, manufacturing site codes, or any other detail that could reveal the manufacturer's supply chain. The circuit

implementation used to generate the proof is not disclosed in public documentation. The verifier receives the certificate and can confirm its validity using AffixIO's public verification interface.

Layer 3: Field Attestation

When the device is deployed in the field, it can present its ZK attestation certificate to any relying party that requests it. Relying parties include: the operator's network admission control system, which may require a valid attestation certificate before granting the device network access; the operator's security operations centre, which may include attestation status in its asset inventory; and regulatory auditors who require evidence of supply chain security compliance under NIS2, DORA, or the CRA. The verifier confirms that the certificate is valid, was issued by a manufacturer whose attestation public key is on the operator's trusted-manufacturer list, and attests to the compliance criteria required by the deployment context. The verifier learns none of the underlying manufacturing details.

> **Privacy boundary:** The ZK attestation certificate crosses the boundary between the manufacturer's confidential supply chain domain and the operator's compliance verification domain. What crosses the boundary is proof of compliance, not evidence of compliance. The evidence remains with the manufacturer.

SECTION 7

Merkle-Anchored Device Records

Each device attestation record generated by AffixIO's API is anchored in a SHA-256 Merkle tree. The Merkle leaf for a given device contains a hash derived from the device attestation certificate and the device's hardware identity public key. The Merkle root is computed after each batch of insertions and signed with an ML-DSA-65 post-quantum signature. The signed root is published to an append-only roots log. This architecture is described in detail in WP-011 (Merkle Tree Audit Architecture); the present section focuses on its application to hardware device records specifically.

Merkle anchoring provides two properties that are particularly valuable for critical infrastructure operators. First, tamper-evident records: any attempt to modify a device attestation record after it has been anchored into the Merkle tree will be detectable by any party that holds the corresponding inclusion proof and the signed root. The inclusion proof allows recomputation of the root from the leaf; if the root produced by recomputation differs from the signed root, the record has been modified. This property holds without trust in AffixIO's infrastructure: the verification is purely cryptographic and can be performed offline.

Second, fleet completeness verification. An operator managing a large fleet of IoT devices in critical infrastructure can verify that every device in the fleet has a corresponding attestation record in the Merkle tree. The operator holds a list of device hardware identity public keys, acquired at procurement time. By querying the Merkle tree for inclusion proofs for each device identity, the operator can confirm that every device in the fleet has been attested. Any device for which no attestation record can be found represents a compliance gap that should trigger investigation: either the device was not attested at manufacture (a supply chain control failure) or a device has been added to the fleet without following the standard procurement process.

The Merkle tree also provides an audit history. Because the tree is append-only, previous states of the tree are recoverable by reference to historical signed roots. If a device's compliance status changes (for example, because a vulnerability is discovered in the firmware it was certified as running), the original attestation record remains in the tree, and a new record recording the updated compliance status is added. The audit trail shows the complete history of the device's compliance status throughout its operational life, with each state transition recorded as a dated entry anchored in the tree.

For regulators and supervisors, this architecture provides an independently verifiable audit record that meets the requirements of Article 21 of NIS2 and Article 28 of DORA for documented, assessable supply chain risk management records. The Merkle-anchored records can be included in regulatory submissions, provided to auditors as part of conformity assessment for the CRA, and retained as evidence in the event of a security incident investigation.

SECTION 8

Post-Quantum Signing for Long-Lived Device Certificates

IoT devices in critical infrastructure have long operational lifetimes that are unusual in the broader technology landscape. Energy metering infrastructure is typically designed for 15 to 20 years of service. Industrial control systems in process industries routinely operate for decades without replacement. Medical devices may require certification records and audit trails to be maintained for the lifetime of the patient who receives the implant or treatment. A device attestation certificate issued today may need to remain verifiable for 20 or more years.

Classical public-key cryptography, including RSA-2048 and ECDSA using elliptic curves such as P-256 or P-384, is expected to be vulnerable to attack by cryptanalytically relevant quantum computers. The timeline for such computers is uncertain, but NIST's post-quantum cryptography standardisation programme, which concluded with the publication of FIPS 204 (ML-DSA), FIPS 205 (SLH-DSA), and FIPS 203 (ML-KEM) in 2024, was specifically motivated by the assessment that quantum computers capable of breaking these algorithms could emerge within the next 10 to 15 years. For devices with 20-year operational lifetimes, signatures applied today with classical algorithms may be forgeable before the device reaches end of life.

ML-DSA-65 (Module-Lattice Digital Signature Algorithm, NIST FIPS 204, security level 3) post-quantum signatures ensure that device attestation certificates and Merkle root signatures remain secure against quantum attack throughout the device's operational lifetime. ML-DSA-65 is a lattice-based signature scheme whose security rests on the hardness of the Module Learning With Errors (MLWE) problem, which is not known to be vulnerable to quantum algorithms. Signatures produced with ML-DSA-65 today are expected to remain unforgeable even under quantum attack.

The post-quantum risk for device attestation has a specific character that is worth making explicit. The concern is not merely that historical communications might be decrypted in the future. For attestation, the relevant risk is what might be termed "harvest now, forge later": an adversary

who collects a large set of genuine ML-DSA attestation signatures today could, in principle, use those signatures as templates for forging new attestation certificates in the future if a quantum algorithm for breaking ML-DSA were discovered. Adopting ML-DSA-65 now, rather than transitioning later, eliminates this risk for any attestation record created after the transition. Attestation records created with classical signatures before the transition remain in the audit tree but carry a known cryptographic risk that operators should document in their risk registers.

The post-quantum transition also has implications for the hardware root of trust layer. TPM chips implementing only classical ECC keys will need to be assessed against the organisation's cryptographic agility policy. Newer TPM specifications and DICE implementations support post-quantum identity keys. Operators procuring devices with long operational lifetimes should specify post-quantum capable hardware identity mechanisms in their procurement requirements, so that the entire attestation chain from hardware identity to Merkle root is quantum-resistant.

> **NIST FIPS 204 (ML-DSA-65):** All AffixIO Merkle root signatures and attestation certificates use ML-DSA-65, standardised by NIST in August 2024. Security level 3 provides post-quantum security broadly comparable to AES-192. See also WP-002 (Post-Quantum Attestation) for a detailed treatment of the algorithm selection rationale.

SECTION 9

Cross-Border Trade Compliance Without Exposing Supply Chain Details

International trade in critical infrastructure components involves customs declarations, export control compliance, and dual-use regulations. The Wassenaar Arrangement governs the export of goods, software, and technology that have potential military or surveillance applications; many categories of advanced electronics, network equipment, and embedded systems fall within its scope. Exporting a security-critical IoT device to

certain destinations requires demonstrating to export control authorities that the device meets applicable security standards and that the export complies with the applicable controls.

A manufacturer exporting a security-critical IoT device may simultaneously face two conflicting requirements. The importing country's customs and regulatory authorities may require technical evidence that the device meets local security standards, which in turn may require disclosure of firmware specifications, component details, or certification documentation. The exporting country's commercial confidentiality obligations, and the manufacturer's own interest in protecting trade secrets, counsel against sharing exactly those details. In practice, this tension is often resolved by providing broad contractual assurances rather than technical evidence, which satisfies neither the importing authority's need for verification nor the manufacturer's interest in providing credible compliance evidence.

ZK compliance attestations for trade resolve this tension at the technical layer. A manufacturer can generate a ZK proof that a device meets the importing country's security requirements without disclosing firmware details that might assist an adversary in identifying vulnerabilities, without revealing component sourcing that might identify the manufacturer's subcontractors, and without exposing manufacturing process details that constitute competitive intelligence. The ZK certificate is presented to customs and regulatory authorities alongside the export declaration. The authority can verify the certificate against the manufacturer's public attestation key, confirming compliance without requiring the manufacturer to disclose the underlying evidence.

This approach is aligned with emerging work on digital trade facilitation. The World Trade Organisation's Joint Statement Initiative on Electronic Commerce, and standards work being conducted within ETSI, CEN/CENELEC, and the IETF RATS (Remote ATtestation procedureS) working group, are all developing frameworks for interoperable security attestation in cross-border trade contexts. ZK attestation certificates that conform to IETF RATS attestation formats (particularly the Entity Attestation Token, EAT, specification) are designed to be verifiable by authorities using standard verification tooling, regardless of which attestation issuer produced them.

For UK exporters specifically, the post-Brexit trade environment has introduced new administrative requirements for goods crossing the UK-EU border, including electronics goods with dual-use potential. UK manufacturers exporting critical infrastructure components to EU customers who are subject to NIS2 supply chain obligations now have an additional channel through which ZK attestation adds value: the UK manufacturer can provide its EU customer with ZK attestation certificates that satisfy the customer's NIS2 Article 21 supply chain risk management documentation obligations without requiring the UK manufacturer to share supply chain details with a competitor who might be bidding for the same end customer's business through a different procurement route.

SECTION 10

Integration with Existing PKI and Hardware Security Modules

Most organisations deploying critical infrastructure have established Public Key Infrastructure (PKI) for device identity management. An IoT device deployed in a managed network typically holds a device certificate issued by the operator's internal certificate authority or by a trusted commercial CA, which is used for network authentication, TLS communications, and code signing verification. ZK device attestation is designed to complement rather than replace this existing PKI investment. The two mechanisms serve different purposes: the PKI certificate proves the device's network identity; the ZK attestation certificate proves its security compliance and manufacturing provenance. Both are necessary for a complete picture.

Integration Pattern 1: PKI Certificates with Attestation References

In this pattern, the PKI-issued device certificate carries an extension field referencing the device's ZK attestation record in AffixIO's Merkle tree. The extension contains the Merkle leaf identifier and a URI pointing to the inclusion proof. When the device presents its certificate at network admission, the network admission control system can retrieve the inclusion

proof and verify the device's attestation status as part of the admission decision. This pattern requires no modification to the device's hardware or firmware; the reference is added to the PKI certificate at issuance time, using information provided by the manufacturer at the time of device delivery.

Integration Pattern 2: TPM Attestation Report Extension

In this pattern, the ZK attestation certificate is embedded in the device's TPM attestation report as an extension field. During remote attestation (using the TPM's standard quoting mechanism), the attestation report includes both the TPM's standard platform measurements, specifically the PCR (Platform Configuration Register) values that record firmware and boot-sequence measurements, and the ZK compliance certificate that covers the manufacturing-time compliance claims. The relying party receives both the TPM attestation and the ZK certificate in a single response, enabling verification of both runtime state and manufacturing provenance in one operation. This pattern is well-suited to high-security deployments where both runtime integrity and manufacturing provenance must be verified at each connection.

Integration Pattern 3: HSM-Based Manufacturing Attestation

In this pattern, Hardware Security Modules at the manufacturer's production sites generate the compliance witness data and pass it to AffixIO's attestation API. The HSM holds the manufacturer's attestation signing key; AffixIO holds the ZK proving infrastructure. The two systems collaborate to produce the final attestation certificate without AffixIO ever accessing the raw compliance data (component identifiers, firmware hashes, test results) that constitute the underlying evidence. This separation of concerns allows manufacturers to adopt ZK attestation without disclosing their supply chain details even to their attestation service provider.

SPDM Compatibility

SPDM (Security Protocol and Data Model, DMTF DSP0274) is a standardised protocol for device attestation that is increasingly supported by server management controllers, network interface cards, and storage devices in data centre and critical infrastructure contexts. SPDM defines a message format

for requesting and receiving device attestation reports, and supports extension mechanisms that allow additional attestation data to be included in the response. ZK attestation certificates can be carried as SPDM extensions within the attestation response, enabling ZK attestation to be integrated into environments that already use SPDM for device integrity verification without requiring changes to the SPDM deployment.

SECTION 11

Known Limitations

ZK device attestation is a significant improvement over conventional supply chain assurance mechanisms, but it is not without limitations. Operators and manufacturers adopting this architecture should understand those limitations clearly, so that they can be addressed with appropriate complementary controls rather than left as unrecognised gaps.

Hardware Root of Trust Dependency

ZK device attestation is only as strong as the hardware root of trust it is built on. If the hardware identity can be cloned, the attestation can be compromised: an adversary who can clone a device's hardware identity can present a genuine attestation certificate for a fraudulent device. Some older TPM implementations are vulnerable to hardware-level attacks that can extract identity keys under physical access conditions. Devices using DICE-based identity tied to one-time-programmable fuses or using PUF circuits provide substantially stronger resistance to hardware-level cloning, because the identity depends on physical properties that cannot be replicated. Operators specifying devices for high-security deployments should require hardware identity mechanisms that have been formally evaluated against physical attack. Manufacturers seeking to provide the strongest attestation guarantees should similarly move towards DICE or PUF-based identity for new device designs.

Manufacturing Integrity Assumption

The ZK attestation certificate certifies that the device met the stated compliance criteria at the time of manufacture. It does not provide real-time assurance that the device has not been physically modified since deployment. An adversary with physical access to a deployed device could, in principle, modify the device's internals in ways that are not reflected in the attestation certificate, because the certificate was issued before the modification occurred. For high-security deployments, cryptographic attestation should be complemented by physical security controls: tamper-evident enclosures, secure installation environments, access logging, and periodic re-attestation using the device's hardware root of trust to generate fresh measurements of the device's current state. Re-attestation at intervals appropriate to the deployment's risk profile provides ongoing assurance rather than a one-time snapshot at manufacture.

Trust in the Manufacturer

The ZK attestation framework proves that a device satisfies criteria as defined and assessed by its manufacturer. It does not independently verify the accuracy of the manufacturer's assessment. An unscrupulous manufacturer could issue ZK attestation certificates for devices that do not genuinely meet the stated criteria; the ZK proof would be valid (in the sense of being mathematically correct), but the underlying compliance claims would be false. This risk is analogous to the risk of false self-declaration in any certification scheme. It is mitigated by due diligence on the manufacturer (including third-party audits of the manufacturer's attestation processes), by regulatory oversight of manufacturers under the Cyber Resilience Act's market surveillance provisions, and by requiring manufacturer attestation keys to be registered with a trusted authority that can revoke them if misconduct is established. The attestation framework provides accountability that did not previously exist; it does not eliminate the need for manufacturer assessment.

Re-Attestation Intervals and Vulnerability Management

A device's compliance status is not static. Vulnerabilities are discovered in firmware and components after a device has been certified; patches are released and may or may not be applied to deployed devices; components reach end-of-support and may no longer receive security updates. An attestation certificate issued at manufacture reflects the device's compliance

status at that point in time. Operators should establish re-attestation policies that align with their vulnerability management cycles: when a new vulnerability is assessed as affecting a category of devices in the fleet, those devices should be re-attested (or their attestation status should be updated to reflect the vulnerability, with a remediation deadline recorded) before the next compliance reporting period. The Merkle audit tree supports this lifecycle management by recording each attestation event as a timestamped entry, allowing the compliance history of each device to be reconstructed and reported.

SECTION 12

Conclusion

Supply chain security for IoT devices in critical infrastructure is no longer a future concern or an optional enhancement to security programmes. NIS2, DORA, and the Cyber Resilience Act create concrete legal obligations, now in force or imminently coming into force, for organisations operating in the EU to verify and document the security of the devices they deploy. Similar requirements are advancing in the UK through the Product Security and Telecommunications Infrastructure Act, in the United States through NIST SP 800-161 and the Biden administration's supply chain executive orders, and across the Asia-Pacific region through national cybersecurity frameworks and critical infrastructure protection legislation.

The core challenge is one of trust without exposure. Operators need to verify device authenticity and security compliance; manufacturers need to provide that verification without disclosing commercially sensitive supply chain details. This is not a problem that can be resolved by procurement contracts or supplier questionnaires alone. It requires a technical mechanism that can generate verifiable proof of compliance without revealing the evidence that underlies that proof. ZK attestation is the cryptographic solution to this specific challenge, and its application to hardware device provenance is a natural extension of the same techniques that ZK proofs bring to identity, credentials, and AI governance.

The combination of ZK compliance certificates, Merkle-anchored device records, and ML-DSA-65 post-quantum signatures provides an attestation infrastructure that is verifiable today, auditable throughout the operational life of a device, and remains cryptographically secure even after quantum computers capable of breaking classical cryptography become available. For devices with operational lifetimes measured in decades, this long-term security guarantee is not a peripheral consideration; it is a central requirement.

AffixIO's attestation and audit infrastructure provides the cryptographic layer for this architecture. The hardware identity roots, manufacturing processes, component sourcing, and device-specific security controls remain entirely within the manufacturer's domain. AffixIO converts the compliance outcomes of those processes into tamper-resistant, post-quantum-signed, regulator-readable attestation records that operators can present to supervisors, auditors, and conformity assessment bodies with confidence. The supply chain evidence stays where it belongs; the compliance proof goes where it needs to go.

Related AffixIO White Papers

- WP-011 — Merkle Tree Audit Architecture: The append-only Merkle tree and inclusion proof architecture that underpins device record anchoring.
- WP-002 — Post-Quantum Attestation: ML-DSA-65 algorithm selection, key management, and migration considerations.
- WP-018 — AI-BOM: Model Supply Chain Provenance: ZK attestation applied to AI model supply chains; parallels with hardware SBOM and HBOM obligations.
- WP-020 — DORA and MiCA AI Compliance: Comprehensive treatment of DORA's ICT risk management requirements for financial entities.

FREQUENTLY ASKED QUESTIONS

FAQ

What is a hardware root of trust?

A hardware root of trust is a set of cryptographic functions embedded in a device's hardware that can be trusted to behave correctly because they cannot be modified by software. Common implementations include TPM (Trusted Platform Module) chips, DICE (Device Identity Composition Engine) architecture, and PUF (Physical Unclonable Function) circuits. They provide the foundation for device identity and attestation: all cryptographic claims a device makes about itself ultimately rely on the hardware root of trust being genuine and uncompromised.

Does ZK device attestation replace physical security inspections?

No. ZK attestation provides cryptographic evidence of a device's compliance status at manufacture and can support ongoing monitoring through re-attestation. It does not replace physical security controls for highly sensitive deployments, where visual inspection, tamper-evident enclosures, access logging, and secure installation environments remain necessary complements to cryptographic attestation. The two approaches address different threat vectors: ZK attestation addresses supply chain integrity and manufacturing provenance; physical controls address post-deployment interference and unauthorised access.

How does ZK device attestation relate to SBOM requirements under the Cyber Resilience Act?

The CRA requires manufacturers to provide an SBOM (Software Bill of Materials) documenting a product's software components. ZK attestation complements this requirement in two ways. First, where an SBOM entry lists a software component, a ZK compliance certificate can provide cryptographic evidence that the component meets specified security standards without revealing the component's supplier, version, or configuration details that might be commercially sensitive or exploitable by an adversary who knows which specific version is in use. Second, ZK attestation extends naturally from

software components to hardware components (an HBOM, or Hardware Bill of Materials), providing the same privacy-preserving compliance verification for the hardware layer that SBOM attestation provides for the software layer.

AffixIO White Paper WP-028 · June 2026 · affix-io.com