International Journal of AI, BigData, Computational and Management Studies
Noble Scholar Research Group | Volume 7, Issue 1, 142-147, 2026
ISSN: 3050-9416 | https://doi.org/10.63282/3050-9416.IJAIBDCMS-V7I1P122

Original Article

Device Identity and Trust Establishment in Mass-Manufactured IoT Systems

Vignesh Alagappan
Sr. Manager, Ecosystem Engineering, Rheem Manufacturing, 1115 Northmeadow Parkway, Suite 100, Roswell, GA.

Received On: 28/12/2025 ***Revised On: 02/02/2026*** ***Accepted On: 08/02/2026*** ***Published On: 20/02/2026***

Abstract: *Security in mass-manufactured IoT systems depends on device identity established during manufacturing and preserved across operational lifecycles spanning 10-20 years. Current deployments use identity models that fail under physical access, supply-chain compromise, or credential abuse. This paper analyzes device identity as an architectural primitive, examines failures in automotive infotainment, HVAC, and water-heating deployments, and presents a hardware-rooted, lifecycle-aware architecture that emphasizes establishing manufacturing-time trust, explicit revocation, and zero-trust operation.*

Keywords: *Device Identity, Iot Security, Mass-Manufactured Iot Systems, Hardware Root Of Trust, Manufacturing-Time Provisioning, Supply Chain Security, Zero-Trust Architecture, Device Attestation, Certificate-Based Authentication, Mutual TLS (Mtls), Credential Revocation, Lifecycle Security Management, Secure Boot, Embedded Systems Security, Long-Term Operational Trust.*

1. Introduction

Mass-manufactured IoT devices operate under constraints absent from enterprise computing: high-volume production across distributed facilities, provisioning optimized for throughput rather than adversarial isolation, deployment in physically accessible environments, and 10–20-year operational lifetimes with intermittent connectivity and limited servicing opportunities.

Device identity in many platforms remains weakly defined: derived from mutable metadata (serial numbers, MAC addresses), implicitly established through enrollment, lacking cryptographic binding to physical hardware. At the manufacturing scale, a single credential exposure or provisioning flaw enables fleet-wide impersonation. Post-deployment, these failures are irreversible without physical replacement.

Prior research focuses on authentication protocols and cryptographic primitives, assuming that device identity is correct and uncompromised. Less attention addresses how identity is created, protected during manufacturing, preserved across firmware transitions, and revoked years post-deployment. Manufacturing environments are rarely modeled as adversarial boundaries despite their role in identity provisioning. Identity failures introduced at manufacturing remain latent until wide deployment, when remediation becomes infeasible.

1.1. Contributions

- Manufacturing-Centric Identity Framing: Establishes manufacturing as the initial and most consequential trust boundary
- Hardware-Bound Identity Requirements: Formalizes properties necessary for long-lived, physically accessible devices
- Lifecycle-Aware Trust Modeling: Introduces explicit device identity lifecycle spanning manufacturing through decommissioning
- Cross-Domain Failure Analysis: Analyzes recurring breakdowns across automotive, HVAC, and water heating systems
- Standards-Contextualized Architecture: Positions architecture within existing PKI and IoT security standards

1.2. Keywords

Device identity, hardware root of trust, manufacturing security, IoT security, public key infrastructure, zero-trust architecture, device lifecycle management, certificate revocation, cryptographic attestation, supply chain security.

2. Problem Statement and Threat Landscape

2.1. Manufacturing-Scale Identity Propagation

Identity failures at manufacturing scale propagate multiplicatively. A development-phase flaw replicated across production lines affects thousands to millions of devices. Manufacturing environments involve semi-trusted actors, shared tooling, and transient personnel. Firmware flashing stations, calibration rigs, and provisioning scripts are reused across products, creating high-value attack surfaces.

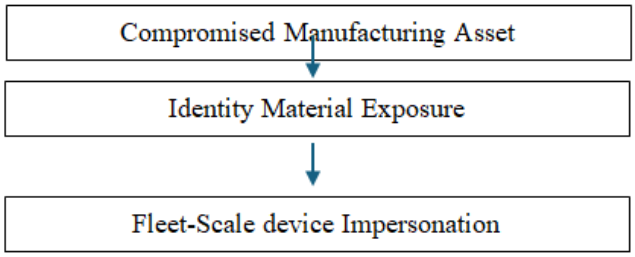

Fig 1: Manufacturing Attack Chain

Table 1: Manufacturing Threat Actor Taxonomy

Threat Actor	Access Level	Identity Risk Vector
Manufacturing insider	Provisioning systems	Credential leakage, provisioning script extraction
Supply-chain adversary	Components/firmware	Identity misbinding, malicious firmware injection
Field attacker	Physical device	Key extraction via debug interfaces, flash dump
Remote adversary	Network access	Device impersonation, replay attacks

3. Device Identity: Definitions and Requirements

Fragility in IoT security architectures stems from imprecise, unenforced definitions of device identity. The term conflates identifiers, credentials, enrollment status, and cloud records. This ambiguity produces architectures functioning under normal operation but failing under adversarial pressure or lifecycle events.

Device identity: A cryptographically verifiable binding between a specific physical device instance and a logical identity recognized by the system.

This definition separates identity from identifiers (serial numbers), authentication mechanisms (tokens), and enrollment workflows. Identity is a property of physical hardware, not a software artifact or database entry.

Table 2: Core Identity Requirements and Failure Modes

Requirement	Technical Definition	Failure Pattern
Uniqueness	Globally unique, non-replicable cryptographic key material per device	Single compromised device → fleet-wide impersonation
Non-extractability	Private keys cannot be read, exported, or reconstructed outside device boundary	Debug access → key extraction → cloning attacks
Cryptographic verifiability	Identity verifiable using standard cryptographic mechanisms, public material only	Symmetric secrets → single point of trust failure
Lifecycle persistence	Identity survives firmware updates, factory resets, power loss events	Update → identity loss → re-enrollment abuse
Revocability	Permanent invalidation capability post-compromise, independent of device cooperation	No revocation → permanent fleet compromise

4. Taxonomy of Device Identity Approaches

Table 3: Identity Architecture Comparison Matrix

Property	Software Identity	Symmetric Key	PKI + HRoT
Uniqueness	Weak	Moderate	Strong
Non-extractability	None	Limited	Strong
Verifiability	Low	Low	High
Lifecycle persistence	Poor	Moderate	Strong
Revocability	Poor	Complex	Native
Manufacturing risk	Low	High	Moderate

5. Hardware-Rooted Identity Foundations

Hardware Roots of Trust (HRoT) enforce non-extractability and lifecycle persistence. A HRoT establishes a minimal, immutable trust anchor remaining secure under application firmware compromise.

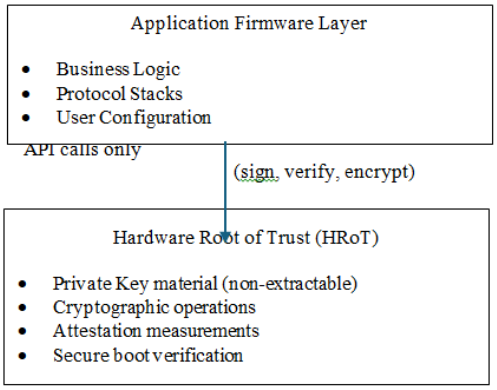

Fig 2: HRoT Architectural Isolation

Table 4: HRoT Implementation Trade-offs

Implementation	Security Strength	BOM Impact	Deployment Notes
Discrete Secure Element	Very high	$0.50-2.00/unit	Strong physical isolation, FIPS 140-2/3 capable
TPM 2.0 module	High	$0.30-1.50/unit	Standardized TCG interfaces, attestation support
MCU TrustZone	Medium-High	No incremental cost	ARM v8-M+ only, software integration required
Software-only crypto	Low	None	*Fails non-extractability requirement*

6. Manufacturing-Time Trust Establishment

Manufacturing defines the inflection point where inert hardware becomes a trusted system participant. Identity decisions here persist for device lifetime. Manufacturing Environments optimize for throughput and yield, not adversarial isolation. Provisioning infrastructure is shared across products, operators rotate frequently, and firmware images are reused to minimize downtime.

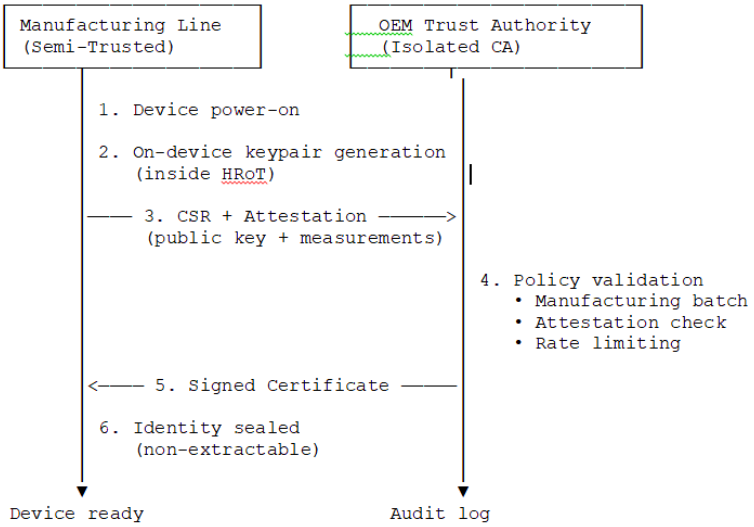

Fig 3: Secure Manufacturing Identity Flow

Table 5: Manufacturing Identity Controls

Threat	Control Mechanism	Implementation
Private key exposure	On-device generation	Keys generated inside HRoT boundary, never transmitted
Certificate mis-binding	Attestation-based issuance	CSR includes HRoT attestation proving hardware integrity
Batch compromise	CA scoping per batch	Separate intermediate CA per manufacturing batch for blast radius control
Provisioning abuse	Issuance rate limiting	Maximum certificates per time window based on production schedule
Debug interface abuse	Post-provisioning lockdown	JTAG/SWD permanently disabled or cryptographically locked post-identity-seal

Table 6: CA Scoping and Blast Radius Analysis

CA Scope	Blast Radius	Operational Cost	Recovery Time
Global CA	Entire fleet	Extremely high	Months-years
Product-line CA	Product family	High	Weeks-months
Factory CA	Single site	Moderate	Days-weeks
Batch CA	Limited batch	Low	Hours-days

7. Device Identity Lifecycle Model

Device identity evolves through manufacturing, deployment, updates, compromise events, and retirement. Modeling identity as a lifecycle enables explicit reasoning about permissible state transitions and failure containment.

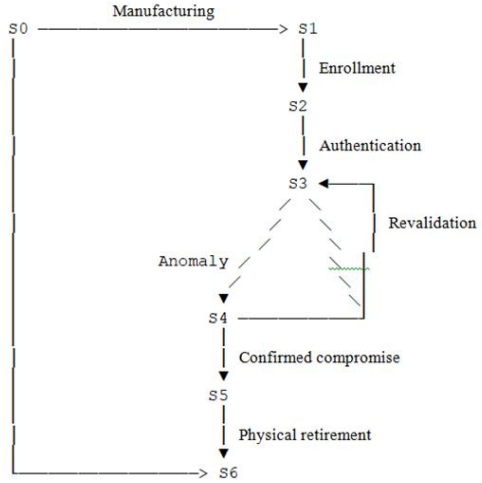

Fig 4: Identity State Transition Diagram

States:
S0: Uninitialized S1: Provisioned S2: Enrolled
S3: Operational S4: Suspended S5: Revoked
S6: Decommissioned

Table 7: Identity States and Authorized Transitions

State	Description	Authorized Transitions
S0: Uninitialized	Device manufactured, no identity assigned	S0 → S1 (manufacturing provisioning) S0 → S6 (manufacturing reject)
S1: Provisioned	Hardware identity established, not yet enrolled	S1 → S2 (device enrollment) S1 → S6 (pre-deployment reject)
S2: Enrolled	Registered with backend, pending first authentication	S2 → S3 (successful authentication) S2 → S5 (enrollment fraud detection)
S3: Operational	Actively authorized for normal operations	S3 → S4 (anomaly detection) S3 → S5 (confirmed compromise) S3 → S6 (decommission request)
S4: Suspended	Temporarily restricted pending investigation	S4 → S3 (revalidation successful) S4 → S5 (compromise confirmed) S4 → S6 (administrative decision)
S5: Revoked	Permanently invalidated, all access denied	S5 → S6 (physical retirement only)
S6: Decommissioned	Physically retired, identity destroyed	Terminal state - no outbound transitions

Table 8: Forbidden State Transitions and Attack Vectors

Forbidden Transition	Attack Enabled	Enforcement Mechanism
S5 → S3	Reactivation of compromised identity	Revocation check in authentication path
S6 → Any	Reuse of retired device identity	Cryptographic identity destruction on retirement
S3 → S1	Identity rollback attack	Hardware-enforced identity persistence
S4 → S2	Re-enrollment bypass	Enrollment history verification

8. Zero-Trust Operational Model

Deployed IoT devices operate where network topology, physical access, and peer behavior cannot be trusted. Zero-trust principles provide the framework for managing identity and authorization under these conditions.

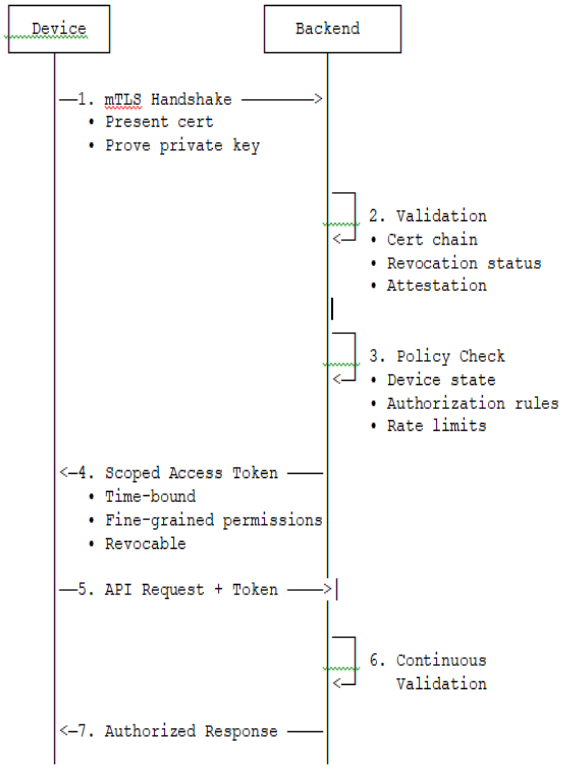

Fig 5: Zero-Trust Authentication and Authorization Flow

Table 9: Zero-Trust vs. Traditional IoT Security Models

Aspect	Traditional Model	Zero-Trust Model
Trust boundary	Network perimeter	Per-request cryptographic validation
Trust duration	Permanent after enrollment	Time-bound, continuously validated
Authorization	All authenticated devices equal	Fine-grained, state-dependent
Compromise detection	Reactive, post-incident	Continuous monitoring, anomaly-triggered suspension
Lateral movement	Uncontrolled within network	Prevented by per-device authorization

9. Cross-Domain Failure Analysis

Empirical analysis of deployed systems across automotive infotainment, HVAC, and water heating domains reveals structurally similar identity failures despite different cost models, regulatory contexts, and operational requirements. These failures stem from architectural decisions rather than domain-specific defects.

Table 10: Cross-Domain Identity Failure Comparison

Domain	Identity Model	Root Cause	Persistence Mechanism
Automotive Infotainment	VIN-based enrollment	Metadata-bound identity, debug interfaces enabled	Late provisioning (dealer activation)
HVAC Systems	Serial number enrollment	Gateway-mediated transitive trust	Contractor installation model
Water Heating	Flash-stored credentials	Non-revocable shared secrets	Cost optimization priority

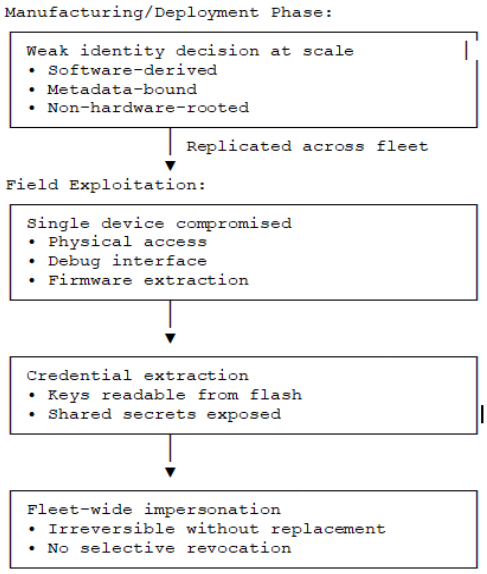

Fig 6: Common Attack Pattern across Domains

10. Implementation Guidance

Table 11: Phased Implementation Roadmap

Phase	Key Activities	Success Criteria	Timeline
Phase-1: Foundation	Select HRoT technology, design PKI hierarchy, prototype manufacturing flow	Validated HRoT integration, CA infrastructure operational, pilot batch provisioned	3-6 months
Phase 2: Manufacturing	Deploy provisioning at scale, implement batch-level CA scoping, establish audit logging	Production line throughput maintained, zero key escrow incidents, complete audit trail	6-12 months
Phase 3: Operations	Deploy zero-trust backend, implement continuous validation, enable revocation mechanisms	Device authentication via mTLS, real-time revocation enforcement, state-based authorization	12-18 months
Phase 4: Maturity	Deploy anomaly detection, establish lifecycle management, conduct penetration testing	Automated threat response, complete lifecycle visibility, validated security posture	18-24 months

11. Conclusion

Device identity determines security outcomes in mass-manufactured IoT systems. Architectural decisions during manufacturing establish whether devices can be trusted, revoked, or recovered across 10-20 year operational lifetimes. Analysis across automotive infotainment, HVAC, and water heating domains demonstrates that identity failures share structural causes: weak manufacturing-time trust establishment, absence of hardware-rooted protection, and inadequate lifecycle modeling.

The architecture presented treats identity as a hardware-bound, lifecycle-managed systems primitive. Manufacturing becomes an explicit adversarial boundary where trust is established through cryptographic binding to non-extractable key material. Zero-trust operational principles ensure continuous validation rather than one-time enrollment trust.

Deployments achieving resilience proportional to scale and longevity require: on-device key generation within hardware roots of trust, attestation-based certificate issuance with batch-scoped CAs, explicit device lifecycle state machines preventing forbidden transitions, and continuous authorization gated on identity state rather than historical enrollment. These mechanisms compose to enable decisive incident response where compromised devices can be revoked or suspended without fleet-wide service disruption.

References

1. NIST, "Digital Identity Guidelines," NIST Special Publication 800-63, Rev. 4, 2023.
2. NIST, "Zero Trust Architecture," NIST Special Publication 800-207, 2020.
3. NIST, "IoT Device Cybersecurity Capability Core Baseline," NISTIR 8259A, 2021.
4. ISO/IEC, "Trusted Platform Module (TPM) Library Specification," ISO/IEC 11889, 2015.
5. IEEE, "Secure Device Identity," IEEE Std 802.1AR-2018.
6. ISO/SAE, "Road Vehicles — Cybersecurity Engineering," ISO/SAE 21434, 2021.
7. Connectivity Standards Alliance, "Matter Core Specification," Version 1.2, 2023.

8. Connectivity Standards Alliance, "Device Attestation Architecture," 2023.
9. D. Cooper et al., "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile," IETF RFC 5280, 2008.
10. M. Pritikin et al., "Enrollment over Secure Transport," IETF RFC 8554, 2019.
11. M. Richardson et al., "Bootstrapping Remote Secure Key Infrastructures," IETF RFC 8995, 2021.
12. ETSI, "Cyber Security for Consumer Internet of Things," ETSI TS 103 645, 2020.
13. ENISA, "Baseline Security Recommendations for IoT," European Union Agency for Cybersecurity, 2020.
14. ARM Ltd., "Platform Security Architecture (PSA) Certified Framework," 2022.
15. J. Großschädl et al., "Hardware Security for the Internet of Things," IEEE Design & Test, vol. 34, no. 1, pp. 5–15, Feb. 2017.
16. M. Ammar et al., "Internet of Things: A Survey on the Security of IoT Frameworks," Journal of Information Security and Applications, vol. 38, pp. 8–27, 2018.
17. S. Sicari et al., "Security, Privacy and Trust in Internet of Things: The Road Ahead," Computer Networks, vol. 76, pp. 146–164, 2015.