Enterprise 3 (E3)

Security Architecture White Paper

SensThys, Inc. · Cupertino, CA · www.sensthys.com

Executive Summary

The SensThys Enterprise 3 (E3) is designed from the ground up with security as a core architectural principle, not an afterthought. By eliminating the operating system attack surface, implementing bare-metal firmware, and incorporating the proprietary EPIC data-integrity protocol, the E3 achieves what SensThys believes is the strongest security posture of any commercially available fixed RFID reader. A full NIST SP 800-213 / 8259A compliance report is available upon request. This white paper describes the E3's security architecture, threat model, and compliance posture.

Threat Model

RFID infrastructure in manufacturing, logistics, and sensitive commercial environments faces four primary threat categories:

- Data integrity attacks — corrupted or spoofed EPC tag data causing downstream errors in inventory, traceability, or process control systems
- Network-level attacks — unauthorized access, denial-of-service, or man-in-the-middle attacks on reader-to-host communications
- Physical interface attacks — unauthorized access via exposed ports, firmware manipulation, or configuration tampering
- IoT-layer attacks — exploitation of reader OS vulnerabilities, unpatched services, or insecure default configurations common to general-purpose embedded Linux platforms

Architectural Security Principles

Bare-Metal Firmware — No OS Attack Surface

The E3 runs exclusively on SensThys bare-metal firmware. There is no general-purpose operating system (Linux, RTOS, or otherwise) on the E3. This eliminates the entire class of OS-level attacks including kernel exploits, privilege escalation, shell injection, and package-level vulnerabilities that represent the majority of CVEs disclosed against IoT devices. An attacker who gains network access to the E3 cannot escalate privileges to an OS shell because no shell exists.

Minimal Attack Surface

Only network services required for operation are active: the REST API, TCP configuration port, and the web configuration interface. All services can be individually disabled. There are no open SSH, Telnet,

FTP, or remote management ports. The attack surface is quantifiably smaller than any OS-based reader.

EPIC — Data Integrity at the RF Layer

EPIC (Error Protection and Integrity Correction) is a SensThys-proprietary protocol that operates natively between the E3 and EPIC-capable tags. EPIC provides:

- Cryptographic verification of tag EPC memory contents — ensures that what is written to a tag is exactly what is read back, protecting against memory decay and data corruption
- Automatic correction of single-bit errors in tag memory without host involvement
- Infinite effective tag lifetime — EPIC continuously refreshes tag memory, eliminating the wear-related data degradation that affects standard RFID tags over time
- Detection and rejection of spoofed or cloned tags that fail EPIC verification

Network Security

API Authentication

All REST API endpoints require authentication via HTTP Bearer token over TLS. API access can be restricted to specific IP ranges via the network access control configuration. The hardware and software infrastructure are available for disabling access to different APIs based on customer needs.

TLS / HTTPS

HTTPS with TLS 1.2 or higher is required for all production API access. The reader ships with a self-signed certificate; customers can install their own CA-signed certificates via the web UI. HTTP access is available for initial setup only and should not be used in production deployments.

Firmware Integrity

Firmware images are digitally signed by SensThys. The bootloader verifies the firmware signature before loading. Unsigned or tampered firmware images will be rejected, preventing malicious firmware from executing even if an attacker obtains physical access to the device. During a legitimate firmware update, the E3's status LED provides tamper-evident visual feedback: the Blue LED flashes continuously while firmware is actively being written, and the Red LED lights periodically as the reader reboots between update steps. Any deviation from this expected LED pattern during an update should be investigated before reconnecting the reader to a production network.

Secure Boot

The E3 implements a secure boot chain. Each stage of the boot process verifies the integrity of the next stage before execution. This ensures that the device cannot be compromised by boot-time attacks even with physical access.

Physical Security

The E3 does not expose a debug UART, JTAG, or serial interface on accessible external connectors. Internal debug interfaces are fused in production units. The USB-C port is used for controlling external USB devices and USB thumb drives — it does not provide a debug or recovery interface in shipping firmware.

NIST SP 800-213 / 8259A Compliance

SensThys has produced a formal NIST SP 800-213 (IoT Device Cybersecurity) and NIST IR 8259A (IoT Device Cybersecurity Capability Core Baseline) compliance assessment for the SensArray product family including the E3. The report covers all six core baseline activities:

NIST 8259A Activity	E3 Implementation	Status
Device Identification	Unique hardware ID, MAC-based hostname, certificate-bound identity	Compliant
Device Configuration	Minimal defaults, forced credential change, configurable service enable/disable per customer needs	Compliant
Data Protection	TLS-encrypted API, firmware signing, no plaintext credential storage	Compliant
Logical Access	Role-based access, IP-range restriction	Compliant
Software Updates	Signed firmware images, update integrity verification, rollback protection	Compliant
Cybersecurity Awareness	NIST report published, vulnerability disclosure program available	Compliant

The full NIST 8259A compliance report is available at sensthys.com/security or upon request from your SensThys account representative.

Security Best Practices for Deployment

- Enable HTTPS and install a CA-signed certificate in production
- Disable HTTP access after initial configuration
- Restrict API access to specific management VLANs or IP ranges
- Enable EPIC mode for all deployments where data integrity is critical
- Keep reader firmware updated — subscribe to SensThys security notifications
- Place readers on a dedicated IoT VLAN, isolated from general corporate network
- Use PoE++ switches with port-level security (802.1X or MAC-based filtering) for physical port protection

Vulnerability Disclosure

SensThys maintains a responsible vulnerability disclosure program. If you discover a security vulnerability in any SensThys product, please report it to info@sensthys.com. We commit to acknowledging reports within 72 hours and providing remediation timelines within 30 days of confirmed vulnerability classification.