SENSORBEE AB

EN 18031-1:2024

Compliance Evidence Document

Common Security Requirements for Internet-Connected Radio Equipment

Product:	Sensorbee Air Pro 2 Cellular (SB8202 / SB8203)
Applicable Standard:	EN 18031-1:2024 (EU Radio Equipment Directive, Art. 3(3)(d))
Declaration Type:	Self-Declaration of Conformity
Document Version:	1.0
Date:	February 2026
Prepared by:	Sensorbee AB, Linköping, Sweden
Classification:	Customer-facing / External

1. Executive Summary

This document provides evidence of compliance of the Sensorbee Air Pro 2 Cellular environmental monitoring station (models SB8202 and SB8203) with EN 18031-1:2024, the harmonised European standard establishing common security requirements for internet-connected radio equipment under the EU Radio Equipment Directive (RED) 2014/53/EU, Article 3(3)(d).

EN 18031-1:2024 defines eleven security mechanism categories. This document demonstrates compliance with each applicable mechanism through a combination of architectural design evidence, firmware code verification, and operational procedures. The Sensorbee Pro2 leverages the LwM2M (Lightweight M2M) protocol as its core device management framework, which was designed with IoT security as a foundational principle and natively satisfies many of the standard's requirements.

Compliance summary: Of the eleven mechanism categories defined in EN 18031-1, nine are applicable to the Pro2 and two are not applicable (NMM and TCM, which target network routing equipment). All nine applicable categories are assessed as **compliant** based on the verified firmware security stack, hardware-backed credential storage, and DTLS-encrypted communications.

2. Product Description and Scope

2.1 Product Overview

The Sensorbee Air Pro 2 Cellular is a professional-grade environmental monitoring station designed for deployment on construction sites, urban environments, and industrial perimeters. It provides continuous measurement of particulate matter (PM1, PM2.5, PM10, TSP), noise levels, and meteorological parameters, transmitting data to the Sensorbee Cloud platform via cellular connectivity.

Characteristic	Description
Product Models	SB8202 (MCERTS) / SB8203
Manufacturer	Sensorbee AB, Linköping, Sweden
Radio Technology	LTE-M / NB-IoT (Nano SIM)
Device Management	OMA LwM2M ≥1.1 over CoAP/DTLS
Cloud Platform	Sensorbee Cloud (hosted by AVSystem)
Network Interfaces	Cellular uplink to cloud backend (CoAPS)
Local Interfaces	Modbus RS-485 (M8/M12), USB-C (internal, sealed)
Firmware Update	OTA via LwM2M Object 5; USB-C serial (sealed enclosure)
Power Supply	Solar / external 5–24 VDC, 20 Ah internal battery
Enclosure	IP65 rated, tool-based disassembly required
CE Marking	CE marked (existing)

2.2 Applicable Standard Parts

Standard	Scope	RED Article	Pro2
EN 18031-1	Internet-connected radio equipment	Art. 3(3)(d)	**APPLICABLE**
EN 18031-2	Child-related data processing	Art. 3(3)(e)	NOT APPLICABLE
EN 18031-3	Financial/payment data processing	Art. 3(3)(f)	NOT APPLICABLE

EN 18031-2 and EN 18031-3 are not applicable because the Pro2 does not process child-related personal data nor financial or payment transaction data. The device's sole purpose is environmental monitoring on construction and industrial sites.

2.3 Device Classification

The Pro2 is classified as an internet-connected radio equipment endpoint. It is not network equipment: it does not route, switch, bridge, or forward network traffic for other devices. It communicates exclusively upstream to the Sensorbee Cloud platform. This classification is significant because it renders the Network Monitoring Mechanism (NMM) and Traffic Control Mechanism (TCM) requirements not applicable.

3. Compliance Overview

The following table summarises the compliance status for each EN 18031-1 mechanism category. Detailed evidence for each category is provided in Section 4.

Ref	ID	Mechanism	Applicability	Status
6.1	**ACM**	Access Control Mechanism	Applicable	✓ COMPLIANT
6.2	**AUM**	Authentication Mechanism	Applicable	✓ COMPLIANT
6.3	**SUM**	Secure Update Mechanism	Applicable	✓ COMPLIANT
6.4	**SSM**	Secure Storage Mechanism	Applicable	✓ COMPLIANT
6.5	**SCM**	Secure Communication Mechanism	Applicable	✓ COMPLIANT
6.6	**RLM**	Resilience Mechanism	Applicable	✓ COMPLIANT
6.7	**NMM**	Network Monitoring Mechanism	*Not Applicable*	N/A
6.8	**TCM**	Traffic Control Mechanism	*Not Applicable*	N/A
6.9	**CCK**	Confidential Cryptographic Keys	Applicable	✓ COMPLIANT
6.10	**GEC**	General Equipment Capabilities	Applicable	○ IN PROGRESS
6.11	**CRY**	Cryptography	Applicable	✓ COMPLIANT

Note on GEC (General Equipment Capabilities): *GEC-1 (vulnerability scanning) is an ongoing activity. An initial CVE assessment has been completed with no critical findings. Continuous monitoring is in place. All other GEC sub-requirements are compliant.*

4. Detailed Compliance Evidence

4.1 [ACM] Access Control Mechanism (EN 18031-1, Clause 6.1)

4.1.1 ACM-1: Applicability

The Pro2 manages security assets (DTLS credentials, firmware signing keys, device configuration) and network assets (LTE-M connectivity parameters, APN settings, LwM2M server URIs) that require access control. Access control mechanisms are therefore applicable and implemented.

4.1.2 ACM-2: Appropriate Access Control

Evidence:

- **LwM2M Access Control Object (ID: 2):** The LwM2M Security Object v1.1 is enabled (CONFIG_LWM2M_SECURITY_OBJECT_VERSION_1_1=y) with dual security instance support, providing per-object, per-server access control for all device resources.
- **Cloud Web Interface:** The Sensorbee Cloud provides role-based access control with distinct user roles (administrator, operator, viewer) governing access to device configuration, sensor data, and administrative functions.
- **Local Modbus Interface (M8/M12):** Access control is provided by physical proximity. These are wired RS-485 interfaces requiring direct cable connection to the device at the deployment site.
- **Internal USB-C Serial Interface:** Protected by physical access control requiring tool-based disassembly of the IP65-rated sealed enclosure. Access is limited to authorised service personnel. This provides a stronger access control boundary than the external Modbus ports.

Verdict: Compliant. Multi-layered access control spanning protocol-level (LwM2M ACL), application-level (cloud RBAC), and physical-level (sealed enclosure) mechanisms.

4.2 [AUM] Authentication Mechanism (EN 18031-1, Clause 6.2)

4.2.1 AUM-1/AUM-2: Authentication Applicability and Mechanisms

Two primary network authentication paths are implemented:

- **LwM2M DTLS-PSK Mutual Authentication:** The Pro2 authenticates to both the LwM2M bootstrap server and management server using DTLS with Pre-Shared Keys. Mutual authentication ensures both device and server verify each other’s identity before any data exchange.
- **Cloud Web Interface:** User authentication via username/password with password strength requirements enforced by the Sensorbee Cloud platform.

4.2.2 AUM-3: Authenticator Validation

DTLS handshake validates PSK credentials before establishing the secure session. Invalid or mismatched credentials result in connection rejection. The bootstrap flow (bootstrap.c) implements proper credential validation with error handling.

4.2.3 AUM-4: Changing Authenticators

- **PSK rotation:** Supported via LwM2M bootstrap (bootstrap_reset() function) and via the USB-C service menu (lwm2m_bs_psk_set.c). This enables credential rotation without physical device replacement.
- **Web interface passwords:** Users can change passwords through the Sensorbee Cloud account management interface.

4.2.4 AUM-5: Password Strength

The Sensorbee Cloud platform enforces password complexity requirements including minimum length, character diversity, and rejection of common passwords.

4.2.5 AUM-6: Brute Force Protection

DTLS has inherent protections against brute force attacks through the handshake mechanism. The cloud web interface implements rate limiting and account lockout policies.

Verdict: Compliant. Device-level DTLS-PSK mutual authentication with per-device unique credentials, complemented by cloud-level user authentication with appropriate policies.

4.3 [SUM] Secure Update Mechanism (EN 18031-1, Clause 6.3)

4.3.1 SUM-1: Update Mechanism Exists

The Pro2 provides two independent firmware update mechanisms, both enforcing identical security validation:

- **OTA (Primary):** LwM2M Firmware Update Object (Object 5) using CoAP block transfer over DTLS-secured cellular connection. Enabled via CONFIG_LWM2M_CLIENT_UTILS_FIRMWARE_UPDATE_OBJ_SUPPORT=y.
- **USB-C Serial (Service):** Internal physical interface accessible only by disassembling the sealed IP65 enclosure. Uses the same MCUboot signature validation as OTA.

4.3.2 SUM-2: Secure Updates (Integrity and Authenticity)

Evidence:

- **Secure Boot Chain:** nRF9160 ROM → MCUboot bootloader → Application firmware. Each stage verifies the cryptographic signature of the next before execution.
- **Firmware Signing:** ECDSA P-256 digital signatures (CONFIG_BOOT_SIGNATURE_TYPE_ECDSA_P256=y). Signing key: sensorbee-ec256-priv.pem. Private key held exclusively in Sensorbee's secure build infrastructure; only the public key is embedded in the device bootloader.
- **Tamper Rejection:** Both OTA and USB-C update paths route through MCUboot signature validation (CONFIG_DFU_TARGET_MCUBOOT=y). Unsigned, corrupted, or tampered firmware images are rejected regardless of the update method used.
- **Secure Boot Flag:** CONFIG_SECURE_BOOT=y (config/prj.conf:67) ensures the secure boot chain is enforced at every power cycle.

4.3.3 SUM-3: Automated Updates

The LwM2M Firmware Update Object supports server-initiated firmware campaigns. Administrators can manage update deployment schedules through the Sensorbee Cloud platform.

Verdict: Compliant. Cryptographically signed firmware with ECDSA P-256, enforced on all update paths via MCUboot secure boot chain.

4.4 [SSM] Secure Storage Mechanism (EN 18031-1, Clause 6.4)

Security and network assets stored on the Pro2 are protected using hardware-backed and physically secured storage mechanisms:

Asset	Storage Location	Protection
DTLS PSK / Identity	nRF9160 modem secure storage via modem_key_mgmt_write()	Hardware-isolated from application processor
Bootstrap Configuration	Zephyr NVS settings (lwm2m:sec subtree)	Protected by secure boot chain
SIM Credentials	SIM module secure element	Hardware secure element

Network Configuration (APN)	Zephyr NVS flash storage	Protected by secure boot, IP65 enclosure
Firmware Signing Keys	Only public key in MCUboot; private key never on device	Private key in secure build infrastructure
Buffered Sensor Data	Flash FIFO (CONFIG_FLASH_FIFO=y)	Protected by secure boot, IP65 enclosure

Verdict: Compliant. Critical credentials (DTLS PSK, SIM keys) stored in hardware-isolated secure storage. All other assets protected by secure boot chain and physical enclosure.

4.5 [SCM] Secure Communication Mechanism (EN 18031-1, Clause 6.5)

All Pro2 network communication is secured via DTLS (Datagram Transport Layer Security) as mandated by the LwM2M protocol:

Sub-Req	Requirement	Implementation Evidence
SCM-1	Applicability	All cloud communication uses DTLS-protected LwM2M over CoAPS (coaps:// URI scheme). CONFIG_LWM2M_DTLS_SUPPORT=y.
SCM-2	Integrity and Authenticity	DTLS provides message authentication codes (MAC) ensuring data integrity and origin authenticity for every packet.
SCM-3	Confidentiality	DTLS provides AES-CCM/AES-GCM encryption. Up to 5 cipher suites supported (CONFIG_LWM2M_SECURITY_DTLS_TLS_CIPHERSUITE_MAX=5).
SCM-4	Replay Protection	DTLS includes sequence numbering and anti-replay windows. Connection ID support enabled (CONFIG_LWM2M_CLIENT_UTILS_DTLS_CID=y) for mobile environments.

Local Modbus interface: The RS-485 Modbus connections (M8/M12 connectors) are local physical interfaces without network-layer encryption. This is acceptable under SCM-1 as physical proximity and direct wiring serve as the access limitation. The Modbus interface does not traverse any network boundary.

Verdict: Compliant. DTLS over LwM2M satisfies all four SCM sub-requirements for network communications. Local physical interfaces are justified by operational environment.

4.6 [RLM] Resilience Mechanism (EN 18031-1, Clause 6.6)

The Pro2 implements multiple resilience mechanisms to maintain essential monitoring functionality during adverse conditions:

- **Network Outage Resilience:** Built-in flash FIFO data buffer (CONFIG_FLASH_FIFO=y) stores sensor measurements during cellular connectivity loss. Data is automatically replayed to the cloud when connectivity is restored.
- **Power Resilience:** 20 Ah internal battery with solar charging capability ensures continued operation during external power interruptions.

- **Automatic Recovery:** The LwM2M client implements automatic reconnection logic with exponential backoff. DTLS session caching (CONFIG_LWM2M_TLS_SESSION_CACHING=y) enables efficient session resumption.
- **Protocol Resilience:** The CoAP/DTLS stack processes incoming packets through the nRF modem's network stack, which provides baseline protection against malformed packets. The Zephyr RTOS provides memory protection and task isolation.
- **Core Function Preservation:** Sensor sampling and local data logging continue independently of cloud connectivity, ensuring the primary monitoring function is maintained during any network disruption.

Verdict: Compliant. The Pro2 maintains its essential monitoring function during network disruptions through local buffering, automatic recovery, and independent sensor operation.

4.7 [NMM] Network Monitoring Mechanism (EN 18031-1, Clause 6.7)

Applicability: NOT APPLICABLE

NMM requirements apply specifically to network equipment that connects other devices to the internet (routers, gateways, switches, bridges). The Sensorbee Pro2 is an endpoint sensor device. It does not route, switch, bridge, or forward any network traffic for other devices. It communicates exclusively upstream to the Sensorbee Cloud platform using its own cellular connection. Therefore, NMM requirements are not applicable to this product.

4.8 [TCM] Traffic Control Mechanism (EN 18031-1, Clause 6.8)

Applicability: NOT APPLICABLE

TCM requirements target network equipment with traffic forwarding capabilities. The Pro2 only generates its own sensor data traffic and does not provide any traffic forwarding, NAT, or firewall services. The same rationale as NMM applies. Therefore, TCM requirements are not applicable to this product.

4.9 [CCK] Confidential Cryptographic Keys (EN 18031-1, Clause 6.9)

4.9.1 CCK-1: Appropriate CCK Protection

All confidential cryptographic keys are inventoried and protected:

- **DTLS Pre-Shared Keys:** Stored in nRF9160 modem secure storage (hardware-isolated partition) via modem_key_mgmt_write() under security tag 35724862.
- **Firmware Signing Key:** Private key (sensorbee-ec256-priv.pem, ECDSA P-256) is held exclusively in Sensorbee's secure build environment. Only the corresponding public key is embedded in the MCUboot bootloader on the device.
- **SIM Keys:** Managed by the SIM module's hardware secure element, outside the application processor's access.

4.9.2 CCK-2: Key Generation

DTLS session keys are derived during the DTLS handshake using the nRF9160 modem's cryptographic engine, which includes a hardware random number generator (HRNG) for entropy.

4.9.3 CCK-3: No Static Default CCKs

Evidence (Manufacturing Provisioning Flow):

- **Provisioning tool:** halen/configure.py executes per-device during manufacturing.

- **Per-device unique PSK:** modem_set_psk {unique_psk} → stored in modem secure storage. Each device receives a unique pre-shared key.
- **Per-device unique identity:** modem_set_identity sb_{serial} → stored in modem secure storage. Each device has a unique LwM2M endpoint name derived from its serial number.
- **No hardcoded defaults:** The device will not function without completing the manufacturing provisioning process. There are no factory-default shared credentials.
- **Credential rotation:** PSK can be changed via LwM2M bootstrap or via the USB-C service menu, ensuring credentials can be updated throughout the device lifecycle.

Verdict: Compliant. Per-device unique cryptographic credentials provisioned during manufacturing, stored in hardware-isolated secure storage, with rotation capability.

4.10 [GEC] General Equipment Capabilities (EN 18031-1, Clause 6.10)

Ref	Requirement	Status	Evidence
GEC-1	No known exploitable vulnerabilities	○ **IN PROGRESS**	Initial CVE assessment completed on nRF Connect SDK, Zephyr RTOS, TinyCrypt, and LwM2M stack. No critical vulnerabilities identified. Continuous monitoring established.
GEC-2	Limit exposed services in factory default	✓ **COMPLIANT**	Pro2 only exposes the LwM2M/CoAP endpoint over DTLS in factory default state. No debug ports, telnet, SSH, or other unnecessary network services are active.
GEC-3	Optional services enable/disable	✓ **COMPLIANT**	The REST API and PUSH API are configurable services that can be enabled or disabled by authorised administrators through the Sensorbee Cloud platform.
GEC-4	Document exposed interfaces	✓ **COMPLIANT**	All external interfaces are documented in this evidence document (Section 2) and in the product technical documentation provided to customers.
GEC-5	No unnecessary external interfaces	✓ **COMPLIANT**	All physical interfaces serve necessary functions: M8 (sensor connection), M12 (Modbus sensors), USB-C (internal service/update), power input. USB-C is internal requiring enclosure disassembly.
GEC-6	Input validation	✓ **COMPLIANT**	The CoAP/LwM2M stack (Zephyr) performs protocol-level input validation. The Modbus RTU interface validates function codes and register addresses. The nRF modem handles low-level network packet validation.

Verdict: Five of six GEC sub-requirements are compliant. GEC-1 (vulnerability management) has an initial assessment complete with continuous monitoring established. No critical vulnerabilities identified.

4.11 [CRY] Cryptography (EN 18031-1, Clause 6.11)

All cryptographic algorithms used by the Pro2 are current best practices, aligned with NIST SP 800-57 and BSI TR-02102-1 recommendations:

Function	Algorithm	Standard	Reference
Firmware Signing	ECDSA P-256	NIST approved	CONFIG_BOOT_SIGNATURE_TYPE_ECDSA_P256=y
Hashing	SHA-256 (TinyCrypt)	NIST approved	CONFIG_TINYCRYPT_SHA256=y
Message Authentication	HMAC-SHA256	NIST approved	CONFIG_TINYCRYPT_SHA256_HMAC=y
Transport Encryption	AES-128/256-CCM/GCM	NIST approved	nRF modem DTLS stack
Key Agreement	DTLS-PSK handshake	NIST approved	nRF modem crypto engine

Deprecated algorithms: No deprecated algorithms (MD5, SHA-1, DES, RC4, 3DES) are in use anywhere in the firmware. All key sizes meet or exceed minimum requirements (256-bit ECDSA, 128/256-bit AES).

Verdict: Compliant. All cryptographic primitives are current best practices with no deprecated algorithms in use.

5. Security Architecture Summary

The following diagram summarises the Pro2's security architecture layers:

Layer	Implementation
Secure Boot Chain	nRF9160 ROM → MCUboot (ECDSA P-256 verification) → Application. Signature verified at every boot.
Communication Security	All cloud communication via DTLS-encrypted CoAP (CoAPS). Bootstrap and management servers both secured.
Credential Storage	DTLS PSK and identity stored in nRF9160 modem hardware-isolated secure storage. SIM credentials in SIM secure element.
Manufacturing Provisioning	Per-device unique PSK, identity, and endpoint provisioned via halen/configure.py. No shared defaults.
Firmware Updates	OTA via LwM2M Object 5 and USB-C serial. Both paths enforce MCUboot ECDSA P-256 signature validation.
Physical Security	IP65 sealed enclosure. Internal interfaces (USB-C) require tool-based disassembly. Tamper-evident design.
Operational Resilience	20 Ah battery, flash FIFO data buffering, automatic reconnection with DTLS session resumption.

6. Declaration

Sensorbee AB hereby declares that the Sensorbee Air Pro 2 Cellular (models SB8202 and SB8203) has been assessed against EN 18031-1:2024 and meets the applicable requirements of the standard as documented in this evidence document.

This self-declaration is made in accordance with the provisions of the EU Radio Equipment Directive 2014/53/EU, Article 3(3)(d), for the protection of the network.

The security measures described in this document are maintained as part of Sensorbee's ongoing product security programme, which includes continuous vulnerability monitoring, firmware updates, and periodic reassessment.

Signed:

David Löwenbrand, CEO

Name / Title

Date:

2026-02-23

Date

Sensorbee AB

Organisationsnummer: 559118-0092

Linköping, Sweden