EELINK | SECURITY WHITE PAPER

GPT12-X Ultra

Security & Data Integrity Architecture

How the Nordic nRF9161 SiP's hardware security foundation, secure FOTA, transport encryption and tamper detection deliver a trustworthy asset tracking platform — and how GPT12-X Ultra aligns with the EU Radio Equipment Directive (RED) cybersecurity requirements and the upcoming Cyber Resilience Act.

Version 1.0 · July 2026

Shenzhen Eelink Communication Technology Co., Ltd. · www.eelinktech.com · info@eelinktech.com

1. Why Security Matters for Asset Tracking

An asset tracker is, by definition, a remote device operating without physical supervision for years at a time. It sits on a trailer chassis in a yard, inside a shipping container crossing an ocean, or under a pallet in a cold warehouse. It cannot be rebooted by an operator when something goes wrong. It cannot be physically inspected between deployment cycles. And it sends location, movement and tamper data that may be used for insurance claims, regulatory compliance, or theft recovery — contexts where data integrity is not optional.

For IoT platform brands and ODM buyers evaluating GPT12-X Ultra, three security questions dominate:

- **Can someone tamper with the firmware** to disable tracking, forge positions, or suppress alarms?
- **Can someone intercept the data in transit** to extract location patterns, customer identities, or operational intelligence?
- **Does the device meet the regulatory security requirements** for the markets where it will be deployed — particularly the EU, where cybersecurity is now mandatory for CE marking?

This white paper addresses each of these concerns by documenting the security architecture of GPT12-X Ultra at the hardware, firmware, transport and regulatory layers.

2. Hardware Security: The nRF9161 Foundation

GPT12-X Ultra is built around the Nordic Semiconductor nRF9161 System-in-Package, which integrates the LTE-M / NB-IoT modem, application MCU, and hardware security in a single package. Security is not a software add-on — it is designed into the silicon.

2.1 Security features of the nRF9161 SiP

Security feature	What it provides
Arm TrustZone	Hardware-enforced isolation between secure and non-secure execution environments on the Arm Cortex-M33 processor. Cryptographic keys, secure boot code and critical parameters run in the secure world, isolated from the application firmware. Even a compromised application cannot access secure assets.
Arm CryptoCell 310	Hardware-accelerated cryptographic engine supporting AES, SHA-256, ECC, RSA and TRNG (True Random Number Generator). Offloads cryptographic operations from the CPU for both speed and energy efficiency — critical in a battery-powered device where every milliamp counts.
Secure boot	The boot chain validates firmware integrity at every power-on before executing application code. If the firmware has been modified or corrupted, the device refuses to boot into the application. This prevents unauthorized firmware from running on the device.
Root of trust	A hardware root of trust anchored in the nRF9161 establishes the chain of trust from silicon through bootloader through application firmware. Cryptographic keys used for secure boot and FOTA verification are stored in protected memory regions that cannot be read or modified by application code.
Trusted firmware updates	Firmware images are cryptographically signed before distribution. The secure bootloader verifies the signature against the root of trust before

	applying the update. Unsigned, tampered or rollback firmware is rejected.
Secure key storage	Private keys and credentials are stored in the secure partition of the nRF9161, protected by TrustZone. They are not accessible from application code or via debugging interfaces in production devices.

> **Hardware security vs. software-only security**
> Many IoT trackers implement security entirely in software — encryption libraries, software-based key storage, and bootloaders without hardware root of trust. This approach is fundamentally weaker because a compromised OS or debugger can extract keys and modify boot code. The nRF9161's TrustZone + CryptoCell architecture provides hardware-enforced boundaries that software-only designs cannot match.

3. Transport Security: Protecting Data in Motion

GPT12-X Ultra communicates over LTE-M / NB-IoT cellular networks using the EELINK binary protocol over TCP or UDP. Multiple layers protect data between the device and the tracking platform:

3.1 Cellular network encryption

LTE-M and NB-IoT networks provide built-in over-the-air encryption between the device and the base station, using 3GPP-standardized algorithms. This protects the radio link against casual interception — but does not protect data end-to-end through the operator's core network.

3.2 Application-layer security

For end-to-end protection, GPT12-X Ultra supports TLS / DTLS encrypted connections between the device and the customer's server, using the nRF9161's built-in TLS stack and CryptoCell hardware acceleration. This ensures:

- **Confidentiality:** position, sensor and alarm data is encrypted in transit and cannot be read by intermediate network nodes.
- **Authentication:** the device authenticates the server (and optionally the server authenticates the device) using certificates, preventing man-in-the-middle attacks and rogue server redirection.
- **Integrity:** any modification of data in transit is detected and rejected.

3.3 SIM-level authentication

The SIM card (nano-SIM or eSIM/eUICC) provides an additional layer of network authentication. The device must present valid SIM credentials to attach to the cellular network; without a provisioned SIM, the device cannot transmit. For ODM programs requiring enhanced security, eSIM profiles with remote provisioning and certificate-based authentication can be integrated.

4. Secure Firmware Over-the-Air (FOTA)

Field-deployed asset trackers must be updatable — to patch vulnerabilities, add features, or adapt to new network requirements — without physical access. GPT12-X Ultra supports secure FOTA over LTE-M / NB-IoT using the nRF9161's built-in security features.

4.1 How secure FOTA works

- **Firmware images are cryptographically signed** by Eelink using keys anchored in the hardware root of trust.
- **The update is delivered over the air** via the LTE-M / NB-IoT connection at the next device check-in or on-demand via downlink command.
- **The secure bootloader verifies the signature** before applying the update. If verification fails, the update is rejected and the device continues running the previous firmware.
- **Rollback protection** prevents downgrading to older, potentially vulnerable firmware versions.
- **Dual-bank architecture** allows the new firmware to be written to a secondary partition. If the update fails or the device loses power during the process, it boots back into the previous working firmware — no bricked devices.

4.2 FOTA and battery planning

A FOTA session is a significant energy event: the device must stay awake to download, verify and flash the firmware image. For a 5000 mAh primary-battery device with multi-year life, every FOTA session must be planned. Eelink recommends budgeting FOTA energy explicitly in battery-life calculations (see the Battery Life White Paper) and limiting over-the-air updates to essential security patches and feature releases.

5. Physical Tamper Detection

Security extends beyond the digital domain. GPT12-X Ultra includes hardware sensors designed to detect physical interference:

Sensor	Security function
Light sensor	Detects enclosure opening or device removal from a concealed mounting position. A sudden change in ambient light triggers a tamper alarm that is reported to the platform immediately, even if the device was in deep sleep.
3-axis accelerometer	Detects unauthorized movement, towing, shock and impact events. Wakes the device from PSM to report the event, providing real-time notification of asset disturbance.
IP67 sealed enclosure	The sealed housing has no user-accessible battery door or external connectors (USB Type-C is for configuration/debugging only, not daily operation). This eliminates the most common physical attack vector: opening the case to remove the SIM, disable the antenna, or extract data.

Together, these sensors ensure that physical interference with the device is detected, timestamped and reported — providing an evidence trail for theft recovery, insurance claims and chain-of-custody disputes.

6. EU RED Cybersecurity Requirements

> **Mandatory since August 1, 2025**
> The EU Radio Equipment Directive (RED) Articles 3.3(d), 3.3(e) and 3.3(f) are now mandatory for internet-connected radio equipment placed on the EU market. Non-compliant devices cannot receive CE marking and cannot be legally sold in the EU. The harmonized compliance pathway is EN 18031-1/2/3:2024.

GPT12-X Ultra, as an LTE-M / NB-IoT device that connects to the internet and processes location and sensor data, falls within the scope of the RED cybersecurity requirements. The nRF9161's security architecture provides the technical foundation for compliance.

6.1 How GPT12-X Ultra's architecture maps to RED requirements

RED Article	Requirement	GPT12-X Ultra capability
Art. 3.3(d)	Network protection: device must not harm networks or cause service degradation	PSM + eDRX minimizes network resource usage. Configurable data rate and retry behavior. No always-on connection that could flood networks. LTE-M/NB-IoT standards compliance ensures coexistence. EN 18031-1 pathway.
Art. 3.3(e)	Privacy & data protection: safeguard personal data and user privacy	TLS/DTLS transport encryption. Secure key storage in TrustZone. No unnecessary data collection (device reports position, battery and sensor status only). Configurable data minimization. EN 18031-2 pathway.
Art. 3.3(f)	Fraud protection: protect against unauthorized use	Secure boot prevents unauthorized firmware. Signed FOTA with rollback protection. SIM-based network authentication. No default passwords in production devices. EN 18031-3 pathway.

Eelink manages CE RED certification — including the cybersecurity requirements — on behalf of ODM buyers. The specific EN 18031 compliance status for each GPT12-X Ultra variant is documented in the product-specific Certification & Compliance Matrix (available on request).

6.2 Key EN 18031 control areas and GPT12-X Ultra

EN 18031 control area	GPT12-X Ultra implementation
Access control	Configuration access via USB Type-C and SMS commands. SMS command authentication via authorized admin numbers. No open network services or debug ports in production firmware.
Authentication	SIM-based mutual authentication with cellular network. TLS certificate-based server authentication. Device identity via IMEI. No default or empty passwords.
Secure update mechanism	Cryptographically signed FOTA via LTE-M/NB-IoT. Dual-bank architecture for safe rollback. Rollback protection against firmware downgrade.
Secure storage	Cryptographic keys and credentials stored in TrustZone secure partition. Not accessible from application code or external interfaces.
Data minimization	Device collects and transmits only: GNSS position, cell-ID, battery status, sensor events (motion, tamper), and device state. No audio, video, biometric or personal content.
Resilience	Watchdog timer, secure boot recovery, dual-bank FOTA. Device recovers from power loss, failed updates, or transient faults without external intervention.

7. Looking Ahead: The EU Cyber Resilience Act (CRA)

The Cyber Resilience Act (Regulation (EU) 2024/2847) introduces additional cybersecurity obligations that will apply from December 2027 onward. While RED focuses on radio equipment, the CRA applies broadly to all products with digital elements sold in the EU.

Key CRA requirements relevant to IoT asset trackers include:

- **Software Bill of Materials (SBOM):** manufacturers must document all software components, including open-source libraries, and make this available to market surveillance authorities.
- **Vulnerability handling:** manufacturers must implement a coordinated vulnerability disclosure (CVD) process and provide security updates for the expected product lifetime.
- **Security by design:** products must be designed with security from the outset, not bolted on after development.
- **Ongoing support obligation:** manufacturers must provide security updates for a minimum period after placing the product on the market.

> **RED compliance today is CRA preparation**
> EN 18031 security controls are designed to align with the CRA's security-by-design philosophy. Eelink's approach — hardware root of trust, secure FOTA, access control, and data minimization — builds a compliance foundation that extends naturally to CRA requirements when they take effect. ODM buyers who build on GPT12-X Ultra inherit this foundation.

8. Security Architecture Summary

Layer	Mechanism	Threat addressed
Silicon	Arm TrustZone + CryptoCell 310 + secure boot + root of trust	Firmware tampering, key extraction, unauthorized code execution
Firmware	Signed FOTA + dual-bank + rollback protection	Malicious updates, firmware downgrade, bricked devices
Transport	TLS/DTLS + 3GPP over-the-air encryption + SIM authentication	Data interception, man-in-the-middle, rogue servers
Physical	Light sensor + accelerometer + IP67 sealed enclosure	Device removal, enclosure opening, unauthorized movement
Access	SMS admin auth + no default passwords + production debug lockdown	Unauthorized configuration, remote hijacking
Regulatory	EN 18031 (RED) pathway + CRA preparation	Market access risk, non-compliance penalties

9. What This Means for ODM Buyers

If you are building a tracking platform on GPT12-X Ultra hardware, the security architecture described in this document provides:

- **A hardware security foundation you do not need to build yourself** — TrustZone, CryptoCell, secure boot and root of trust are embedded in the nRF9161 SiP.
- **A regulatory compliance pathway for the EU market** — the architecture maps directly to EN 18031 control areas for RED Articles 3.3(d), (e) and (f).
- **A secure update mechanism for multi-year deployments** — signed FOTA with rollback protection means you can patch vulnerabilities without recalling hardware.
- **Physical tamper detection as a platform feature** — light and motion sensors provide evidence for insurance, compliance and recovery use cases.
- **CRA readiness** — the security-by-design approach positions your product for the next wave of EU regulation without a major redesign.

Eelink's engineering team can provide detailed security documentation, EN 18031 compliance evidence and certification support as part of ODM and volume evaluation programs.

10. About Eelink

Shenzhen Eelink Communication Technology Co., Ltd., founded in 2004, is an ODM manufacturer of GPS and IoT tracking hardware serving customers in 100+ countries. R&D is based in Shenzhen, with dual manufacturing sites in Yibin, China and Haiphong, Vietnam providing 500,000+ units/month combined capacity for supply chain resilience, operating under ISO 9001, ISO 14001, IATF 16949 and ISO 45001 quality systems.

GPT12-X Ultra product page: www.eelinktech.com/gpt12-x-ultra-lte-m-nb-iot-asset-tracker/

Sales and engineering inquiries: info@eelinktech.com · www.eelinktech.com/contact-us/