QORONEX LTD
Oxford, UK · 2026

BRIEF 1 · 5 MIN READ

HNDL and the Automotive Fleet: Why Your OTA Traffic Is Already Recorded

Harvest Now, Decrypt Later (HNDL) turns today's recorded, encrypted OTA/telemetry traffic into tomorrow's decryption and retroactive exposure.

The Problem Statement

"HNDL" stands for Harvest Now, Decrypt Later. Nation-state actors can record encrypted TLS traffic and other OTA-related communications today. When a Cryptographically Relevant Quantum Computer (CRQC) arrives (often discussed for a credible 2030–2035 window), those recordings become decryptable retroactively.

Firmware update traffic to vehicles is therefore a harvest target. The attacker's advantage is asymmetric: recording can be low-cost and scalable; the resulting decryption capability can be catastrophic.

Why Automotive Is Uniquely Exposed

Automotive's structure makes the HNDL exposure hard to "close out" quickly. The same encrypted traffic that looks safe today may become strategically valuable later.

• Vehicle lifetime: 10–15 years means cars sold today can still be on the road when a CRQC window becomes credible (2030–2035).

• OTA firmware updates: each update creates another harvest opportunity across the installed base.

• V2X certificate and keying material: recorded today, with decryption possible years later under CRQC capabilities.

• Provisioning ecosystems: credential and key provisioning inputs (including long-lived or replayable materials) can themselves be harvest targets.

• Fleet scale: 1 million vehicles translates into 1 million long-lived harvest targets per OEM programme.

What ECDSA P-256 and RSA Give the Attacker

If the cryptographic primitives underpinning OTA trust are based on classical public-key schemes, HNDL changes the problem from “break on first use” to “break retroactively.”

• Shor’s algorithm on a CRQC: both ECDSA P-256 verification and RSA key exchange/signing become vulnerable in polynomial time.

• ECDSA P-256 verification: harvest + later key availability can enable retroactive firmware-signature forgery for legacy vehicles.

• RSA key exchange/session material: recorded traffic can become decryptable when CRQC capabilities arrive.

• Combined outcome: an attacker can identify what firmware was present at points in time, spot security patch timing, and potentially undermine future updates for long-lived fleets.

The Regulatory Deadline You Are Already Missing

Post-quantum migration is increasingly being treated as an evidence and governance requirement, not only a cryptography roadmap.

• UNECE R155 Annex 5 requires an annual cybersecurity management review that includes cryptographic risk assessment.

• Interpreting R155 as “not applicable” to HNDL is a mistake: the threat thinking includes nation-state adversaries, and CRQC capability (2030–2035) is the relevant forward-looking capability.

• BSI TR-03116 explicitly calls out the PQC migration timeline; if your annual review does not mention PQC, your posture may be non-compliant.

What to Do (Evidence-First, Not Panic-First)

You do not need a full “rewrite everything” plan to create momentum. You need an auditable posture that treats HNDL as a lifecycle exposure and aligns cryptographic risk thinking with the realities of 2030–2035 CRQC capability.

• Assess where classical cryptography (e.g., ECDSA/RSA primitives) sits in your OTA and trust pathways and what that implies for retroactive exposure.

• Translate that exposure into a phased, programme-level evidence narrative suitable for UNECE R155 annual review scrutiny.

• Engage a structured partner that can help translate your fleet reality into governance-grade outputs.

QORONEX can deliver this as a structured engagement. Start with a cryptographic footprint assessment of your ECU firmware fleet. For enquiries, please contact info@qoronex.co.uk.

QORONEX LTD · Oxford, UK · info@qoronex.co.uk