Radio Equipment Directive (RED)

Am 30. Januar 2025 hat die Europäische Kommission die EN 18031-Serie offiziell im Amtsblatt der Europäischen Union unter der Funkanlagenrichtlinie **(RED – Radio Equipment Directive)** gelistet.

Diese Normenreihe wurde entwickelt, um Herstellern von Funkanlagen einen harmonisierten Standard zur Erfüllung der ab dem **1. August 2025 verbindlichen Cybersicherheitsanforderungen** bereitzustellen.

Was ist die EN 18031?

Die EN 18031-Serie umfasst drei Teile, die spezifische Sicherheitsanforderungen für verschiedene Arten von Funkanlagen festlegen:

- EN 18031-1: Bezieht sich auf mit dem Internet verbundene Funkanlagen und adressiert den Schutz vor Netzwerkschäden und Dienstleistungsbeeinträchtigungen.
- EN 18031-2: Deckt Funkanlagen ab, die Daten verarbeiten, einschließlich Geräte für die Kinderbetreuung, Spielzeug und tragbare Geräte, mit Fokus auf den Schutz personenbezogener Daten und der Privatsphäre der Nutzer.
- EN 18031-3: Richtet sich an internetfähige Funkanlagen, die virtuelle Währungen oder monetäre Werte verarbeiten, und legt Maßnahmen zur Betrugsprävention fest.

Tel.: 0212 710 55
Fax: 0212 765 43
www.heitland-gmbh.de
info@heitland-gmbh.de

Radio Equipment Directive (RED)

Was ist die RED-Richtlinie?

Der delegierte Rechtsakt erweitert die bestehende Funkanlagenrichtlinie, um die Cybersicherheit für vernetzte Produkte abzudecken, die in der EU verkauft werden, einschließlich solcher, die sich indirekt über ein anderes Gerät verbinden.

Die RED-Richtlinie bildet einen verbindlichen Rahmen für alle elektrischen und elektronischen Geräte, die Funkwellen nutzen. Diese Geräte müssen unter anderem strenge Anforderungen in Bezug auf elektrische Sicherheit, elektromagnetische Verträglichkeit (EMV) und die effiziente Nutzung des Funkspektrums erfüllen.

Diese Änderungen dienen dem Schutz von Menschen, Gebäuden und Netzwerken, um sicherzustellen, dass nur sichere und vertrauenswürdige Geräte online zugelassen werden.

Hinweis: Nicht alle drei Vorschriften gelten für jedes Produkt. Die Abdeckung hängt davon ab, wie sich das Gerät verbindet und welche Art von Daten es verarbeitet.

Die RED bezogen auf Ultraschallwasserzähler

Die neuen Cybersicherheitsanforderungen hier sehr interpretationsbedürftig, und es gibt keine festgelegten Vorgehensweisen.

Es heißt lediglich, dass der interne Speicher des Zählers sicher sein muss. Es gibt diverse Möglichkeiten, dies zu gewährleisten. Der Richtlinie ist flexibel gestaltet und schreibt keine bestimmte technische Lösung vor. Stattdessen definiert sie Sicherheitsmechanismen (z. B. Verschlüsselung, Zugriffskontrollen) und bietet Leitlinien und Bewertungskriterien an. Das bedeutet, dass Hersteller selbst entscheiden können, wie sie die entsprechend notwendige Sicherheit im Produkt implementieren, solange diese die erforderlichen Sicherheitsziele erfüllen. Grundsätzlich ist es sehr schwierig zu überprüfen, ob ein Produkt tatsächlich RED-konform ist, da eine Konformitätserklärung im Zusammenhang mit der CE-Kennzeichnung ausreicht. Nur durch Audits eigenständiger Dritte, kann das bestätigt werden.

Um das komplette Spektrum etwas mehr zu verdeutlichen haben wir im Folgenden einige Punkte näher ausgeführt:

Tel.: 0212 710 55
Fax: 0212 765 43
www.heitland-gmbh.de
info@heitland-gmbh.de

Radio Equipment Directive (RED)

Die wichtigsten Punkte
Anforderungen an Geräte (allgemein) gemäß EN 18031-1:

Zugriffskontrolle:
- Geräte müssen den Zugriff so beschränken, dass nur autorisierte Benutzer sie nutzen können.
- Standardmäßige, einfache Passwörter (wie „admin“ oder „1234“) sind nicht zulässig.
- Benutzer müssen ein Passwort festlegen und verwenden. Wenn ein Gerät die Nutzung ohne Passwort zulässt, ist dies ein Verstoß gegen die Norm.

Authentifizierung:
- Das Gerät muss überprüfen, ob die Person, die darauf zugreift, tatsächlich diejenige ist, für die sie sich ausgibt (d. h. ordnungsgemäße Authentifizierung).

Sichere Firmware-/Software-Updates:
- Das System muss sichere Software-/Firmware-Updates unterstützen, um schädliche Updates zu verhindern.
- Updates sollten so durchgeführt werden, dass die Integrität erhalten bleibt (d. h., Angreifer können sie nicht manipulieren).

Sichere Speicherung:
- Alle sensiblen Daten (z. B. Zugangsdaten, kryptografische Schlüssel), die auf dem Gerät gespeichert sind, müssen geschützt werden.
- Verwenden von Verschlüsselung oder andere Mechanismen, um die Daten zu schützen, solange diese auf dem Gerät gespeichert sind.

Sichere Kommunikation:
- Über ein Netzwerk gesendete Daten müssen geschützt sein (Vertraulichkeit, Integrität).
- Es muss ein Schutz vor Replay-Angriffen vorhanden sein (d. h. Angreifer dürfen keine alten Nachrichten abfangen und erneut senden können, um das Gerät zu täuschen).
- Verwenden von für die Kommunikation bewährte kryptografische Protokolle („Best Practices“).

Ausfallsicherheit:
- Das Gerät muss netzwerkbasierten Angriffen wie DoS (Denial of Service) widerstehen und sich davon erholen können.
- Es sollte Mechanismen zur Erkennung und Abwehr von Überlastungs- oder Missbrauchsversuchen seiner Netzwerkfunktionen besitzen.

Netzwerküberwachung:
- Der Netzwerkverkehr muss überwacht werden, um mögliche Angriffsmuster (z. B. Anzeichen eines DoS-Angriffs) zu erkennen.
- Es sollten Mechanismen vorhanden sein, die bei Erkennung verdächtigen Datenverkehrs Alarm schlagen oder reagieren.

Tel.: 0212 710 55
Fax: 0212 765 43
www.heitland-gmbh.de
info@heitland-gmbh.de

Radio Equipment Directive (RED)

Verwaltung kryptografischer Schlüssel
- Die vom Gerät verwendeten Schlüssel (z. B. zur Verschlüsselung) müssen sicher verwaltet werden.
- Das Gerät sollte „schwache“ oder standardmäßige kryptografische Schlüssel vermeiden, die leicht zu erraten sind.

Geräte Sicherheit / Allgemeine Sicherheit:
- Unnötige „offene“ Dienste oder Schnittstellen einschränken; nicht benötigte Dienste deaktivieren.
- Alle Eingaben (z. B. Daten aus dem Netzwerk) validieren, um das Risiko von Sicherheitslücken zu minimieren.
- Sicherheitslücken regelmäßig beheben (d. h. einen Plan zur Behebung entdeckter Sicherheitslücken bereithalten).

Protokollierung:
- Das Gerät sollte wichtige Sicherheitsereignisse protokollieren.
- Die Protokolle sollten dauerhaft gespeichert und mit einem Zeitstempel versehen sein, um Untersuchungen und Audits zu erleichtern.

Verfahren für Kryptografie:
- Verwenden von starken, aktuellen kryptografischen Algorithmen.
- Sicherstellen, dass kryptografische Operationen korrekt implementiert sind (keine Hintertüren oder schwache Standardeinstellungen).

Sicherheit von Anfang an im Design berücksichtigen („Secure by Design“):
- Sicherheit sollte von Beginn an integriert sein: Hersteller sollten bei der Geräteentwicklung Sicherheit in Hardware, Firmware, Lieferkette usw. einbeziehen.
- Mehrschichtige Sicherheitsvorkehrungen treffen: Mehrere Sicherheitsmaßnahmen kombinieren, nicht nur auf eine einzige setzen.

Geräte mit Internetzugang

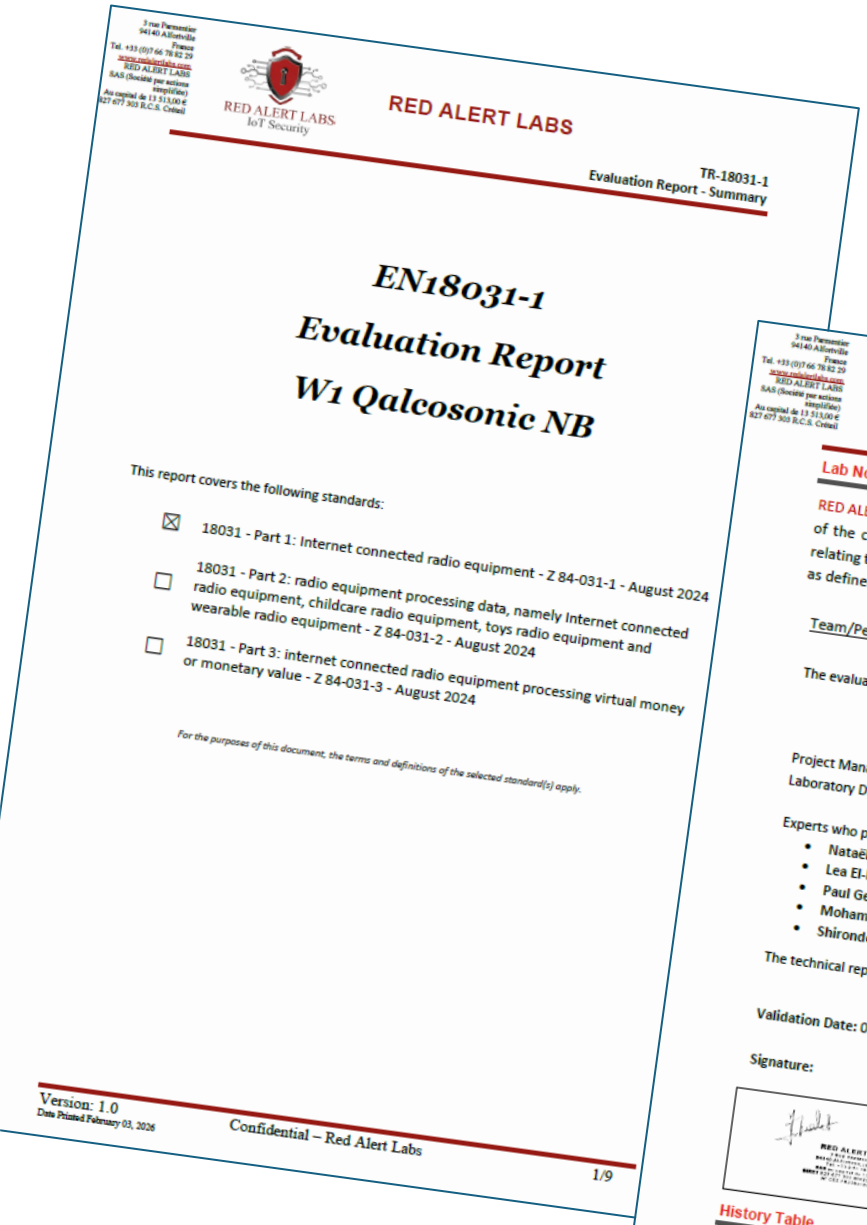
Diese Richtlinie gilt generell für Geräte mit Internetzugang. Das erschwert die Interpretation zusätzlich, da nicht vollumfänglich beschrieben wird, wie und wann ein Zugang zum Internet vorliegt. NB-IoT und LoRa sind theoretisch solche Zugänge, wMBus möglicherweise auch. Alles abhängig von der jeweiligen Infrastruktur. Es gibt viele Diskussionen darüber, aber wir (AXIOMA) hat bereits zahlreiche Maßnahmen zur Einhaltung der Richtlinie in den Ultraschallwasserzählern umgesetzt bzw. Implementiert.

In den entsprechenden CE-Erklärungen der Zähler bestätigen wir (AXIOMA) die Konformität entsprechend u.a. den Richtlinien:

(EU) 2022/30
EN 18031-1:2024

Tel.: 0212 710 55
Fax: 0212 765 43
www.heitland-gmbh.de
info@heitland-gmbh.de

Radio Equipment Directive (RED)



RED ALERT LABS
IoT Security

RED ALERT LABS

TR-18031-1
Evaluation Report - Summary

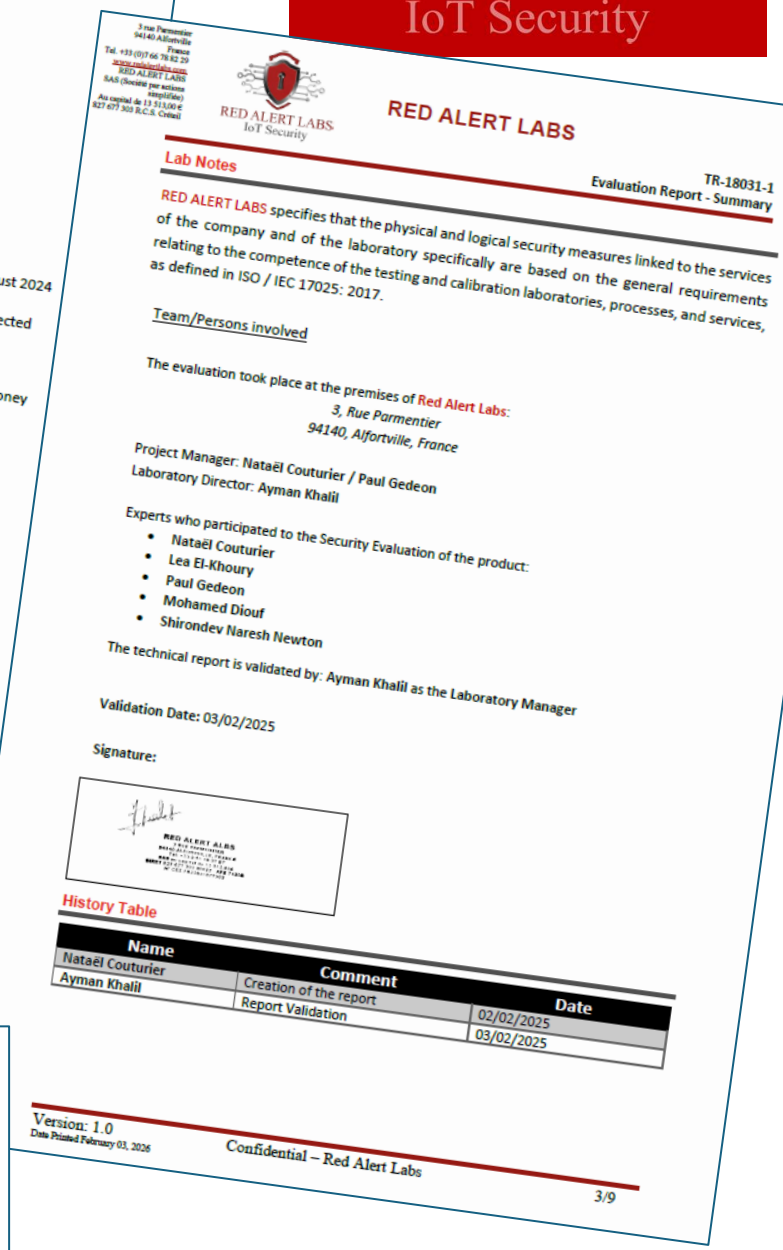
EN18031-1
Evaluation Report
W1 Qalcosonic NB

This report covers the following standards:

- ☒ 18031 - Part 1: Internet connected radio equipment - Z 84-031-1 - August 2024
- ☐ 18031 - Part 2: radio equipment processing data, namely Internet connected radio equipment, childcare radio equipment, toys radio equipment and wearable radio equipment - Z 84-031-2 - August 2024
- ☐ 18031 - Part 3: internet connected radio equipment processing virtual money or monetary value - Z 84-031-3 - August 2024

For the purposes of this document, the terms and definitions of the selected standard(s) apply.

Version: 1.0
Date Printed February 03, 2026
Confidential – Red Alert Labs
1/9



RED ALERT LABS

TR-18031-1
Evaluation Report - Summary

Lab Notes

RED ALERT LABS specifies that the physical and logical security measures linked to the services of the company and of the laboratory specifically are based on the general requirements relating to the competence of the testing and calibration laboratories, processes, and services, as defined in ISO / IEC 17025: 2017.

Team/Persons involved

The evaluation took place at the premises of Red Alert Labs:
3, Rue Parmentier
94140, Alfortville, France

Project Manager: Nataël Couturier / Paul Gedeon
Laboratory Director: Ayman Khalil

Experts who participated to the Security Evaluation of the product:
- Nataël Couturier
- Lea El-Khoury
- Paul Gedeon
- Mohamed Diouf
- Shirondev Naresh Newton

The technical report is validated by: Ayman Khalil as the Laboratory Manager

Validation Date: 03/02/2025

Signature:

History Table

Name	Comment	Date
Nataël Couturier	Creation of the report	02/02/2025
Ayman Khalil	Report Validation	03/02/2025

Version: 1.0
Date Printed February 03, 2026
Confidential – Red Alert Labs
3/9

This report is a summary of both conceptual tests and functional tests. The detailed analysis of each part can be found in the attached report:

- TR-18031-1- Conceptual – W1 Qalcosonic NB
  - *[Annex 1] TR-18031-1 - Conceptual* – W1 Qalcosonic NB – *Version 3.0*
- TR-18031-1- Functional – T91WC
  - *[Annex 2] TR-18031-1&2 - Functional* – W1 Qalcosonic NB – *Version 1.0*

Evaluator Verdict on the conceptual evaluation	PASS
Evaluator Verdict on the functional evaluation	PASS
Final Evaluator Verdict against EN18031-1.	PASS