Document reference: SSD-EN18031-002 (revision 2)
Issue date: 03 November 2026
Supersedes: SSD-EN18031-001 of 23 July 2025

SOFTWARE SECURITY DECLARATION

Directive 2014/53/EU (RED) Article 3(3)(d) – EN 18031-1:2024

Software provider: MESHLE GmbH, Parkstr. 42, 47877 Willich, Germany · Contact: info@meshle.com, +49 2154-9304-690

Software	MESHLE firmware, version 2.1.x, in the current release provided by MESHLE (via the MESHLE App, MESHLE Gateway or MESHLE firmware portal), and subsequent updates that do not change the security architecture or security-relevant mechanisms
Hardware	Raytac MDBT50Q-1MV2 radio module, based on the Nordic Semiconductor nRF52840 SoC
Brand name	MESHLE

Scope

- This declaration covers the MESHLE firmware on the hardware specified above. It supports, but does not replace, the conformity assessment of the manufacturer of the end product (OEM).
- It addresses Article 3(3)(d) of Directive 2014/53/EU (protection of the network) as specified by EN 18031-1:2024. Where the end product falls within the scope of Article 3(3)(e) of Directive 2014/53/EU, EN 18031-2:2024 may be relevant to the OEM's conformity assessment. The security measures described below may support that assessment. Article 3(3)(f) and EN 18031-3:2024 (financial transactions) do not apply to lighting control applications.
- This document is not an EU declaration of conformity and does not cover other essential requirements of the RED (Article 3(1) and 3(2)). Raytac provides the radio module and its associated regulatory documentation. The manufacturer of the finished radio equipment remains responsible for its conformity assessment under the applicable RED requirements.

1. Authentication and access control

- No fixed, universal or hard-coded default credentials are used
- Device onboarding requires authenticated commissioning procedures
- Access control mechanisms restrict operations to authorized entities
- Unauthorized access attempts are rejected by design

2. Secure communication

- Security-relevant communication is encrypted
- Integrity and authenticity of communicated data are ensured
- Device-specific cryptographic material is used

3. Secure software and firmware updates

- Software and firmware updates are cryptographically verified by the bootloader
- Unauthorized or modified updates are rejected
- Installation of unauthenticated software is prevented

4. Network exposure

- No unnecessary network services or open ports are exposed
- Communication interfaces are limited to required operational functions
- Debug or test interfaces are disabled in production use

Vulnerability reporting

Security vulnerabilities can be reported to security@meshle.com. Further information on security, updates and support period: meshle.com/compliance

Conditions

This declaration is valid only if the software is used without modification to security-relevant components, is programmed as described in the MESHLE integration documentation, and the integration follows that documentation.

Declaration

We declare that the software listed above, on the hardware specified, implements security measures intended to meet the requirements of EN 18031-1:2024 under Article 3(3)(d) of Directive 2014/53/EU, within the defined scope. Where the end product falls within the scope of Article 3(3)(e), these measures may also support the assessment under EN 18031-2:2024.

Willich, 03 November 2026



Nikolay Patrikeev
CEO