RED 3.3 IOE for Renesas Wi-Fi Devices

Date: 27 March 2026

Renesas has asserted the compliance of its Wi-Fi products:

Technology	Product Name
Wi-Fi	RA6W1 Arm® Cortex®-M33-based Dual Band Wi-Fi 6 SoC
Wi-Fi	DA16200 Ultra-Low Power Wi-Fi SoC for Battery-Powered IoT
Wi-Fi / BT	RA6W2 Arm® Cortex®-M33-based Dual Band Wi-Fi 6 & BT LE SoC

with the following:

Essential requirements **Radio Equipment Directive 2014/53/EU**	**Standards**
Network Harm (Article 3.3d)	ETSI EN 18031-1 (2024)
Personal Privacy (Article 3.3e)	ETSI EN 18031-2 (2024)

that was based on the IOE (Intended Operating Environment) defined below.

Renesas provides more detailed guidance in the form of a “Cybersecurity Integration Guide” that can be provided on request.

Intended Operating Environment:

- Renesas devices are intended to be used in internet connected devices.
- Renesas device is used in an end-product (the “Product”) and is placed on a Printed Circuit Board according to the provided Instructions by Renesas
- The Product is included in an enclosure or otherwise sealed, to prevent direct access by unauthorized users
- The Product application is developed using the latest released SW development kit (SDK) provided by Renesas
- The Product fall within the scope of RED articles 3.3d, 3.3e as defined in Commission Delegated Regulation (EU) 2022/30 of 29 October 2021

- When used in Network Equipment such as routers and access points, additional cybersecurity mechanisms may be required, as deemed necessary by the specifics of each application.
- If provisioning is achieved by the device acting as a temporary Wi-Fi access point, the user’s identity must be ensured by physical or other technical means.
- During phase 1 authentication, wpa_supplicant must be configured to verify the network's TLS certificate.
- Product keys must be securely managed during design, testing, production and market deployment.
- The device Development Kit is intended for evaluation and product development. In the default configuration some protection mechanisms are not enabled to allow debugging and testing. It must not be connected to an internet connected Wi-Fi network unless all relevant cybersecurity protection mechanisms are enabled.