SOLIDWARETOOLS

CRACheck

DOCUMENT 2

Technical Documentation

Art. 31 + Annex VII

NovaBridge Technologies Inc.

NovaBridge SmartHub v3.1

Reference: CRACHK-Y8IV87
Date of issuance: 15/10/2026
Contact: Sarah Chen, VP of Compliance
compliance@novabridge.io

Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 (Cyber Resilience Act)

This document does not constitute legal advice. Sole responsibility of the manufacturer.

1 GENERAL PRODUCT DESCRIPTION (Annex VII, point 1)

INTENDED PURPOSE [Annex VII, 1(a)]

WiFi/Zigbee smart home hub for centralised control of smart home devices (lights, smart locks, security cameras, motion and temperature sensors). Includes iOS/Android mobile app and cloud backend (AWS eu-west-1) for remote access and push notifications. Intended for residential consumers in the EU, sold through Amazon.de, Amazon.fr and Amazon.es.

SOFTWARE VERSION [Annex VII, 1(b)]

3.1.0

PRODUCT TYPE

Hardware + software (IoT device, connected appliance, etc.)

REMOTE DATA PROCESSING

Yes — The product relies on a manufacturer cloud/backend service

DETAIL

Cloud backend on AWS (eu-west-1) for: remote access to the hub via mobile app, configuration and scene storage, OTA update distribution, push notifications for security events. Without this backend, remote control and notifications do not work (local control via Zigbee does work).

USER INFORMATION [Annex VII, 1(d)]

See Document 4 — User Information and Instructions

This document does not constitute legal advice. Sole responsibility of the manufacturer.

2 DESIGN, DEVELOPMENT, PRODUCTION AND VULNERABILITIES (Annex VII, point 2)

2(a) Design and development

The system architecture and the description of how software components are integrated are detailed in the risk assessment (Document 3) and in the responses to the essential requirements of Annex I.

2(b) Vulnerability management

SBOM [Annex VII, 2(b)]

Yes — SBOM generated and maintained — Format: CycloneDX — Top-level dependencies: 47

CVD POLICY [Annex VII, 2(b)]

Coordinated disclosure policy published at https://www.novabridge.io/security/cvd-policy. Reporting channel: security@novabridge.io + HTTPS web form. Commitment to acknowledgement within 48 business hours. Target remediation time: 90 days from vulnerability confirmation. Coordinated public disclosure after patch availability. Active bug bounty programme on HackerOne (https://hackerone.com/novabridge) with $100-$5,000 rewards based on CVSS severity.

VULNERABILITY CONTACT [Art. 13.17]

security@novabridge.io · https://www.novabridge.io/security · +1 302 555 0142 (EST hours)

SECURE UPDATE DISTRIBUTION [Annex VII, 2(b)]

OTA (Over-The-Air) with Ed25519 digital package signing. TLS 1.3 end-to-end encrypted channel. Firmware integrity verification (SHA-256) before and after installation. Automatic rollback to previous firmware in case of verification failure. Security updates separated from functional ones whenever technically feasible. Each security update remains available for download for a minimum of 10 years (Art. 13.9).

2(c) Production and monitoring

The production processes, quality control and continuous monitoring are the responsibility of the manufacturer. Verification measures include the security tests documented in point 6 of this technical documentation.

3 CYBERSECURITY RISK ASSESSMENT (Annex VII, point 3)

The complete risk assessment pursuant to Art. 13.2-4, including the mapping against the essential requirements of Annex I, is found in Document 3 (Cybersecurity Risk Assessment) of this dossier.

4 SUPPORT PERIOD (Annex VII, point 4)

SUPPORT PERIOD [Art. 13.8]

5 years — until 03/2031

JUSTIFICATION [Annex VII, point 4]

5-year period based on: (1) expected lifetime of a smart home hub according to market studies (Consumer Technology Association: 5-7 years for smart home devices); (2) consistency with support periods for similar products on the market (Google Nest Hub: 5 years, Amazon Echo: 4 years, Samsung SmartThings: 5 years); (3) availability of the operating environment (Android/iOS support devices for ~5 years); (4) support periods of comparable products on the market.

5 APPLIED STANDARDS AND SPECIFICATIONS (Annex VII, point 5)

APPLIED STANDARDS [Art. 27]

ETSI EN 303 645 v2.1.1 (2020-06): Cyber Security for Consumer Internet of Things — applied in full. ISO/IEC 27001:2022: Information security management system — certification in progress (audit in progress). IEC 62443-4-1:2018: Secure product development lifecycle — applied to the development process. NIST SP 800-183: Networks of Things — used as reference for IoT security architecture. No CRA (Reg. 2024/2847) harmonised standards published in the OJEU as of the date of this dossier.

6 TEST REPORTS (Annex VII, point 6)

SUMMARY OF TESTS PERFORMED [Annex VII, point 6]

(1) External penetration test — NCC Group, report ref: NCG-2026-0412, date: 15/03/2026. Result: 0 critical vulnerabilities, 1 medium (fixed in v3.1.0-patch2), 3 informational. (2) Static code analysis — SonarQube v10.4, last run: 01/04/2026. Result: 0 critical bugs, 0 vulnerabilities, 2 minor code smells. (3) Dependency scan — Snyk, last audit: 20/04/2026. Result: 0 known CVEs in direct dependencies, 47 total dependencies scanned. (4) MQTT protocol fuzzing — AFL++ v4.09c, 72h execution. Result: 0 reproducible crashes.

7 EU DECLARATION OF CONFORMITY (Annex VII, point 7)

See Document 5 of this dossier — EU Declaration of Conformity pursuant to Art. 28 and Annex V.

8 SBOM — SOFTWARE BILL OF MATERIALS (Annex VII, point 8)

The manufacturer maintains the SBOM in CycloneDX format, covering 47 top-level dependencies. It is provided upon reasoned request from the market surveillance authority, pursuant to Annex VII, point 8.

This document has been generated by CRACheck (SolidwareTools) from the information provided by the manufacturer. It does not constitute legal advice or a third-party audit. The accuracy of the data and effective compliance with applicable legal

obligations are the sole responsibility of the manufacturer. The structure follows Regulation (EU) 2024/2847 as reviewed by SolidwareTools at the date of issuance. For personalised advice, consult a qualified professional.