Statement of Compliance for the Cybersecurity Label

Structure and Directions

The goal of this form is to provide information on the security of an IoT product to NCSC-FI as well as technically inclined users. The form is published as a part of a consumer material kit when a label is granted.

Chapter 1 lists general information of the IoT product and the surrounding ecosystem such as mobile applications and cloud services provided by the vendor or third parties. The sections of chapter 2 list security threats that are relevant to consumers as well as security requirements that, when met, mitigate these threats. Where possible, the requirements are accompanied by tables that may be used as part of the response. Some descriptive texts for describing the security posture of the product are suggested.

The ETSI references within the text are related to provisions in the standard ETSI TS 303 645 "CYBER; Cyber Security for Consumer Internet of Things". The final draft (v2.1.0, 2020-04) is available at https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.00_30/en_303645v020100v.pdf.

Contact Information

Company name:	Ruuvi Innovations OY
Business ID:	FI27499438
Contact person:	[Redacted]
Email:	[Redacted]
Telephone number:	[Redacted]

Send your application to tietoturvamerkki@traficom.fi

- Bluetooth environmental sensor beacon RuuviTag, firmware version 2.5.9
- Mobile application Ruuvi Station for viewing the data.

1. Product Description

Describe the product or product family (the "Product") under application, along with ecosystem provided by the vendor or third parties (the "Service") that is relevant for core functionalities of the Product.

1.1. Support Period

The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period (ETSI 5.3-13). Specify the support period and describe how the information can be accessed.

Support for hardware, firmware and applications is available until end of 2025. https://ruuvi.com/terms/lifecycle/ .

1.2. Security Guidance

The manufacturer should provide users with guidance on how to securely set up their device (ETSI 5.12-2). Specify where the security guidance is available in Finnish.

There’s no specific setup steps, not applicable.

1.3. Other Certifications

Specify other certifications and requirements the product fulfills. As an example, the product has a CE marking and/or FCC label; the product is has certification X (e.g. the UK security label, provide link); the service components of the product have been verified by Y (provide link); have certification

- CE, FCC, IP67, ISED, RoHS, RTCA DO-160G, TELEC - All certificates are available at https://github.com/ruuvi/certifications

Z (e.g. the STAR certification from the Cloud Security Alliance, provide link).

2. Protections Against Common IoT Threats

The Product has protections for common IoT threats as described by the following sections.

2.1. Weak, Guessable, or Hardcoded Passwords

Requirement regarding passwords is as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compli-
Where passwords are used and in any state other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user (ETSI 5.1-1).	☐	☒	☐	☐

Describe how the Product is protected against the threats caused by weak or hardcoded passwords. As an example, if the threat is compensated by using security controls beyond identification, or if user identification does not use passwords, describe how the resulting security level is equal to using strong and unique passwords.

Security of RuuviTags is based on requirement of physical proximity to devices. To update firmware or change operation mode of RuuviTag, user must press physical button on device.

2.2. Use of Insecure or Outdated Components

Requirement regarding insecure or outdated components are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compli-
When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates (ETSI 5.3-2).	☒	☐	☐	☐
An update shall be simple for the user to apply (ETSI 5.3-3).	☒	☐	☐	☐
Updates shall be timely (ETSI 5.3-8).	☒	☐	☐	☐
The manufacturer should inform the user in a recognizable and apparent manner that a security update is required together with information on the risks mitigated by that update (ETSI 5.3-11).	☒	☐	☐	☐
The manufacturer shall make a vulnerability disclosure policy publicly available (ETSI 5.2-1).	☒	☐	☐	☐
Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period (ETSI 5.2-3).	☒	☐	☐	☐

Describe how the Product and Service are protected against the threat of insecure or outdated components. As an example, describe how vulnerability follow-up is performed throughout the supply chain for all the components, including operating systems, network services and software libraries. Describe how timeliness, ease of installation, quality control and secure transfer and installation is ensured in updates of the Product. Typical update cycles range from 30 to 90 days, though this may vary greatly depending on the nature of the product.

On RuuviTags, this requirement is not applicable. On Ruuvi Station, both iOS and Android applications are scanned monthly with OWASP dependency check for vulnerable components.

New releases update libraries, typically a bugfix release goes from implementation to end users in 6-8 weeks and gets distributed by app stores. A critical security update could be pushed as soon as Apple review team approves update, typically few days. On Android, the update can be pushed immediately after development.

2.3. Insufficient Privacy Protection

Requirement regarding privacy protection is as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compli-
The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers (ETSI 6.1).	☒	☐	☐	☐

Describe how it is ensured that the handling and storage of personally identifiable information (PII) within the Product and the Service is performed in a manner that is transparent to the user and limited to the extent necessary for providing the functionality.

- RuuviTags are not connected to Internet.
- Ruuvi Station sends data only if user opts in to configure a gateway feature.
- Analytics, such as install and crash metrics are anonymized.
- Privacy policy is available at https://ruuvi.com/terms/privacy/

You can describe the personally identifiable information (PII) in the following table. Listing the PII will help in their evaluation.

PII	**Product/Service/ Component**	**Purpose**	**Data Processor**
Email	Forum	Notificiations, account creation	Digital Ocean
Address, phone number, email	Shop	Product delivery	SiteGround
Email	Station	Feedback, bug reports	Google

2.4. Insecure Data Transfer and Storage

Requirements regarding data transfer and storage are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compli-
Sensitive security parameters in persistent storage shall be stored securely by the device (ETSI 5.4-1).	☐	☒	☐	☐
The consumer IoT device shall use best practice cryptography to communicate securely (ETSI 5.5-1).	☐	☒	☐	☐
The manufacturer shall follow secure management processes for critical security parameters that relate to the device (ETSI 5.5-8).	☐	☒	☐	☐

Describe how the Product and the Service, as well as the communication between the Product and the Service, are protected against the threats caused by lacks in data encryption and access control. For protecting passwords, this typically includes the usage of hash functions.

Data is protected by requiring physical proximity to the device, there's no passwords or other similar sensitive information.

2.5. Insecure Network Services and Ecosystem Interfaces

Requirements regarding network services and ecosystem interfaces are as follows. State the compliancy for each requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compli-
Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication (ETSI 5.5-5).	☐	☒	☐	☐
All unused network and logical interfaces shall be disabled (ETSI 5.6-1).	☒	☐	☐	☐
Software should run with least necessary privileges, taking account of both security and functionality (ETSI 5.6-7).	☒	☐	☐	☐
The consumer IoT device software shall validate data input via user interfaces or transferred via Application Programming Interfaces (APIs) or between networks in services and devices (ETSI 5.13-1).	☒	☐	☐	☐

Describe how the Product is protected against the threats caused by the vulnerabilities in the exposed network services such as web interfaces and remote management. Also consider the used radio interfaces.

Describe how the exposed network interfaces in the Service, are protected against threats such as unauthorized access and breaches of confidentiality. These interfaces are typically related to functionalities such as the cloud-based data storage and management of the Product.

- RuuviTag: Updating firmware requires physical access
- Ruuvi Station: Sending in-application push messages to users require 2-FA authentication, only one person has access. Weather API exposes only position data without name, email, tracking ID or other identifiable information.

You can use the following table in your response to sections 2.4 and 2.5. Listing the tools and methods used to test the Product and the Service will help in their evaluation.

Network port / Radio technology	**Encryption / access control**	**Usage**
Bluetooth - DFU update	Public key cryptography	Update signing
Bluetooth - Data transfer	None	Data transfer
Weather API	HTTPS	Displaying local conditions without physical sensor
Gateway function	User selectable	Logging sensor data to user backend.
Push messages	HTTPS	Advertising, security updates

2.6. Insecure Default Settings

Requirement regarding insecure default settings is as follows. State the compliancy for the requirement using the checkboxes.

	Compliant	Not applicable	Uncertain	Not compli-
Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability (ETSI 5.12-1).	☒	☐	☐	☐

Describe how the Product and the Service are protected against the threats caused by insecure factory or default settings. Also describe how the user is guided to maintain a secure configuration.

There’s no settings to configure for security.