Compliance statement 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:	Finnish institute for health and welfare

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.

Koronavilkku is a contact tracing app to help citizens find out whether they may have been exposed to coronavirus. Koronavilkku is both Android and iOS app with a backend server. Koronavilkku also utilizes Omaolo medical device software for contacting public health care.

The source codes of the mobile applications as well as backend server have been publishes as open source.

TRAFICOM
Finnish Transport and Communications Agency

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 time is between 2020-08-31 and 2021-12-31 as required by Finnish law Tartuntalautilaki.

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.

Tietoturva specifically

1.3 Other Certifications

Specify other certifications are requirements the product fulfills. As an example, the product has a CE marking and/or FCC label; the product 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 Z (e.g. the STAR certification from the Cloud Security Alliance, provide link).

Not applicable

2 Protections Against Common IoT Threats

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

TRAFICOM
Finnish Transport and Communications Agency

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 compliant
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.

Instead of passwords system uses Rotating Proxomity Identifiers (RPIs) and Temporary Exposure Keys (TEK). RPIs are random IDs derived from TEKs and generated every 10-20 minutes. TEKs are randomly generated keys every 24 hours.

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.

TRAFICOM
Finnish Transport and Communications Agency

	Compliant	Not applicable	Uncertain	Not compliant
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.

Automatic OWASP dependency check run daily. Manual follow-up on software library vulnerabilities. Email channel for security issues. Collaboration with Apple and Google. Possibility to publish a new release in a few days.

2.3 Insufficient Privacy Protection

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

TRAFICOM
Finnish Transport and Communications Agency

	Compliant	Not applicable	Uncertain	Not compliant
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.

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

No sensitive personal information is stored. Rotating Proximity Identifiers (RPIs) are protected in OS level and cannot be accessed by the software. Temporary Exposure Keys (TEK) can only be retrieved from OS with a pin code provided by a certified health care professional when the user has been tested positive of COVID-19 virus. The user is asked for an explicit permission to submit the TEKs to the back-end server. Access to back-end server and its database is highly restricted and data is automatically deleted after 21 days.

PII	Product/Service/ Component	Purpose	Data Processor
Rotating Proximity Identifiers	Google/Apple Exposure Notification System (ENS)	Tracing encounters of devices using Bluetooth low energy (BLE) technology	Mobile device operating system only
Temporary Exposure Keys	ENS / Koronavilkku	To report a verified infection and allow other users to identify possible exposures to the virus.	ENS, Koronavilkku mobile apps and back-end server.

TRAFICOM
Finnish Transport and Communications Agency

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 compliant
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.

Communication over HTTPS between app and back-end. There is only one POST endpoint for the TEK data, which is comprised of seemingly meaningless pseudo-random bytes that cannot be further interpreted in anyway.

TRAFICOM
Finnish Transport and Communications Agency

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 compliant
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.

BLE traffic completely controlled by mobile OS. Certificate pinning has been implemented to mobile apps. Application firewall validates user-agent string and message format and is also used for prevention of DDOS attacks.

TEK POST endpoint on back-end server: publicly open endpoint over HTTPS, pin code validation, json format and data length validation. Admin access to servers restricted to hosting party's internal network and protected according to government IT security standards.

TRAFICOM
Finnish Transport and Communications Agency

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 low energy	BLE beacon, no encryption	Tracing encounters between devices
443	HTTPS POST, pin code protection	To submit TEKs

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 compliant
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.

Not applicable