Compliance statement for the NCSC-FI IoT 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 103 645 "CYBER; Cyber Security for Consumer Internet of Things", available at https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

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

An end-of-life policy shall be published for the Product that explicitly states the minimum length of time for which it will receive software updates (ETSI 4.3-4). For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable. The period of hardware replacement support and an end-of-life policy should be published. (ETSI 4.3-8, 4.3.9)

1.2 Security guidance

Security guidance for the Product is available in Finnish at http://example.com/vendor/security/Product[1] (ETSI 4.12-1).

1.3 Other certifications

The product has a CE marking. 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), or have certification 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 sections below.

2.1 Weak, Guessable, or Hardcoded Passwords

All IoT device passwords shall be unique and shall not be resettable to any universal factory default value (ETSI 4.1-1).

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.

2.2 Use of Insecure or Outdated Components

All software components in the Product should be securely updateable (ETSI 4.3-1). The consumer should be informed that an update is required (ETSI 4.3-2). Updates shall be timely (ETSI 4.3-3). The need for each update should be made clear to consumers and an update should be easy to implement (ETSI 4.3-5). The vendor shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues (ETSI 4.2-1).

[1] Replace this link with your own.

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.

2.3 Insufficient Privacy Protection

Device manufacturers and service providers shall provide consumers with clear and transparent information about how their personal data 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 4.8-1).

Describe how it is ensured that the handling and storage of personally identifiable information 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 use the table below in your response to section 2.3.

PII	Product/Service/Component	Purpose	Data Processor

2.4 Insecure Data Transfer and Storage

Security-sensitive data, including any remote management and control, should be encrypted in transit, with such encryption appropriate to the properties of the technology and usage (ETSI 4.5-1). All keys should be managed securely (ETSI 4.5-2). Credentials and security-sensitive data shall be stored securely within services and on devices (ETSI 4.4-1).

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.

2.5 Insecure Network Services and Ecosystem Interfaces

Unused software and network ports should be closed (ETSI 4.6-1). Software should run with least necessary privileges, taking account of both security and functionality (ETSI 4.6-5). Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated (ETSI 4.13-1).

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.

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 and access control	Usage

2.6 Insecure Default Settings

Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability (ETSI 4.12-1).

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.

2.7 Contact information

Company name:

Business ID:

Contact person:

Email:

Telephone number:

Send your application to tietoturvamerkki@traficom.fi