Date 11.5.2021

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: Datek Smart Home AS

TRAFICOM
Finnish Transport and Communications Agency

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.

> DSH Home Hub is a CE-marked, Zigbee 3.0 certified gateway for the home. It provides a central access point for Zigbee devices and acts as a Zigbee co-ordinator. The gateway connects to a centralized backend using a LAN interface towards the home user's own internet router. The centralized backend along with an app is also developed and operated by Datek.

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.

> The user is informed from the user manual.
> The software is maintained for at least five years (the maximum product warranty period in any targeted market)

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.

> The device is setup in a secure manner with minimal access by default. All augmentation must be done manually through several authentication layers (in app, in backend and on gateway). For instance, no local access to the gateway (in the local LAN) is allowed by default. All ports are closed by default. Changes to this can only be done by an administrator through a protected interface over an encrypted link.
> All installation instructions are provided in the user manual (unfortunately currently only in English and Norwegian.

TRAFICOM
Finnish Transport and Communications Agency

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

> The Product is CE marked, evaluated and approved by Nemko.
>
> The product is also Zigbee 3.0 certified as a gateway: https://zigbeealliance.org/zigbee_products/datek-home-hub/
>
> The backend runs on AWS. It has been audited by multiple third parties and has also received the "well architected" stamp from Amazon.

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 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.

> The device uses strong and unique passwords

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 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).	☒	☐	☐	☐

TRAFICOM
Finnish Transport and Communications Agency

> ETSI 5.3-11: Updates are being done automatically.
>
> ETSI 5.2-3: Products are regularly patched and updated according to known vulnerabilities.

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.

> Datek is both ISO-9001 (quality) and ISO-27001 (information security) certified. All the mentioned procedures are documented and implemented as part of the relevant processes.
>
> Vulnerabilities shall be mended within 90 days (also documented in the user guide).

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 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).	☒	☐	☐	☐

TRAFICOM
Finnish Transport and Communications Agency

> See below

Describe how it is ensured that the handling and storage of personally iden-
tifiable 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.

> All data is handled in a GDPR-compliant way. All data shared via the
> gateway to the backend and stored/processed centrally is regulated
> through data processing agreements and presented to the user in
> the proper manner according to GDPR
>
> The gateway can connect to different ecosystems/backends, and the
> content in the table below depends on which ecosystem the gateway
> interacts with. The PII also depends on which devices (ie. over
> zigbee) the gateway interacts with. Thus, we have opted not to fill in
> the table below, since it greatly varies with the configuration.

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

2.4 Insecure Data Transfer and Storage

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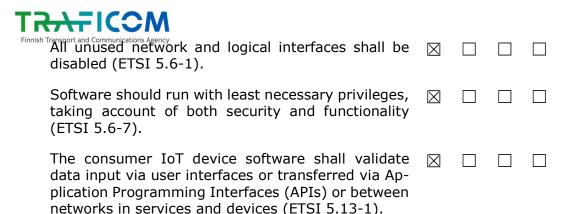compliancy for each requirement using the checkboxes.

	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.

All communication – both over ZigBee and with the different configured servers – requires encryption. Un-encrypted communication is not supported/provided.

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.

> The device does not have an active web interface. There are only two network interfaces on the device, Zigbee (local) and LAN-based internet access.
>
> There are no open interfaces towards the gateway. The only access to the gateway is through a commissioned server address using encrypted communication. All local ports on the gateway are closed by default, and can only be opened by authorized support personnel. The local Zigbee interface does not accept network traffic from unidentified devices. The home user must first pair devices with the gateway manually before they can communicate with the gateway.

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
Zigbee	Zigbee 3.0 best practice	Local connection to end devices
Ethernet/LAN	HTTPS/authentication	SSL/TLS is used, with valid certificates issued by a well known authority. The gateway only communicates with a limited set of servers, and only using secure connections.

TRAFICOM
Finnish Transport and Communications Agency

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.

The user is provided with the following information in the user manual:

Your device communicates securely
As soon as your product is setup and connected towards your app, it operates using secure communication.

Your app (or any other interface used towards the G9 Hub) should provide you information about the status of the device, as well as the current firmware version, the date the device was last upgraded and the last time the device was connected to the internet.

The gateway follows a simple flow during installation with much thought put into the security aspects. When new Zigbee devices are installed/paired with the gateway, Zigbee mandated security mechanisms are used.