7.2.2021

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:	Cozify Oy
Business ID:	2552557-5

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.

Cozify Hub is a manufacturer and protocol agnosic Smart Home Controller that connects and controls different IoT devices, systems and traditional building automation. The product supports wide variety of different smart home and building automation standards, enabling one single system to control the home and building.

Cozify Hub is a part of Cozify Smart Living offering, a full stack IoT platfrom to control and manage our built environment.

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.

Cozify Hub is being supported with automated security fixes, feature updates and value-added services at least 5 years from the date of application. Cozify plans to provide new versions of Cozify Hub, which are similaliry compatible with Cozify Smart Living Platform and with the most important standards and ecosystems in Smart Home and Smart Building ecosystems.

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.

Security guidance along with other user instructions for the Product is available in Finnish at https://tuki.cozify.fi/support/home

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 has a CE marking.

For consumer offering, Cozify back-end runs on AWS, which is well certified IaaS provider and is compliant with Data Protection Act 1998, ISO 27001: 2013, "UK Cyber Essentials" and "UK Cyber Essentials Plus" and GDPR. See https://aws.amazon.com/compliance/programs/ . Other backends may be used in various business settings, for example when the location of data is restricted by the customer or regulations.

TRAFICOM
Finnish Transport and Communications Agency

The security architecture of Cozify Hub, related Cloud Services and End user interfaces, is verified by a third-party security experts.

Cozify's technical infrastructure and Company's processes have gone through several audits by an independent 3rd party auditors as well as Cozify's partners, including global insurance companies, electricity providers and real estate companies. More information per request.

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.

In consumer setting, Cozify hub is not accessed with traditional passwords especially no hardcoded passwords are being used. Instead, user device (e.g. mobile application or a partner system) first identifies itself to Cozify cloud. Identification methods differ, most used one being a one-time-password sent to the email associated to user's account.

After user is identified, the UI app receives a keyring, including Java Web Access Tokens to each hub user's account is associated, with proper role-based permissions. Access Tokens in the keyring contain a random key and they are electronically signed by Cozify Cloud, that maintains all user permissions to access each Hub. Access Tokens signatures can be verified by the Cozify Hub, with no direct connection to the cloud. Access Tokens have a finite lifetime. User device may renew the Access Token without user intervention.

TRAFICOM
Finnish Transport and Communications Agency

Permissions to access the hub can be changed by a) Owner/Administrator of the Cozify Hub b) Respected channel partner selling Cozify Hub or c) Cozify Support personnel. This applies to resetting the hub as well.

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).	☒	☐	☐	☐

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.

Finnish Transport and Communications Agency

1) *Cozify Hub is provided with continuous Over-The-Air (OTA) software updates, typically once per 30 to 60 days. On top of the typical update cycle, Critical Security Updates can take effect as fast as within hours from detecting a security threat.*

   Software updates contain security fixes and new features and new value-added services for the end user. Software updates for the Cozify Hub (and 3rd party devives) are done automatically by the platform and no user action is required – only requirement is to have the hub in power and a connection to the internet.

   Users are informed about security updates, along with new features, over the email, while the automated updates are being executed.

2) *Cozify does automated OTA updates to selected set of third-party devices that are connected to the hub. The availability of an update is defined by a third party responsible for the device. OTA updates for third-party devices are typicaslly also automated. In some cases, user may be informed about the update in the mobile app UI.*

3) *Cozify mobile app is provided with continuous updates, which can be downloaded from appropriate application store. The user is informed about a new version within the mobile application itself, typically after the hub software has been updated.*

4) *Issues on security or any other questions can be addressed to support@cozify.fi. On top, Cozify provides partner specific contacts to channel partners.*

5) *Continuous software updates are being provided to all different levels of software stack, from low-level firmware, operation systems, middleware and applications.*

6) *Cozify actively follows the public information about the new security threats, e.g. arising from commonly used OS or middleware libraries. Cozify conducts security external security 3rd party audits on the system in timely manner. Automated tools are being used to detect old and deprecated software components in the release packages.*

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

TRAFICOM
Finnish Transport and Communications Agency

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.

Cozify does not store personal data unless a) there is a clear legitimate interest b) the data is required for providing a feature or c) (when in doubt) there is a separate permission from the person to do so.

Cozify Privacy Policy defines the main uses of the data. It is provided at the web site:

- *In English: https://en.cozify.fi/pages/privacy-policy*
- *In Finnish: https://www.cozify.fi/pages/privacy-policy*

Cozify core personnel has passed Security Clearances conducted by Finnish Security and Intelligence Service and have gone through internal trainings for basic security manners during the development and operations.

Cozify's internal security policy defines how to categorize and process different kind of data. The main principals for data and privacy protection are as follows:

1) *Data Classification defines the required level of required security actions.*
2) *Both physical and virtual access to information is protected.*
3) *The data use is restricted to well defined causes. Access to data is narrowed and restricted. Autonomisation and pseudonomization of data is encouraged while designing the information architecture and services.*
4) *Authentication and privilege policies are in place in all different layers of the system.*
5) *Data is encrypted whenever possible and meaningful and especially when transporting over a public network.*
6) *Backup systems are in place. Redundant systems for high availability are in place. Appropriate logs are kept for audit trails. Unnecessary and old data is removed.*

Partner policies are reviewed to make sure they are in line with Cozify principals. List of most important data processors are being listed in Cozify Privacy Policy.

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.

1) *All data passed over internet is encrypted with well-known encryption algorithms. This includes remote control, backups, data harnessing, video feeds and so on.*

2) *Whenever possible, all parties involved in the data exchange, are identified with strong credential and signature mechanisms.*

3) *Credential information (when needed) is hashed when possible, otherwise strongly encrypted. The requirements for protecting data at rest is constantly reviewed. The most sensitive data is encrypted.*

4) *In home LAN (Wifi) network, local communication between UI and Hub is currently not encrypted. If the local network is considered unsecure or open to many different users and systems (for example in public environments such as offices), local communication can be turned off to increase the level of security. In this case, all communication is routed via encrypted communication via Cozify Cloud.*

5) *The protection of data transfer between Cozify Hub, sensors and other peripherals are typically dependent on the communication standard available as well as choices made by a 3rd party manufacturer's. To protect the end consumer, Cozify educates the customers with the information about secure and insecure protocols and standards.*

TRAFICOM
Finnish Transport and Communications Agency

6) *Back-end resides in well known, widely certified IaaS service provider (AWS).*

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.

1) *For the hub OS software, all unnecessary services are turned off. For IP traffic, ports are opened only for known services which support real features and use cases.*

2) *The security of different radios and protocols varies a lot. While Cozify is an open platform there are some compromises regarding third party protocols and devices. Whenever Cozify integrates new devices and protocols, the security level is evaluated. Cozify works together with different alliances and manufacturers to provide better overall security. Also, information about*

safety of different technologies and peripheral devices is being provided in Cozify web pages and other channels.

3) *Design and implementation of API's (Cozify Hub, back-end services) follow basic principles defined in earlier chapters. They are also audited on timely basis. This includes requirements for encryption, authentication, authorization and so on.*

4) *APIs and API libraries are designed to be protected from well-known vulnerabilities, such as injection attacks, cross-site scripting, replay attacks, spoofing and so on.*

5) *APIs are exposed for security audits. All findings are taken seriously, categorized and, considering the overall risk, fixed without unnecessary delay.*

6) *Back-end resides in well known, widely certified IaaS service provider (AWS).*

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
Inbound: 8887/tcp http	upnp event server	Upnp devices (e.g. Sonos) are configured to send events to this port.
Inbound: 8893/tcp http	Hub command api for LAN	For UI and other systems to connect with the Hub
Inbound: 5353/udp open	zeroconf	Avahi server advertising hub in LAN with Bonjour.
Outbound: https	Https and Websocket	Hub uses https/REST and websocket for comms to the cloud. Used for remote control, data harvesting, updates, configuration etc.
JWT Token for API communication	Length of the signature hash key: 512 bytes Signing algorithm: HS512	Bearer token for granting access right and permissions to different parties in the Cozify network.
Zigbee (HA 1.2)	Communication is encrypted and devices have proper pairing protocols. Each hub has its own random network key for communication.	For connecting Zigbee devices. Hub
Z-Wave	Communication is encrypted and devices have proper pairing protocols.	For connecting Z-wave devices.
433Mhz devices	On-Off-keying protocol does not provide security.	For connecting 433Mhz devices.

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).	☒	☐	☐	☐

TRAFICOM
Finnish Transport and Communications Agency

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.

Cozify's attempt is to provide a secure system even, when the end user installs the system by themselves. We believe we achieve this with the following principals:

1) *Whenever Cozify Hub gets connected to network, is will download the latest firmware and configuration from Cozify Cloud. These settings are predefined for different user group to match their needs for using Cozify. The update procedure works fully automatically and user does not have to do anything. This is especially important during the first usage and while executing maintenance or security update.*

2) *Software updates are transaparent for the end user. They happen in the background and do not prevent from using the system. When the actual update happens, the downtime of the system is typically less than 5 seconds.*

3) *Basic security measures are taken in account already in the default settings. While the system is open and user still has the choice (e.g. for selecting insecure peripheral devices over secure ones), Cozify works on educating users.*

4) *Whenever a security problem (e.g. no firewall between public internet and home LAN) is detected in the backend, affected users are informed about this over email.*