Cybersecurity

# The Finnish Cybersecurity Label

TRAFICOM

Finnish Transport and Communications Agency

# About the Finnish Transport and Communications Agency Traficom and the National Cyber Security Centre Finland

TRAFICOM
Finnish Transport and Communications Agency

The National Cyber Security Centre Finland (NCSC-FI) develops and monitors the operational reliability and security of communications networks and services. It produces and publishes situational awareness of cybersecurity, acting as as the National Communications Security Authority.

NCSC-FI is part of Traficom, the Finnish National Transport and Communications Agency, the authority responsible for permit, licence, registration, approval, safety and security matters in Finland.

https://kyberturvallisuuskeskus.fi/en
https://traficom.fi/en

Cybersecurity

# The Finnish Cybersecurity Label

## What is the Cybersecurity Label?

The Finnish Transport and Communications Agency Traficom has created the Cybersecurity Label to help the consumer make more secure choices when purchasing IoT devices or services. The Label also helps companies to show that making devices and services secure by design is important for them.

## What does it mean?

The Label can be given to products which collect and transmit data in digital format. The Label shows that the product is secure by design, and that certain security features are updated for the duration of the Label. The aim of the Label is to tackle the most common security threats affecting consumers on the Internet. It does not try to solve physical access-related security issues.

Cybersecurity

## Safer choices for consumers

Identifying secure IoT products is very difficult. A Cybersecurity Label on the device or service informs consumers that it has passed an audit based on security requirements set by Traficom's Cyber Security Centre.

## Competition advantage for companies

For companies, the Cybersecurity Label is a way of telling customers and partners that the company is a responsible actor in security issues, and that security has been identified as an important factor in the design of the product. Passing the requirements of the Finnish Cyber Security Centre also implies that the company is well ahead when it comes to future EU-wide requirements or standards on IoT security.

TRAFICOM
Finnish Transport and Communications Agency

Cybersecurity

# The Aim of the Cybersecurity Label

The development and increasing number of IoT devices make more choices and services possible for consumers. It also brings new security risks. With the Cybersecurity Label Traficom aims to:

Help consumers make more secure choices when purchasing IoT devices and services

Guarantee the security of IoT devices by setting security requirements

Raise awareness of cybersecurity issues and their effects on consumers

Support the competitiveness of companies which invest in their products' security features from the very beginning (Secure by Design)

# Applying for the Cybersecurity Label

# Applying for the Cybersecurity Label is Voluntary

The EU Cybersecurity Act came into force in June 2019. One of the Act's aims is to create a framework for European Cybersecurity Certificates for products, processes and services.

- The creation of such a cybersecurity certification framework incorporates security features in the early stages of their technical design and development (security by design).
- It also enables their users to ascertain the level of security assurance, ensuring that these security features are independently verified.
- The framework will be valid throughout the EU, but the timing remains open.

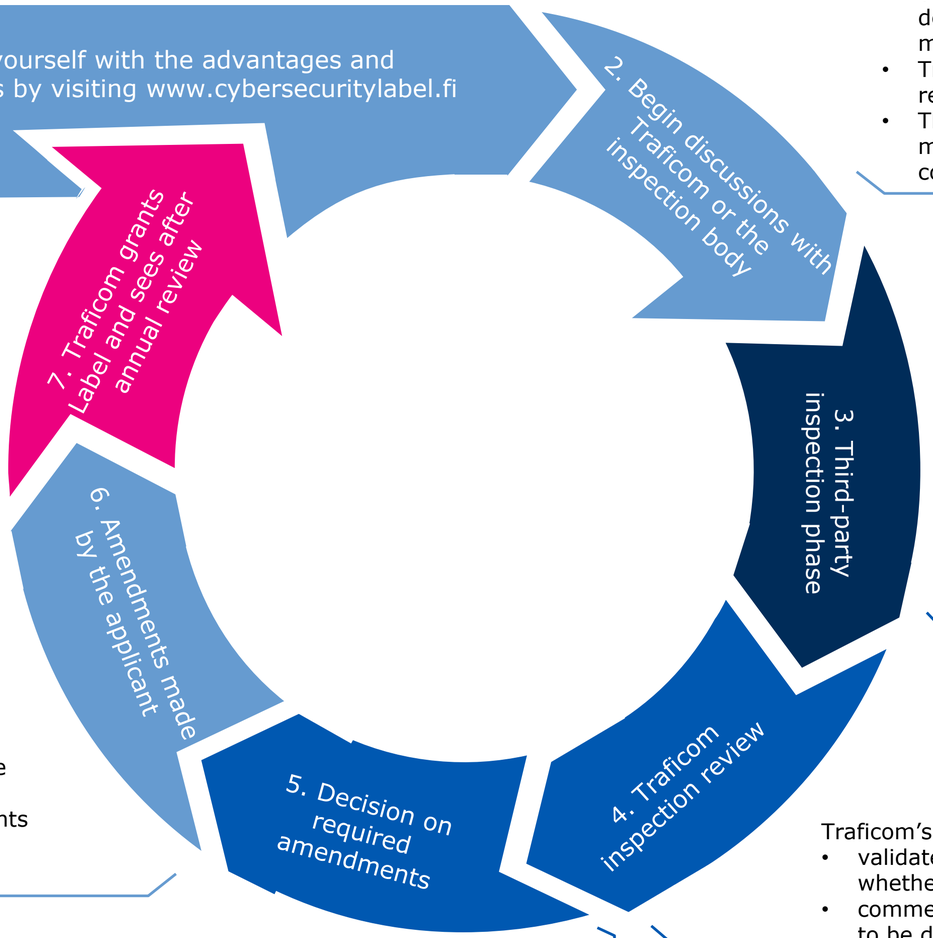
The requirements of the Finnish Cybersecurity Label are based on ETSI EN 303 645.

- It is foreseen that requirements for IoT device security will be given and made mandatory, with EU-wide standards and legislation
- Traficom has been involved in the preparation of the European standards and has worked towards common requirements.
- The Finnish Cybersecurity Label builds on the European development on standards, seeking to be in line with future schemes.

§ Applying for the Cybersecurity Label is voluntary. There is no legislation on the Label, but a standard on the security of consumer IoT devices has been published.

# Application and Inspection Processes

# Main Steps of the Application Process




- To receive the right to use the Label, the device or service must be secured from the most common IoT threats.
- Traficom's NSCS has set security requirements which must be met.
- This will be inspected by a third party, which may be a security company chosen by the company and approved by Traficom.

- The product or device must pass the inspection.
- The inspection will verify that the product meets the requirements and will provide for thorough documentation.

Traficom's cyber security specialists
- validate the outcome of the inspection and whether the product meets the requirements.
- comment on possible amendments that need to be done.

- If the received information is deemed sufficient and in conformity with the requirements, the Label can be granted.
- If any issues remain open or fail to meet the requirements, these need to be amended.
- The list of required amendments is sent to the applicant and the inspection body.

- To receive the Label, the applicant needs to correct the shortcomings, and send the necessary proof and documents to the inspection body and Traficom.

- After the Cybersecurity Label is granted, the company can attach it to the audited products and use it when marketing them. It may not be used for other purposes.
- The product information will also be added to the Cybersecurity Label web pages: www.cybersecuritylabel.fi

Applicant

Inspection body

Traficom

TRAFICOM
Finnish Transport and Communications Agency

Cybersecurity

# The Inspection

## Piloting the Inspection

Traficom began the pilot for the Cybersecurity Label inspection with three applicants in 2019. The inspection was undertaken by a cybersecurity specialist from Traficom's NCSC.

→ The experience was documented to gain insights into the main challenges and questions affecting the inspection process and the set of requirements.

## Inspection in 2020 and beyond

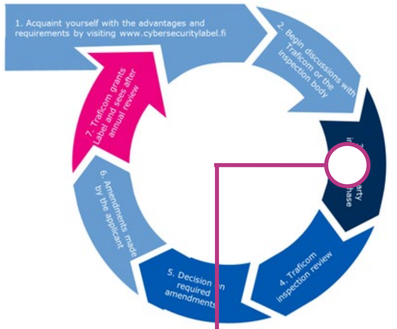
Since the Cybersecurity Label was published at the end of 2019, the number of applicants has risen as hoped for and expected. It was therefore deemed necessary to outsource the inspections to third parties to keep the process as smooth and fast as possible.

→ The inspection can be made by Cybersecurity companies specialising in security inspections and approved by Traficom

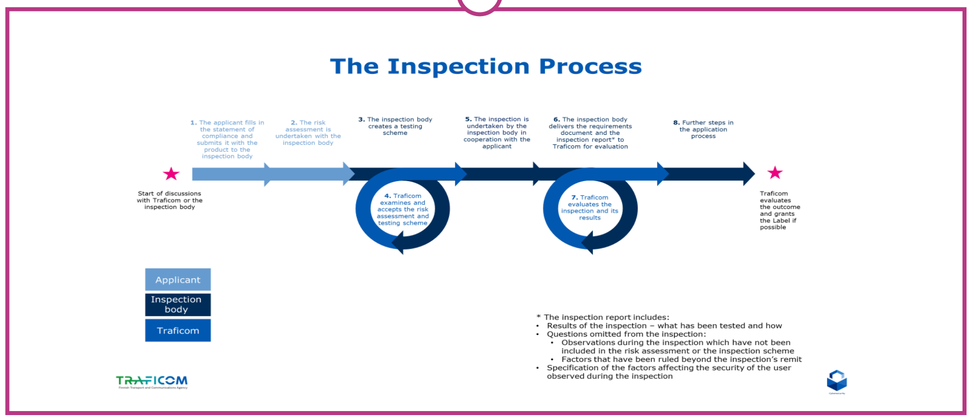
→ Traficom has prepared various documents which ensure the validity and conformity of the inspections

→ Traficom will validate the outcome and documentation of the inspection with the parties involved.

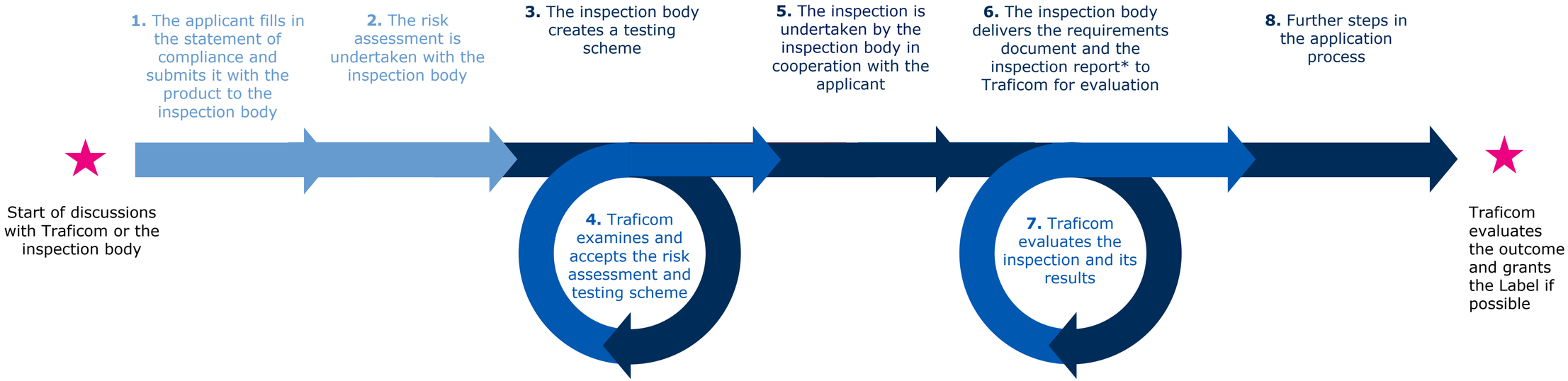
## Process cycle




(detailed description on the following page)



# The Inspection Process




Applicant

Inspection body

Traficom

* The inspection report includes:

- Results of the inspection – what has been tested and how
- Questions omitted from the inspection:
  - Observations during the inspection which have not been included in the risk assessment or the inspection scheme
  - Factors that have been ruled beyond the inspection's remit
- Specification of the factors affecting the security of the user observed during the inspection

# Maintenance of the Label

Holder *(applicant)

Traficom

Inspection body

1. Notice of annual review

- Traficom annually reviews the products and services which have received the right to use the Cybersecurity Label. Traficom informs the Holders (applicants) that the Label is expiring and needs to be reviewed. If the review is not undertaken, the right to use the Label expires.

2. Holder of the Label submits the requirements documents with necessary new details

- The Holder (applicant) submits information on the changes made to the product or service after the inspection.
- If the changes are significant and affect the security of the product/service, the inspection process may have to be undertaken again.

3. Traficom reviews the documents

- If no major changes have been made since the inspection, the process proceeds directly for approval and the continuation of the right to use the label.
- If a new inspection is required, products/services proceed to the inspection process.

New inspection if necessary

4. Inspection if required due to changes

5. Evaluation of the inspection's results and documents

6. Approval and continuation of the right to use the Label

- When approval from Traficom has been received, the right to use the Label continues.

# Validity of the Label

# Annual review

**Notice**

Traficom informs the company that the annual check is closing well in advance.

→ The need for annual supervision is to ensure that the security features of the products still meet the requirements.

→ Traficom is always made aware of changes which affect or may affect the security features of the labelled product, also during the Label's granted validity period.

**Evaluation**

During the evaluation, possible changes to the security features are discussed.

→ If no changes have been made, or the changes do not affect the security features, the Label will remain valid for the next period.

→ If multiple changes have been made, or the changes affect the product's security features, a new inspection process may be necessary.

**Amendments**

→ The necessary documents are updated, evaluated and stored

→ In addition, possible amendments to product information details are made on the Cybersecurity Label web pages.

# Summary and costs

## Products

The Cybersecurity Label can be granted to devices or services that collect and transmit data in digital format.

- Devices can be connected to the Internet, and services use the transmission/communication channels of the web

The Cybersecurity Label is not intended for common use products such as laptops and mobile phones.

## Requirements

Applying for the Cybersecurity Label is voluntary.

The requirements of the Label are based on ÉTSI EN 303 645 CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.

The requirements have been prioritized using the OWASP IoT TOP 10 Threat List (2018)

- The aim of the Label is to tackle the most common security threats affecting consumers on the Internet. It does not attempt to solve security issues connected with physical access.

## Costs

The cost of the inspection depends on the amount of work and the pricing of the inspection body, who have the right to price their work independently.

- The duration of the inspection is individual and varies between approximately 5 and 20 working days. The ability of the applicant to supply required information during the inspection process significantly affects the swiftness of the process.

The cost per product includes the
- Right to use the Label: 350 euros
- Annual review: 350 euros.

# Contact and More Information

Cybersecurity

www.cybersecuritylabel.fi

cybersecuritylabel@traficom.fi

TRAFICOM
Finnish Transport and Communications Agency