Finnish Transport and Communications Agency's guidelines on the evaluation of cryptographic and security enforcing products

Version history

Date	Description/change
7 February 2025	The following guidelines are merged: - *Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät - Tilaajan näkökulma* [Evaluation and approval of cryptographic products by the Finnish Transport and Communications Agency Traficom – Customer perspective] (1487/651/2017, 6 March 2020) and - *Liikenne- ja viestintävirasto Traficomin suorittamat turvallisuuskriittisten tuotteiden arvioinnit ja -hyväksynnät - Tilaajan näkökulma* [Evaluation and approval of security enforcing products by the Finnish Transport and Communications Agency Traficom – Customer perspective] (1487/651/2017, 4 January 2022) The following items are added and updated: - preconditions concerning the manufacturer's country of origin - definition of evaluation assurance levels - evaluation procedures/methods - evaluation process description - documentation required for evaluation (appendix) - EU and NATO (cryptographic) product approvals - statements and decisions issued by Traficom as a result of an evaluation and when information about the outcome of the evaluation can be public - handling of documents and material under the Act on the Openness of Government Activities

Contents

1. Introduction

1.1 Purpose of the guidelines

These guidelines describe the main principles of the evaluation and approval processes of cryptographic products and other security enforcing products and present the different situations in which the Finnish Transport and Communications Agency (Traficom) can perform evaluations. The guidelines concern products intended to provide protection for the handling of classified information by electronic means.

The guidelines are intended for public authorities responsible for the security of their information systems and for companies manufacturing cryptographic and security enforcing products. The purpose of the guidelines is to describe the product evaluation processes and the types of statements and approvals Traficom can issue based on the evaluation. The objective of Traficom's evaluations is to enhance the authorities' ability to acquire sufficiently secure products for the protection of classified information, and thereby support the authorities' risk management efforts to protect the information systems they use to handle classified information. The evaluations also indirectly improve manufacturers' competitiveness and their opportunities to participate in information system projects associated with the protection of EU or NATO classified information as product suppliers.

The intended use of a product affects the evaluation. One of the key differences between evaluation types is whether the evaluation concerns the protection of national classified information or an international information security obligation. The nature of the evaluation also depends on whether the evaluation is an independent product evaluation or part of an evaluation of an information system.

In the context of protecting national classified information, the authority responsible for an information system has the power to decide, based on a risk assessment, which products it uses in its system, and product evaluations are voluntary. International information security obligations, on the other hand, typically require that only security enforcing products evaluated and approved by the competent information security authority are used in the protection of classified information.

In addition to these guidelines, Traficom provides case-by-case guidance and advice on the details of the evaluation.

1.2 Legal basis of the guidelines

The guidelines are based on Traficom's supervisory duties. Provisions on these duties are laid down in section 4 of the Act on the Evaluation of the Information Security of Public Authorities' Information Systems and Telecommunications Arrangements (1406/2011, Evaluation Act), section 9, subsection 3 of the Security Clearance Act (726/2014) and section 4 of the Act on International Information Security Obligations (588/2004).

Under section 4 of the Act on International Information Security Obligations, Traficom acts as the national Crypto Approval Authority (CAA) as referred to in Article 10(6) of and Annex IV to the Council Decision on the security rules for protecting EU classified information 2013/488/EU.

Traficom also acts as the National CIS Security Authority (NCSA) as referred to in paragraphs 11 and 13 of Enclosure "F" to the NATO security rules C-M(2002)49-REV1 (see Act on the Agreement between the Parties to the North Atlantic Treaty

for the Security of Information and on Security Rules (907/2023), Finnish Treaty Series 55/2023; Decree, Finnish Treaty Series 56/2023).

Traficom's duties are defined in the Act on the Finnish Transport and Communications Agency (935/2018). According to the Act, the National Cyber Security Centre Finland (NCSC-FI) at Traficom supports, guides and supervises information security and the protection of privacy in electronic communications. It maintains national situational awareness about cyber security. The activities of the NCSC-FI promote and ensure the information security of information systems and telecommunications arrangements.

The relevant provisions are discussed in more detail later in this document.

1.3 Relationship with other product regulation and evaluations

1.3.1 CRA

These guidelines do not concern product security evaluations in accordance with the EU Cyber Resilience Act (CRA) (EU) 2024/2847. According to Article 2(7), the Regulation does not apply to products with digital elements developed or modified exclusively for national security or defence purposes or to products specifically designed to process classified information. However, the Regulation does not prevent the evaluation of a product available on the market for the purpose of protecting the classified information of an authority. The CRA applies to products and software with digital elements that are made available on the EU internal market and are directly or indirectly connectable to another device or network.

1.3.2 Inspection bodies or other assessment entities

Evaluation duties concerning **international information security obligations** are assigned to Traficom in the Act on International Information Security Obligations. Outsourcing the duties under a contract to an information security inspection body or enabling such a body to obtain the required competence would require regulatory changes.

The legal basis would also need to be supplemented to enable the partial or complete outsourcing of Traficom's product evaluations carried out to protect **national classified information** under the Evaluation Act.

In principle, it would be possible to apply for the competence for the evaluation of products used for the handling of **national classified information** under the Act on Information Security Inspection Bodies (1405/2011, Act on Inspection Bodies). This would require, for example, defining criteria for the demonstration of competence and building the required expertise in information security inspection bodies. If necessary, Traficom supports the evaluations carried out by inspection bodies as regards cryptographic solutions and other security enforcing products.

Under the Act on the Finnish Transport and Communications Agency, Traficom carries out evaluations on the basis of an agreement upon request by manufacturers. In this context, Traficom has concluded an individual agreement with an external assessment entity as a pilot project. If parties so agree on a case-by-case basis, the assessment entity may carry out testing and inspection for a specific security enforcing product type under Traficom's guidance and Traficom can use the outcome of the inspection in its own statement. The procedure requires the manufacturer to conclude an agreement with the assessment entity in question. Traficom is not a party to the agreement between the manufacturer and the assessment entity, and the assessment entity is not a party to the agreement between the manufacturer and Traficom. Traficom reviews the product evaluation plan. The assessment entity complies with the criteria specified by Traficom,

provides Traficom with all the information concerning the evaluation and complies with Traficom's guidance and policies in all stages of the evaluation process. Traficom assesses whether the preconditions for issuing a statement are met and issues the statement.

1.3.3 Electromagnetic emissions and management of cryptographic material

These guidelines do not address the evaluation of cryptographic or security enforcing products' ability to provide protection against the threats of unintentional electromagnetic emissions (TEMPEST protection measures). They are evaluated in accordance with their own rules and guidelines, if necessary.

These guidelines do not cover the management of cryptographic equipment or other cryptographic material, such as cryptographic keys (COMSEC procedures).

1.4 Entry into force of the guidelines and additional information

These guidelines enter into force on 7 February 2025. They will remain in force until further notice.

These guidelines merge and update the following previous guidelines: *Liikenne- ja viestintävirasto Traficomin suorittamat salaustuotearvioinnit ja -hyväksynnät - Tilaajan näkökulma* [Evaluation and approval of cryptographic products by the Finnish Transport and Communications Agency Traficom – Customer perspective] (1487/651/2017, 6 March 2020) and *Liikenne- ja viestintävirasto Traficomin suorittamat turvallisuuskriittisten tuotteiden arvioinnit ja -hyväksynnät* - Tilaajan näkökulma [Evaluation and approval of security enforcing products by the Finnish Transport and Communications Agency Traficom – Customer perspective] (1487/651/2017, 4 January 2022).

The guidelines will be supplemented and modified as necessary. Modified versions are listed in the version history on page 2.

For more information, please contact ncsa@traficom.fi.

2. Definitions

This chapter defines the terms used in these guidelines. The purpose of the definitions is to make the guidelines easier to understand. The definitions take into account the terminology used in different legal instruments, but the terminology used in the applicable regulation is not entirely consistent. National regulation does not specifically address the products, and the details of EU and NATO security rules differ. Therefore, when interpreting each statute, it is always important to examine the definitions used in the text in question.

Cryptographic product means a product or solution whose primary and main functionality is to protect the confidentiality, integrity, availability, authenticity and/or non-repudiation of information through one or more cryptographic mechanisms.

Security enforcing product means a product that has a critical role in an information system in the protection of classified information. A product typically has a critical role if it protects classified information from external operators. In such a case, any security deficiencies cannot typically be compensated for by other means of protection. Typical examples include gateways used to separate environments for different security classification levels.

International information security obligation means what is meant by the term in the Act on international information security obligations. For example, the protection of EU and NATO classified information involves obligations concerning

the approval of cryptographic and certain other products and regulation on requirements for the products and their manufacture.

Manufacturer means a company that develops, designs, manufactures, assembles and maintains a product.

Significant subcontractor means a company whose component or other part included in the product is essential in terms of the product properties evaluated.

Public authority customer means a public authority that needs to integrate a product as part of its information system and therefore supports the evaluation of the product. The definition does not require the existence of a procurement contract.

Requirement means either legal requirements or criteria used in the evaluation.

Criteria mean predetermined rules for the protection of classified information that are commonly used or specified and defined by Traficom in its official duties and against which a product is compared. In international information security obligations, criteria are determined in accordance with the requirements laid down by the international obligations applicable. National classified information is protected within the framework of the general requirements laid down in the Act on Information Management in Public Administration (hereinafter 'Information Management Act') and the Government Decree on Security Classification of Documents in Central Government (hereinafter 'Security Classification Decree') based on common good technical practices defined by Traficom taking into account international practices.

Inspection means the concrete observation and testing of the technical, functional and logical components of a product and its manufacture, such as the device, algorithms and software code, by various means.

Evaluation means an inspection and the analysis of documentation, reports and inspection findings concerning the manufacturer and the product and their comparison against criteria and requirements.

Assurance level means the impact of the combination of evaluation methods used on how reliable of an understanding of the product's security can be formed. Therefore, assurance level is not a classification of product security but an indication of the extent to which it has been possible to evaluate a product's security. The assurance level classification used in these guidelines is not directly used in other regulatory documents, but the term is common in the field. In these guidelines, the purpose of the classification is to give the authorities and manufacturers information about the confidence in the product's conformity provided by the evaluation and to serve as a tool for determining the specifics of the evaluation.

Conformity means the compliance of the circumstances associated with the protection of a product's properties, manufacture and maintenance with the criteria used in the evaluation. The conformity of cryptographic products and security enforcing products is always determined in accordance with a security classification. Conformity can be determined in relation to national security classification levels (TL I – TL IV) or/and international classification levels (e.g. EU-R or NR).

Statement means Traficom's written evaluation of whether a product meets the criteria for protecting information in accordance with a specific security classification level applied in the evaluation.

Approval means Traficom's written administrative decision stating that the evaluated product meets the requirements applied in the evaluation as regards the protection of information at a specific security classification level in accordance with an international information security obligation.

Usage policy means a description of practices and procedures to ensure the protection required by the security classification level. The policy is prepared by Traficom and accompanies the statement or approval issued by Traficom.

3. Provisions

The following sections present the provisions under which Traficom carries out product evaluations and on which these guidelines are based.

3.1 Product evaluations in the protection of national classified information

3.1.1 Requests by public authorities

Traficom evaluates products as part of its evaluations of the information security of public authorities' information systems or telecommunications arrangements under section 4 of the Evaluation Act (1406/2011). The Act only refers to requests by public authorities and does not, therefore, provide Traficom with a legal basis to perform evaluations upon request by manufacturers. Provisions on evaluation criteria are laid down in section 7 of the Act.

Evaluation Act, *section 4, Duties of the Finnish Communications Regulatory Authority*

To promote and ensure the information security of public authorities' information systems and telecommunications arrangements, the Finnish Communications Regulatory Authority is tasked with:
(1) evaluating, upon request by a public authority, the conformity of the information security of an information system or telecommunications arrangement that is under the authority's control or that the authority is planning to acquire;
[…]

Evaluation Act, *section 7, Information security evaluation criteria*

When evaluating the information security of public authorities' information systems and telecommunications arrangements, the Finnish Communications Regulatory Authority may use the following criteria:
(1) information security requirements for the activities of public authorities laid down by an act or a decree and information security guidance issued by the Ministry of Finance;
(2) guidance on the implementation of international information security obligations issued by the national security authority referred to in the Act on International Information Security Obligations;
(3) information security provisions and guidance issued by the European Union or some other international institution;
(4) published and commonly or regionally applied information security provisions, regulations or guidance;
(5) information security requirements included in an adopted standard.

The Finnish Communications Regulatory Authority examines whether an information system or telecommunications arrangement meets the information security requirements that have been included in the evaluation criteria. The evaluation may also be carried out as a partial evaluation.

Traficom also carries out product evaluations as part of facility security clearances when it prepares a report on the level of information security in information systems and telecommunications arrangements under section 9, subsection 3 of the Security Clearance Act upon request by the Finnish Security and Intelligence Service or the Defence Command.

Security Clearance Act, *section 9, Competent Authorities*

[…]

The Finnish Transport and Communications Agency shall prepare a report on the level of information security in information systems and telecommunications arrangements as part of the facility security clearance.

[…]

3.1.2 Requests by manufacturers

Traficom also carries out product evaluations upon requests by manufacturers. However, these requests must also be based on a public authority's need for the product in question. Processing an evaluation request by a manufacturer requires an agreement with the manufacturer. Traficom's ability to enter into such agreements is based on the Act on the Finnish Transport and Communications Agency (935/2018, Act on Traficom). The duty to promote information security, as laid down in the Act, is related to the Security Classification Decree, for example. The fees charged for the evaluations are subject to separate provisions.

Act on Traficom, *section 3, Duties of National Cyber Security Centre Finland at Traficom*

National Cyber Security Centre Finland at the Finnish Transport and Communications Agency (hereinafter 'NCSC-FI') supports, guides and supervises information security and the protection of privacy in electronic communications. It maintains national situational awareness about cyber security. The activities of the NCSC-FI promote and ensure the information security of information systems and telecommunications arrangements. The NCSC-FI acts as the responsible authority for the public regulated satellite service and as a national coordination centre in accordance with Article 6 of Regulation (EU) 2021/887 of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres. The NCSC-FI also ensures the communications sector's preparedness for incidents under normal conditions and for emergency conditions, promotes and supervises the reliability of electronic communications and supports in its own sector the overall preparedness of society for incidents under normal conditions and for emergency conditions. (1002/2021)

[…]

The Finnish Transport and Communications Agency may provide services under public law or services priced on a commercial basis that are based on the NCSC-FI's duties referred to in subsection 1 and conclude agreements on the provision of such services.

3.2 Product approvals under international information security obligations

International information security obligations concern classified information obtained from another country or from an international organisation or institution and its protection in Finland. Obligations concerning such *specially protected information* are laid down in the Act on International Information Security Obligations (588/2004). The obligations apply to all organisations and persons handling classified information.

International information security obligations are based on an international agreement binding on Finland or some other obligation imposed on Finland. Finland's General Security Agreements (GSA) can be found on the website[1] of the Finnish Ministry for Foreign Affairs, which is the National Security Authority (NSA). Obligations concerning the protection of EU and NATO classified information are

[1] https://um.fi/information-security-agreements-in-force-in-finland

based on Council Decision 2013/488/EU on the security rules for protecting EU classified information[2] and the NATO Security Policy C-M(2002)49-REV1[3].

Traficom's product evaluation task is based on its duty as Designated Security Authority (DSA) in matters concerning the information security of information systems and telecommunications arrangements as laid down in section 4 of the Act on International Information Security Obligations. EU and NATO security rules and international information security agreements lay down more detailed provisions on obligations concerning the evaluation and approval of cryptographic products or other security enforcing products. In these situations, evaluations and approvals are mandatory unlike in the protection of national classified information.

Act on International Information Security Obligations, *section 4, Security authorities and their duties*

The Ministry for Foreign Affairs acts as the Finnish National Security Authority in the implementation of international information security obligations. The Ministry of Defence, the Defence Command, the Finnish Security and Intelligence Service and the Finnish Communications Regulatory Authority act as the Designated Security Authorities referred to in international information security obligations.

The National Security Authority is, in particular, tasked with guidance and supervision to ensure the appropriate protection and handling of the specially protected information referred to in this Act.

Designated Security Authorities undertake the tasks provided in this Act and other tasks under international information security obligations. The Ministry of Defence, the Defence Command and the Finnish Security and Intelligence Service serve as the National Security Authority's experts in matters concerning personnel, industrial and physical security and the Finnish Communications Regulatory Authority in matters concerning the information security of information systems and telecommunications arrangements. (731/2014)

Traficom's tasks under international information security obligations, as referred to in section 4 of the Act on International Information Security Obligations, include acting as the Crypto Approval Authority (CAA) under the security rules of the Council of the European Union.

2013/488/EU, *Article 10, Protection of EUCI handled in communication and information systems*

6. Where the protection of EUCI [EU classified information] is provided by cryptographic products, such products shall be approved as follows:

(a) the confidentiality of information classified SECRET UE/EU SECRET and above shall be protected by cryptographic products approved by the Council as Crypto Approval Authority (CAA), upon recommendation by the Security Committee;

(b) the confidentiality of information classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED shall be protected by cryptographic products approved by the Secretary-General of the Council ('the Secretary-General') as CAA, upon recommendation by the Security Committee.

Notwithstanding point (b), within Member States' national systems, the confidentiality of EUCI classified CONFIDENTIEL UE/EU CONFIDENTIAL or RESTREINT UE/EU RESTRICTED may be protected by cryptographic products approved by a Member State's CAA.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32013D0488
[3] See Act on the Agreement between the Parties to the North Atlantic Treaty for the Security of Information and on Security Policy (907/2023), Finnish Treaty Series 55/2023; Government Decree, Finnish Treaty Series 56/2023. The document C-M(2002)49-REV1 and its translation into Finnish are included in government proposal HE 4/2023 vp: https://www.eduskunta.fi/FI/vaski/HallituksenEsitys/Documents/HE_4+2023.pdf

Annex IV, *25. Cryptographic products for protecting EUCI shall be evaluated and approved by a national CAA of a Member State.*

Annex IV, *46. The Crypto Approval Authority (CAA) shall be responsible for ensuring that cryptographic products comply with national cryptographic policy or the Council's cryptographic policy. It shall grant the approval of a cryptographic product to protect EUCI to a defined level of classification in its operational environment. As regards the Member States, the CAA shall in addition be responsible for evaluating cryptographic products.*

Cf. Annex IV, 48. Security Accreditation Authority: (g) endorsing the selection of approved cryptographic and TEMPEST products used to provide security for a CIS.

Traficom's tasks under international information security obligations, as referred to in section 4 of the Act on International Information Security Obligations, include acting as the National CIS Security Authority (NCSA) (CIS, communications and information systems).

C-M(2002)49-REV1, Enclosure "F", *11. CRYPTOGRAPHIC SECURITY*
11.1 When cryptographic products or mechanisms are required to provide confidentiality and non-confidentiality protection, whether during information transmission, processing or storage (data at rest), such products or mechanisms shall be specifically approved for the purpose and specific cryptographic requirements for physical, procedural and technical measures shall be implemented to achieve the required Security Objectives.

11.3 During transmission, the confidentiality of information classified NS [NATO SECRET] and above shall be protected by cryptographic products or mechanisms approved by the NATO Military Committee (NAMILCOM).

11.4 During transmission, the confidentiality of information classified NC [NATO CONFIDENTIAL] or NR [NATO RESTRICTED] shall be protected by cryptographic products or mechanisms approved by either the NAMILCOM or a NATO member nation.

13.4 National CIS Security Authority (NCSA)

13.4.1. Each NATO and non-NATO nation, where applicable to the latter, shall identify an NCSA, which may be established as an agency in the national security infrastructure. The NCSA is responsible for:
(a) controlling cryptographic technical information related to the protection of NATO information within their nation;
(b) ensuring that cryptographic systems, products and mechanisms for protecting NATO information are appropriately selected, operated and maintained;
(c) ensuring that CIS security products for protecting NATO information are appropriately selected, operated and maintained within their nation;
[…]

More detailed regulation (AC/35-D/2005-REV3) also takes a stand on the evaluation and approval procedure for other security enforcing products (SEP).

9.3.5 The approval of a security enforcing product is a formal statement, by a National CIS Security Authority (NCSA), supported by an independent review of the conduct and results of an evaluation and/or a certification, approving the use of a product for a specific purpose and under specific conditions. The approval of a security enforcing product for a CIS is a two-step process: while the approval by an NCSA is required to declare the product suitable for the protection of NATO information, the approval by an SAA is related to its use in the context of a specific CIS, as part of the security accreditation process.

4. Publicity of information relating to evaluations

4.1 Document publicity and non-disclosure

Traficom will always evaluate and decide case by case whether the material and information obtained in the context of its evaluation tasks and the documents it

has prepared on the basis of the evaluation are public or partly or completely non-disclosable or also classified.

4.1.1 Material obtained by Traficom

Material and information provided to Traficom in connection with an evaluation are official documents that Traficom handles in compliance with the Act on the Openness of Government Activities (621/1999), the Information Management Act and the Security Classification Decree.

Traficom always evaluates the publicity of information or the grounds for its non-disclosure or security classification of its own motion and consults the manufacturer or public authority customer, if necessary. Provisions on the grounds for non-disclosure are laid down in section 24 of the Act on the Openness of Government Activities. Under the section, the business and professional secrets of a trader are non-disclosable. Non-disclosable information may also include information on the security arrangements of information and communications systems or national defence, for example.

Traficom's product evaluations are always related to the need to protect classified information. Detailed material concerning a manufacturer's products may include information that is protected as a business or professional secret or information that affects the security arrangements of information and communications systems. For example, the source code of a product is typically information that must be protected under the Act on the Openness of Government Activities as a business or professional secret and as information affecting the security arrangements of information and communications systems. Because of business and professional secrets, the Act on the Openness of Government Activities would allow Traficom to disclose information to a public authority customer only with the manufacturer's consent. The security arrangement element, on the other hand, requires the information to be assigned a security classification and be protected in information systems during processing as required by the classification level assigned.

4.1.2 Documents prepared by Traficom

The publicity or the full or partial non-disclosure of documents that Traficom prepares during an evaluation or issues as a result of the evaluation is determined in accordance with the Act on the Openness of Government Activities based on the information included in the document. When determining the publicity of the outcome of Traficom's evaluation, a distinction must be made between the outcome of the evaluation and the various documents relating to the matter, such as the statement or decision itself or the accompanying usage policy, evaluation report or cryptographic statement.

Information about the outcome of Traficom's evaluation may be public or non-disclosable. This depends on the assurance level of the evaluation, among other things.

- As a rule, the outcome of an evaluation with a high assurance level (A) can be public. In that case, Traficom will publish on its website information about a statement or approval being issued for the product, unless otherwise agreed for a justified reason associated with the authority's activities. The full document will not be published on the website. However, anyone has the right to access the public parts of the document upon request under the Act on the Openness of Government Activities.

- The outcome of an evaluation with a medium (B) or low (C) assurance level is non-disclosable by default and is only made available to the authority that requested the evaluation and notified to the product manufacturer.

- The usage policy or instructions on requirements prepared by Traficom in connection with a statement or approval can typically be either non-disclosable or security classified. The same applies to the evaluation report and cryptographic statement, as they both invariably include details affecting security arrangements.

As noted above, Traficom may carry out a product evaluation upon request by a manufacturer, if the preconditions for making a product evaluation agreement between the manufacturer and Traficom have been met. In such cases, the general terms of the model agreement are usually public. However, the name of the company and the products to be evaluated may be non-disclosable information prior to the completion of the evaluation. The agreement and the product evaluation may be non-disclosable information even after the evaluation, if there are grounds for non-disclosure as described above. As a rule, however, only those evaluations are carried out based on an agreement that have a high assurance level, meaning that the conditions for the publicity of the outcome are usually met.

4.2 Release of non-disclosable and security classified documents

Under the Act on the Openness of Government Activities, Traficom may, if necessary, release information on a product evaluation to a public authority or certain other third parties interested in acquiring the product. Under the Act, the release of information containing business or professional secrets requires the manufacturer’s consent. Traficom may, without the manufacturer’s consent, assess the release of information considered non-disclosable under certain other grounds provided in section 24 of the Act on the Openness of Government Activities on a case-by-case basis in accordance with the requirement of harm clause specified for each non-disclosure criterion in the section. In its consideration, Traficom assesses whether the release of information can cause harm to the protected interests. The recipient of non-disclosable information is subject to the non-disclosure obligation and obligation to remain silent laid down in the Act on the Openness of Government Activities.

Traficom may release non-disclosable and security classified documents to a manufacturer of cryptographic and security enforcing products in connection with an evaluation.

When documents are security classified and Traficom releases them onward, Traficom must ensure that the classified documents and information to be released are handled in compliance with the requirements.

Security Classification Decree, *section 6, Preconditions for granting access to a classified document*

A central government authority shall ensure in advance that the protection of a classified document is duly organised if the authority grants access to a classified document to a party other than a central government authority. The requirement does not apply to disclosing information on the contents of a document based on a party's right of access to information. […]

The manufacturer must commit to keeping secret the document or information that it has obtained from Traficom and that Traficom has marked or announced as non-disclosable or that is classified. The manufacturer may release non-disclosable documents relating to a product to a public authority that needs them for the potential acquisition or use of the product. The manufacturer must inform the

authority in advance about the non-disclosure and potential classification of the document to enable the authority to consider how it handles the document. The release of documents and information to another company must be discussed case by case with Traficom.

If there is a justified need (need-to-know) to release documents that are specially protected under an international information security obligation, i.e. classified documents, to the manufacturer, Traficom obligates the manufacturer to handle and protect the information in accordance with applicable requirements and to use the information only for the purposes of the evaluation and related product development. In practice, before releasing information, Traficom prepares a commitment that the company must sign. The commitment document specifies the requirements based on the security classification. Traficom also introduces the company to the requirements of protecting the information. The commitment requires the manufacturer to protect and handle the released information in accordance with national provisions and the current version of the guidelines *Kansainvälisen turvallisuusluokitellun tietoaineiston käsittelyohje*[4] [Guidelines on the handling of international classified information] issued by the National Security Authority. If necessary, the manufacturer is required an international Facility Security Clearance (FSC) corresponding to the released information.

Act on International Information Security Obligations, section 6, Non-disclosure obligation and the use of information

Specially protected information material must be kept secret, unless international information security obligations stipulate otherwise. (885/2010)

Specially protected information material may be used and released only for the purpose it was provided for, unless the party that classified the material has provided consent to do otherwise.

Authorities handling specially protected information material must ensure that only those that need the information to carry out their tasks have access to the material. These persons must be named in advance in cases specified in international information security obligations. The same applies to a business operator referred to in section 1, subsection 2.

5. General preconditions for an evaluation

5.1 Product-related preconditions

To qualify for evaluation, a product must enable the use of technical limits and it must be suitable for the encryption or other protection of information in information or telecommunications systems. Interpretations of whether a product type qualifies for evaluation rely on the principles and application practices of international information security obligations.

Where applicable, the manufacture of cryptographic products and other security enforcing products must meet the following preconditions that are interpreted in relation to the security classification that the evaluation concerns:

Traficom must be provided with information about the development of a cryptographic product, and Traficom must be provided with an opportunity to express its views about and influence the product development. Traficom also endeavours to examine the product development of products other than cryptographic products and, if necessary, produce related information as part of its statement or decision.

[4] Guidelines on the handling of classified information – Ministry for Foreign Affairs (available in Finnish)

- Traficom must be given access to all of the product's relevant source code at Traficom's facilities or, upon separate agreement, at some other facility that meets the security requirements and can be arranged with reasonable effort.
- The requirements concern the technical entity including the platform, and Traficom must have access to the technical entity for inspection and sufficient information about the platform.
- Product development, intellectual property rights and product maintenance must be under the legal, economic and actual control of the manufacturer or a trusted subcontractor during the entire product life cycle.
- Commonly available open-source components and other commonly available general-purpose components may be used even if they are not produced by the manufacturer or a trusted subcontractor.

5.2 Manufacturer-related preconditions and the requirement of a public authority customer at different assurance levels

5.2.1 Summary

This chapter describes the preconditions for all evaluations that must be met to initiate a product evaluation.

There are certain requirements for the countries of origin of manufacture and the supply chain depending on the product's purpose of use, on the security classification of the information to be protected and on the originator of the information (e.g. EU or NATO).

The risks associated with the country of origin in manufacturing are always evaluated. The requirements for risk management depend of the security classification and originator of the information. The depth at which the implementation of management measures is evaluated depends on the assurance level of the evaluation. In evaluations with a high assurance level, Traficom will examine it to the extent necessary. In evaluations with lower assurance levels, finding out the manufacturing country of origin and the evaluation of its significance may be left to the public authority customer on a case-by-case basis.

Traficom's evaluation also always requires information about a public authority customer's need for the product in the protection of classified information and the authority's support for conducting the evaluation.

Requirements concerning the security of the manufacturing environment also depend on the security classification, and the reliability of the evaluation of their fulfilment depends on the assurance level of the evaluation.

5.2.2 Manufacturer-related preconditions

This section focuses on the preconditions of evaluations with a high assurance level. Such evaluations may be required, for example, if the objective is to have a cryptographic product included in a public list of products approved for the protection of EU or NATO classified information.

There are no specific provisions on the evaluation of cryptographic solutions or other security enforcing products for national classified information or requirements for their manufacturers or manufacture. According to the Security

Classification Decree, the solutions must be *sufficiently* reliable. Traficom's practice of applying provisions is based on the principle of issuing public statements only for products whose manufacture and life cycle management Traficom itself can verify to a sufficient degree.

Product evaluations require that Traficom can analyse the risks of foreign ownership, control and influence (FOCI) associated with the product's manufacture. The extent of this analysis depends on the scope of the product evaluation and the security classification of the information to be protected. It also depends on whether the product is evaluated for the protection of national classified information or because of an international information security obligation.

The precondition for an evaluation with a high level of assurance for the purpose of protecting national classified information is that the product manufacturer is a Finnish company operating in Finland. The requirement is that the essential parts of the manufacture and development of the product take place in Finland. Factors that may affect this include the ownership structure and control of the product manufacturer and the origin of the suppliers of essential product-specific security components (significant subcontractors).

If necessary, matters concerning the manufacturer and significant subcontractors may be demonstrated, for example, with a facility security clearance certificate or, if one is not available, by means of other reliable evidence that Traficom assesses acceptable. When Traficom makes an agreement about a product evaluation with a company, the evidence is assessed before making the agreement and it is appended to the agreement. The manufacturer undertakes to inform Traficom without delay of any changes to the contents of the evidence it has provided.

Traficom assesses the sufficiency of the evidence it has received on a case-by-case basis, taking into account Finland's usual trust frameworks with the Nordic countries or with EU and NATO Member States, for example. The evidence is assessed in relation to the relevant security classification.

A public authority may also request the case-specific evaluation or approval of a product of foreign origin. In the protection of national classified information, Traficom and the public authority customer must agree on how to assess the risk of foreign influence. Decisions about risks fall under the responsibility of the public authority customer. In the evaluation of whether international information security obligations are fulfilled, Traficom evaluates the matter and notes it in its approval decision or as part of the statement on the approval of an information system. Traficom may also examine how to take into account a valid approval issued in another country under EU or NATO security rules and any information available on the product.

A precondition for an evaluation associated with an international information security obligation is that the risks of foreign influence must be assessed in accordance with EU or NATO security rules. The manufacturer and public authority customer must be aware of the fact that if they, in relation to an international information security obligation, need Traficom's approval for the use of a product in the protection of EU or NATO classified information, the manufacturing process' dependence on different countries or Traficom's control opportunities may affect the approval conditions.

5.2.3 A public authority's need for a product evaluation

Under the Evaluation Act and the Act on Traficom, Traficom's task is to carry out evaluations upon request by a public authority and to promote the security of information systems and telecommunications arrangements.

Thus, taking a product under evaluation requires that a public authority needs the product to be evaluated. If the party applying for / requesting the evaluation is a public authority, the need is established in the request/application. If the evaluation is requested by the manufacturer, Traficom must be provided with written evidence stating that one or more public authorities need acquire the product for their information systems. It must be established that the product can meet the authorities' known needs, but an actual procurement contract is not required.

Ensuring that a public authority has a need for the product may also have relevance for the fees that Traficom charges for the evaluation. When designing the evaluation, it is important to clearly define in advance whether the charges are paid by the manufacturer or the public authority.

5.2.4 Evaluation of manufacturing environment

The manufacturing environment and the manufacture of subcontracted components affect the reliability of a product. The appropriateness of the manufacturing environment can be ensured by different means, including the following:

- self-evaluation by the manufacturer; Traficom usually requires the manufacturer to use the Katakri criteria
- security agreement between the public authority customer and the manufacturer
- review or inspection by Traficom
- facility security clearance certificate covering the operating environment.

Traficom determines the appropriate procedures case by case.

5.2.5 General advice for public authorities

At least the following must be taken into account when choosing cryptographic products or other security enforcing products needed for public authorities' information systems and telecommunications arrangements:

- Is the product used to protect national classified information or information in accordance with an international information security obligation?
- Could the need be met by a product that Traficom already has evaluated and that is included in the list[5] available on the Traficom website? If yes, it is necessary to find out the exact content of the evaluation, any limitations and the content of the usage policy.
- It is good to keep in mind that the party responsible for assessing risks and making decisions about deploying products is the information management entity, i.e. the public authority, and that any statements issued by Traficom are intended to support the information management entity's own risk assessment and possible decision to begin using a product.
- In the electronic processing of EU and NATO classified information, the protection of information with a cryptographic solution requires Traficom's approval for the product (an approval decision) or a system-specific approval as part of an information system accreditation. Also in this

[5] https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa/cryptography-solutions-approved-traficoms-ncsa-fi
https://www.kyberturvallisuuskeskus.fi/en/our-activities/ncsa/security-critical-products

context, the decision about using the product in an information system is made by the authority responsible for the system.

- When there is a need to protect electronic data transmission based on a bilateral security agreement between two countries, it may be possible to use a product approved by one of the parties or a jointly agreed product approved by the EU or NATO.

- Could the need be met by a product included in the public product lists of the EU or NATO?[6] If yes, it is necessary to find out the exact content of the product approval, any limitations and whether more detailed information is available on the approval. To the extent possible, Traficom supports the use of other countries' approval decisions and usage policies (SecOps) by Finnish authorities. It is good to note that EU and NATO classified information must be protected from other organisations, just like from any other external and third parties, and that this affects crytographic solutions, in particular.

6. Evaluation requirements and criteria

6.1 National requirements for public authorities: Information Management Act and Security Classification Decree

Public authorities' needs for product evaluations are based on their obligations in protecting the electronic processing of classified information. Provisions on these obligations are laid down in sections 13 and 14 of the Act on Information Management in Public Administration (906/2019, Information Management Act) and in the Government Decree on Security Classification of Documents in Central Government (1101/2019, Security Classification Decree). These statutes lay down requirements for the protection of information and the cryptographic products used to provide electronic protection. There are no provisions on evaluation obligations.

Information Management Act, *section 13, Information security of datasets and information systems*

An information management entity shall monitor the state of the information security of its operating environment and ensure the information security of its datasets and information systems over their entire lifecycle. The information management entity shall determine the material risks to data processing and dimension the information security measures in accordance with the risk assessment.

The resilience and operational availability of the information systems that are material with regard to performance of the tasks of the authorities shall be ensured with adequate testing on a regular basis.

The authority shall plan the information systems, the internal structure of the information pools and related processing so that the publicity of documents can be easily implemented.

In its acquisitions, the authority shall ensure that appropriate information security measures have been implemented in the information system to be acquired.

Separate provisions are laid down on the assessment of the information security of the information systems and telecommunications arrangements of the authorities.

Information Management Act, *section 14, Transfer of data in an information network*

[6] EU LAPC, general information: https://www.consilium.europa.eu/en/general-secretariat/corporate-policies/classified-information/information-assurance/ and the List of Approved Cryptographic Products: https://www.consilium.europa.eu/media/x0ebv5jn/st09931en24.pdf
Nato Information Assurance Product Catalogue (NIAPC): https://www.ia.nato.int/NIAPC

The authority shall perform the transfer of data in a public information network using an encrypted or otherwise protected data transfer connection or practice if the transferred data are non-disclosable. In addition, the data transfer shall be arranged so that the recipient is ascertained or identified in a sufficiently information secure manner before the recipient is allowed to process the transferred non-disclosable data.

[…]

Information Management Act, *section 15, Ensuring dataset security*

…

Security Classification Decree, *section 11, Requirements concerning information systems and telecommunications arrangements*

The information systems and telecommunications arrangements used for handling classified documents shall be implemented so that:

1) taking into account the security classification level of the documents handled therein, they are separated in a sufficiently reliable manner from the information systems and telecommunications arrangements at a lower security level;

[…]

7) the encryption solutions used are adequately secure, taking into account the security classification level of the documents handled in the information system or telecommunications arrangement.

[…]

Security Classification Decree, *section 12, Transfer of a document in an information network*

Provisions on the transfer of non-disclosable data in a public information network are laid down in section 14 of the Information Management Act.

Classified documents may be transferred only in encrypted form in other than a public information network outside the security areas of authorities or via an information system or telecommunications arrangement at a lower security level than the said security classification level. If the transfer of classified documents takes place in a security area in other than a public information network and sufficient protection of the information can be implemented by physical protection measures, unencrypted transfer or encryption at a lower security level may be used.

Security Classification Decree, *section 13, Carriage of a document*

Classified documents may be carried outside security areas by protecting the electronic data carriers with adequate encryption.

[…]

Security Classification Decree, *section 15, Destruction of a document*

A classified document which is no longer required shall be destroyed in such a way that recreation and reconstruction of the information in whole or in part is prevented in a manner that is sufficiently reliable for said security classification level.

[…]

6.2 Criteria for the protection of national classified information

This section describes how Traficom defines the criteria it uses to evaluate a product.

Traficom has published some of the criteria used in evaluations. Traficom also applies non-disclosable or classified criteria that it has established. The criteria concern security classification levels and typical risks in handling and storage environments. They are also in line with essential commonly accepted international criteria. The fundamental principle of evaluation is that the greater the expected risks, the stricter the required security mechanisms. Below is a list of the main public criteria applied in evaluations:

Cryptographic instructions

- *Kryptografiset vahvuusvaatimukset luottamuksellisuuden suojaamiseen - kansalliset turvallisuusluokat* (Cryptographic requirements for confidentiality – national protection levels; Guideline 190/651/2015, 9 December 2024)[7]

- *Hyväksytyt TLS-cipher suitet turvallisuusluokille IV-III* (Approved TLS cipher suites for security classification levels IV–III; Memorandum, 13 October 2022)[8]

Where technically applicable, the Katakri auditing tool is applied in the evaluation of cryptographic equipment and security enforcing products.

- *Information security auditing tool for authorities - Katakri* (guideline issued by the National Security Authority)[9]

Traficom has issued guidelines on certain security enforcing product types that are also applied in Traficom's own evaluations

- *Tallennusvälineiden tyhjennys ja uusiokäyttö* (Emptying and reuse of storage media, 28 June 2024)[10]

- *Ohje yhdyskäytäväratkaisujen suunnitteluperiaatteista ja ratkaisumalleista* (Guideline on the design principles and models of gateway solutions, 2 December 2021)[11]

The guideline on secure product development and the evaluation of security enforcing products is applied to numerous products and their evaluation

- Secure development: towards approval (Guide 2018)[12]

The criteria for evaluations for the protection of national classified information have been formulated so that they are as uniform as possible with international practices.

The objective is that the outcome of a product-specific evaluation carried out to protect national classified information could be utilised and used as a basis if the public authority customer or manufacturer decides to try to have the same product approved for the protection of EU or NATO classified information. In practice, evaluations for the protection of national classified information and international information security obligations can be carried out in parallel.

[7] Kryptografiset_vahvuusvaatimukset_-_kansalliset_turvallisuusluokat_1.pdf (in Finnish)
[8] TLS cipher suites for security classification levels IV-III (in Finnish)
[9] https://um.fi/information-security-auditing-tool-for-authorities-katakri
[10] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Tallennusv%C3%A4lineiden%20tyhjennys%20ja%20uusiok%C3%A4ytt%C3%B6.PDF (in Finnish)
[11] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/file/Yhdyskaytavaratkaisuohje.pdf (in Finnish)
[12] https://www.kyberturvallisuuskeskus.fi/sites/default/files/media/publication/Secure%20development%20%20towards%20approval%20003_2018J.pdf

6.3 International information security requirements

6.3.1 Bilateral general security agreements

The main rule in bilateral general security agreements between countries is the principle of reciprocity: classified information obtained from the other country is protected in the same manner as national information with a corresponding security classification. The cryptographic solutions to be used in data transmission between the countries are agreed upon by the relevant authorities in the countries party to the agreement. In Finland, the authority is Traficom. Cryptographic solutions may be subject to agreement-specific or project-specific requirements.

Example of a provision in a security agreement

Agreement between the Republic of Finland and the Kingdom of Belgium on Mutual Protection of Classified Information (Finnish Treaty Series 8 and 9/2022)[13]

Article 5, Protection of Classified Information
1. The Parties shall take all appropriate measures under their national laws and regulations so as to protect Classified Information referred to in this Agreement. They shall afford such information the same protection as they afford to their own information at the corresponding classification level.
[…]

Article 7, Transmission of Classified Information
[…]
2. Classified Information shall be transmitted between the Originating Party and the Recipient electronically only by secure means agreed between the Competent Security Authorities.

6.3.2 EU and NATO

Policies and guidelines issued under Article 6 of the EU Council security rules (2013/488/EU) and the directives and instructions included in the NATO security policy specify in different ways the requirements set for cryptographic solutions and other security enforcing products and their evaluation. As a rule, these documents are non-disclosable or classified. Releasing information about these documents is discussed on section 4.2 of these guidelines.

In addition to the above-mentioned EU and NATO documents, Traficom may also supplement the evaluation criteria with the criteria set for the protection of national information.

6.4 Collection of evaluation requirements

The requirements applied in evaluations are illustrated in Table 1.

Table 1. Requirements applied in evaluations.

Requirements for a product and its life cycle	Examples
Public requirements for the product's technical features	Cryptographic strength of encryption Security features of the gateway solution

[13] https://www.finlex.fi/api/media/treaty/20150/mainPdf/main.pdf?timestamp=2022-01-27T00%3A00%3A00.000Z

Non-disclosable requirements for the product's technical features	Detailed technical requirements Requirements based on product-specific threat modelling
Requirements for product manufacture and development	Protection of the access control and integrity of the product development environment Control of manufacturing
Managing risks posed to product manufacture and supply chains by foreign ownership, control and influence (FOCI)	Limitations concerning the processing of information at certain security classification levels and/or from certain originating authorities
Need and support of a public authority customer	The need for the use of the product in question and support for its evaluation as expressed by a public authority

7. Evaluation procedures and assurance levels

7.1 Content of evaluations

The content of an evaluation depends on the security classification: products intended for the protection of information at higher classification levels and for protection covering the product life cycle are subject to more comprehensive and stricter requirements and a heightened threat environment. The product's structure and threat assessment also affect the contents of tests.

Table 2 illustrates the impact of the classification level on evaluation content in the case of a product evaluation at a high assurance level. The detailed evaluation methods are always selected on a case-by-case basis when planning the evaluation.

Table 2. Impact of classification level on the minimum content of an evaluation at a high assurance level

Evaluation process	TL II	TL III	TL IV
Inspection of general and technical documentation	X	X	X
Inspection of settings and life cycle management	X	X	X
Detailed inspection of general and technical documentation	X	X	
Limited review of source code (cryptographic code)	X	X	X
Review of components affecting the security of source code	X	X	
Overall review of source code	X		

Limited solution testing	X	X	X
Basic solution testing	X	X	
Comprehensive solution testing	X		
Development process control by CAA	X	X	

Testing levels determine the most common evaluation methods. The scope of the evaluation also depends on the use case, threat environment and product structure.

The purpose of **limited testing** is to gain an understanding of the functioning and settings of the device to be able to assess potential risks and verify key aspects of secure use. The objective is to test that no obvious problems are detected in the ordinary use of the product.

Limited testing evaluates the correct functioning of the product by carrying out superficial testing via the user interface and external interfaces and by monitoring product operation. It is also ensured that the product's internal or external interfaces and security controls do not have known and easily exploitable weaknesses.

The purpose of **basic testing** is to supplement limited testing by ensuring the security of the device's internal implementation. These tests ensure the device settings and functions at a more detailed level than that visible to those responsible for device maintenance, e.g. operating system hardening. The tests include a mapping of the risks of advanced attacks and an examination of the device's response to such attacks. Testing may involve separate tests on individual critical components.

The purpose of **comprehensive testing** is to assess the product's technical functioning in depth. Individual components are tested as individual parts. The testing involves comprehensive tests on individual components without the protective mechanisms of the surrounding product components. Test methods also include highly advanced attacks.

7.2 Evaluation assurance levels

The higher the classification level, the more comprehensive and stricter are the requirements applied. The more comprehensively the fulfilment of these requirements is evaluated, the greater the certainty of the product's functioning and reliability. This is referred to as 'assurance level'. Assurance level is not an indication of a product's conformity; instead, it indicates the reliability of the evaluation of whether the product meets the applicable requirements.

The assurance levels of evaluations are presented in Table 3. Assurance level high (A) of a product evaluation is the starting point of evaluations. It is also a precondition for international product approvals and public statements about national products. Evaluations with a lower assurance level are only intended to support public authorities in their own risk assessments and decisions. They are carried out if needed by an authority and a product that could be evaluated at a high level does not exist or is not available for the use in question.

Table 3. Evaluation assurance levels.

Level of assurance	Depth of evaluation (reliability)
Low (C)	Superficial
Medium (B)	Basic
High (A)	In-depth

Evaluations at different assurance levels require different kinds of information and material from the product manufacturer. In C-level evaluations, the product is mainly evaluated on the basis of related documentation. In B-level evaluations, a functioning product sample must be provided for evaluation. A-level evaluations require the most comprehensive set of information and material on the product, including source code.

7.3 Selecting evaluation procedures

Traficom determines and selects the procedures used in the evaluation in accordance with the product-related requirements that are based on the classification level, the threat assessment and the desired level of assurance. The procedures applied in the product evaluation are agreed upon during the planning stage.

7.4 Assurance level and the publicity of a statement or decision

As a rule, product evaluations are carried out at assurance level high. In such cases, the resulting statement is public unless the public authority needs it to remain non-disclosable. Statements regarding evaluations at lower levels of assurance are usually non-disclosable.

Traficom decides on a case-by-case basis whether a statement or decision is public. When assessing the publicity of the documents, Traficom takes into account the justified needs of the public authority customer and the manufacturer.

This is to ensure that product users are not mistaken about the content of the evaluation when they make product choices for their own systems. Traficom's public evaluations could easily be mistaken for universally applicable evaluations despite their limitations, and the effects of the limitations could go unnoticed by the authorities using the products. Therefore, Traficom only issues public statements about the fulfilment of requirements if it has access to sufficient information about the manufacture and technical implementation of the product and access to resources and information essential to the inspection and evaluation.

Combined with the need to control manufacture, this means that evaluations with high assurance levels can be carried out on foreign products only at classification levels IV/NR/EU-R.

7.5 Recognition of other approvals or certificates

Traficom may at its discretion take into account in its evaluation an evaluation of the product by an authority in another country or by a certification organisation. The use of this other evaluation depends on the purpose and basis of the evaluation and the information available on its content.

Product evaluations for the protection of classified information are always related to the protection of national classified information or the fulfilment of international information security obligations. These obligations do not involve any statutory requirements for the mutual recognition or crediting of evaluations by other parties (with the exception of international bilateral security agreements). Therefore, Traficom assesses the usability of other evaluations on a case-by-case basis.

8. Evaluation process

This chapter describes the main phases of the evaluation process. The evaluation process is illustrated in Appendix 1.

8.1 Tripartite process: Traficom, public authority customer and manufacturer

A product evaluation by Traficom becomes pending at the public authority customer's or manufacturer's request. These requests are discussed in more detailed in the next section. Regardless of who requests the evaluation, it is usually important that all parties together go through the objectives and main elements of the evaluation process.

All parties must have a common understanding of the assurance level at which the evaluation can be carried out and whether the intended outcome is public information about the result of the evaluation (or whether this would even be possible) or authority-specific information for a specific system. The actual technical evaluation process usually mainly consists of dialogue and actions between Traficom and the manufacturer, but it is advisable that all parties together identify the relevant reporting and information sharing needs. It is also important to have a common understanding of the fees charged for the evaluation.

8.2 Request for evaluation or approval

For Traficom to be able to evaluate a product, a public authority or the product manufacturer must request its evaluation.

It is advisable to contact Traficom about the need for an evaluation already when designing the product so that Traficom can provide guidance on the matter, take different needs into account in its prioritisations, plan the allocation of resources to evaluations and, if necessary, participate in the product development from the outset (see above, concerns security classification levels II and III).

An evaluation carried out at the manufacturer's request requires a product evaluation agreement between Traficom and the manufacturer and evidence of a public authority's need for the product.

Under the Evaluation Act, a public authority may request the evaluation of an information system. The evaluation may also only concern a part of an information system. The authority may request the evaluation of a product for the protection of national classified information or the approval of a product for the protection of EU or NATO classified information. The request may concern the evaluation of a product so that the outcome can be published as a universally applicable

evaluation (taking into account the preconditions concerning the origin of manufacture) or so that the product evaluation or approval only applies to a specific case and use in a specific authority's information system.

If necessary, Traficom will evaluate the product **as part of an authority's overall system**. At the request of an authority, Traficom can also evaluate an individual cryptographic solution or product that the authority is planning to acquire.

An authority may also request the case-specific evaluation or approval of a product of foreign origin. In the protection of national classified information, Traficom and the public authority customer must agree on how to assess the risk of foreign influence. Decisions about risks fall under the responsibility of the public authority customer. In the evaluation of whether international information security obligations are fulfilled, Traficom evaluates the matter and notes it in its approval decision or as part of a statement on the approval of an information system. Traficom may also examine how to take into account a valid approval issued in another country under EU or NATO security rules and any information available on the product.

The evaluation request must indicate the nature of the product the request concerns, the product development phase (design, preparation, production) and the intended security classification of the product.

Traficom may request additional information to determine whether the preconditions of an evaluation are met. If necessary, Traficom informs the manufacturer and the public authority customer in writing of the nature and main elements of the evaluation process (e.g. assurance level and whether the outcome can be public). Traficom will also inform them if the product does not qualify for an evaluation, stating the grounds for the refusal.

The party requesting the evaluation is required to provide sufficient information for the preparation of an evaluation plan, to name at least one suitable technical contact person to answer any questions that may arise during the evaluation and to commit to the evaluation project timeline. The party requesting the evaluation is also required, for its part, to enable the resources required for the evaluation project. This typically includes providing Traficom with the product to be tested, the requested documentation and product-related training, and reserving suitable personnel and facilities for the project.

Requests for a statement addressed to Traficom by accredited information security inspection bodies in connection with their own assignments are discussed in the guidelines for inspection bodies.

8.3 EU and NATO approvals

8.3.1 Approval of cryptographic products for the protection of EU classified information

Traficom has competence to approve cryptographic products for the handling of EU classified information in national systems at security classification levels EU RESTRICTED (EU-R) and EU CONFIDENTIAL (EU-C). Higher security classification levels always require an additional second party evaluation (SPE) by an AQUA[14] country and approval by the Council.

The inclusion of cryptographic products in the EU list of approved cryptographic products (LACP[15]) always requires an SPE by an AQUA country in addition to an evaluation and approval by a national CAA at all security classification levels.

[14] AQUA = Appropriately Qualified Authority
[15] LACP = List of Approved Cryptographic Products

Table 5 summarises Traficom's (CAA) competence in the approval of cryptographic products for EU classified information.

Table 4. Competence in EU cryptographic product approvals.

EU security classification (Finnish Treaty Series 77/2015, Article 2)	**Corresponding national security classification** (Finnish Treaty Series 77/2015, Annex)	**Traficom's CAA duty in cryptographic product approvals** EU Council security rules, 2013/488/EU, Article 10(6)
TRES SECRET UE / EU TOP SECRET (TS-UE/EU-TS)	ERITTÄIN SALAINEN YTTERST HEMLIG (TL I)	• **competent approval authority: Council** upon recommendation by the Security Committee • approval is based on a second party evaluation (SPE) and recommendation by an AQUA country • national CAA carries out a first party evaluation (FPE)
SECRET UE / EU SECRET (S-UE/EU-S)	SALAINEN HEMLIG (TL II)	• **competent approval authority: Council** upon recommendation by the Security Committee • approval is based on a second party evaluation (SPE) and recommendation by an AQUA country • national CAA carries out a first party evaluation (FPE)
CONFIDENTIEL UE / EU CONFIDENTIAL (C-UE/EU-C)	LUOTTAMUKSEL-LINEN KONFIDENTIELL (TL III)	• **national CAA may approve a cryptographic solution in a national system** • cryptographic solutions approved by the Council may also be used in a national system
RESTREINT UE / EU RESTRICTED (R-UE/EU-R)	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG (TL IV)	• **national CAA may approve a cryptographic solution in a national system** • cryptographic solutions approved by the Council may also be used in a national system

8.3.2 Approval of cryptographic products for the protection of NATO classified information

Traficom has competence to approve cryptographic products for the handling of NATO classified information at security classification levels NATO RESTRICTED (NR) and NATO CONFIDENTIAL (NC). Higher security classification levels always require an additional second party evaluation (SPE) by a SECAN authority and approval by the NATO Military Committee.

A company can also apply for the inclusion of its cryptographic product in the NIAPC[16] list but this requires, in addition to the approval, an endorsement by the national NCSA. The NIAPC website includes application forms for the inclusion of products in the list.

Table 6 summarises Traficom's (NCSA) competence in the approval of cryptographic products for NATO classified information.

[16] NIAPC = Nato Information Assurance Product Catalogue

Table 5. Competence in NATO cryptographic product approvals.

NATO security classification	Corresponding national security classification	Traficom's NCSA duty in cryptographic product approvals C-M(2002)49-REV1, Enclosure F, paragraph 11
COSMIC TOP SECRET (CTS)	ERITTÄIN SALAINEN YTTERST HEMLIG (TL I)	• **competent approval authority: Military Committee (NAMILCOM)** • approval is based on a second party evaluation (SPE) by a NATO body • national NCSA carries out a first party evaluation (FPE)
NATO SECRET (NS)	SALAINEN HEMLIG (TL II)	• **competent approval authority: Military Committee (NAMILCOM)** • approval is based on a second party evaluation (SPE) by a NATO body • national NCSA carries out a first party evaluation (FPE)
NATO CONFIDENTIAL (NC)	LUOTTAMUKSEL-LINEN KONFIDENTIELL (TL III)	• **national NCSA may approve a cryptographic solution in a national system** • cryptographic solutions approved by the Military Committee (for NS or CTS) may also be used in a national system
NATO RESTRICTED (NR)	KÄYTTÖ RAJOITETTU BEGRÄNSAD TILLGÅNG (TL IV)	• **national NCSA may approve a cryptographic solution in a national system** • cryptographic solutions approved by the Military Committee (for NS or CTS) may also be used in a national system

8.3.3 Security enforcing products in NATO security policy

Several NATO security policy documents refer to security enforcing products (SEP). The rules define certain categories of security enforcing products that always require NCSA approval in national systems. As part of a system inspection, NCSA approval may also be required for products not belonging in the specified categories.

The approval can be described as a two-step process:

- Approval of the product's suitability for the processing of NATO classified information in a national system (product approval by NCSA)
- Approval for using the product as part of a specific system (part of approval statement by SAA)

For some products, special requirements are set in the security policy. In other respects, national requirements apply, supplemented by applicable NATO documents, if necessary. The release of information to the manufacturer is discussed in section 4.2.

Security enforcing products may also be included in the NIAPC list. The NIAPC website includes application forms for the inclusion of products in the list. A company can also apply for the inclusion of its product in the NIAPC list but this requires, in addition to the approval, an endorsement by the national NCSA.

8.4 Traficom's prioritisation principles

Traficom prioritises product evaluation requests according to the same principles as requests for the evaluation of information and telecommunication systems. These principles are laid down in the Evaluation Act.

Evaluation Act, *section 4, Duties of the Finnish Communications Regulatory Authority subsection 3: The Finnish Communications Regulatory Authority carries out the tasks referred to in this Act within the limits of the resources available to it, taking into account compliance with international information security obligations and the significance of the requested measures for the general improvement of information security in the authorities' information systems and telecommunications arrangements.*

Thus, evaluation and approval tasks are prioritised taking into account compliance with international information security obligations and the significance of the requested measures for the general improvement of information security in the information systems and telecommunications arrangements of public authorities, i.e. an authority's need for a product. To be accepted for evaluation by Traficom, products must be needed by public authorities and they must have the potential to meet the needs of the authorities.

The evaluation of products intended for the protection of national classified information, in particular, requires that Traficom has sufficient personnel resources to carry out the task.

The scope of evaluations and the security classifications of information to be protected by the products are also factors taken into account in the prioritisation of tasks. A higher priority in product evaluations and approvals is given to products that can be evaluated at a high assurance level. The law does not include provisions on the origin of manufacture, but in practice the preconditions of evaluations with a high assurance level are mainly met by domestically manufactured products that are under Finnish jurisdiction. Limited evaluations are only intended for a restricted set of cases, for example as part of the evaluation of an information system. As a rule, prioritisation also depends on the availability of corresponding products. Evaluation requests must include an examination of whether corresponding products are already included in the list of products approved by Traficom or whether there is a need for the evaluation of a new product.

The regulatory framework does not include provisions on the possibility that a manufacturer would apply for an EU or NATO approval for its product. EU and NATO security rules do not take a stand on national administrative processes. Traficom prioritises needs associated with the information systems and telecommunications arrangements of public authorities, in accordance with the Evaluation Act.

8.5 Preliminary meeting between the manufacturer and Traficom

A preliminary meeting is held among the manufacturer and the evaluators from Traficom. If necessary, the public authority customer may also be represented to ensure the need for the product and to go through the whole evaluation process with all relevant parties. At the meeting, the parties agree on the practical aspects of the evaluation.

At the preliminary meeting, the parties discuss the information provided in advance by the customer. These include, as applicable, the following:

- Functional description of the product

- Discussion of the product promise and the functionality and performance of the product
- Discussion of the product's overall architecture, the surrounding elements and threat models

- Cryptographic techniques used in the product
  - Discussion of the product's cryptographic properties and solutions and the management of keys
- Evaluation target level
  - Discussion of the security classification and evaluation assurance level pursued and the related preconditions in the product's intended use
- Previous evaluations and tests
  - Discussion of any evaluations and tests the product may have undergone before
- Security issues concerning industrial security and product development
  - Review of the manufacturer's information security arrangements and the customer's/authority's potential need to request a facility security clearance on the manufacturer

At the preliminary meeting, Traficom discusses with the manufacturer and the public authority customer whether they want to share information about the product or the on-going evaluation with other authorities.

The documentation required for the evaluation is described in Appendix 2. Before the evaluation plan is prepared, the required documentation must be submitted to Traficom to the extent considered sufficient. However, the first preliminary meeting can be held even if exact documentation has not been provided on all the required topics. If the information needed to plan the evaluation cannot be delivered by the preliminary meeting or within reasonable time after the meeting, Traficom may suspend the process and use the allocated resources for other evaluations.

8.6 Estimated workload

For each product and product version, Traficom estimates the amount of work involved in the evaluation. The estimate gives a general description of the time needed for the different parts of the product evaluation and the total workload.

The manufacturer and the public authority customer are given an opportunity to comment on the estimate. The estimate is revised during the evaluation if the estimated amount of work changes significantly.

The purpose of the estimate is to help anticipate the schedule and the fee charged for the evaluation. The fee is discussed in the next section.

8.7 Traficom's fees

Traficom charges a fee for evaluations in accordance with the Decree of the Ministry of Transport and Communications on fees collected by the Finnish Transport and Communications Agency for services related to electronic communications[17] currently in force. The fee is determined according to the cost

[17] https://finlex.fi/fi/laki/ajantasa/2018/20180935 (in Finnish)

price based on the work and time needed to carry out the inspection and evaluation and to prepare and issue a statement or approval.

Under the Decree, a fee is also charged for any substantial performances associated with the processing of changes or derogations. A fee is also charged for the time spent on a suspended evaluation.

The liability to pay the fee applies to measures undertaken during the validity of the agreement with the manufacturer even if the validity of the agreement has ended.

The party ultimately responsible for the fee is either the manufacturer with whom Traficom has made the agreement under which the evaluation request is processed or the authority at whose request the application has become pending (upon application under the Evaluation Act) and processed by Traficom. However, the manufacturer and the public authority customer can agree on the liability for the fee and on whose invoicing details are provided to Traficom.

8.8 Evaluation

The purpose of the evaluation is to investigate whether the product meets the relevant information security requirements and whether it functions in the manner described.

During the evaluation, key observations are reported to the manufacturer and the public authority customer, enabling the manufacturer to make changes to the product. If changes are made, the required tests are performed again and the product evaluation is continued in accordance with the plan. Any changes and corrections made to the product during the evaluation may affect the evaluation schedule and costs.

The evaluation can be started once the customer has provided sufficient information about the product at the development stage.

8.9 Statement or approval decision and other documents

Once the evaluation has been completed, Traficom will issue a statement or an approval decision.

- Statement on compliance with the requirements for the protection of information at the security classification level [TL IV–TL II]
- Statement on partial compliance with the requirements for the protection of information at the security classification level [TL IV–TL II]
- (Statement on non-compliance with the requirements or an evaluation report indicating non-compliance)
- Decision on the approval of the product for the protection of [specific EU or NATO security classification level] information
- Decision on the (case-specific) approval of the product for the protection of [specific EU or NATO security classification level] information [in the information system of authority X]
- (If necessary, decision on non-compliance with the requirements)

Traficom’s statement or approval decision may be accompanied by the following documents, for example:

- Evaluation report
- Cryptographic statement
- Usage policy (SecOps)

8.10 Product life cycle management

8.10.1 Fixed-term validity of statements and approvals and the evaluation of changes

The statements and approval decisions that Traficom issues on compliant products are always valid only for a fixed term, as a rule no longer than three years. After the original period, the validity may be extended if the security of the product still meets the applicable requirements. The period of validity may also be shorter.

The manufacturer must actively maintain the security of the product. Critical software vulnerabilities must be fixed as quickly as possible, and Traficom must be informed about the matter without delay.

A statement or approval usually only applies to a specific product version. New software or product versions may therefore require a new evaluation. If a statement or approval is sought for an amended product, Traficom must be contacted about the matter. However, Traficom and the manufacturer may agree during the evaluation process on the types of changes that can be implemented in the approved product without the need to separately contact Traficom.

The above-mentioned management of changes applies to cases in which a statement has been issued on the product's compliance with the requirements for the protection of national classified information, and information about the statement has been published. It also applies to cases in which Traficom has approved a product for the protection of international classified information, and information about the approval has been published.

If Traficom has issued an authority with a statement on the protection of national classified information or a system-specific approval for the use of the product as part of an information system as required by an international information security obligation, the responsibility for monitoring changes in the product's information security features and, for example, the installation of updates lies with the authority responsible for the information system.

Notifications about technical changes can be classified as follows:

1) Planned changes must always be notified to Traficom for evaluation and approval before they are implemented if the changes may affect the product's cryptographic properties, operational safety, software architecture or any other factor central to product security.

   Traficom investigates and verifies the product's security features in part or in full, depending on the scope of the change.

2) Planned changes and their details must be notified to Traficom at least four weeks before the intended time of implementation when minor changes, such as configuration changes, are to be made to an approved product and these changes do not affect the product's security.

   Traficom evaluates the nature of the change and informs the manufacturer of whether the change can be implemented and distributed without a separate evaluation or whether the change requires an inspection by Traficom before it can be implemented and distributed.

The cryptographic and central information security features of the product must correspond to the approval even after the change, and it must be possible to use the product in accordance with its usage policy. If the actual software functionalities remain the same after the change, the change is considered minor and can be implemented without Traficom's evaluation.

3) When security updates are made for a product, Traficom must be informed without delay and in as much detail as possible about the distribution and scope of the change to the product.

   Depending on the scope and content of the security update, Traficom will evaluate the change either before or after the update.

   Security updates must be made to a product and distributed to customers without delay.

4) When a product undergoes brand-related superficial changes or similar changes that do not affect its cryptographic properties, Traficom must be informed about the distribution and content of the changes without delay and in as much detail as possible.

   Such changes can be implemented and distributed without Traficom's evaluation.

   The cryptographic and central information security features of the product must correspond to the original statement even after the change, and it must be possible to use the product in accordance with its usage policy.

Appendices

1. Description of the evaluation process
2. Materials required for evaluation (This appendix has been divided into two parts, a public one and a classified one. The classified part is disclosed separately to those who need it.)
3. Form for requesting the evaluation of a cryptographic product
4. Form for requesting the evaluation of a security enforcing product