SCHEME DEFINITION

Cybersecurity certification scheme for cryptographic modules certification based on ISO/IEC 19790

Content

Motivation

Cybersecure information and communications technology (ICT) requires using cryptographic mechanisms and protocols as a foundation layer. Having assurance in the correctness and security of such foundation layer is a prerequisite to be able to rely on any given ICT product. The classic design solution to provide this foundation layer is to concentrate the cryptographic services in a highly secure and specialized "cryptographic module".

The critical role of such cryptographic modules has always been recognized by ICT security experts, and their applicable security requirements have been subject to a currently mature level of standardization, testing and certification processes mainly carried by governmental parties.

The need to expand the assurance and cybersecurity certification of cryptographic modules to the industry at large has been the motivation for the definition of this private certification scheme, fully based on international standards, well-known governmental schemes, and supported by DEKRA owned bodies: a Certification body (CB) and a testing lab (ITSEF). It will help cryptographic modules manufacturers to provide greater visibility to final users and other stakeholders on the security capabilities of cryptographic modules.

Introduction

A certification scheme, as defined in ISO/IEC 17067, describes the rules, methods and organizational procedures for carrying out certifications related to specific products according to International / National standards and specifications.

This document describes a cryptographic module security certification scheme. The objective of the scheme is to provide an industry-wide security assurance framework to provide increases transparency of security capabilities of cryptographic modules.

The aim of the scheme is the independent conformity assessment by a third party for all interested organizations from the cryptographic modules industry. This certification scheme is applicable worldwide.

This certification scheme describes the organizational and functional approach for the conformity assessment of cryptographic modules. The basis for the conformity assessment are defined in the referenced standards and specifications.

How to apply?

Any manufacturer of cryptographic modules can apply for their products to be certify according to the rules and scope of this certification scheme.

The manufacturer can request the certification by sending an email to certification.cbs@dekra.com showing the interest for the certification. The manufacturer will receive the corresponding forms requesting information of the cryptographic module/s as well as information of the cryptographic algorithms implemented in the cryptographic module. The forms will contain the information related to accepted algorithms by this scheme.

The manufacturer shall submit the application consisting of the forms duly filled. The application form submitted must be signed by the manufacturer´s authorised representative.

Upon application review and approval, the manufacturer will receive a proposal for the certification including technical requirements, general conditions, prices, efforts and the certification agreement that is considered to be accepted with the acceptance of the proposal by the manufacturer.

DEKRA will assign a project manager which will act as a point of contact for the whole process.

Scope of the Scheme

Scope

This scheme is developed to cover products cybersecurity certification understanding it as the provision of assessment and impartial third-party attestation that fulfilment of specified requirements has been demonstrated. Products cybersecurity certification is carried out by DEKRA´s certification body which is ISO/IEC 17065 conformant.

The scope of this cybersecurity certification scheme is the security of cryptographic modules. The specified requirements for the cryptographic modules are contained in the ISO/IEC 19790 standard.

A cryptographic module may be implemented as software, hardware, firmware, or any combination of them. It can either be a part of a product or an entire product. The important aspect is that a cryptographic module implements cryptographic security functions and has a precise definition and a defined boundary.

The scheme covers the following security levels defined in the ISO/IEC 19790 standard for any type of cryptographic module:

Security level	Features	Expected use, notes
Level 1	Baseline level of security	In controlled environments, with complementing security provided by the operational environment
Level 2	Enhanced with tamper-evidence mechanisms and role-based authentication	Supports the operational security with evidence of tampering. This is the maximum level achievable by software means

The purpose of this certification scheme is to

a) provide consumers, users and, more generally, all interested parties of cryptographic modules assurance in the correctness of the cryptographic algorithms and security mechanisms implementation as well as in the security of the cryptographic modules, as required for different use and risk scenarios;
b) to allow manufacturers to demonstrate to the market that their cryptographic module has been attested to fulfil the ISO/IEC 19790 requirements by an impartial third party body.

Type of the Scheme

This cybersecurity certification scheme is developed to meet the requirements for a product cybersecurity certification **type 2** as defined in ISO/IEC 17067 requiring a third-party testing and a design appraisal of a cryptographic module against the requirements of ISO/IEC 19790, and in compliance with the rest of applicable testing standards and a surveillance program as a systematic iteration of conformity assessment activities for maintaining the validity of the certificate issued for a cryptographic module.

Functional approach

This cybersecurity certification scheme addresses a functional approach according to ISO/IEC 17067 consisting of the following functions:

- **Selection,** includes planning and preparation activities in order to collect or produce all the information and input needed for the subsequent determination function;
- **Determination,** conformity assessment activities such as testing to provide information regarding the product requirements as input to the review and attestation functions;
- **Review,** which means verification of the suitability, adequacy and effectiveness of selection and determination activities, and the results of these activities, with regard to fulfilment of specified requirements;
- **Decision** on certification;
- **Attestation**, which means issue of a statement of conformity, based on a decision following review, that fulfilment of specified requirements has been demonstrated;
- **Surveillance,** which means systematic iteration of conformity assessment activities as a basis for maintaining the validity of the statement of conformity.

NOTE 1: *Selection*. The activities are carried out by the ITSEF personnel. Upon request, the applicant shall provide the necessary documents or information to the ITSEF before, during or after the testing of the product.

NOTE 2: *Determination*. Conformity assessment activities such as documents review, testing and measuring are carried out by the ITSEF personnel.

NOTE 3: *Selection* and *Determination* functions are combined and will be referred to as "*Evaluation*".

NOTE 4: *Review*: Verification of the suitability, appropriateness and effectiveness with regard to the *Evaluation* activities, and the results of these activities, with regard to fulfilment of specified requirements. This activity is carried out by the CB personnel. The results of these activities are documented in the certification report.

NOTE 5: *Decision*: On the basis of the certification report, the certification body decides on the certification.

NOTE 6: *Attestation*: The conformity statement is confirmed by the issuance of a certificate of conformity by the certification body.

NOTE 6: *Surveillance*: The certification body will periodically carry out a surveillance during the certification period by carrying out validity reviews of each published certificate which shall serve as a basis for maintaining the validity of the certificates. The certification body also monitors the correct use of the certificate by the holder of the certificate.

Owner of the Scheme

Owner and Legal responsibility

The owner of the scheme is DEKRA Testing and Certification S.A.U. (DEKRA TC).

DEKRA Testing and Certification S.A.U. (DEKRA TC) is a legal entity in and of itself whose main shareholder is DEKRA España S.L. (owned by DEKRA SE).

Obligations of the Scheme Owner

The scheme owner has the following obligations:

- Design, development, operation and maintenance of the scheme (definition of the scheme scope, alignment with standards);
- Establishment of Certification Criteria (definition of security requirements, and assurance levels);
- Governance structure and Oversight;
- Quality Management System (QMS) establishment which uphold impartiality and independence in the certification process;
- Appeals and Complaints Handling;
- Develop a surveillance and monitoring program;
- Ensure the compliance with ISO 17067.

All the scheme owner obligations are delegated to the certification body.

Maintenance of the scheme

The scheme owner is responsible for the maintenance of the scheme.

This maintenance would supposed, but not limited to:

- Re-definition of the scheme scope or rules;
- Changes on the standards affecting the rules of the scheme;
- Changes on approved algorithms.

For changes on the rules, standards, approved algorithms or others affecting the certified products, the owner of the scheme will establish a transition period during which, rules or versions of the standard or algorithms previously accepted by the scheme and new rules or versions of the accepted standard or algorithms will coexist.

The manufacturer will be informed of the changes through the scheme web site. The manufacturer will be responsible for the maintenance of its certificates affected by the changes as defined in section Certificate lifecycle.

Bodies

DEKRA Testing and Certification S.A.U. holds a Conformity Assessment Body (CAB) consisting of a Certification Body (CB) and an Information Technology Security Evaluation Facility (ITSEF) or lab.

Certification body

The Certification Body is responsible for the certification activities, supporting and monitoring the performance of the ITSEF.

The CB also assumes all the scheme owner obligations.

The Certification Body operates in accordance with the provisions and expectations of ISO/IEC 17065 and is responsible for maintaining the accreditation including the ISO/IEC 19790 within the scope of ISO/IEC 17065 accredited certification activities.

ITSEF: Testing Laboratory

The ITSEF is responsible for the evaluation activities, as well as the execution of the surveillance program.

The ITSEF also supports the CB in its obligations. Among others, supporting in the

- Maintenance of the scheme;
- Establishment of Certification Criteria (definition of security requirements, and assurance levels);
- Quality Management System (QMS) operation;
- Develop a surveillance and monitoring program;

The ITSEF operates in accordance to the provisions and expectations of ISO/IEC 17025 and is responsible for maintaining the accreditation including the ISO/IEC 19790 within the scope of ISO/IEC 17025 accredited certification activities.

"Approved" algorithms are those accepted by the CAB. The ITSEF manager is responsible for the periodic revision (bi-monthly)of the [ACM], [TRAN] or Annex C of ISO/IEC 19790 [4] documents to update the list of "Approved" algorithms accepted by the CAB. The list of accepted algorithms is communicated to the manufacturer in the forms for the certification application.

Impartiality committee

The CB is dedicated to undertaking certification activities impartially and also eliminating risks to impartiality which arise from its activities and the activities of its personnel.

To safeguard the impartiality, the scheme includes an impartiality committee which meets once a year analysing the following aspects:

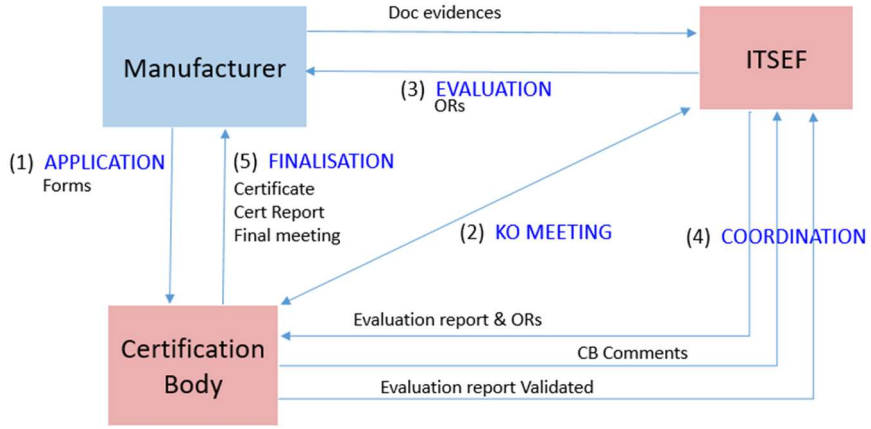
- Policies and principles concerning the impartiality of its activities within the Certification scheme;
- Any Conformity Assessment Body tendency to allow commercial or others considerations that impede the impartial and consistent provision of certification activities;

- Issues that affect the impartiality and confidence in the certification process, including transparency and aspects relating to Conformity Assessment Body staff.

Certification process

General

The certification process is represented by the following states and transitions:



[1] APPLICATION. The certification process begins with the manufacturer submitting an application by email. After receiving acknowledgement of the application from the Scheme, there is no further direct communication between the vendor and the CB, until the Evaluation report is issued by the ITSEF has been validated and the product is ready to receive the certification.

[2] KO MEETING. Scheme internal. Occurs only between the CB and the ITSEF and after the acceptance of the application.

[3] EVALUATION. This state addresses the scheme *Selection* and *Determination* functions. The evaluation is managed and executed by the ITSEF. The CB monitors the evaluation execution. The ITSEF becomes the interface with Observation Reports that will be sent to both the vendor and the CB, and the Evaluation reports submitted to the Scheme for their validation.

[4] COORDINATION. This state addresses the scheme *Review* function. The CB reviews the Evaluation reports sent by the ITSEF and may eventually send comments requesting additional information or clarifications and modifications to the reports.

[5] FINALISATION. This state addresses the scheme *Decision* and *Attestation* functions. When the Evaluation report is validated, the CB generates the certification report and the certification decision is addressed with a certification resolution. If the resolution is positive, the certificate is issued and it will be published in the web-site.

Application

An official application is required to begin the certification process signed by an authorized representative of the manufacturer which includes:

- Identification of the product to be certified.
- The scope of the product certification requested.
- Implemented algorithms and schemes
- Corporate entity, name, legal status, address of its physical location(s) and any relationships within a larger corporation, when applicable.

- Any other information relevant to the scope of certification for which is necessary for initial evaluation and surveillance.

The application forms are sent to the manufacturer by email.

On accepting the application, a proposal will be developed and sent to the manufacturer. The proposal will include the certification agreement which is considered accepted by the manufacturer on proposal acceptance. The manufacturer will receive a formal communication with the information associated to the project dossier and the ITSEF point of contact.

Evaluation

The evaluation process consists of two main phases:

1. Cryptographic algorithms validation. This phase addresses the validation of the approved algorithms implementation against the corresponding standards. "Approved" algorithms are those accepted by the CAB. "Approved" algorithms as well as transitions associated with the use of cryptography in respect to specific algorithms or key establishment schemes, security strengths, key lengths or crypto functions used as underlying algorithms will be according to [ACM], [TRAN] or Annex C of ISO/IEC 19790 [4] documents. "Approved" would include in this sense also as per a legacy use of the crypto function to process already protected information with an algorithm no longer valid. The algorithms will be tested against well-known implementations for the validation of their conformity with the standards. The well-known implementation is used in the corresponding testing tool and validation methodology.
2. Cryptographic module evaluation. This phase addresses the evaluation of the Cryptographic module itself to check the fulfilment of the requirements set for the Security level and CM category and characteristics according to [ISO 19790] and using the methodology described in [ISO 24759]. The Cryptographic module evaluation phase requires that the cryptographic algorithms have been previously validated in the Cryptographic algorithms validation phase.

Additionally and depending on characteristics and features of the cryptographic module, there are other activities that may need to be executed as part of the evaluation process:

For possible interpretations on how to apply the standard ISO/IEC 19790, the document [IG] maintained by the NIST shall be applicable.

Remote testing is allowed under the conditions defined in section 7.4 of [CMVP] document.

External certificates recognition

Certificates of crypto functions coming from well-established schemes, i.e. certificates of algorithms, Random Number Generator or key establishment schemes, will be recognized and accepted by the CAB. The existence of these certification schemes is not very frequent because it refers to schemes that certify the algorithms, Random Number Generator or key establishment schemes (such as CAVP).

In this case, public information of the certificate shall be enough to confirm that the certificate covers the algorithms or other elements declared (key length, modes, etc.) as well as the platform where the testing has been performed for the certification.

If the platform on which the algorithm has been tested was not the same as for the implementation under testing, the original certificate and the operational scenario will be

analysed case by case and the ITSEF shall include the corresponding rationale of the decision made in the evaluation report.

Finalisation

This state addresses the scheme *Decision* and *Attestation* functions.

Certification decision

Upon completion of the evaluation, the ITSEF submits the evaluation technical report to the Certification Body for its formal review. After the evaluation technical report approval, the CB prepares a Certification Report with a recommendation of certification which will be the base for the Certification decision.

The CB is solely responsible for the certification decision and is documented in the certification documentation.

When formulating a decision in regards to the ISO/IEC 19790 standard compliance, the certification decision would be one of the following natures:

a) certified: the target of the certification fulfils the criteria and its conformity is certified;

b) not certified: the target of the certifications does not fulfil the criteria and its conformity cannot be certified.

If the CB refuses approval of the certification, the manufacturer will be notified identifying the reason for disapproval and next steps.

The Certification decision is applicable to the different certification processes including:

- Granting initial target of certification
- Extending or reducing the scope of certification
- Suspension or withdrawal of certification
- Reinstatement of certification

Attestation

In case of a positive certification decision, a certificate is issued that reflects the scope of the certification, security assurance level and the validity period. Formal certification documents are issued only after approval of certification by the CB.

Upon approval of certification, the cryptographic module will be formally listed on CB's directory of certified products in the web site. The directory identifies the manufacturer name and address, the cryptographic module, the security policy, the date of certification, and the standard under which the product is certified and security level. The security policy will be published together with the certification documentation.

The CB provides formal certification documents to the manufacturer achieving certification which includes:

- The Certificate
- The Certification Report

Certificate lifecycle

Validity of the Certificate

The certificate validity period for a certificate is of five (5) years from the last or more recent issuance date.

Termination, Reduction, suspension or withdrawal of the certification

Upon a non-conformity of a certified cryptographic module or non-compliance by the client with the certification requirements (either as a result of surveillance or otherwise), the responsible of CB shall determine, based on the severity of the non-compliance, the appropriate actions to be taken by CB. Actions may include:

- Require the holder of the certificate to provide a reason for the non-conformance and a plan for corrective actions taken within 30 days.
- Require the holder of the certificate to immediately ensure that any continuing production and finished inventory is in compliance.
- Increased surveillance intervals.
- Issue a recall or public notice regarding the affected cryptographic modules.
- Administrative hearing.
- Reduce the scope of certification.
- Suspend certification.
- Withdraw certification.

If the action includes reduction of the scope, suspension or withdrawal of certification, the CB shall provide their approval before the action is carried out. Then, the CB shall take the actions specified by the certification scheme and shall make all necessary modifications to formal certification documents, public information, authorizations for use of the certificate, etc., in order to:

- for suspension/withdrawal: ensure that it does not provide any indication that the cryptographic module is still certified;
- for reduction of the scope: the reduced scope of certification is clearly communicated to the holder of the certificate and clearly specified in certification documentation and public information.

If certification is suspended, the CB shall assign one or more persons to formulate and communicate to the holder of the certificate the actions needed to end suspension and restore certification for the cryptographic module(s).

Upon suspension, withdrawal or a reduction of the scope of a certification, the CB immediately notifies the holder of the certificate of the decision and modifies all formal certification documents to indicate as such. Any revised certification documents are provided to the holder of the certificate.

It is the responsibility of the CB to assemble a plan for reinstatement which will allow the holder of the certificate to reconcile their certification status and communicate this plan to the manufacturer. If the plan for reinstatement involves complete re-testing of the cryptographic module, all applicable processes for product certification shall be followed.

Upon reinstatement of the certification status or a change in the scope of certification, the manufacturer shall be allowed to resume the use of the condition of certified cryptographic module.

If the certification is terminated by request of the holder of the certificate, the CB will ensure that there is no indication that the cryptographic module continues to be certified.

Certificate Maintenance

A certified cryptographic module refers to the version of the cryptographic module that has been evaluated and for which a certificate has been issued. The cryptographic module can suffer changes deriving it to a new version that differs in some respect from the previously certified. The new cryptographic module can therefore be, for example:

- a new release of the cryptographic module;
- the certified cryptographic module with patches applied to correct discovered bugs or vulnerabilities;
- the same basic version of the certified product, but in a new operational environment (e.g. on a different hardware or software platform) as reflected in a new Security Policy.
- changes affecting the cryptographic module certification due to scheme maintenance activities (e.g. re-definition of the scheme rules, changes on the standard, changes on approved algorithms).

Changes to a certified cryptographic module can therefore be:

- *Minor changes* has an impact that is sufficiently minimal to not affect the cryptographic modules assurance claim to the extent that the module does not need to be re-evaluated by a third party (the manufacturer is expected to have tested the changes as part of its standard regression testing) or a change in the manufacturer development life-cycle procedures in which the change can be shown to have no effect on the assurance obtained at the time of the original certification. Patches related to minor changes or patches implementing non-security related functionalities are changes included in this category.
- *Major changes* typically consist of changes to the claims about the cryptographic module and may result in changes to the previous certified product. They can be of technical or procedural nature that can impact security product integrity. They are substantial enough that affect the cryptographic modules assurance claim to the extent that the module needs a third party evaluation. Patches related to major changes or patches related to a confirmed vulnerability with effects on the security of the cryptographic module are changes included in this category.

An Impact Analysis Report (IAR) shall be developed by the manufacturer and refers to a report which records the analysis of the impact of changes to the certified product.

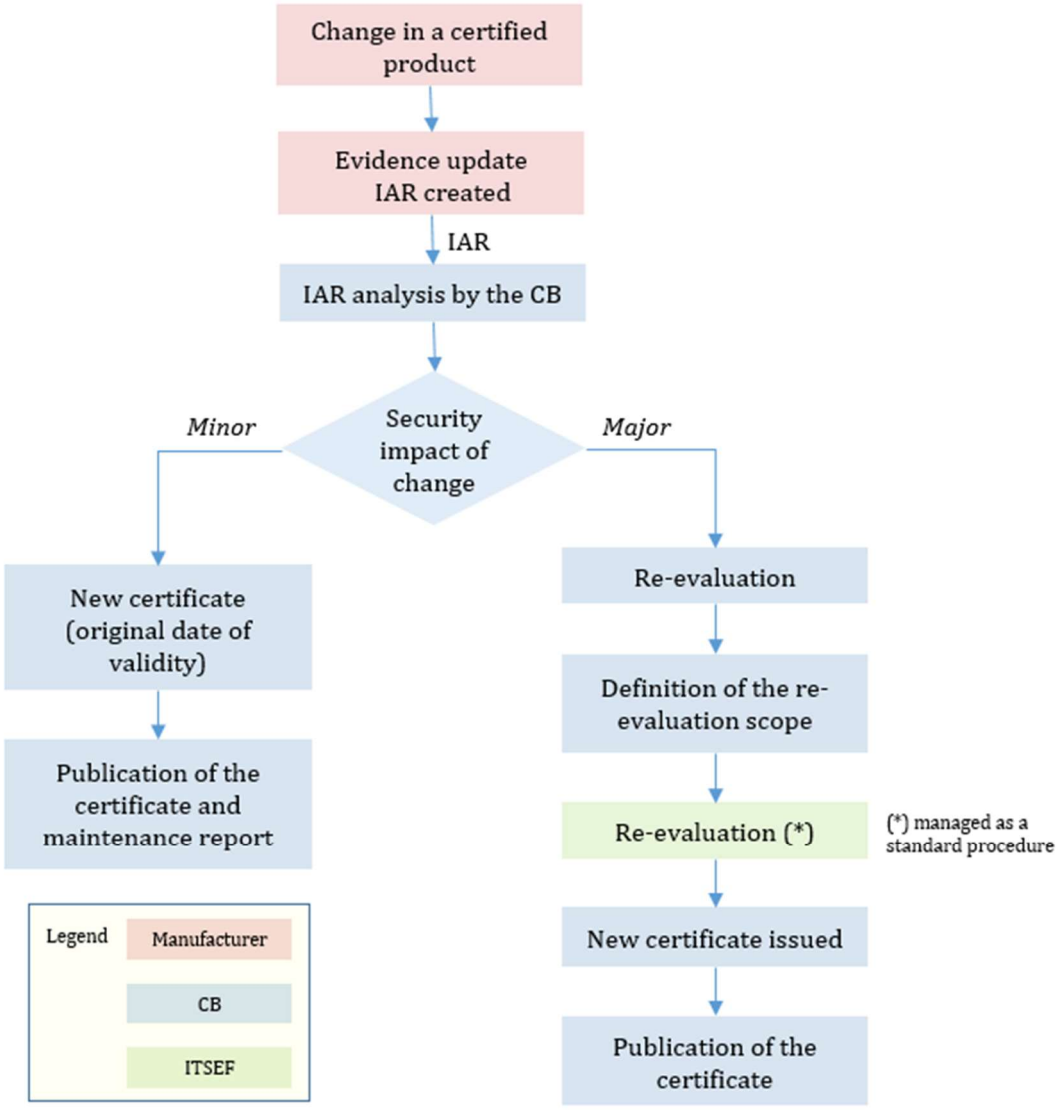
The CB shall examine the changes described in the IAR in order to validate their impact upon the assurance of the certified target of evaluation, as proposed in the conclusions of the IAR. Following the examination, the CB determines the scale of a change as *minor* or *major* in correspondence to its impact.

Where the changes have been confirmed by the CB to be *minor*, a new certificate shall be issued for the modified cryptographic module and a maintenance report to the initial

certification report will be produced. The validity date of the new certificate shall not exceed the date of the initial certificate.

Where the changes have been confirmed to be *major*, a re-evaluation shall be carried out in the context of the previous evaluation and by reusing any results from the previous evaluation that still apply. The re-evaluation process follows the evaluation procedure described in this document. Where applicable, a new certificate will be issued.

The following diagram summarises the process.



Surveillance

The surveillance involves periodically taking samples of the product from the market and subjecting them to determination activities to check that items produced subsequent to the certificate fulfil the specified requirements. As the acquisition of products on the market may in most cases be an impracticable scenario due to the price of cryptographic modules and the complexity of testing environments, this scheme defines a reasonable surveillance activity taking into account this particularity.

The CB will periodically carry out a surveillance during the period of validity of the certificate.

Every two (2) years, the certification body will carry out a validity review of each published certificate. Nevertheless, regardless of the official periodic reviews, in any time of a certified product cycle life the conditions that granted the certification are modified, the CB is entitled to withdraw the certificate according to the rules defined for the scheme maintenance.

The CB will inform the holder of the certificate that the surveillance process has started asking the holder of the certificate to submit to the CB:

- an updated analysis that the cryptographic module continues to meet the requirements established when the certification was granted;
- an updated copy of the record of the complaints received by the holder of the certificate relative to the security of the certified product or any other non-conformity found by any stakeholder in the cryptographic module compromising the requirements established when the certification was granted;
- the list of configuration items or Bill Of Materials (SBOM and HBOM where applicable) conforming the cryptographic module currently put on the market.

The holder of the certificate has two (2) months to send the requested documentation. Failing to do so the CB will suspend the certificate.

The CB will review the security policy of the cryptographic module and the documentation provided by the holder of the certificate identifying possible technological changes, new vulnerabilities or any other aspect that could invalidate the statements included in the security policy. In addition, the ITSEF will compare the list of configuration items or Bill Of Materials (SBOM and HBOM where applicable) provided by the holder of the certificate with the Bill Of Materials (SBOM and HBOM where applicable) obtained during the initial certification1 so that evidence of equality can be obtained.

The CB will also monitor the correct use of the certificate and mark of conformity by the certificate holder analysing publicly available sources of product information, such as web-sites, brochures, or technical documents that the manufacturer uses in promotion, sales or operation.

The CB will inform the holder of the certificate the conclusions of the surveillance including the new certificate status according to the conclusions. The new certification status could lead to the actions described in section Termination, Reduction, suspension or withdrawal of the certification.

[1] During the initial Certification, the ITSEF will request the manufacturer to provide the list of configuration items along with the corresponding hashes as part of the cryptographic module evaluation.

Rules for the use of the certificate and marks of conformity

The rules for the use of the certificate and marks of conformity are intended to ensure that the use of the certificate and marks aligns with the certification scheme's objectives and maintains the trust and confidence of stakeholders. These rules guide the holders of the certificates on how they can use the certificates, marks and associated information.

Only entities that have successfully undergone the certification process and have been issued a valid certificate are authorized to use the certificate and label the cryptographic module with a conformity mark.

The following rules apply for the use of the certificate or the marks of conformity used for labelling a cryptographic module as complying with the requirements of ISO/IEC 19790.

The holder of the certificate must use/reference the certificate and marks accurately and in a manner that reflects the specific scope, security assurance level and details of the certification.

The certificate shall not be altered, modified, or misrepresented in any way.

False or misleading claims that may give the impression of a broader certification scope or higher assurance level shall be avoided.

Where a manufacturer uses a certified cryptographic module within a product or products series, the certificate holder or the product manufacturer (if different entities) may assert the condition of certified cryptographic module by referencing the certificate when describing the characteristics of the product or by labelling the product identifying the condition of certified cryptographic module.

The reference shall be used in such a way that it is clear that it is the cryptographic module that is certified and not the product containing it.

In case of suspension, withdrawal or termination of a certificate, the holder of the certificate shall not provide any indication that the cryptographic module continues to be certified.

This scheme does not define specific label or marks formats and the holders of the certificate may use their markings as long as they comply with the rules for the use defined above.

The CB reserves itself the rights to update or modify the rules for the use of the certificate and conformity marks, and communicate changes to certified entities in a timely manner.

Complaints and appeals

Applicants of this certification service may appeal the conclusions of the CB.

- Written request by the manufacturer (or competent administration) sent by email to certification.cbs@dekra.com, formally showing and exposing as many allegations as it is considered appropriate in relation to the certification process. The CB shall perform acknowledgment of receipt of the appeal.
- The appeal will be owned by DEKRA TC DQA, thereby guaranteeing the impartiality of the process. The DQA shall ensure that there are no interest conflicts of during the process.
- The CB will analyse the matter, confirming if this is an aspect related to the certification activities.
- The CB shall adopt the corrective/preventive measures raised after the analysis. The staff involved in the certification activities covered by the complaint or appeal shall not participate in the analysis.
- After analysis, the conclusion will be notified to the applicant and appropriate corrective measures will be applied (if needed).

The interposition of the reasoned appeals will not discontinue the application of the adopted agreements. In case of any resource, complaint or appeal, the CB shall send an immediate response to the applicant with, at least, an acknowledgment of reception.

DEKRA TC reserves the right to make additional evaluations to solve the complaint. The costs of such additional assessments will be charged to the applicant or to the complaining party depending on the result.

In any case, this process of interposition of appeals, complaints and disputes will be reported to the applicant requesting the certification service.

Retention of records

The CB retains all records generated during the cryptographic module certification process which provide evidence that all of the requirements of certification are fulfilled.

Records by the CB shall be subject to a five (5) year retention policy.

Obligations of the holder of the certificate

The holder of the certificate must:

- ensure that all always fulfils the certification requirements, including implementing appropriate changes when they are communicated by the certification body;
- meet the procedural and legal requirements as per the certification agreement;
- follow the obligations of the evaluation and the surveillance procedure;
- follow the rules for the use of the certificate.
- keep a record of all complaints made known to it relating to compliance with certification requirements and makes these records available to the certification body when requested, and
    a. takes appropriate action with respect to such complaints and any deficiencies found in products that affect compliance with the requirements for certification;
    b. documents the actions taken;
- in case of providing copies of the certification documents to others, the documents shall be reproduced in their entirety or as specified in the certification scheme.

Certification fees

Certification activities

The following table shows the certification fees structured by security level. They cover the following certification activities: Management, Reports review, Certification report and Certificate issuance applicable to the evaluation or re-evaluation activities of the cryptographic module certification. These fees do not cover the evaluation of the cryptographic module itself.

Security level	Base Fees (€)	Notes
Level 1	5.000,00	
Level 2	8.000,00	

Entropy source validation

Regardless of the security level, in case of entropy sources validation, a delta fee of **500€** shall be added to the total certification fees.

Surveillance activities

The following table shows the certification fees for surveillance structured by security level.

Security level	Base Fees (€)	Notes
Level 1	1.000,00	
Level 2	2.000,00	

Certificate maintenance activities

The following table shows the certification fees for certificate maintenance. In case of re-evaluation, the corresponding certification activities table above shall be applied.

Security level	Base Fees (€)	Notes
Level 1	400,00	
Level 2	800,00	

References, Acronyms and Definitions

References

[1] ISO/IEC 17025. General requirements for the competence of testing and calibration laboratories.
[2] ISO/IEC 17065. Conformity assessment — Requirements for bodies certifying products, processes and services.
[3] ISO/IEC 17067. Conformity assessment — Fundamentals of product certification and guidelines for product certification schemes.
[4] ISO/IEC 19790. Security requirements for cryptographic modules.
[5] [IG] CMVP - Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program (NIST-National Institute of Standards and Technology / Canadian Centre for Cyber Security)
[6] [CMVP] FIPS 140-3 Cryptographic Module Validation Program Management Manual
[7] [ACM] SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms
[8] [TRAN] NIST Special Publication 800-131A Revision 2 Transitioning the Use of Cryptographic Algorithms and Key Lengths
[9] [NIST SP 800-90B] Recommendation for the Entropy Sources Used for Random Bit Generation
[10] [AIS20] BSI. Funktionalitätsklassen und Evaluationsmethodologie für deterministische Zufallszahlengeneratoren. Version 3.0 (15.05.2013)
[11] [AIS31] BSI. Funktionalitätsklassen und Evaluationsmethodologie für physikalische Zufallszahlengeneratoren. Version 3 (15.05.2020)

Acronyms

BSI	Bundesamt für Sicherheit in der Informationstechnik
CAB	Conformity Assessment Body
CAVP	Cryptographic Algorithms Validation Program
CB	Certification Body
CMVP	Cryptographic Modules Validation Program
DEKRA TC	DEKRA Testing and Certification S.A.U.
DQA	Director of Quality Assurance
ESV	Entropy Source Validation
HBOM	Hardware Bill of Materials
IAR	Impact Analysis Report
IG	Implementation Guidance
ITSEF	Information Technology Security Evaluation Facility
NIST	National Institute of Standards and Technology
QMS	Quality Management System
SBOM	Software Bill of Materials

Definitions

- Certification body (CB): means an entity of a conformity assessment body performing certification and related compliance activities related to the issuance of certificates
- Conformity assessment: process demonstrating whether specified requirements relating to a product, process, service, system, person or body have been fulfilled.
- Conformity assessment body (CAB): Entity that performs conformity assessment activities including calibration, testing, certification and inspection.
- Conformity assessment scheme/certification scheme, set of rules and procedures that describes the objects of conformity assessment, identifies the specified

requirements and provides the methodology for performing conformity assessment.

- Cryptographic algorithm, is a well-defined computational procedure that takes variable inputs, which may include cryptographic keys and produces an output
- Cryptographic module is a set of hardware, software and/or firmware that implements security functions within the cryptographic boundary.
- Information Technology Security Evaluation Facility (ITSEF), is an entity either subcontracted to or integrated in a conformity assessment body performing security evaluation, testing and auditing activities
- Owner of a scheme, person or organization responsible for the development and maintenance of a conformity assessment scheme.