BSI Certification Scheme for Cryptographic Module Security

Scheme outline

Your partner
in progress

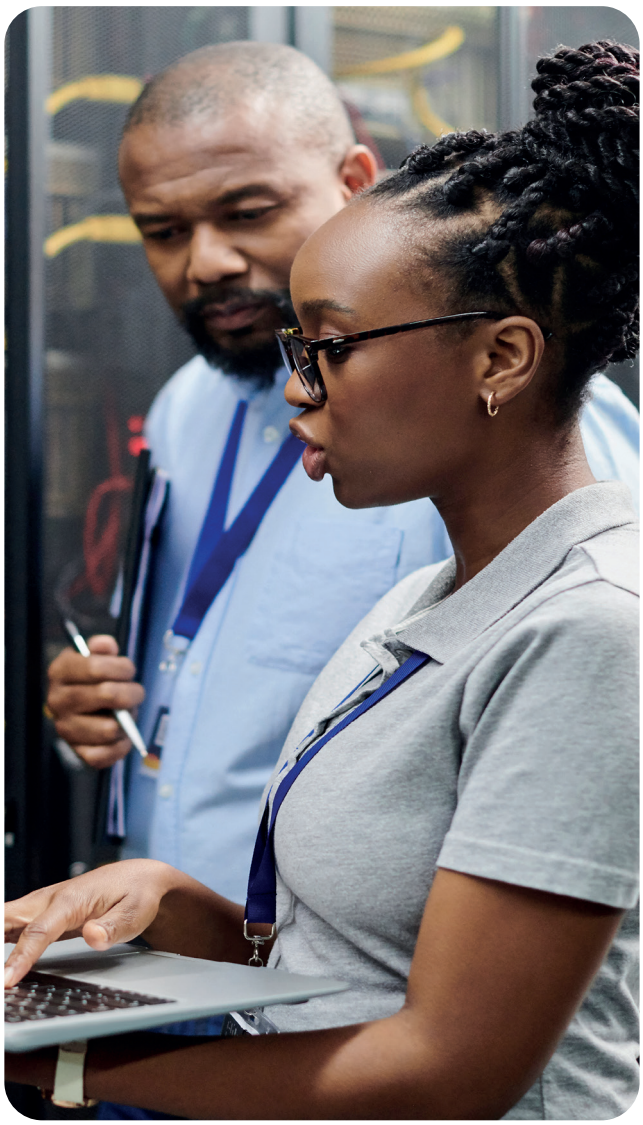
Introduction

This document contains details for the BSI certification scheme for cryptographic module security. This is a type 1a certification scheme in accordance with ISO/IEC 17067.

This scheme is based on independent evaluation of cryptographic module security against the requirements of ISO/IEC 19790, the international standard for cryptographic module security, by application of the test methods specified in ISO/IEC 24759. The output of this scheme is a Certificate of Conformity, valid for up to 3 years.

The objective of this scheme is to provide confidence to specifiers, purchasers, and users of cryptographic modules that the product incorporates security mechanisms conforming with the declared security level requirements of the globally recognised ISO/IEC 19790 standard. This is to aid the selection of cryptographic modules with a trusted level of security appropriate to their application.

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 defined boundary.



The scheme covers the four security levels defined in ISO/IEC 19790:

Security level	Description	Comments
Level 1	Baseline level of security.	Appropriate for use 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 modules.
Level 3	Includes measures to limit access to cryptographic secrets, and initial protections against hardware attacks.	Provides initial resistance against certain attacks that require hardware-based countermeasures. Useful for operational environments with less-than-optimal security.
Level 4	The highest level of security, includes special protection features against hardware attacks.	Provide state of the art hardware protection mechanisms, including active zeroization of secrets in case of tamper detection.

Roles and responsibilities

Applicant

The applicant is the entity seeking certification of a cryptographic module to ISO/IEC 19790.
The applicant is responsible for making available to the other parties the necessary access and information to enable the certification process to be carried out, including the cryptographic module security policy outlined in Annex B of ISO/IEC 19790.

Evaluator

The evaluator is an entity that is independent of the applicant, that carries out evaluation of the module(s) against the requirements of ISO/IEC 19790, according to ISO/IEC 24759.

The evaluator is responsible for producing report(s) confirming the results of their evaluation, the manner of testing employed, and providing details of the module(s) tested including information necessary to identify the module(s) tested, including version details.

The evaluator is responsible for providing their report(s) to the applicant upon completion of evaluation.

Technical reviewer

The technical reviewer is a person, operating on behalf of BSI, that is independent of the applicant and the evaluator.

The role of the technical reviewer is to review the evaluator's report(s), together with the cryptographic module security policy, to confirm:

- That compliance with the requirements of ISO/IEC 19790 has been achieved.
- The scope of compliance (e.g. modules covered, security level(s) achieved, coverage of requirements) is adequately documented, and can support certification.
- That the details of the test report(s) and the cryptographic modules, security functions and security levels described are in line with the cryptographic module security policy.
- The evaluator satisfies BSI data acceptance requirements (e.g. holds appropriate accreditation).

The technical reviewer may be the same person as the certification manager.

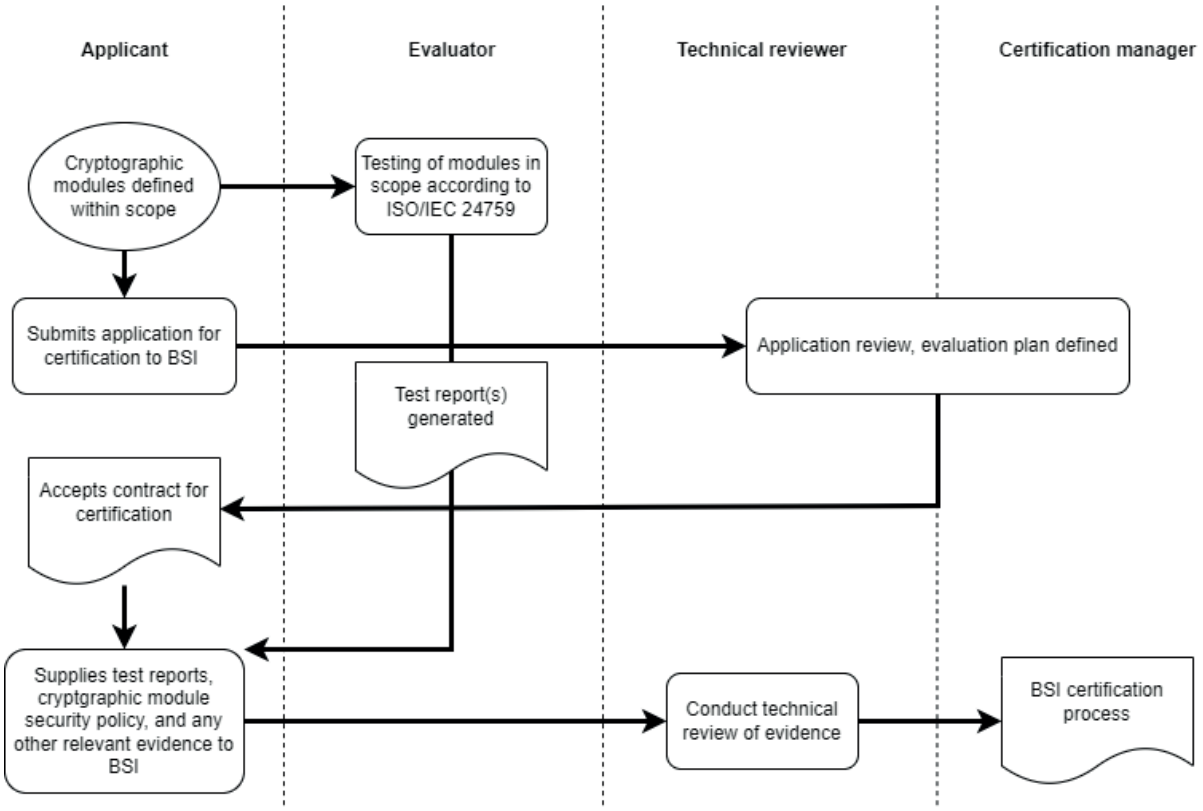
Certification manager

The certification manager is a BSI employee responsible for preparing the certificate of conformity and carrying out the certification review process in accordance with ISO 17065 certification process requirements.

The certification manager (in conjunction with the technical reviewer, where they are not the same person) is also responsible for the application review, which includes defining and documenting the evaluation plan.

The certification manager may be the same person as the technical reviewer.

Process outline



Certificate maintenance

Certificate modifications

It is recognised that changes may be made to certified modules, requiring the version stated on a certificate to be updated. A detailed change identification, description and impact analysis is to be provided by the module manufacturer and verified by the certification manager/technical reviewer.

Changes are permitted according to the following:

Type of change	Maintenance strategy	Example
Changes with no impact on the standards compliance or cybersecurity level.	Reissue of the certificate to the new module version.	Administrative changes. Addition of features not related to the certified functionality.
Mitigation of publicly known vulnerabilities, not modifying the module definition in the Security Policy.	Reissue of the certificate to reference the new module version.	Patches of vulnerabilities affecting open-source components that do not modify or correct the component functionality.
Changes to security-relevant features of the module or the declared security level.	Issue of a new certificate based on a regression or complete testing of the new module version.	Addition of new cryptographic algorithms. Modification of the module access control mechanisms.

Certificate renewal

Renewal of a certificate (e.g. at the end of the 3 year validity period) is based on the same testing as for initial certification. New test report(s) will be required and any report issued by the evaluator must clearly state that the module complies with all applicable requirements for the security level covered.

Any requirements not covered as part of the test plan must be referenced to a previous test program, and rationale for this provided (e.g. following verification by the evaluator that relevant parts of the module have not changed).

Find out more about BSI Certification Scheme for Cryptographic Module Security at:

https://page.bsigroup.com/cryptographicmodulesecuritycertification

BSI Group
389 Chiswick High Road
London, W4 4AL
United Kingdom
+44 345 080 9000
bsigroup.com

Your partner
in progress