Unlocking swift market access for cryptographic module security certification

A BSI white paper

Executive summary

In our increasingly connected world, we need to find a common, global approach to add pace to cryptographic module security certification.

ISO/IEC 19790 standard offers a practical baseline for cryptographic module security, accelerating the certification process by providing a common core that can be expanded as requirements evolve.

For several years, BSI has been actively engaging with manufacturers, users, and specifiers of cryptographic modules to comprehend the diverse needs and challenges across various industries.

By ensuring that test labs and their processes are standardized and accredited, it’s possible to build layers of trust to create a more transparent and efficient approach to certification around the world.

Cryptographic module security certification must be dynamic, adaptable, and pragmatic to support the evolving digital landscape. BSI is also investigating methods to expand the certification scheme’s scope to meet future needs.

Introduction

This is the third white paper in a series addressing cryptographic module security certification. In our increasingly digitally connected world, we need to find a common, global approach to improve the process of getting these important products to market.

To that end, BSI has engaged with manufacturers, users and specifiers of cryptographic modules to bring together the needs and challenges from different industry perspectives. In doing so, we are helping to shape a global solution based on international standards, supported by a flexible ecosystem of organizations and technologies.

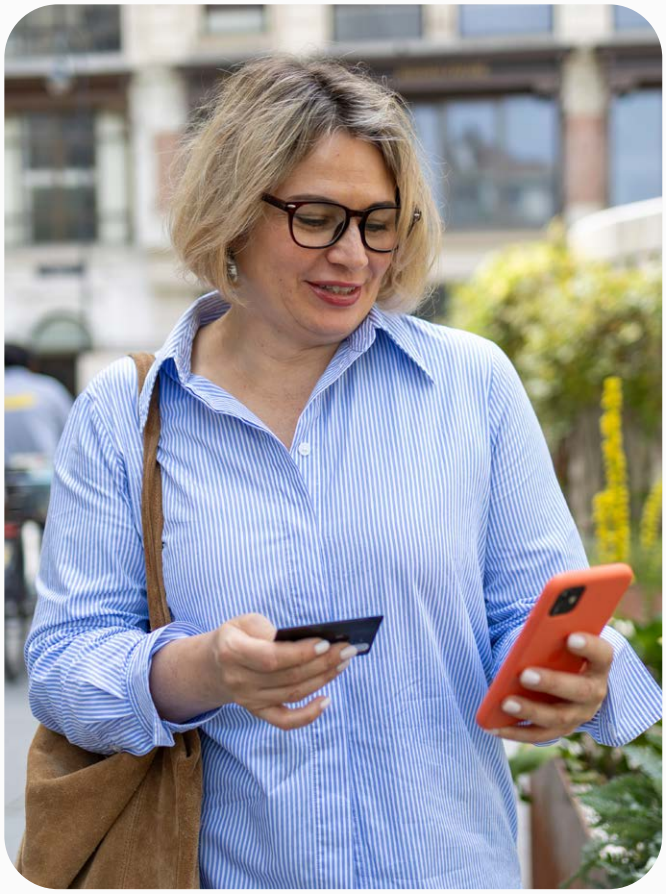
The cryptographic module market: Where we are and where we're going

Growing concerns around data breaches and cyberattacks is creating greater market demand for cryptographic module security certification across different markets, from governments, from education and healthcare, from cloud service operators, and many others.

Demand is also growing across different regions. In the Americas, for example, and in the Asia Pacific (APAC) region, the Middle East, and Europe.

The challenge – and opportunity – for enabling swifter market access for cryptographic modules comes from the trends around the world that are shaping the landscape of cryptographic module certification and related regional regulations.

Different countries and regions need flexibility to cater for regional requirements in cryptographic module security; however, the current lack of a consistent and reliable framework adds time and complexity to achieving certification, creating delays in getting digital products into the global market.



Summary of ISO/IEC 19790 standard based certification schemes worldwide

Country/Region	Regulation/Standard	Certification body/scheme	Standard used
USA	FIPS 140-3	Cryptographic Module Validation Program (CMVP)	ISO/IEC 19790 and ISO 24759 as modified by various NIST publications
Canada	FIPS 140-3	CMVP in partnership with the USA	As above
European Union	European Union Cybersecurity Act	European Union Cybersecurity Certification (EUCC)	Common Criteria for Information Technology Security Evaluation
Germany	Key Lifecycle Security Requirements	Federal Office for Information Security	Guidelines only
Spain	MEMEC	Centro Criptologico Nacional	ISO/IEC 19790
Turkey	TSE Cryptographic Algorithm Validation Program	Turkish Standards Institution (TSE)	ISO/IEC 19790
Japan	Japan Cryptographic Module Validation Program (temporarily suspended)	Information-technology Promotion Agency (IPA)	ISO/IEC 19790
Indonesia	BSSN Regulation No. 11 of 2024	BSSN (National Cyber and Crypto Agency)	ISO/IEC 19790 and ISO 24759
Malaysia	Malaysian Cryptography Validation (MyCV)	Information Security Certification Body (ISCB)	ISO/IEC 19790 and ISO 24759
China	Regulations on Administration of Commercial Cipher Codes	Commercial Cryptography Testing and Certification Center	GM/T 0028 modified from ISO/IEC 19790

The widespread adoption of ISO/IEC 19790 can facilitate such a framework – it is already gaining popularity in APAC, Europe and the Middle East – in turn enhancing trust and interoperability across international borders and increasing the speed to market. For example, NIST in the US has recognised its potential and adopted it as the basis for FIPS 140-3, albeit with modifications.

In the ISO/IEC 19790 standard we have the means to bring clarity and conformity to the global cryptographic module market, as well as the opportunity to accelerate speed to market to help meet the growing demand. It offers a practical baseline for the whole global digital ecosystem, if you will.

Developing a pragmatic approach to certification

ISO/IEC 19790 standard already forms the foundation of many regional standards for cryptographic module security. The certification based on ISO/IEC 19790 is designed to be both practical and broad enough in its scope to be able to comply with local regulations.

As such, it is uniquely positioned to provide an efficient and effective global approach to foundational cryptographic module security certification.

> BSI's certification process is designed to be as quick and efficient as possible, considerably quicker than current national schemes. However, this does not mean there is any compromise in the thoroughness of the certification scheme.

BSI's approach builds layers of trust through the requirement for testing laboratories and certification bodies involved in the certification process to also conform to specified standards. Namely, laboratory accreditation (BSI ISO 17025) and conformity assessment requirements for bodies certifying products (BSI ISO 17065), respectively. We explore how layers of trust are built in more detail on page 7.

Certification of cryptographic modules to BSI ISO/IEC 19790 offers several benefits:

- **Powering security assurance:** guarantee that cryptographic modules meet stringent security standards, ensuring confidentiality and integrity in information and technology devices.
- **Enabling national security and economic development:** supports national security and digital economic growth by providing reliable security guarantees.
- **Validation and trust:** ensures cryptographic modules are validated and trusted for use in a variety of operational environments, enhancing their credibility and global acceptance.
- **Standardization and compliance:** aligns cryptographic modules with internationally recognized standards for security, enabling interoperability across different systems and market applications, such as ICT, industrial, financial and other critical markets.

Because the BSI certification scheme operates independently of national programmes, it enables cryptographic module vendors to demonstrate compliance with the requirements of the standard and at the same time showcase the security level implemented in their cryptographic modules. Ultimately, certification helps to instil confidence in specifiers, purchasers and users of cryptographic modules.

Note:

- ISO 19790 is a type 1a certification scheme in accordance with ISO/IEC 17067 whereby only a representative sample of a product type is tested. The resulting certificate of conformity applies to that product type.
- Scheme based on an independent review of cryptographic module security against the requirements of ISO/IEC 19790, the international standard for cryptographic module security, by applying the test methods specified in ISO/IEC 24759.

Working towards a complete certification solution for emerging requirements

The pace of change in digital technology requires responsive, flexible certification. The BSI certification framework is designed to be just that. Its modular structure aligns with international standards, while national or user-specific requirements are accommodated through scalable security levels and cross-scheme global compatibility.

The existing variety of schemes and standards globally poses significant challenges to developing a universally applicable framework. This difficulty hinders cryptographic module vendors from supplying diverse markets. The time and cost required to gain access to one market limit the availability of these critical products in other markets that have not adopted the same certification requirements. However, it is this very diversity that also presents the opportunity to develop a flexible system that takes advantage of the many different experiences and approaches that exist.

How BSI is creating a flexible certification framework:

- Using key information from both international standards and national requirements
- Defining fundamental certification security requirements
- Establishing tiered security levels
- Instituting regular reviews and updates of the certification mechanisms and procedures.

This framework is designed to adapt to diverse regulatory national environments and requirements. Its success depends on meticulous harmonization strategies; in essence, it must balance security requirements with practical implementation from a testing and certification perspective, taking into consideration the requirements of national security certification, existing technological infrastructure, and local market conditions.

Working towards the creation of a simple and transparent scheme

IT security experts have long recognized that cryptographic modules play a critical role as a foundational part of the digital trust ecosystem. But how do you know if you can trust that a cryptographic module is secure? By applying widely trusted best practices from around the globe, BSI has developed a certification scheme for cryptographic module security that is built on *layers of trust, ensuring that each layer is applied consistently by all parties.*

This consistency – and strength of assurance – comes from the independent certification of each layer of trust:

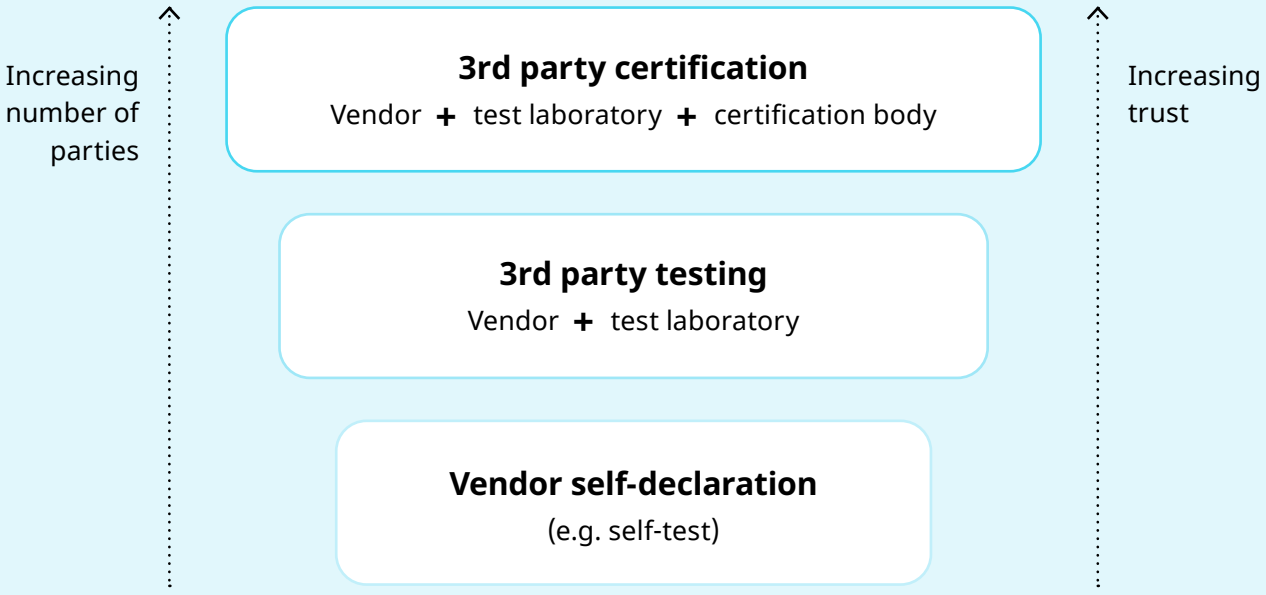
Testing requirements – based on the international standard ISO/IEC 24759 – specifies the methods used by testing laboratories to test whether the cryptographic module conforms to the requirements specified in ISO/IEC 19790. It also specified the information that cryptographic module vendors must provide to testing labs as supporting evidence.

Testing and calibration requirements – based on the international standard ISO/IEC 17025 – enables laboratories to demonstrate that they operate competently and generate valid results.

Certification body requirements – based on the international standard ISO/IEC 17065 – focuses on conformity assessment for bodies certifying products, processes and services.

Technical requirements – based on the international standard ISO/IEC 19790 – defines four security levels for cryptographic modules.

This comprehensive approach ensures that the certification body, testing laboratories and module vendors are all working transparently to the same set of requirements and understood test methods, using a common set of supporting documentation. Ultimately, it enables a common understanding between all stakeholders and a streamlined certification process, wherever in the world they may be.



How the BSI certification scheme works in practice

Role	Organization	Description	Output
Applicant	Cryptographic module vendor or party applying for certification on their behalf	Module development team has observed and implemented the requirements of ISO/IEC 19790 and ISO/IEC 24759 in the module design and documentation	Cryptographic module Cryptographic module documentation (including security policy)
Evaluator	Independent testing laboratory	• Operates according to ISO/IEC 17025 • Applies ISO/IEC 24759 when testing conformity with ISO/IEC 19790 • Minimum of two people involved: tester and reviewer	Testing report
Technical Reviewer	BSI (certification body)*	Conducts technical review of evidence from applicant and evaluator and confirms if conformity has been achieved	Technical review report (internal BSI document)
Certification Manager	BSI (certification body)*	Independent review of certification process to ensure compliance with overall process	Certificate of conformity

*a minimum of two people is involved in any certification. BSI's certification review and decision are never made concurrently by the same person.

What is covered by the certificate?

The BSI certificate of conformity granted relates to a specific module or modules, including the specific build of the module being tested – whether hardware, software or firmware – and the ISO/IEC 19790 security level achieved.

How long does certification last?

The certificate is valid for three years. During this period, the certificate can be updated to reflect changes in the certified module. At the end of three years, the certificate can be renewed.

An agnostic approach

Because the scheme is intended to have global reach, BSI has adopted an agnostic approach with regard to the use of any particular security function or the cryptographic technology permitted to be certified under the scheme. By focusing on security at a high level, it's possible for modules to be more readily applied to more than one context, reducing the need for additional testing and assurance outside of the scheme.

Driving efficiencies through learning

Since 2023, BSI has successfully issued ISO/IEC 19790 certificates to module vendors within an average process time of just five months; the shortest took just three months, with no compromise on quality.

Such short timescales can be transformative for organizations seeking to bring new, secure ICT products to a global market. At BSI, we've learned that the key to such agility is careful planning, clear communication, and adherence to guidelines at every step. For example:

Documentation
Ensure all required documentation is submitted to the certification body. This includes, but is not necessarily limited to:

- **Test reports** of the module in question against ISO/IEC 19790
- **Proprietary security policy** that defines items such as:
  - The modes in which the cryptographic module can operate (approved and non-approved)
  - The cryptographic boundary of the module
  - The input and output interfaces enabled in the module
  - The cryptographic algorithms the module supports
  - Access controls and physical security enforced to the module
  - Self-tests conducted by the module to ensure its correct operations

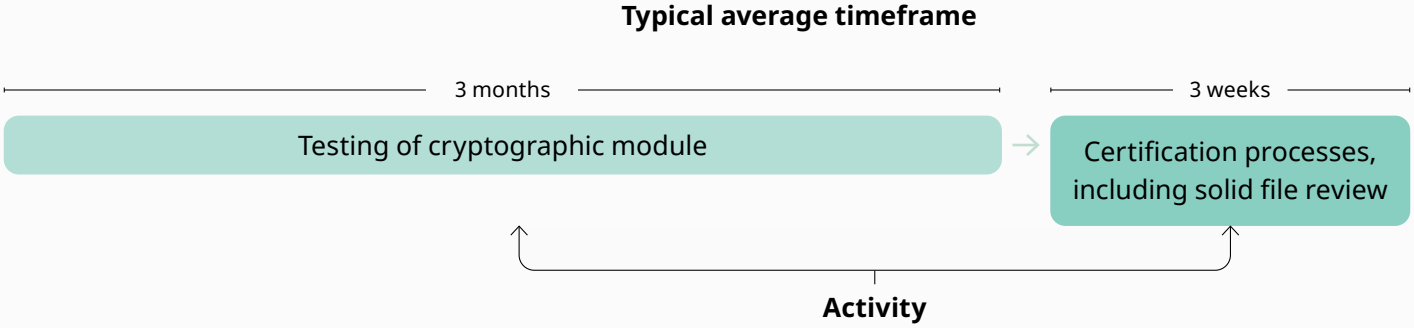
Language
All documentation must be submitted in English.

Details of test Infrastructure
Including details of how the module was accessed. For example, details of any remote connections or of the computer used to execute a software module during testing.

Transmitting and sharing of information between module management, testing laboratory and certification body
This is particularly significant where a module component has been previously tested and certified against the same standard. In such instances, it is possible to reach an agreement that re-testing of the component in question is optional, providing unambiguous evidence is supplied and the request is made in the initial application.

Typical timeframe for achieving ISO/IEC 19790 certification

The BSI certification scheme for cryptographic module security (ISO/IEC 19790) has facilitated organizations in achieving expedited turnaround times, as detailed below:



The latest phase encompasses the formal certification processes, which include a thorough review of the documentation and evidence provided by the organization. The solid file review ensures that all necessary information is complete and accurate, and that the cryptographic module complies with the specified security requirements.

Developing dynamic tools and testing mechanisms

The scope of the standard for cryptographic module security (ISO 19790) – with the standard for testing requirements (ISO 24759) – is currently limited to the following items:

- Cryptographic boundary
- Modes of operation
- Interfaces
- Roles, services and authentication
- Software/Firmware integrity
- Operational environment
- Physical security
- Non-invasive security
- Sensitive security parameter management
- Self-tests
- Life-cycle assurance
- Mitigation of other attacks

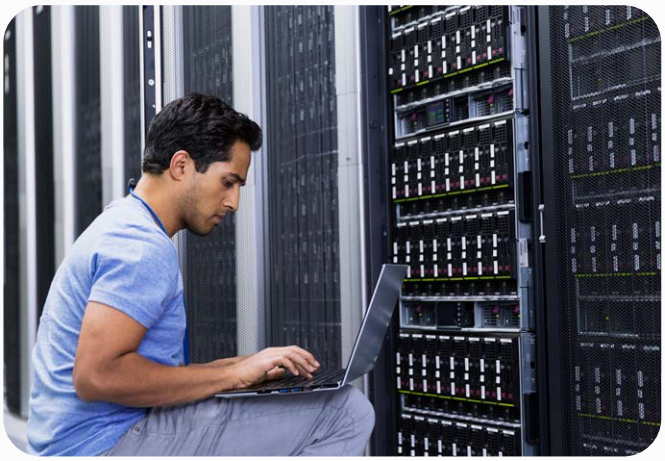
Required within the scope is the verification that the module implements at least one approved cryptographic algorithm when in the approved mode of operation. Annex C of ISO 19790 provides a non-exhaustive list of possible approved cryptographic algorithms. However, at this point in time, the BSI scheme is open to certification of cryptographic modules implementing security functions and algorithms from a variety of sources such as national standards and other known algorithms that are accepted by customers and users of cryptographic modules.

The standard currently does not define methods (or tools) that will allow a lab to evaluate the claimed cryptographic algorithms and therefore assure the correct functioning to prove that it is the algorithm claimed.

BSI is currently working with relevant stakeholders to determine a common approach to validating the implementation of cryptographic algorithms, including evaluating potential test tools.

While the standard and existing national schemes currently address ‘traditional’ approved cryptographic algorithms, industry is working towards post-quantum and quantum-resistant cryptographic algorithms. While significantly more complex than traditional algorithms, progress is being made towards certifying cryptographic modules incorporating such cutting-edge functionality.

BSI recognises the approaching challenge of such algorithms and the needs for our scheme, and the eventual approach to cryptographic algorithm validation in this scheme needs to take these into account. We are following closely the development of technologies such as module-lattice based cryptographic keys, among others. It is expected that a collection of post-quantum approved cryptographic algorithms, along with the tools to validate them, will be available in the future.



Conclusion

The rate of change – and threat – in ICT is ever-increasing. Existing regional cryptographic module security certification schemes have reached maturity and are at a stage where the slow process and lack of consistency in approach across regions is creating an insurmountable burden for organizations involved in the development and production of digital technology.

In contrast, BSI's certification scheme for cryptographic module security (ISO/IEC 19790) creates consistency across industries and regions.

By enabling the faster delivery of secure, innovative and transformative digital products to the global market, it is helping to increase trust in connected products and smart solutions.

BSI seeks to enhance its communication and cooperation with national regulators across various regions in the field of cryptographic module authentication. This will ensure that BSI's cryptographic certificates and testing reports facilitate market entry effectively.

About BSI

For over a century BSI has championed what good looks like and driven best practice in organizations around the world. As one of the founding members of ISO, we help make sure international standards developed address today and tomorrow's business and social needs, while delivering real benefits to an organization and all its stakeholders.

We work closely with leading manufacturers to ensure their products meet the latest Regulations to gain market access. We focus on delivering a testing and certification partnership underpinned by quality, safety, reliability and accuracy aligned to your product development requirements. That's why we're best placed to help you understand standards and to meet the requirements.

From shaping collective best practice with our knowledge solutions to product testing, certification, and environmental health and safety professional services, we are committed to innovating and collaborating with our clients to build a safer more resilient tomorrow – one that protects buildings, assets, the environment and most importantly people.

To learn how BSI can support your cryptographic module security certification and help you achieve swift market access, contact our team at: product.certification@bsigroup.com

For more details, visit www.bsigroup.com

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

