...making excellence a habit.™

# Cryptographic module certification: Ensuring data security with a common global approach

A BSI white paper

# Executive summary

ISO/IEC 19790 is enabling digital transformation by creating a common global approach to the security certification of cryptographic modules.

Standardization in this area provides many benefits to organizations, as some manufacturers are already experiencing.

However, there are still some challenges in moving forward with a common approach, causing increased risk, delays and cost to manufacturers and complexity in the ongoing maintenance of trust in products for users.

Varying national requirements for cryptographic algorithms can lead to increased costs and delays in products reaching certain markets due to the need for multiple certifications. ISO/IEC 19790 can enable a simple verification and  listing of the algorithms present within a module, allowing both manufacturers and users to ensure their products meet applicable use cases, policies and guidelines.

Test laboratory disparities and national preferences for differing test tools and environments present a further challenge to progress towards a common global approach. ISO/IEC 24759 and ISO/IEC 17025 help to ensure that testing is consistent and reliable by standardizing and accrediting test labs and their processes.

Regular updates and patches are essential for keeping digital products secure and resilient. However, regular re-certification is not technically or commercially practical. Creating a process whereby, for low-risk updates, a manufacturer can deliver in-house testing, within a scope pre-agreed by a certification body, can help to expedite release of potentially urgent software updates whilst mitigating data security risks.

ISO standards are key to digital transformation, creating a common approach that enables manufacturers to more quickly and efficiently get products to market, whilst ensuring they remain secure and resilient, and trusted by both manufacturers and end users.

# Introduction:

In our white paper, *Cryptographic module certification: The way forward*, we discussed how ISO/IEC 19790 is enabling digital transformation by creating a common global approach to the security certification of cryptographic modules – that is, the hardware, software, and/or firmware that carries out approved security functions within computer and telecoms systems.

An agreed, common approach to cryptographic module security certification is key to supporting robust crypto security and protecting sensitive information. Standardization in this area provides many benefits to organizations, including improved data security, an ability to build consumer trust across the world, time and cost savings, and reinforced business confidence in developing new digital products and solutions for global markets.

Manufacturers have completed the certification process and have seen the benefits of this new approach, which is currently in use by governmental certification bodies to ensure procurement of secure crypto modules.

There are, however, some key challenges in moving forward to a much more widely applied common approach, including:

- Varying national requirements for cryptographic algorithms
- Test laboratory disparities and national preferences for differing test tools and environments
- Ongoing changes in software and firmware updates making it difficult to maintain certification

> The implications of these challenges for manufacturers are increased risk, delays and cost due to the requirement for multiple certifications, certification method changes, and repeated certifications based on each software/firmware update. From a user's perspective this means delays and complexity in initial procurement, as well as complexity in the ongoing maintenance of trust in the products, with multiple certifications causing potential delays to urgent software updates.

In this white paper, we will explore the current progress of measures that are in place to address these challenges.

# Moving Towards a Common Approach

## Varying national requirements for cryptographic algorithms

Due to differing national use cases, policies and guidelines, there is disparity around which approved algorithms can be used for various applications across different countries and regions. These differing requirements can burden organizations with increased costs and delays in reaching certain markets, as it often means completing the certification process multiple times to meet the varying requirements of individual markets.

> It is essential that data security is maintained, but if the methods to do so are prohibitive, manufacturers will be deterred from developing new products and as a result digital transformation will be hindered.

ISO/IEC 19790 provides a single global standard for cryptographic modules.  It is focused on the security of the complete cryptographic module, including verification of which cryptographic algorithms are present. It deliberately does not test the efficacy of the algorithms used, with algorithms being selected from a pre-approved list. Therefore, certification using ISO/IEC 19790 confirms the security of the design of the cryptographic module and enables a simple listing, on page 2 of the certificate, of the algorithms present. The algorithms can then be tailored to meet the applicable use case, policy or guideline.

Using this flexible approach, national, sector and client-specific algorithms can easily be managed by both manufacturers and users. It allows consistency across industries and regions, and therefore quicker delivery of secure, innovative and transformative digital products to the global market. Specifiers and users can easily confirm with confidence whether the appropriate algorithms are present for a certified product from looking at the list on the certificate, rather than having to spend time searching through detailed test reports. This extends to scenarios where there are separate versions of a product with different algorithms embedded.

## Test laboratory disparities and national preferences for differing test tools and environments

As well as the disparities between algorithms used within different countries and regions, there are differing preferences between test labs and national bodies concerning which specific tools are used to test them.

There are two further ISO standards which exist to ensure that testing is consistent and reliable.

Testing labs are accredited against ISO/IEC 17025, the standard for the competence of testing and calibration laboratories. Within the scope of their accreditation, reference is made to the standards and schemes that they test against, for example ISO/IEC 19790. The purpose of this is to build a common global approach to testing and allow trust in an accredited lab to deliver reliable and consistent testing.

Therefore, test results from a lab can only be accepted if it is accredited to ISO/IEC 17025 with ISO/IEC 19790 within its scope. The certification process also requires that these test results are reviewed by an impartial, consistent and competent certification body, so the final statement of conformity to ISO/IEC 19790 meets all requirements of correctness, technical competence and transparency.

ISO/IEC 24759, which sits beneath ISO/IEC 19790, is a standard that details the required tests to perform for cryptographic modules. It details the specific methods that test labs should use to verify conformity with ISO/IEC 19790 and sets out the specific requirements for information that needs to be supplied by vendors to testing labs, evidencing that their cryptographic modules conform with ISO/IEC 19790.

To make this process more robust, it is recommended that in addition to ISO/IEC 19790, ISO/IEC 24759 is also included within a test lab's ISO/IEC 17025 accreditation scope. This standard adds an additional layer of consistency around the tools and methods used in cryptographic module testing, based on global consensus best practice.

Further assurance is provided by the fact that reputable testing labs can only gain their accreditation through their national accreditation bodies, which should be members of ILAC – the consortium of laboratory accreditation bodies – which applies both national and international standards, thus allowing global recognition (https://ilac.org).

Furthermore, certification bodies are accredited against ISO/IEC 17065 for certification of products. So, to add a further level of trust and consistency globally, certification bodies should have ISO/IEC 19790 within their scope of accreditation under ISO 17065.

> Using this approach builds further trust and consistency in the testing and certification process, removing the need for varying requirements for test processes and tools, as it becomes clear that testing and certification is being performed consistently in line with global best practice.

## Ongoing changes in software and firmware updates making it difficult to maintain certification

In the ever-moving digital world, a crucial element to keeping products secure and resilient is ensuring that regular updates and patches are applied. How can a product maintain its certification when it is constantly evolving? For most manufacturers, frequent re-testing is not technically or commercially viable.

For lower-risk updates, it would be possible for a manufacturer's own accredited test lab to test the update, rather than each individual update being tested by an independent lab. This is already used in practice by some manufacturers, with success. Keeping patch release testing in-house means it can be completed at a quicker rate and more effectively mitigate the risk it is protecting against.

A process to support this would be for the overall scope of a change to be agreed with the certification body, confirming whether an update can be classed as 'minor' and therefore reliably tested by the manufacturer's lab (subject to the lab being ISO/IEC 17025 accredited). The certification body would need to keep on track of the changes being made, to identify when so many minor changes had been applied that they effected a major change, which would then need to be referred back to the third-party testing environment.

> This process would provide sufficient trust in the ongoing validity of the product's certification, whilst offering a pragmatic and operationally viable approach to patch and update testing. It would also provide customers and end-users with the confidence that any potential data risks were being handled quickly and effectively.

# Conclusion

According to cybersecurity expert Miguel Bañón, "the combination of ISO/IEC 19790; setting security requirements to all aspects of a secure cryptographic module specification, design, development and operation; and ISO/IEC 24759 defining the strict conformity testing route that can lead to the compliance statement, provides the most efficient and assured method to mitigate risks associated with the use of cryptography. With these assurances in place, end-users can clearly distinguish which cryptographic modules they can trust for their use case and application scenarios."

David Mudd, Global Digital and Connected Product Certification Director, BSI, adds:

> "ISO standards represent global consensus best practice. They are created by teams of experts from around the world, with input from across all stakeholder groups, using a trusted and well proven development and governance process. Leveraging these incredibly powerful tools, in this case for defining cryptographic module security requirements and test methods, alongside general testing and certification best practice, would significantly help streamline the process of building and maintaining trust in cryptographic modules around the world through a single certification process. These products, so critical for our increasingly digital world, would get to market quicker and potentially vital updates would also be released quicker, whilst maintaining trust in their security and resilience."

# Contributors

**Miguel Bañón** is an expert in cybersecurity evaluation and certification, regulation, policy and standards development. He is a designer and developer of cybersecurity evaluation and certification schemes and labs in Europe, and he supports major vendors in certifying key technologies and products.

**David Mudd** is Global Digital and Connected Product Certification Director for BSI. He acts as expert and ambassador on the IoT, supporting the delivery of excellence and expertise across the 193 countries in which BSI operates. He sits on the IoT Security Foundation's working group for testing and certification, and has authored regulatory and technical guidance, written articles for a range of publications and is a successful global, keynote speaker and presenter.

# Why choose BSI?

Working with over 86,000 clients across 193 countries, BSI is a truly international business with skills and experience across multiple sectors, including automotive, aerospace, built environment, food, and healthcare. Through our expertise in standards development, knowledge solutions, assurance, and professional services, we improve business performance to help clients grow sustainably, manage risk and become more resilient.

# Our products and services

## Knowledge

The core of our business centres on the knowledge that we create and impart to our clients. In the standards arena we continue to build our reputation as an expert body, bringing together experts from industry to shape standards at local, regional and international levels. In fact, BSI originally created eight of the world's top 10 management system standards.

## Assurance

Independent assessment of the conformity of a process or product to a particular standard ensures that our clients perform to a high level of excellence. We train our clients in world-class implementation and auditing techniques to ensure they maximize the benefits of standards.

## Compliance

To experience real, long-term benefits, our clients need to ensure ongoing compliance to a regulation, market need or standard so that it becomes an embedded habit. We provide a range of services and differentiated management tools which help facilitate this process.

For more information on
Cryptographic module certification

Visit: **bsigroup.com**
Call: **+44 345 0765 606**
Email: **product.certification@bsigroup.com**

bsi.