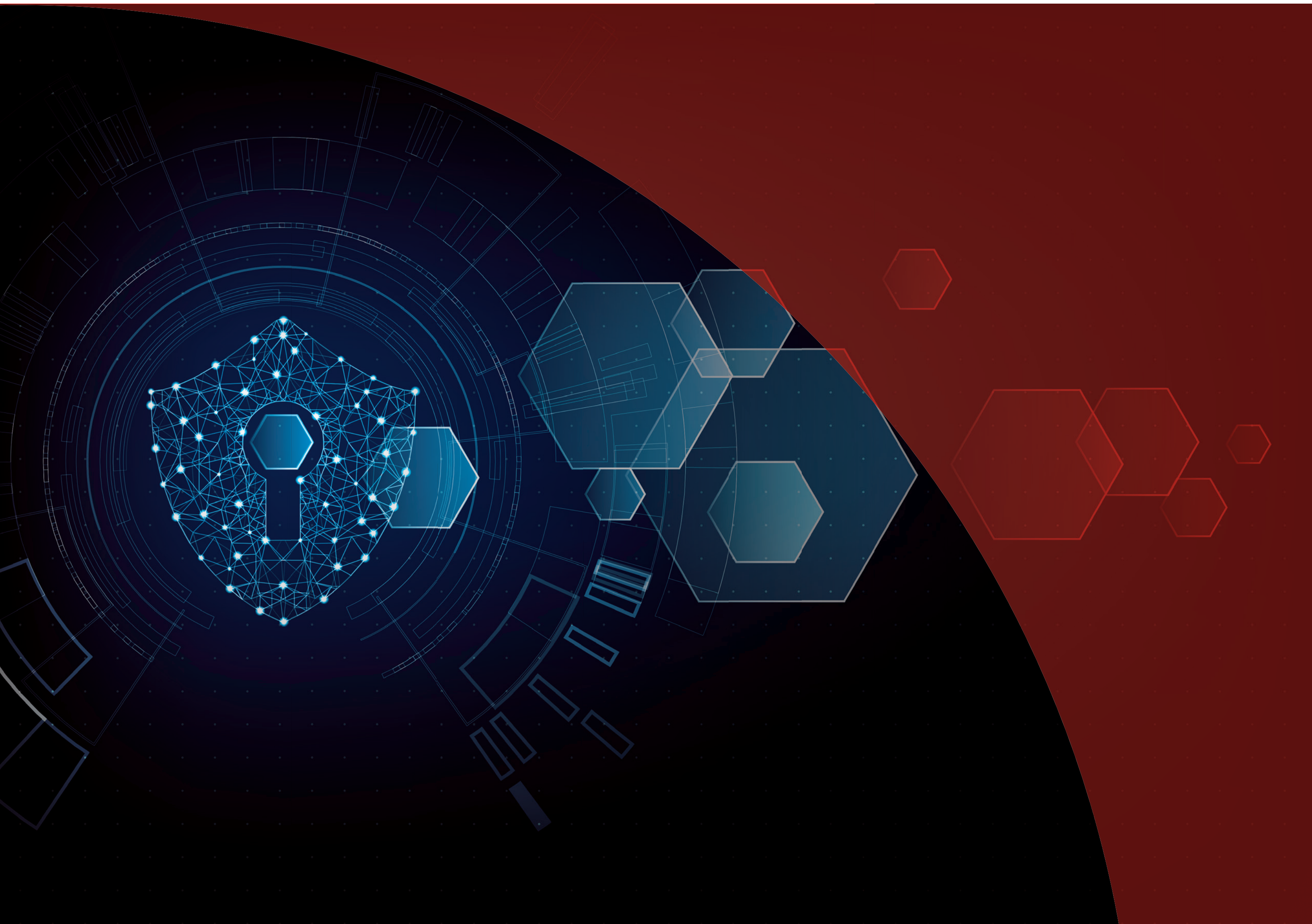
Cryptographic module certification: The way forward

A BSI white paper



1. Executive summary

Digital transformation presents astounding opportunities for industries and communities across the world, ranging from smart cities and future mobility to digital healthcare, fintech and much more.

But to succeed with digital products, services and solutions, global organizations must successfully address the critical challenge of data security.

Weak or compromised data security and safety is a very real and urgent issue, undermining the critical infrastructure supporting digital transformation, and leading to a lack of trust in connected products and smart solutions.

Ultimately, inadequate data security deters digital investment by organizations by destroying their confidence that such investment will yield healthy and reliable returns.

Today, effective data protection is provided by cryptographic mechanisms, and the security and reliability of such mechanisms depends on the cryptographic modules – the hardware, software, and/or firmware that carries out approved security functions – in which they are implemented. Put simply, 'crypto' is critical.

The requirements for verifying the suitability of cryptographic modules are increasingly being based around ISO/IEC 19790, a global standard that specifies the necessary security features. But around the world, approaches to compliance with, and certification to, the standard is fragmented. This inhibits innovation, increases products costs and slows down time to market.

Governments, regulators, manufacturers and other organizations with an interest in promoting successful global digital transformation can enhance data security by addressing and unifying this fragmented approach.

Wider understanding is needed to ensure the underlying assurance and quality of cryptographic services by the industry at large. An agreed, common approach to cryptographic module certification is key to supporting robust crypto security and protecting sensitive information in computer and telecoms systems.

The shared goal is to enable organizations to improve data security, make time and cost savings, build consumer trust across the world, and reinforce business confidence in developing new digital products and solutions for global markets.

BSI can help. By bringing together stakeholders, creating the right ecosystem, and gaining consensus, we can play a leading role in the development of a common approach to cryptographic module certification.

2. Introduction – the fourth industrial revolution

Today's automated/digital trend has been called 'the fourth industrial revolution', a term that describes one of the most rapid periods of change the world has ever experienced.

Centred around the automated collection and sharing of data, alongside communication between human and machine, and machines with each other, innovations such as the Internet of Things (IoT), Big Data, and artificial intelligence (AI), move physical products and assets from static structures into connected ecosystems.

From coping with COVID-19 and cutting carbon emissions to automating mobility and delivering telehealth – and much more – digital transformation presents astounding opportunities for industries and communities across the world.

With the right digital transformation strategies and support in place, organizations will have the tools they need to seize countless new opportunities presented by the fourth industrial revolution. But to do so, they must achieve and maintain resilience, and this means successfully addressing one issue above all others – the challenge of data security.

3. The need for data security

With the dramatic acceleration of digital adoption and transformation comes growing demand for secure and resilient digital infrastructure. Weak or compromised data security and safety is a very real and urgent issue, undermining the critical infrastructure supporting digital transformation, and leading to a lack of trust in connected products and smart solutions.

Ultimately, inadequate data security deters digital investment by organizations by destroying their confidence that such investment will yield healthy and reliable returns.

With the advent of smart cities, automated transport, fintech, and remote healthcare, there is an immediate need across the whole global economic landscape for robust protection of data, in order to:

- Protect data against risks such as unauthorized disclosure or modification
- Authenticate the identity of users or entities that may access the data
- Provide 'non-repudiation' – assurance that the sender of information receives proof of delivery, and the recipient receives proof of the sender's identity, so neither party can later deny having processed the information.

4. 'Crypto' is critical

Such data protection is provided by cryptographic mechanisms, and the security and reliability of cryptographic mechanisms depend on the cryptographic modules – the hardware, software, and/or firmware that carries out approved security functions – in which they are implemented.

To the layman, reference to cryptographic modules may sound like the 'technobabble' of ICT gurus and geeks, and this explains why the importance of 'crypto' remains poorly understood by non-specialists. Experts agree, however, that the key issue facing organizations is not technical, but strategic.

For digital transformation to progress, and for organizations to fulfil their potential around the world, it is vital that decision-makers recognize the common need for transparent and robust data protection and take steps to enable the creation of secure, cryptographic modules that can be relied upon globally.

5. Fragmented history

Over time, nations and economically aligned regions around the world developed their own specific requirements for verifying the suitability of cryptographic modules within their borders, but with increasing globalization this situation has become increasingly untenable.

As cyber security expert Miguel Bañón explains, "Security requires solid crypto and this is very well understood by specialists around the world, but differing requirements were established in many different geographical areas, as suited by different demands." He cites the US government computer security standard FIPS 140-3 as a prominent example. It is also typical in being a government-inspired standard, with take-up led by public sector organizations.

Bañón continues, "A fragmented situation is unhelpful in today's increasingly integrated world – there can be no discussion of globalization without also discussing the need for common cryptographic standards."

He adds:

> "An international approach is a key enabler of so many business models and the development of a global crypto standard has followed this rationale."

6. The global standard – ISO/IEC 19790

In 2012, following a period of worldwide collaboration, a global standard was launched, entitled ISO/IEC 19790: Information technology – Security techniques – Security requirements for Cryptographic modules. The standard was moulded by input from many nations and backed by approval from over 200 national bodies.

In practice, ISO/IEC 19790 specifies the security requirements for a cryptographic module used within a security system protecting sensitive information in an ICT system. It sets out four security levels for cryptographic modules, in order to cater for varying degrees of data sensitivity.

They range from, for example, low-value administrative data to classified government information. The four security levels also take account of different application environments, ranging from, for example, removable media in an unprotected location to a highly guarded data centre.

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

> "The pragmatic approach taken within the standard is to ensure that approved security controls applying to the cryptographic algorithms are in place. This allows for flexibility over which pre-certified algorithms are used and removes the need to verify the efficacy of these controls."

7. Verification challenges

The requirements for validating the suitability of cryptographic modules are now increasingly based around ISO/IEC 19790. This includes, with some modifications, the latest iteration of the US's FIPS 140-3 certification scheme, known as CMVP.

Some other nations, including Spain and Turkey in Europe, and China, Japan, and Korea in Asia, also have their own crypto-module validation process. They are all based on ISO/IEC 19790, but with differing requirements around which approved algorithms can be used and which tools should be used to test them. They also generally require their own national labs to do the testing.

Such geographical disparities have placed an onerous burden on global manufacturers, who currently have to go through a separate certification process for each market they intend to sell into. As Mudd explains, "This adds costs and delays to the detriment of getting the most up-to-date, secure and effective equipment into the market and allowing business growth and resilience through cutting edge IT Infrastructure."

8. Certification solutions

Experts agree that the obvious answer to the problem is to structure industry-based certification schemes that allow common approaches based on the globally accepted best practice encompassed in ISO/IEC 19790. The key objective of such schemes is to reduce the global fragmentation of the management of cryptographic module security, while also allowing for national differences.

Mudd is confident that, through global and pan-industry collaboration, such schemes can be developed, providing "pragmatic certification and continual assurance against ISO/IEC 19790, with a clearly visible schedule of approved algorithms verified and approved test tools used." He adds, "The schemes must also facilitate rapid processes for testing and certification to satisfy technology developers aiming to provide solutions in today's fast-paced global market."

Mudd believes that BSI can help: "As an independent body and a leader in the development of international standards and assurance solutions, we are well-placed to promote cross-border, pan-industry collaboration. We have a world-class cyber security capability, recognized by CREST global accreditation, combined with decades of experience in product assurance and testing."

He continues,

> "By bringing together stakeholders, creating the right ecosystem, and gaining consensus, we can play a leading role in the development of a common approach to cryptographic module certification."

9. Conclusion

Cyber security expert Bañón observes, “We’ve reached a turning point. Until now, crypto-module security has been driven by governments, with commercial organizations lagging, but with today’s massively increasing need for smart solutions, we need crypto security everywhere.”

He adds, “If you want to sell your smart product to the world, you must be trusted from the start, or you won’t succeed. ISO/IEC 19790 is voluntary, but it’s a very effective standard that ensures a high level of crypto security. If your organization adopts it, it won’t let you down.”

According to BSI’s Mudd, wider understanding is needed to ensure the underlying assurance and quality of cryptographic services by the industry at large. An agreed, common approach to cryptographic module certification is key to supporting robust crypto security. “Our shared goal is to enable organizations to improve data security, make time and cost savings, build consumer trust across the world, and reinforce business confidence in developing new digital products and solutions for global markets.”

He concludes,

> “What we need to do now is drive the take-up of ISO/IEC 19790 by creating a common approach to certification against the standard that will be globally recognized and valued.”

10. Contributors

Miguel Bañón is an expert in cyber security 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 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 is the knowledge 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 that help facilitate this process.

For more information
visit: **bsigroup.com**

bsi.