Collaborating towards a secure digital future

A global approach to cryptographic module security through ISO/IEC 19790

Barcelona February 27th 2024

Collaborating towards a secure digital future with ISO/IEC 19790

Subject	Speaker	Organisation	Time
Introduction	David Mudd	BSI	10:15
Keynote talks			
Real-world applications and implications for a generic approach to cryptographic module security certification	Roland Atoui	Red Alert Labs	10:30
Testing tools for ISO/IEC 19790: how to build them and how we can trust them: benefits of a common approach	Luis Garcia	DEKRA	10:50
A global certification scheme for ISO/iEC 19790: an introduction to the process and benefits	Mustanir Ali	BSI	11:10
Networking break			11:30
Panel Discussion: Engaging with industry sectors and regulators to address specific needs/concerns using a consistent global approach. Future trends	BSI, DEKRA, TUV Rheinland, SERMA, RED Alert Labs, ISO WG Convenor, SGS, Huawei	BSI, DEKRA, TUV Rheinland, SERMA, RED Alert Labs, ISO WG Convenor, SGS, Huawei	12:00
Q&A on panel discussion	All	All	12:30
Summary, white paper, next steps	David Mudd	BSI	12:40
Closing remarks	David Mudd	BSI	12:45
Event finishes			12:50

Cryptographic Module Security

A common global approach:

The journey so far….

Surely there’s a better way?

Who benefits from a common approach?

- Manufacturers
- Governments, system providers
- Society, users

bsi.

Cryptographic module certification: The way forward

A BSI white paper

bsi
Cryptographic Module Certification
"Building Trust in a Common Approach"
bsi.

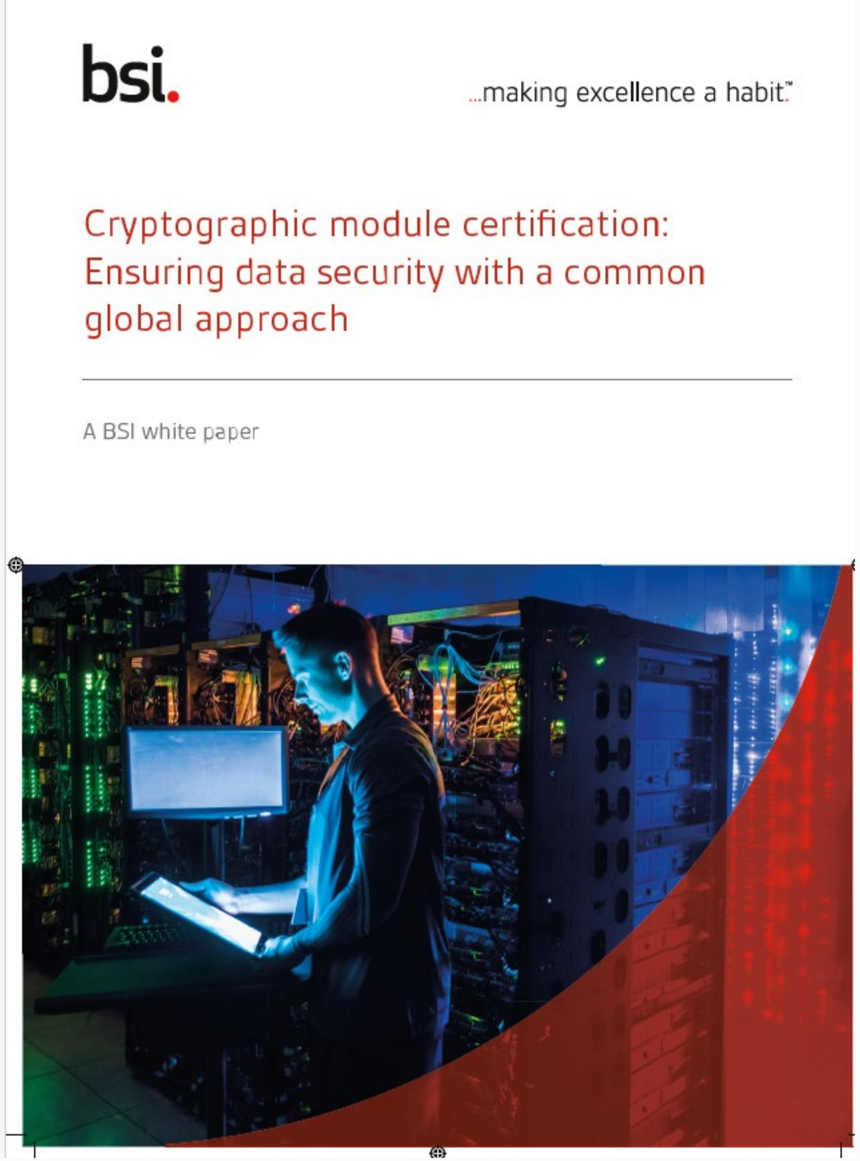
Where do you start with a common approach?

Global consensus best practice

ISO/IEC 19790 – best practice "security by design" for cryptographic modules

What does a common approach look like

- ISO/IEC 19790 – core baseline
- Accommodate national algorithm requirements
- Accredited Lab – test environment
- Accredited Certification Body



bsi. ...making excellence a habit.™

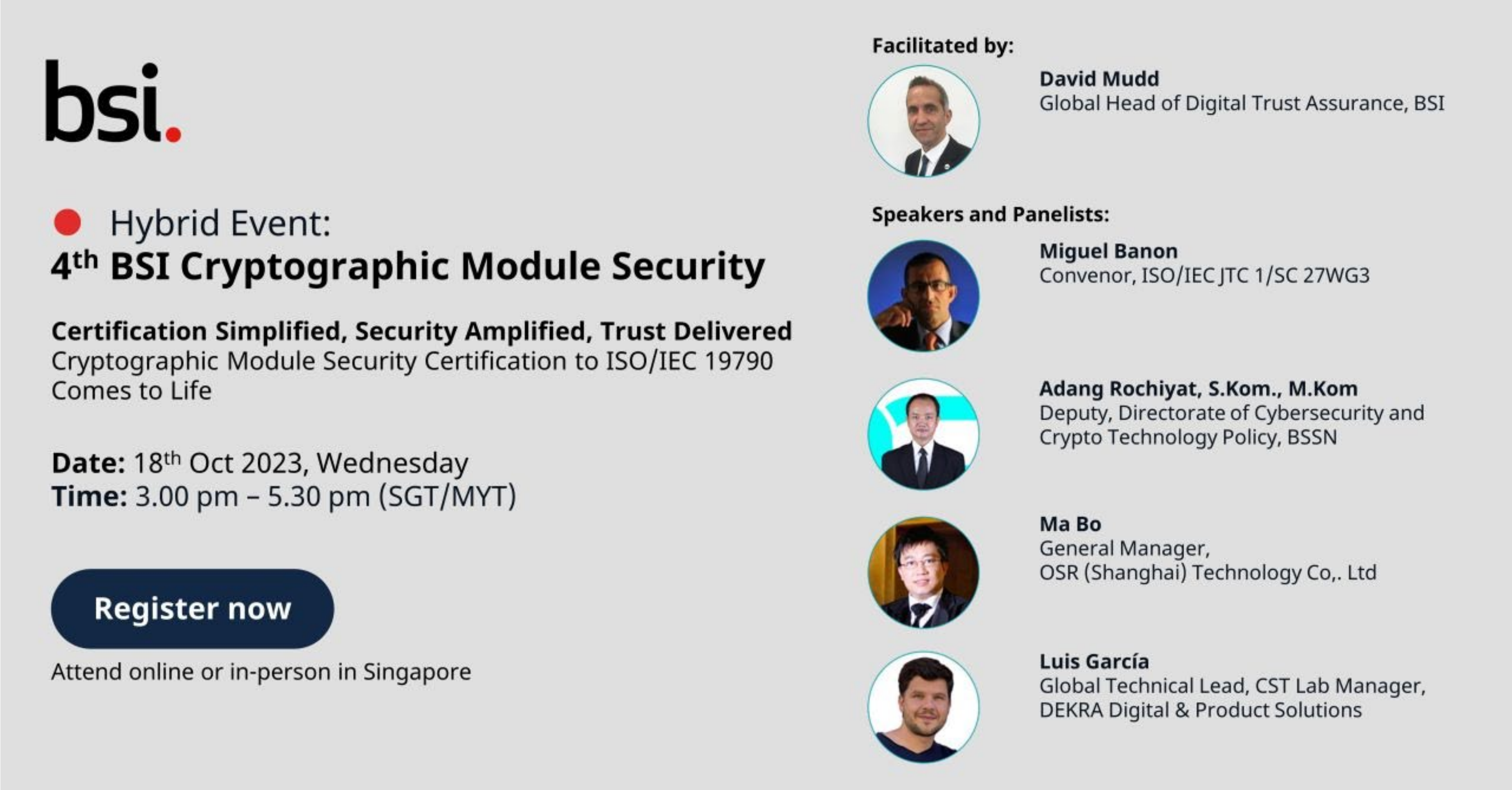
Cryptographic module certification: Ensuring data security with a common global approach

A BSI white paper

Bringing the idea to life

Progress and

- First 4 companies receive certificates against ISO/IEC 19790 for their products
- Exploration around common test tool sets /environments
- Comparison with Common Criteria



bsi.

● Hybrid Event:
4th BSI Cryptographic Module Security

Certification Simplified, Security Amplified, Trust Delivered
Cryptographic Module Security Certification to ISO/IEC 19790 Comes to Life

Date: 18th Oct 2023, Wednesday
Time: 3.00 pm – 5.30 pm (SGT/MYT)

Register now

Attend online or in-person in Singapore

Facilitated by:

David Mudd
Global Head of Digital Trust Assurance, BSI

Speakers and Panelists:

Miguel Banon
Convenor, ISO/IEC JTC 1/SC 27WG3

Adang Rochiyat, S.Kom., M.Kom
Deputy, Directorate of Cybersecurity and Crypto Technology Policy, BSSN

Ma Bo
General Manager,
OSR (Shanghai) Technology Co,. Ltd

Luis García
Global Technical Lead, CST Lab Manager,
DEKRA Digital & Product Solutions

Collaborating towards a secure digital future

Collaborating towards a secure digital future

Keynote talks

RED ALERT LABS
IoT Security

GSMA MWC Barcelona

Real-life applications and implications

for a global certification approach for cryptographic modules.

Roland Atoui | Managing Director at Red Alert Labs

27/02/24

Our Services

SECURITY CONSULTING

- Risk Assessment
- Secure Design
- Certification Schemes
- Strategic plan

SECURITY EVALUATION

- Pentesting
- Regulations
- Standards
- Certification

SECURITY INNOVATION

- Risk Analysis
- Product Assessment
- Trusted Procurement
- Vulnerability Management

SECURITY TRAINING

- Cybersecurity Act
- Certification Schemes
- Common Criteria
- IoT Cybersecurity
- Cyber Resillience Act

RED ALERT LABS
IoT Security

A glance on what we are covering

	Consulting	Testing	Accreditation	Training	Scope
FIPS140-2 / FIPS140-3 / CAVP	✓			✓	cryptographic modules
Common Criteria	✓	✓	🕒	✓	Horizontal
EUCC	✓	✓	🕒	✓	Horizontal (ICT)
ARM PSA	✓	✓		✓	Horizontal (ICT)
GP - TEE & SE	✓			✓	TEE & SE
GSMA IoT Sec	✓	✓	✓	✓	Horizontal (IoT)
FIDO	✓	✓	✓	✓	Authenticator
NIST CSF	✓	✓		✓	(Horizontal) ISMS
ISO 27001	✓	✓		✓	(Horizontal) ISMS
IEC 62443	✓	✓	🕒	✓	Industrial
ISO 21434 & R155	✓	✓		✓	Automotive
ETSI EN 303645	✓	✓		✓	Consumer IoT
FDO IOT	✓	✓	✓	✓	Horizontal
ioXt Alliance	✓	✓	✓	✓	Horizontal
EUCS	✓	✓	🕒	✓	Cloud Services
CSPN	✓	✓	🕒	✓	Horizontal
EN 17640 / FITCEM	✓	✓	🕒	✓	Horizontal
EN 18031	✓	✓		✓	Horizontal (IoT/ICT)
CRA, RED, MDR	✓	✓		✓	Horizontal, Medical

RED ALERT LABS
IoT Security

Cryptographic Modules

Definitions and Components

What is a cryptographic module

Defined by ISO 19790, it is a hardware, software or firmware component for implementing crypto

Cryptographic boundary

The perimeter separating the module from the external environment covering components for crypto functions

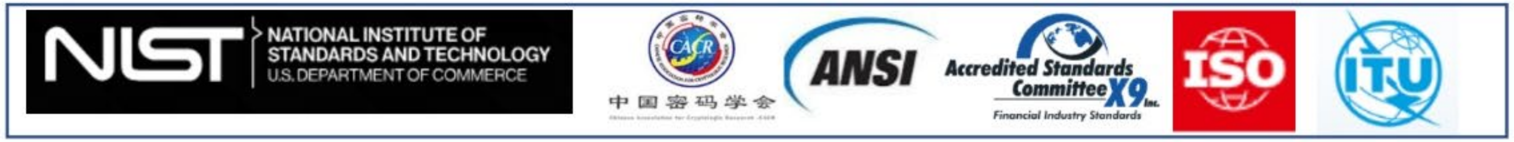
Module components

Includes cryptographic algorithms, key generation and more contained within the boundary

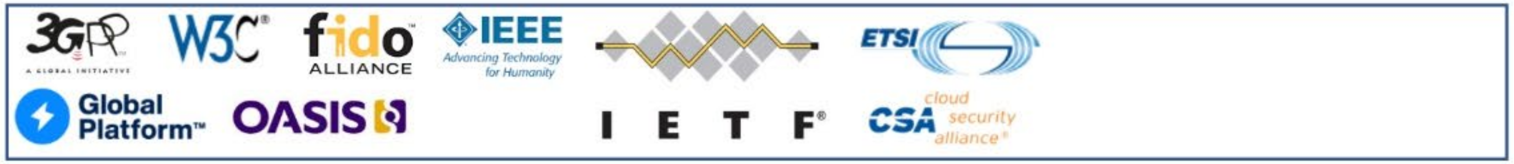
Cryptographic modules are crucial components with clearly defined boundaries for secure implementation of cryptography

Cryptographic Standards & Schemes

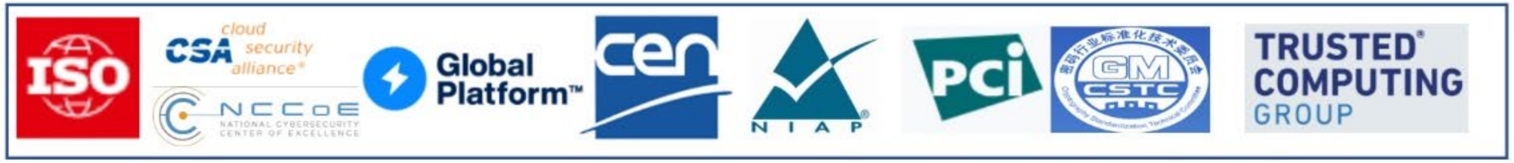
Standards for Cryptography


NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
CACR
中国密码学会
ANSI
Accredited Standards Committee X9 Inc.
Financial Industry Standards
ISO
ITU

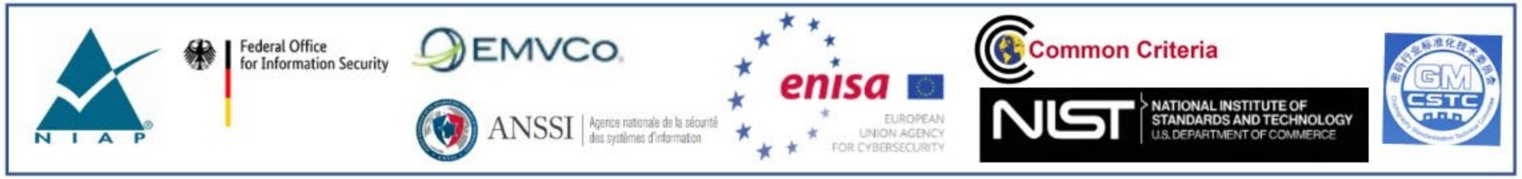
Standards for Protocols



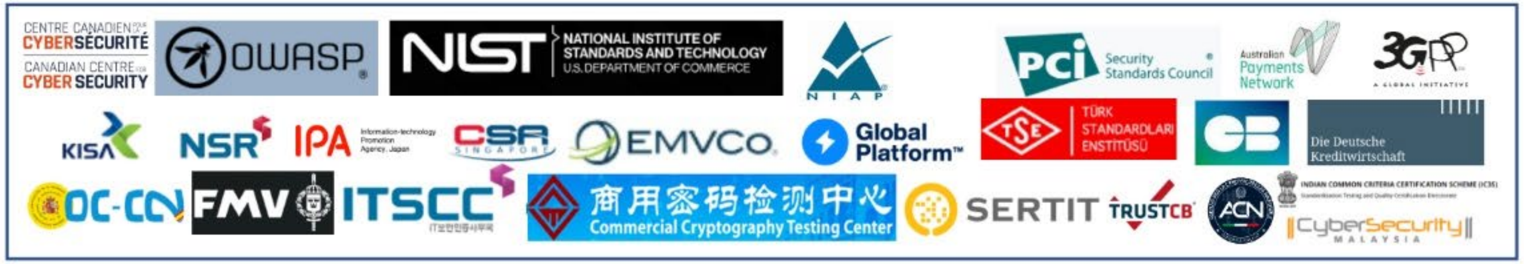
Standards for Crypto Modules


ISO
CSA cloud security alliance
NCCoE NATIONAL CYBERSECURITY CENTER OF EXCELLENCE
Global Platform
cen
NIAP
PCI
GM CSTC
TRUSTED COMPUTING GROUP

Standards for Security Testing


NIAP
Federal Office for Information Security
EMVCo
ANSSI Agence nationale de la sécurité des systèmes d'information
enisa EUROPEAN UNION AGENCY FOR CYBERSECURITY
Common Criteria
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
GM CSTC

Security Testing Schemes


CENTRE CANADIEN POUR LA CYBERSÉCURITÉ
CANADIAN CENTRE FOR CYBER SECURITY
OWASP
NIST NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY U.S. DEPARTMENT OF COMMERCE
NIAP
PCI Security Standards Council
Australian Payments Network
3GPP A GLOBAL INITIATIVE
KISA
NSR
IPA Information-technology Promotion Agency, Japan
CSA SINGAPORE
EMVCo
Global Platform
TSE TÜRK STANDARDLARI ENSTITÜSÜ
CB
Die Deutsche Kreditwirtschaft
OC-CCN
FMV
ITSCC
商用密码检测中心 Commercial Cryptography Testing Center
SERTIT
TRUSTCB
ACN
INDIAN COMMON CRITERIA CERTIFICATION SCHEME (IC3S)
CyberSecurity MALAYSIA

Challenges due to varying certifications across regions

Lack of standardization

Different regions have their own standards and certifications for cybersecurity products, leading to fragmentation.

Complexity

Varying certifications create complexity for vendors to get their products certified globally.

Compatibility issues

Products certified in one region may not work or integrate well with other products certified elsewhere.

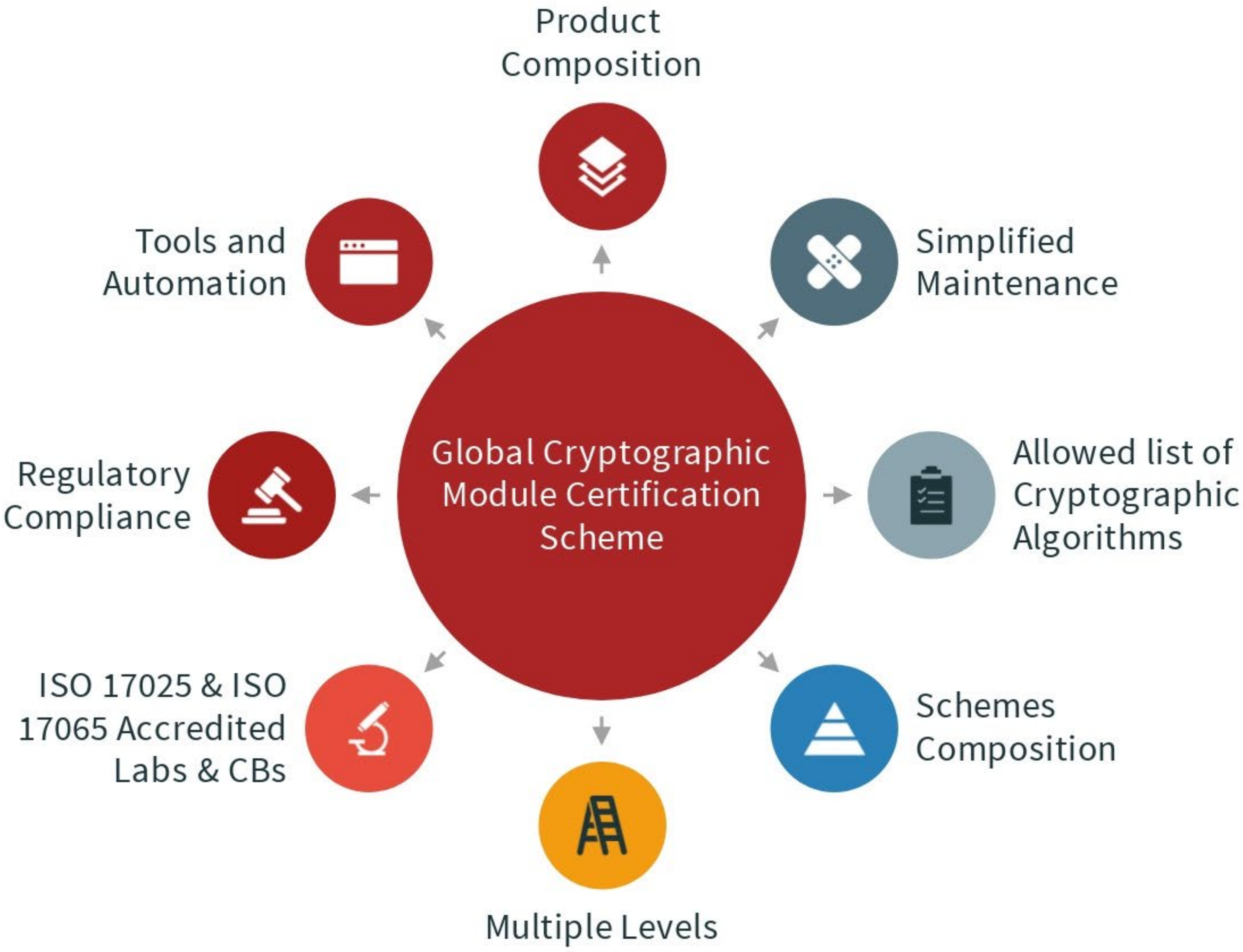
Higher costs

Vendors have to spend more time and money to get certified across multiple regions.

Delayed product releases

The process of obtaining multiple certifications leads to delays in launching products globally.

Transforming Challenges into Opportunities



Global Cryptographic Module Certification Scheme
Product Composition
Simplified Maintenance
Allowed list of Cryptographic Algorithms
Schemes Composition
Multiple Levels
ISO 17025 & ISO 17065 Accredited Labs & CBs
Regulatory Compliance
Tools and Automation

RED ALERT LABS
IoT Security

CM Across Sectors

Cryptographic modules are widely used across sectors and industries

Cryptographic modules, including hardware and software, protect sensitive data in healthcare, finance, government, retail, and more

Cryptographic modules are a critical foundation for cybersecurity across sectors

Financial Services

Examples of Products with CM

Point-of-sale (POS) terminals

POS terminals use cryptographic modules to encrypt cardholder data during transactions

ATMs

ATMs use cryptographic modules to encrypt cardholder data during transactions

Transaction Processing HSMs

Banks and payment processors use HSMs to secure financial transactions and protect against fraud

Mobile Payment Applications

Mobile payment apps use cryptographic modules to secure payments on smartphones and tablets

Cryptographic modules are critical for securing financial transactions across various endpoints like POS, ATMs, bank networks, and mobile devices.

Financial Services

Standards & Schemes

PCI DSS requires cryptographic controls

PCI DSS mandates the use of cryptography for secure transmission and storage of cardholder data.

ISO/IEC 27001 requires cryptographic management

ISO/IEC 27001 standard includes requirements for proper management of cryptographic controls used in financial operations.

EMVCo & Common Criteria

EMVCo certification requires cryptographic evaluation of smart cards with EMVCo banking application most often based on a CC certified platform

Key regulations and standards like PCI DSS, ISO/IEC 27001, and EMVCo drive the use of cryptography to protect financial data and transactions.

Healthcare

Examples of Products with CM

EHR Encryption

Encrypt electronic health records and limit access to authorized users only

Secure Messaging

Provide end-to-end encryption for telemedicine communications

Medical Device Security

Use cryptography to secure patient data on medical devices and ensure integrity

Encryption and cryptography are critical for securing sensitive patient healthcare data across various digital systems and applications.

Healthcare

Standards & Schemes

HIPAA

Cryptographic modules that comply with standards like FIPS 140-2 or FIPS 140-3 are often used to meet these encryption requirements, providing a high level of security assurance

IEC 62304, ISO 13485, and IEC 80001-1

These standards collectively enhance medical device cybersecurity through software life cycle processes, quality management systems with a focus on risk management, and securing IT-networked medical devices against cyber threats.

MDR Cryptographic Requirements

EU regulation requiring medical device manufacturers to implement cryptographic controls and undergo certification to protect patient data.

Government and Defense

Examples of Products with CM

Hardware Security Modules (HSMs)

Devices that securely generate, store, and manage cryptographic keys used for encrypting sensitive government and military communications.

Secure Encrypting Devices

Specialized equipment like Encryptors, used for securing classified and tactical communications over networks.

Secure Voice and Data Communications Systems

Such as a Secure Phone, which provides high-assurance security for voice and data communications up to the Top Secret level.

Government and defense organizations rely on advanced security technologies like HSMs, encryptors, and secure communications systems to protect sensitive information.

Government and Defense

Examples of Certification Standards & Schemes

Government and defense rely on certified cryptographic modules

FIPS 140-3 specifies security requirements for cryptographic modules used in government and defense sectors in USA

Common Criteria provides international standard

Common Criteria ISO/IEC 15408 allows government departments internationally to assess and approve cryptographic modules for handling classified information

Country-specific certification schemes exist

Some countries like China, Japan and Korea have their own certification schemes like OSCCA, JCMVP and KCMVP respectively

A global certification scheme can help enable interoperability and trust across borders while allowing for regional policies.

IT

Example of products with CM

SSL/TLS accelerators

Hardware or software solutions that offload encryption processing from servers for secure communications.

VPN hardware

Devices using encryption modules to secure remote access and site-to-site connections.

Encrypted storage

Secure USB drives, hard drives and cloud services encrypting data at rest.

Various hardware and software solutions utilize encryption to secure data communications and storage.

IT

Standards & Schemes

ISO/IEC 27001

International standard that helps organizations manage information security through the use of cryptographic modules.

FIDO2

FIDO2/U2F/UAF Authenticators requires the usage of FIDO allowed list of cryptography

ETSI Standards

European standards that include cryptographic protection for ICT systems and applications.

Several global standards like ISO/IEC 27001, FIDO, and ETSI provide guidance on implementing cryptographic controls.

Telecom

Examples of Products with CM

Hardware Security Modules (HSMs) store cryptographic keys

HSMs physically secure keys used for telecom network encryption

Virtual Private Network (VPN) gateways enable secure remote connections

VPNs use encryption to securely transmit data over the internet

Secure VoIP solutions encrypt voice data transmission

VoIP encryption ensures private voice comms over IP networks

Cryptographic modules are critical for securing sensitive data and communications in the telecom sector.

Telecom

Standards & Schemes

ETSI, 3GPP, ITU

Setting global ICT standards, focusing on security, cryptographic measures and encryption for communication privacy/integrity

NESAS, EU5G

Ensuring security for telecom network equipment, involving cryptographic modules

Common Criteria for UICC

Security standard for UICC (SIM cards), focusing on security features like cryptographic modules to protect mobiles

IoT

Examples of products with CM

IoT Sector Embedded Cryptographic Modules

Integrated into IoT devices to provide authentication, encryption, secure boot

IoT Security Platforms

Comprehensive platforms with encryption, identity management, secure key storage

Smart Home Gateways

Central hubs securing communications between IoT devices and networks

Cryptographic modules are critical for securing the diverse IoT ecosystem through encryption, access controls, and data integrity protections.

IoT

Standards & Schemes

ETSI EN 303 645

A European standard specifying cybersecurity measures for consumer IoT devices. It sets out a baseline of security provisions for IoT devices to protect users' privacy and safety from common cyber threats.

NISTIR 8259, U.S. Cyber Trust Mark

A cybersecurity labeling program for smart devices designed to give consumers the tools needed to make informed decisions in regard to security when purchasing products to bring into their homes. Based on NISTIR 8259.

SESIP

is a cybersecurity certification methodology developed to ensure the security of IoT devices and platforms.

CRA, CSA, RED, EN18031

The EU Cyber Resilience Act, the EU Cybersecurity Act, the RED Directive Delegated Act and the future harmonized standards do enforce requirements on cryptography supported by the future EU cryptography scheme

Industrial & Automotive

Examples of products with CM

Secure gateways

Industrial Control System (ICS) Security Gateways protect industrial networks using cryptography for secure communication.

Remote access

Secure Remote Access Solutions allow securely managing industrial systems and equipment remotely with encryption.

Telematics Control Unit (TCU)

A TCU in connected cars uses cryptographic modules to secure communications, ensuring data privacy and protection against cyber threats.

Cryptographic modules enable security for a wide range of industrial and manufacturing use cases, from gateways to remote access to embedded devices.

Industrial & Automotive

Standards & Schemes

IEC 62443

Series of standards for secure industrial communication networks using cryptography to protect sensitive systems and data

NIST Framework

Guidelines to manage cybersecurity risks including cryptographic modules in manufacturing

ISO/SAE 21434

Addresses vehicle cybersecurity including cryptographic modules for communications and data

Cryptographic standards help secure sensitive industrial and automotive systems and data.

Retail & e-commerce

Example of products with CM

E-commerce

Secure online transactions and protect customer data during transmission with SSL certificates.

Point-of-Sale

Encrypt credit card information at the moment of swipe or chip insertion with POS encryption devices.

Mobile Payments

Use cryptographic modules to secure payment transactions conducted on mobile devices via mobile payment systems.

Cryptographic technologies like SSL, POS encryption, and mobile payment systems help secure financial transactions in e-commerce, retail, and mobile contexts.

Retail & e-commerce

Standards & Schemes

PCI DSS is required for retail and e-commerce

PCI DSS is an industry standard for retailers to secure cardholder data during transmission over open networks

ISO 27001 protects financial and customer data

ISO 27001 helps retailers protect financial and customer data through encryption and other security measures

GDPR compliance for EU customers

For e-commerce businesses in Europe or with European customers, GDPR requires data protection through encryption

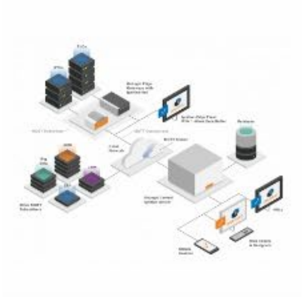
Security standards like PCI DSS, ISO 27001, and GDPR are essential for retailers to protect customer data and transactions.

Energy & Utility

Examples of Products/Systems

Smart meters

Smart meters use cryptographic modules to secure data transmission between the meter and utility provider.



SCADA systems

SCADA Encryption Gateways secure SCADA systems that manage energy and utility networks.

Grid communications

Grid control systems use cryptographic modules to secure communications and operations within the electrical grid.

Cryptographic modules are crucial for securing critical infrastructure in the energy and utility sectors.

Energy & Utility

Standards & Schemes

NERC CIP Standards

North American standards for protecting the bulk power system including cryptographic protection of sensitive data.

ISO/IEC 27001

Information security management practices applicable to utilities for managing cryptographic keys and modules.

IEC 62351

Standards for securing communications in power systems including authentication and data integrity via cryptography.

Energy and utility companies can leverage cryptography standards like NERC CIP, ISO/IEC 27001, and IEC 62351 to protect critical infrastructure and data.

Benefits of unified certification approach

Simplified compliance

A unified certification approach makes it easier for companies to comply with security regulations across regions.

Enhanced security

Standardized certification requirements improve baseline security for all certified products and services.

Increased trust

Mutual recognition of certifications builds trust between organizations operating globally.

Reduce Costs

Standardized requirements simplify development and reduce costs for vendors

A unified certification approach provides multiple benefits for the cybersecurity ecosystem.

Certification in Support to Supply Chain Security

Certifying components builds trust across vendors

A certification program allows vendors to trust parts from other certified suppliers, reducing risk.

Certification enables better traceability

Certified parts can be traced back to the source manufacturer, improving security.

A global certification program for components would improve supply chain security through enhanced trust, traceability and transparency.

Key Takeaway

Use Standards

Use standards as often as possible to address cybersecurity by design and think about compliance and regulatory requirements to access new markets while minimizing your costs.

Collaboration is key

All stakeholders accross sectors should work together to develop a global and recognized certification framework

Compose your Trust

Rely on components that provides transparency and high level of security assurance to build a trusted product.

Get Support & Automate

Get support by third-party experts whenever necessary and use certification platforms such as CyberPass to streamline the process

RED ALERT LABS
IoT Security

Merci

RED ALERT LABS
IoT Security

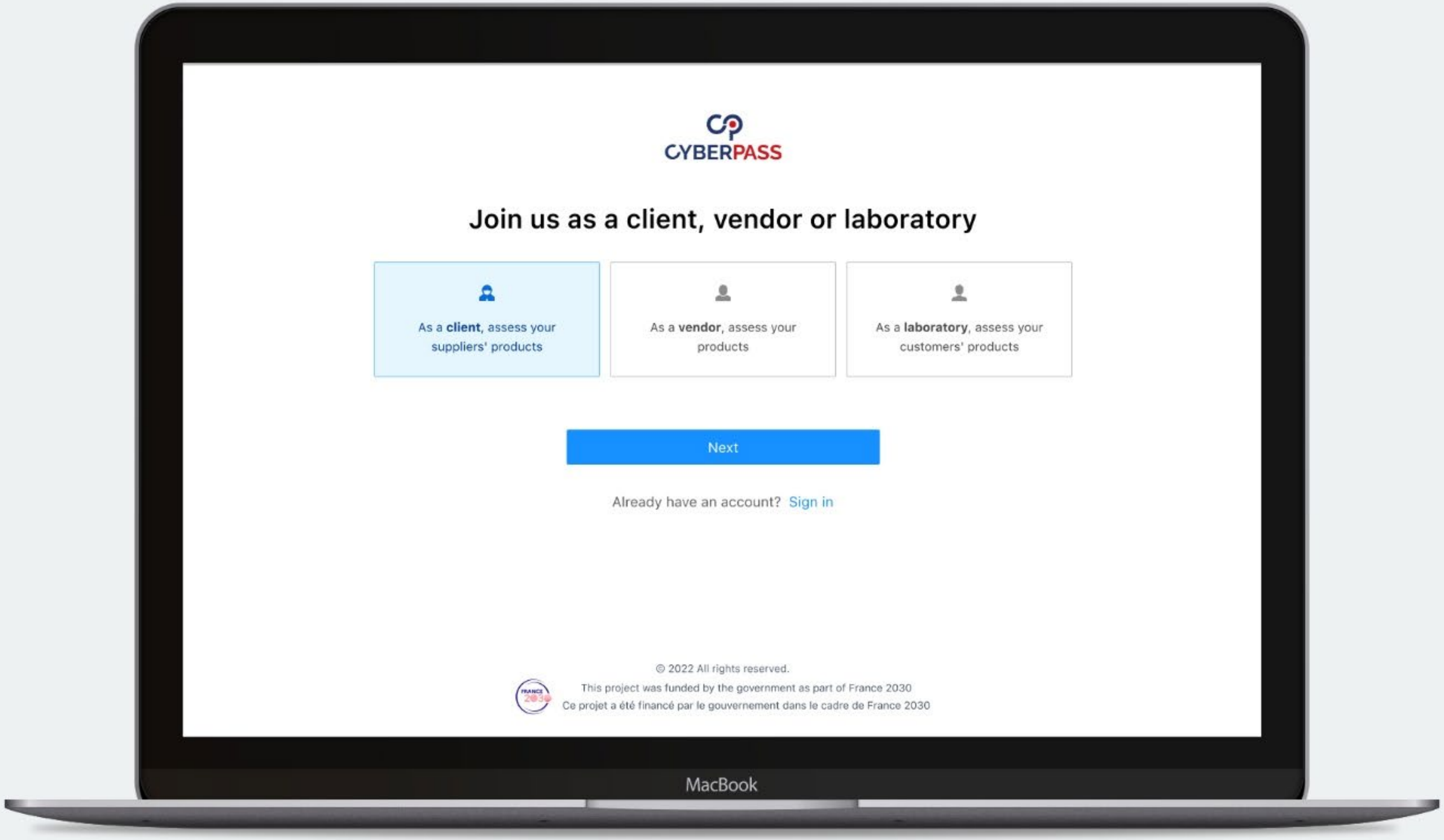
3 rue Parmentier, 94140, Alfortville, France

https://www.redalertlabs.com

@RedAlertLabs

roland.atoui@redalertlabs.com

Curious to know a little more? Join us... https://www.cyber-pass.eu



CYBERPASS

Join us as a client, vendor or laboratory

As a **client**, assess your suppliers' products

As a **vendor**, assess your products

As a **laboratory**, assess your customers' products

Already have an account? Sign in

This project was funded by the government as part of France 2030
Ce projet a été financé par le gouvernement dans le cadre de France 2030

5th BSI Cryptographic Module event

Testing Tools: Why are they needed for cryptographic module security testing and how can we trust them?

Barcelona, Feb 2024

Agenda

- Background
- Testing tools
- Non-testing tools
- Bringing trust
- Conclusions

Luis García

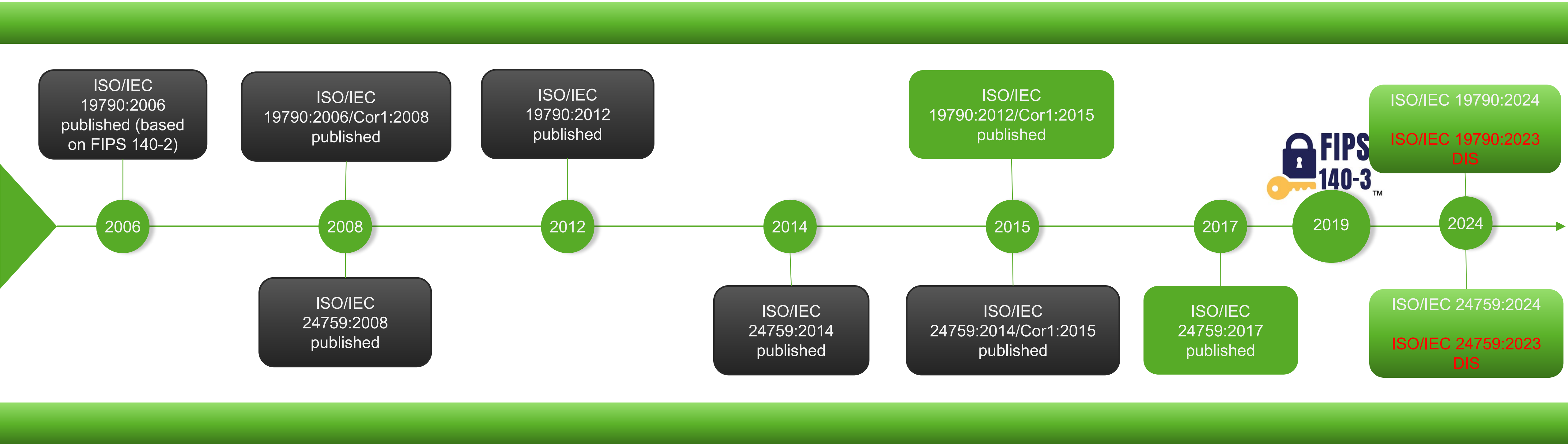
Global Technical Lead

CST Lab Manager

+12 years in the certifications field

Background (I)

Timeline



2006

ISO/IEC 19790:2006 published (based on FIPS 140-2)

2008

ISO/IEC 19790:2006/Cor1:2008 published

ISO/IEC 24759:2008 published

2012

ISO/IEC 19790:2012 published

2014

ISO/IEC 24759:2014 published

2015

ISO/IEC 19790:2012/Cor1:2015 published

ISO/IEC 24759:2014/Cor1:2015 published

2017

ISO/IEC 24759:2017 published

2019

FIPS 140-3™

2024

ISO/IEC 19790:2024

ISO/IEC 19790:2023 DIS

ISO/IEC 24759:2024

ISO/IEC 24759:2023 DIS

Background (II)

Expected impact

19790:2023 DIS VS 19790:2012/Cor1:2015

- Number of requirements is roughly the same (401 vs 399)
- 237 out of 399 requirements are new or updated:
  * Many changes are editorial only but assume at least a quarter of changes impact compliance or test-lab checks

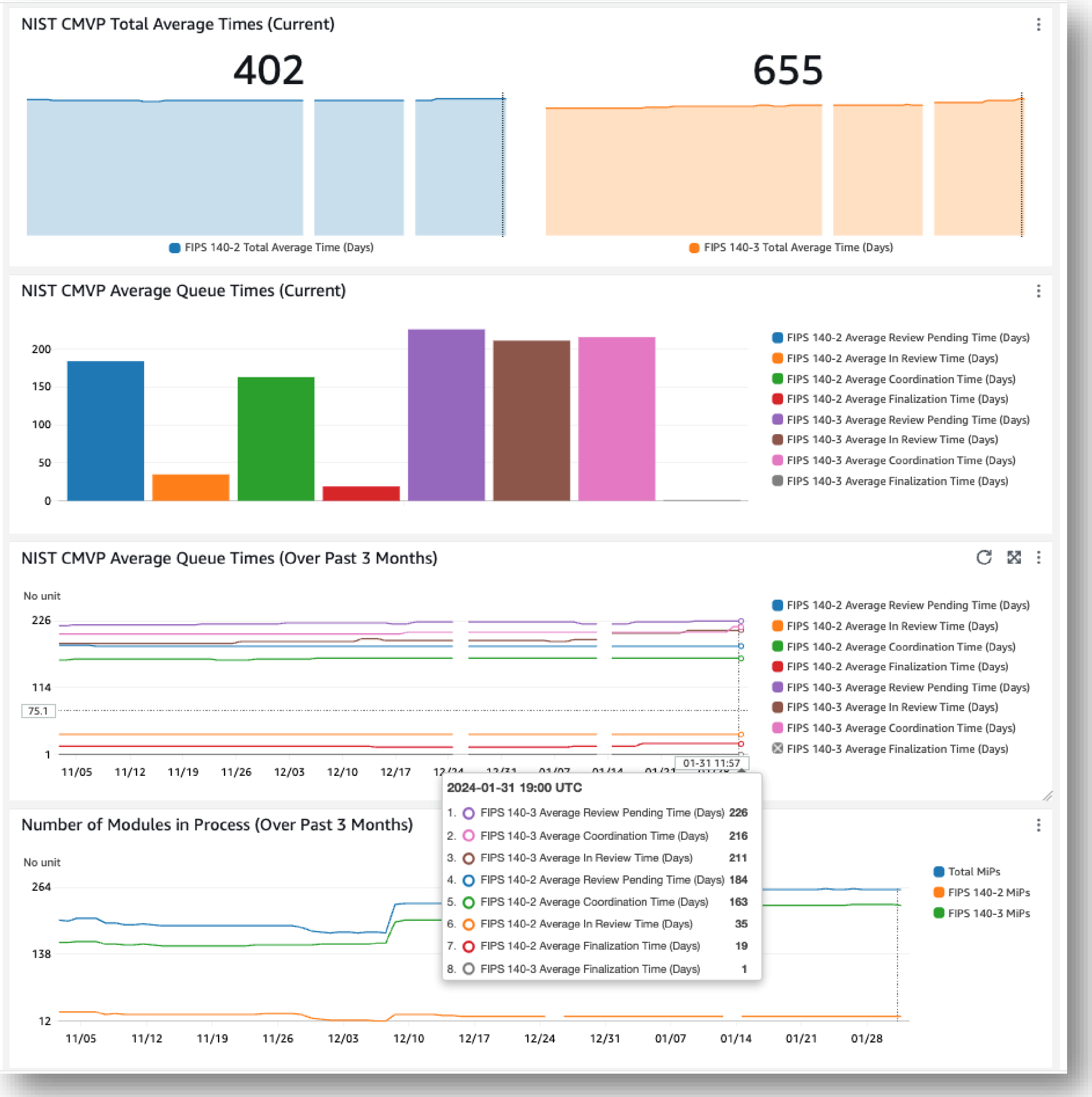
24759:2023 DIS VS 24759:2017

- 49 more VE (400 up from 351)
- 46 more TE (609 up from 563)

ISO 19790 Annexes from DIS
Annex A –Documentation requirements
Annex B –Cryptographic module security policy
Annex C –Approved Security Functions
Annex D –Approved sensitive security parameter generation and establishment methods
Annex E –Approved Authentication mechanisms
Annex F –Approved non-invasive attack mitigation test metrics
Annex G – Module secure development, manufacturing and operation

Background (III)

FIPS 140-2/3 situation



NIST CMVP Total Average Times (Current)

402
655
FIPS 140-2 Total Average Time (Days)
FIPS 140-3 Total Average Time (Days)

NIST CMVP Average Queue Times (Current)

200
150
100
50
0
FIPS 140-2 Average Review Pending Time (Days)
FIPS 140-2 Average In Review Time (Days)
FIPS 140-2 Average Coordination Time (Days)
FIPS 140-2 Average Finalization Time (Days)
FIPS 140-3 Average Review Pending Time (Days)
FIPS 140-3 Average In Review Time (Days)
FIPS 140-3 Average Coordination Time (Days)
FIPS 140-3 Average Finalization Time (Days)

NIST CMVP Average Queue Times (Over Past 3 Months)

No unit
226
114
75.1
1
11/05
11/12
11/19
11/26
12/03
12/10
12/17
01-31 11:57
FIPS 140-2 Average Review Pending Time (Days)
FIPS 140-2 Average In Review Time (Days)
FIPS 140-2 Average Coordination Time (Days)
FIPS 140-2 Average Finalization Time (Days)
FIPS 140-3 Average Review Pending Time (Days)
FIPS 140-3 Average In Review Time (Days)
FIPS 140-3 Average Coordination Time (Days)
FIPS 140-3 Average Finalization Time (Days)

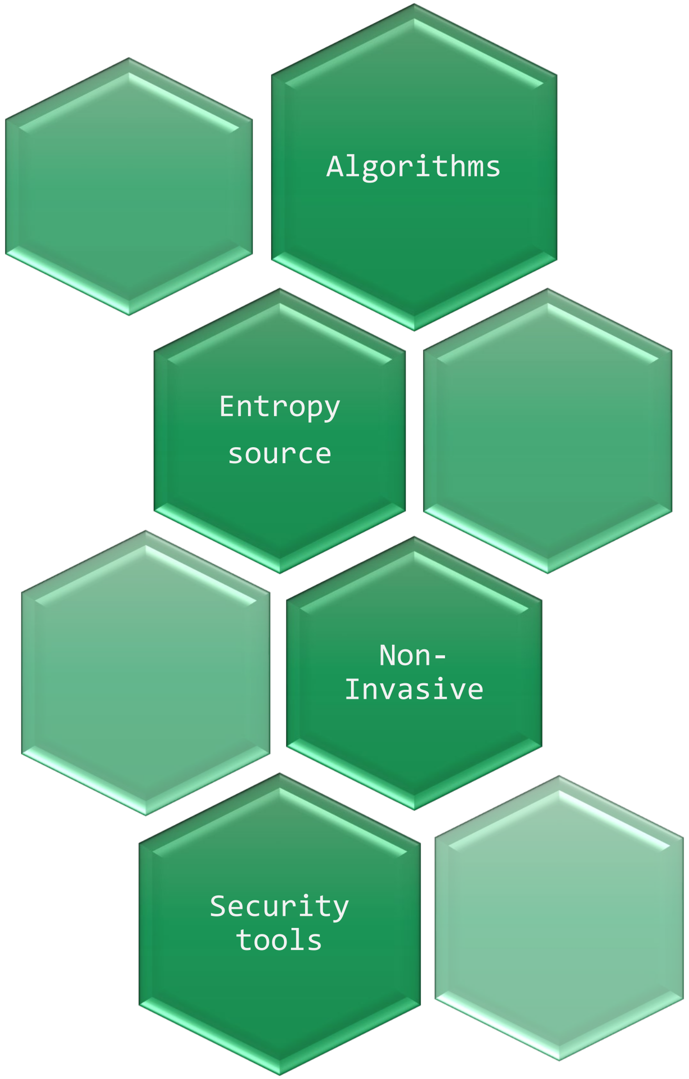
2024-01-31 19:00 UTC

1. FIPS 140-3 Average Review Pending Time (Days) 226
2. FIPS 140-3 Average Coordination Time (Days) 216
3. FIPS 140-3 Average In Review Time (Days) 211
4. FIPS 140-2 Average Review Pending Time (Days) 184
5. FIPS 140-2 Average Coordination Time (Days) 163
6. FIPS 140-2 Average In Review Time (Days) 35
7. FIPS 140-2 Average Finalization Time (Days) 19
8. FIPS 140-3 Average Finalization Time (Days) 1

Number of Modules in Process (Over Past 3 Months)

How?

Decompiling the standards (I)

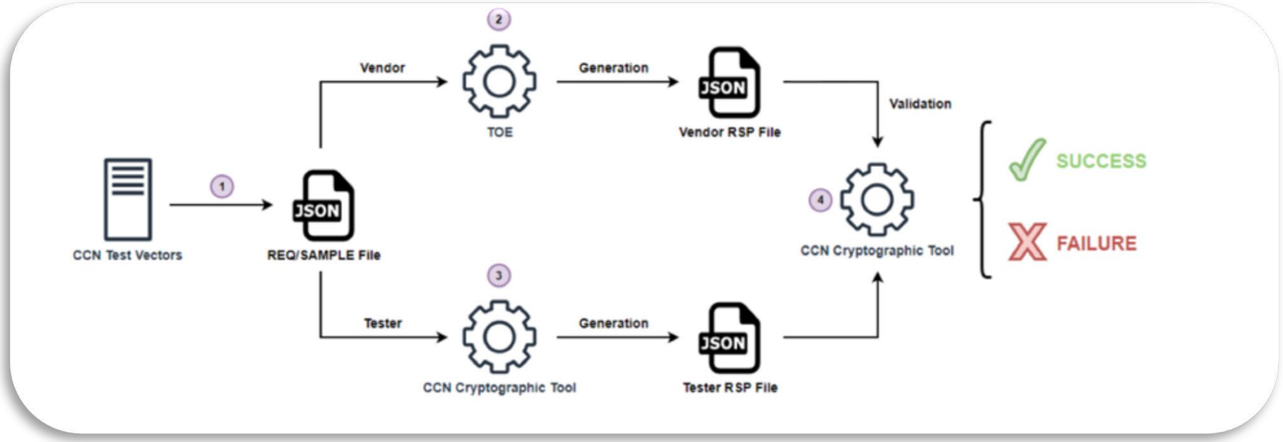


Don’t reinvent the wheel

Testing tools (I)

Algorithms

NIST JCMVP Japan Cryptographic Module Validation Program KCMVP CCN-cert



Open source Crypto libraries

- OpenSSL
- Botan
- Bouncy Castle
- Cryptlib

- Crypto++
- GnuTLS
- LibreSSL
- Libgcrypt

Guidance

SOGIS IT SECURITY CERTIFIED

- Agreed Cryptographic Mechanisms
- Harmonised Cryptographic Evaluation Procedures

ISO

- ISO/IEC 18367 Cryptographic algorithms and security mechanisms conformance testing

Testing tools (II)

Entropy source

SP 800-90A - Deterministic Random Bit Generators
SP 800-90B - Entropy Sources Used for Random Bit Generation
SP 800-90C - Random Bit Generator (RBG) Constructions
SP 800-22 - A Statistical Test Suite for Random

AIS 20: Functionality classes and evaluation methodology for deterministic RNGs
AIS 31: Functionality classes and evaluation of physical RNGs

Guidance

ISO/IEC 20543 test and analysis methods for random bit generators

NIST Statistical Test Suite:
- https://csrc.nist.gov/projects/random-bit-generation/documentation-and-software

NIST Entropy Assessment Tool:
- https://github.com/usnistgov/SP800-90B_EntropyAssessment

usnistgov/**ESV-Server**

Entropy Source Validation Protocol and Server specifications

3 Contributors · 3 Issues · 10 Stars · 11 Forks

BSI AIS20/31 Test Suite:
- https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Zertifizierung/Interpretationen/AIS_31_testsuit_zip.html

GM/T 0005-2021 - Randomness test specification
GM/T 0078-2020 - The design guidelines for cryptographic random number generation module
GM/T 0103-2021 - General Framework of random number generator

Testing tools (III)

Non-Invasive

Guidance

ISO

ISO/IEC 17825: Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

ISO/IEC 20085: Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules:

- Part 1: Test tools and techniques
- Part 2: Test calibration methods and apparatus

Not clear stakeholders, but private sector

DEKRA

SECURE-iC

riscure

Open Source tools

LEDGER DONJON

https://github.com/Ledger-Donjon/lascar

https://github.com/eshard/scared

REASSURE

https://github.com/Riscure/Jlsca

Testing tools (IV)

Security/Functional

Standard

AS11.30:

- […] use automated security diagnostic tools (e.g. detect buffer overflow).
- categorise the types by using the Common Weakness Enumeration (CWE) list

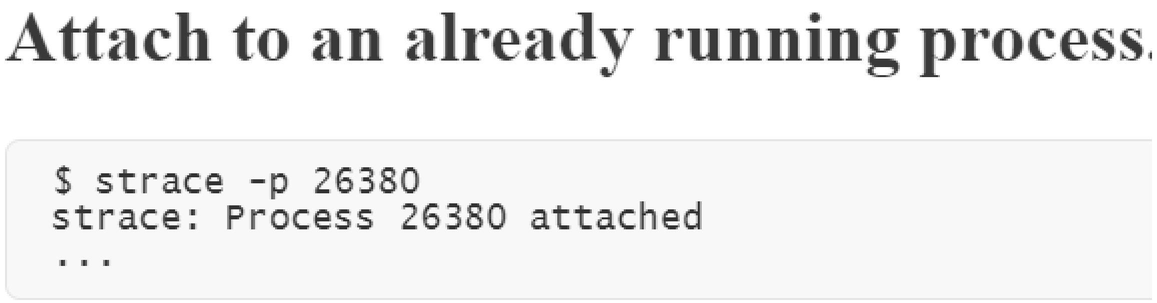
ISO is not requiring that the module and operational environment be free from CVEs but is requiring that vendors use this as one of their tools to provide a more secure product to the end user.

Techniques

- Static Code Analysis
- Dynamic Code Analysis
- Fuzzing
- Debugging
- Memory leak detection

Open Source Tools

- FindBugs
- Cppcheck
- OWASP Dependency-Check
- Wireshark
- Valgrind
- Strace

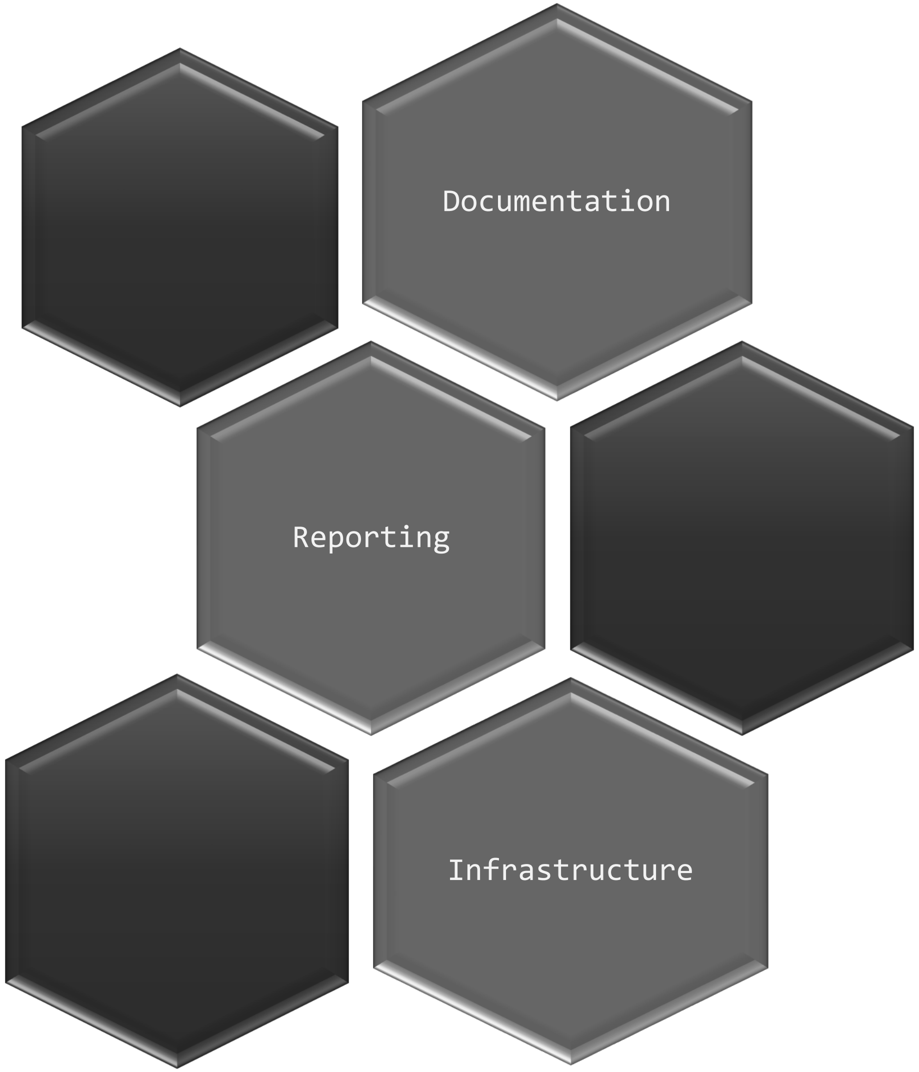


Attach to an already running process.

```
$ strace -p 26380
strace: Process 26380 attached
...
```

Only tools for testing?

Decompiling the standards (II)



Documentation

Reporting

Infrastructure

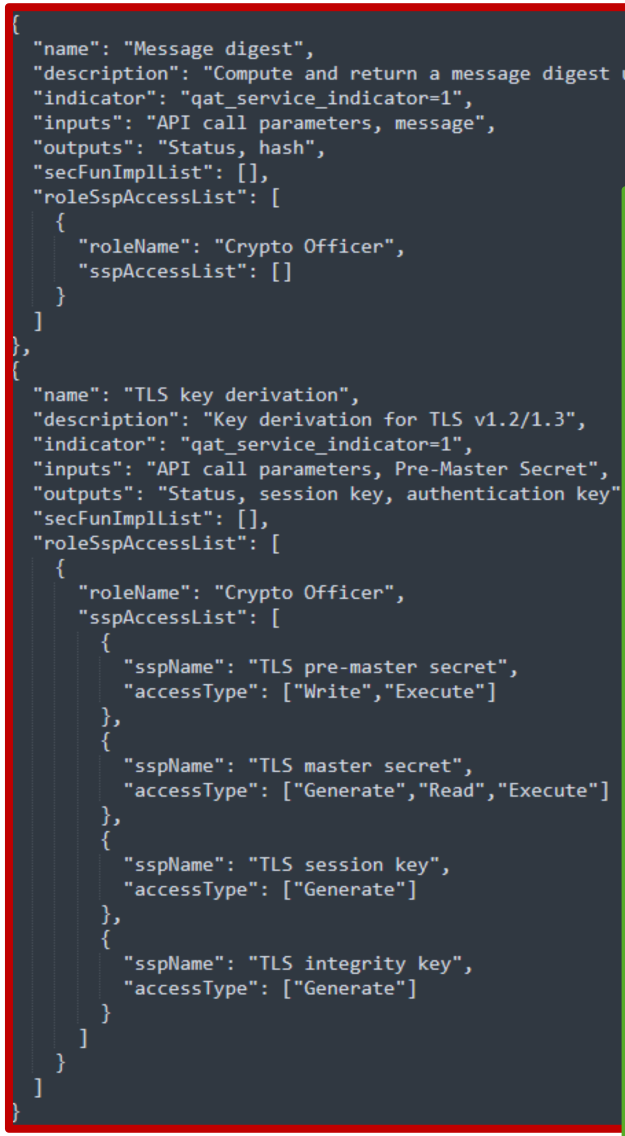
Non-testing tools (I)

Documentation

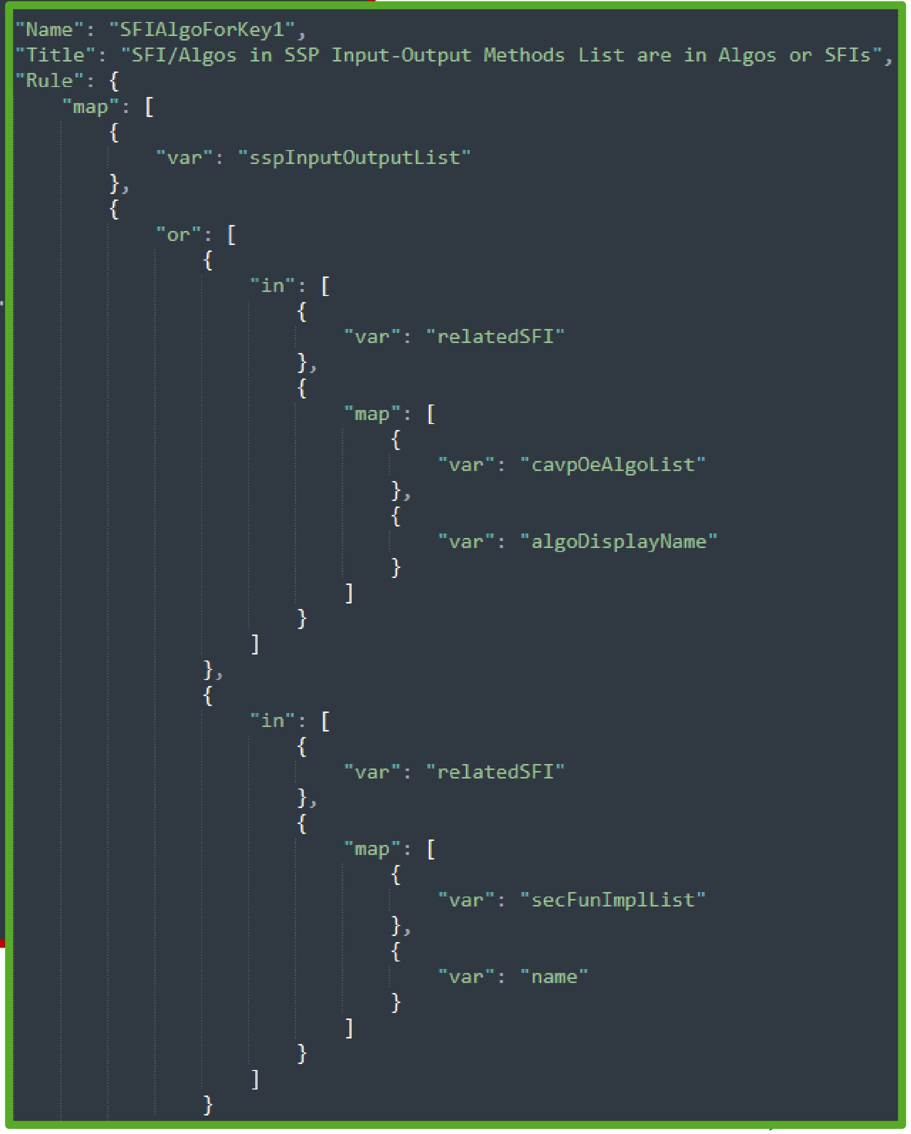
- VE requirements conform ~40% of ISO/IEC 24759 requirements
- Main documents:
  - Security Policy
  - Certificate
  - FSM
- Data interchange formats (Json, XML) templates

Advantages

- Parsing verification tool
- Guarantee a minimum set of information provided before starting the review process



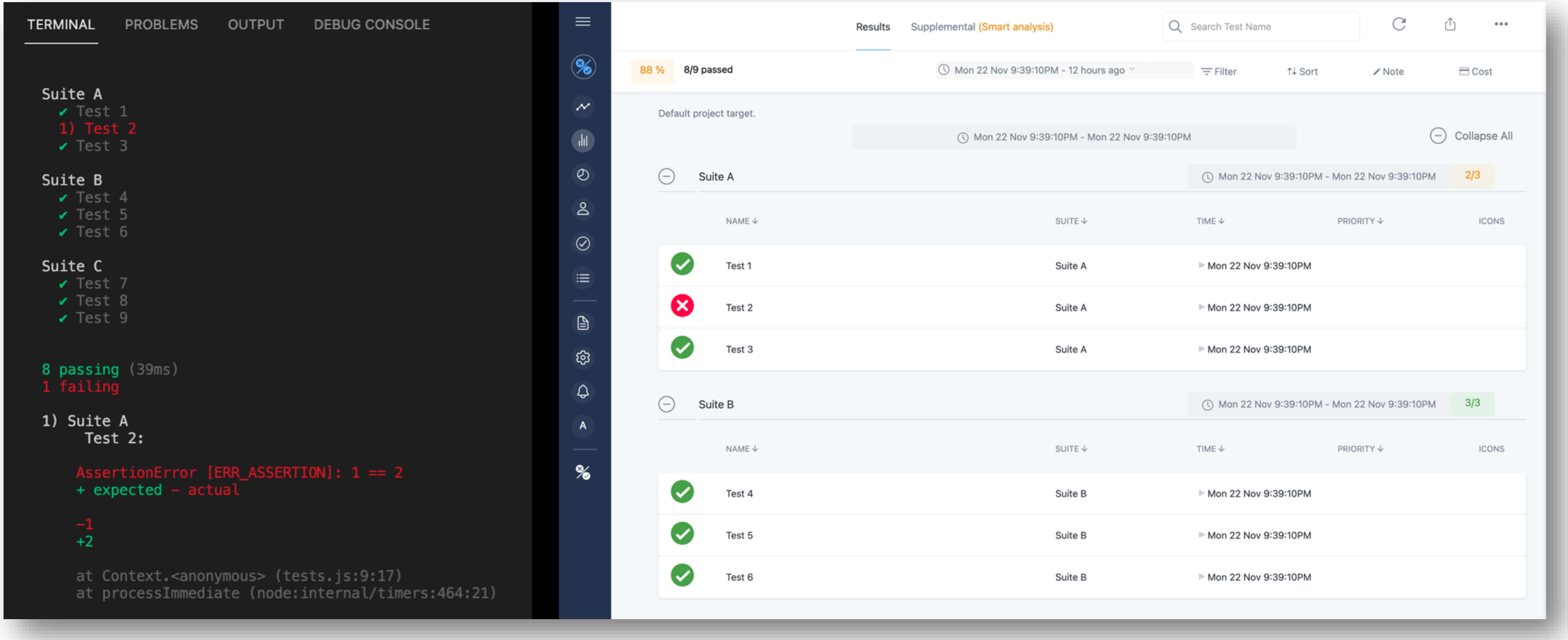
```
{
  "name": "Message digest",
  "description": "Compute and return a message digest using SHS and SHA-3 algorithms",
  "indicator": "qat_service_indicator=1",
  "inputs": "API call parameters, message",
  "outputs": "Status, hash",
  "secFunImplList": [],
  "roleSspAccessList": [
    {
      "roleName": "Crypto Officer",
      "sspAccessList": []
    }
  ]
},
{
  "name": "TLS key derivation",
  "description": "Key derivation for TLS v1.2/1.3",
  "indicator": "qat_service_indicator=1",
  "inputs": "API call parameters, Pre-Master Secret",
  "outputs": "Status, session key, authentication key"
  "secFunImplList": [],
  "roleSspAccessList": [
    {
      "roleName": "Crypto Officer",
      "sspAccessList": [
        {
          "sspName": "TLS pre-master secret",
          "accessType": ["Write","Execute"]
        },
        {
          "sspName": "TLS master secret",
          "accessType": ["Generate","Read","Execute"]
        },
        {
          "sspName": "TLS session key",
          "accessType": ["Generate"]
        },
        {
          "sspName": "TLS integrity key",
          "accessType": ["Generate"]
        }
      ]
    }
  ]
}
```



```
"Name": "SFIAlgoForKey1",
"Title": "SFI/Algos in SSP Input-Output Methods List are in Algos or SFIs",
"Rule": {
    "map": [
        {
            "var": "sspInputOutputList"
        },
        {
            "or": [
                {
                    "in": [
                        {
                            "var": "relatedSFI"
                        },
                        {
                            "map": [
                                {
                                    "var": "cavpOeAlgoList"
                                },
                                {
                                    "var": "algoDisplayName"
                                }
                            ]
                        }
                    ]
                },
                {
                    "in": [
                        {
                            "var": "relatedSFI"
                        },
                        {
                            "map": [
                                {
                                    "var": "secFunImplList"
                                },
                                {
                                    "var": "name"
                                }
                            ]
                        }
                    ]
                }
```

Non-testing tools (II)

Reporting



```
Suite A
  ✔ Test 1
  1) Test 2
  ✔ Test 3

Suite B
  ✔ Test 4
  ✔ Test 5
  ✔ Test 6

Suite C
  ✔ Test 7
  ✔ Test 8
  ✔ Test 9


8 passing (39ms)
1 failing

1) Suite A
     Test 2:

    AssertionError [ERR_ASSERTION]: 1 == 2
    + expected - actual

    -1
    +2

    at Context.<anonymous> (tests.js:9:17)
    at processImmediate (node:internal/timers:464:21)
```

88 % 8/9 passed

Mon 22 Nov 9:39:10PM - 12 hours ago

Default project target.

Mon 22 Nov 9:39:10PM - Mon 22 Nov 9:39:10PM

Suite A — Mon 22 Nov 9:39:10PM - Mon 22 Nov 9:39:10PM — 2/3

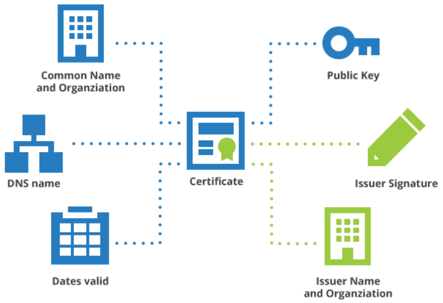
	NAME ↓	SUITE ↓	TIME ↓	PRIORITY ↓	ICONS
✓	Test 1	Suite A	Mon 22 Nov 9:39:10PM		
✗	Test 2	Suite A	Mon 22 Nov 9:39:10PM		
✓	Test 3	Suite A	Mon 22 Nov 9:39:10PM		

Suite B — Mon 22 Nov 9:39:10PM - Mon 22 Nov 9:39:10PM — 3/3

	NAME ↓	SUITE ↓	TIME ↓	PRIORITY ↓	ICONS
✓	Test 4	Suite B	Mon 22 Nov 9:39:10PM		
✓	Test 5	Suite B	Mon 22 Nov 9:39:10PM		
✓	Test 6	Suite B	Mon 22 Nov 9:39:10PM		

Non-testing tools (III)

Secure communication infrastructure



Bringing Trust

Open Source

Why?

Transparency: The source code is available for anyone to inspect. Users can see exactly how the software works and identify any potential improvement points.

Cost-Effective: Open source software is typically free to use, which can lead to significant cost savings for organizations.

Customization: With open source software, you have the freedom to modify the code to suit your specific needs. It can be used as a starting point.

Community Support: Open source projects may bring communities of developers and users who provide support and testing, resulting in rapid development and helping to the ecosystem scalability

Security: The ability to audit the source code allows assessing the software's security in terms of malfunctions or vulnerabilities.

Educational Value: Open source software provides a valuable resource for learning in deep about the functionality implementation.

Ecosystem

Creating a powerful ecosystem

Governance: establish clear governance structures

Define clear goals and objectives: roadmap

Bring to key stakeholders: vendors, labs, institutions and other relevant parties.

Competitive advantages: determine what incentives and value each stakeholder can gain from participating in the ecosystem

Rules of the game: create framework that outlines how different components of the ecosystem will interact with each other. This may include defining roles, responsibilities, and rules of engagement.

Scalability and resilience: Module technology is constantly evolving. Ecosystem needs to be adaptable to changing circumstances and built in resilience against potential disruptions or impacts.

Conclusions

Conclusions

Personal thoughts

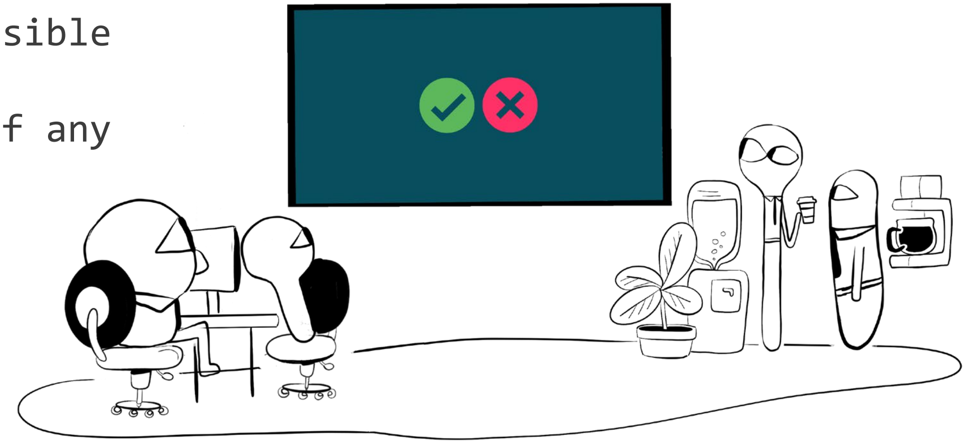
1. The industry requires quick certification programs

2. Homogenization of standards and testing requirements by certification schemes. Vendors cannot develop a specific version of the product for each one.

3. Identify as many tools (testing and non-testing) as possible

4. Tools and automation processes must conform the basis of any certification scheme
   - Efficiency
   - Quality and consistency
   - Increased productivity
   - Data analysis
   - 24/7 Operations

5. There is a lot of work on the table, but you can count on DEKRA to make this alternative happens. So, let's get started!



Thank you!

Luis García
Luis.garciasanchez@dekra.com

Cryptographic module cybersecurity certification according to ISO/IEC 19790

An introduction to the process and related benefits

Mustanir Ali – BSI certification lead

Why ISO/IEC 19790 certification?

- Cryptographic modules are the heart of information security solutions – the security of a system hinges on the security of the crypto module
- Solution builders need a way to select a crypto module that provides appropriate security for their application
- Solution builders need to be able to trust that a module provides the level of security that it claims

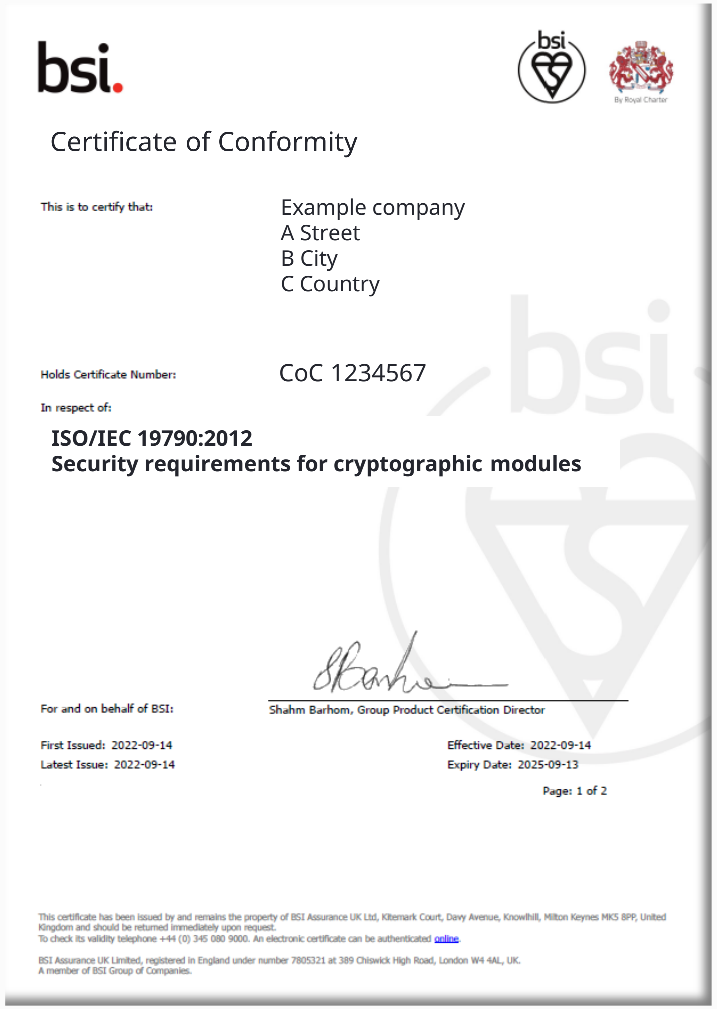
Certification vs. testing

- Testing is a one-off activity
- Output is a detailed test report with information of individual test cases and results
- Considered to be valid only for the specific items tested, at the time of test

- Certification is an attestation of conformity to particular requirement(s)
- Does not contain detail of specific test cases or results
- Considered to be valid more broadly than a test report
- Additional layer of impartiality and trust

Certification

- The rules defining how a certificate is achieved and maintained is called a “certification scheme”
- Key input to a simple product certification scheme is test report(s)
- More complex schemes may have additional inputs, such as:
  - Technical documentation
  - Risk assessments
  - Site audit report(s)



bsi.

Certificate of Conformity

This is to certify that: Example company
A Street
B City
C Country

Holds Certificate Number: CoC 1234567

In respect of:

ISO/IEC 19790:2012
Security requirements for cryptographic modules

For and on behalf of BSI: Shahm Barhom, Group Product Certification Director

First Issued: 2022-09-14
Latest Issue: 2022-09-14

Effective Date: 2022-09-14
Expiry Date: 2025-09-13

Page: 1 of 2

This certificate has been issued by and remains the property of BSI Assurance UK Ltd, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP, United Kingdom and should be returned immediately upon request.
To check its validity telephone +44 (0) 345 080 9000. An electronic certificate can be authenticated online.

BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A member of BSI Group of Companies.

ISO/IEC 19790 certification today

- BSI is carrying out certification of cryptographic modules to ISO/IEC 19790
- Current scheme is a Type 1a scheme (ref. ISO/IEC 17067)
- Currently undergoing ISO/IEC 17065 accreditation for the scheme with UKAS
- Key inputs for certification are
  - Test Report – ISO/IEC 17025
  - Cryptographic module security policy

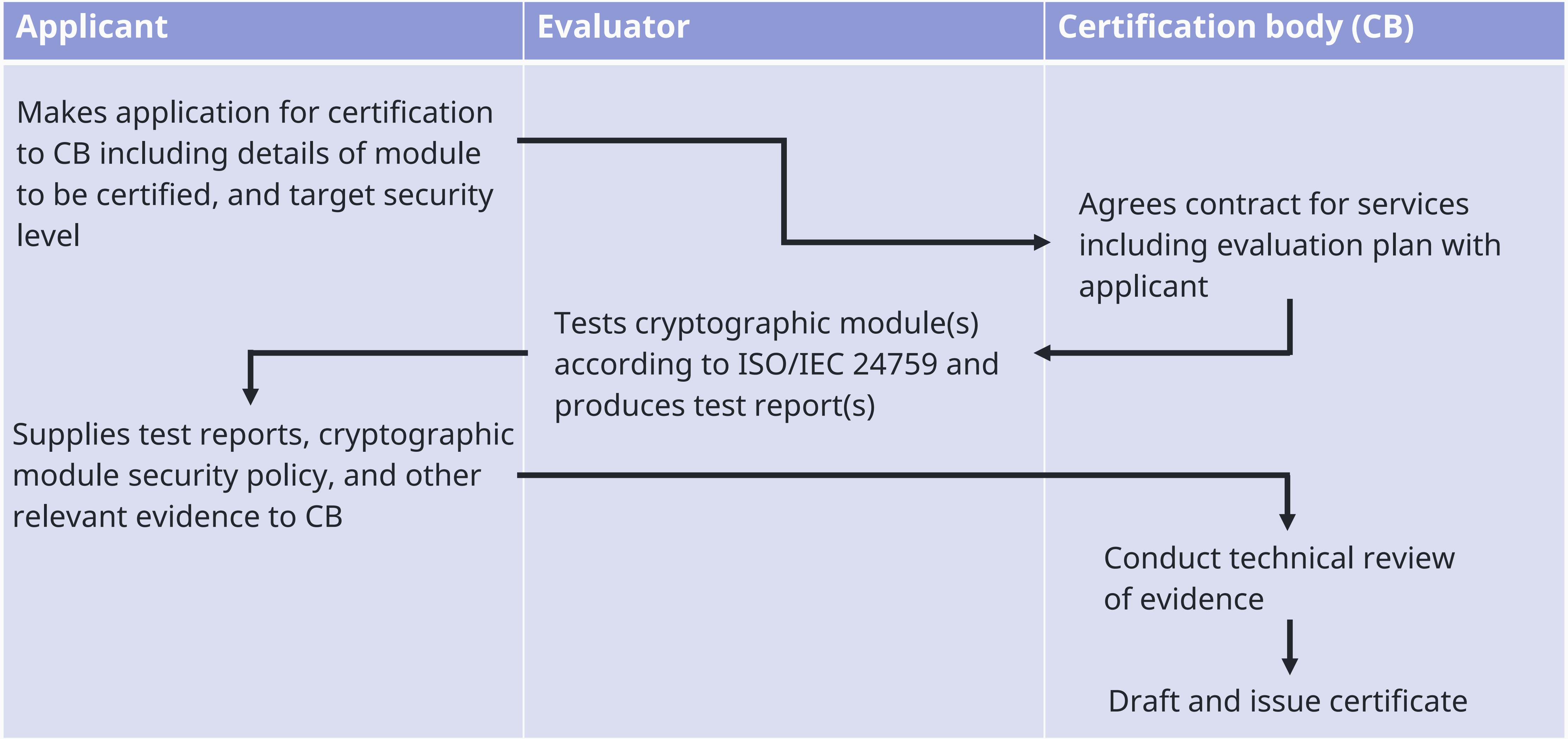
ISO/IEC 19790 certification today

- 8 certificates issued by BSI so far

- 4 organizations have achieved certification for cryptographic modules
    - Huawei Technologies Co., Ltd.
    - Open Security Research, Inc.
    - SinoCipher Technology Development (Shandong) Co., Ltd
    - Kaytus Singapore Pte. Ltd.

- 3 testing laboratories
    - DEKRA Testing and Certification, S.A.
    - Gaowei Cryptography Testing Technology (Shandong) Co., Ltd.
    - SERMA Technologies

ISO/IEC 19790 certification process



Applicant	Evaluator	Certification body (CB)
Makes application for certification to CB including details of module to be certified, and target security level		
		Agrees contract for services including evaluation plan with applicant
	Tests cryptographic module(s) according to ISO/IEC 24759 and produces test report(s)	
Supplies test reports, cryptographic module security policy, and other relevant evidence to CB		
		Conduct technical review of evidence
		Draft and issue certificate

Certificate content

Certificates compliant with this scheme will be valid for a period of three years, and will contain, as a minimum:

- The cryptographic module name and version identifier
- The cryptographic module form (software, firmware and/or hardware)
- The achieved security level from ISO/IEC 19790
- The list of cryptographic mechanisms covered
- Any caveats or important comments that may apply for the use of the cryptographic module

Certificate maintenance

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 the new module version – may require limited evaluation of affected areas	Patches of vulnerabilities affecting open-source components that do not modify or correct the component functionality
Changes to security-relevant features of the module	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

Next steps

- Scheme expansion
  - Surveillance rules?
    - Addressing nonconformities
    - Handling of new publicly known CVEs
  - Algorithm conformance testing
  - Common testing tools
- Continue promotional activities to increase awareness of this initiative

Collaborating towards a secure digital future

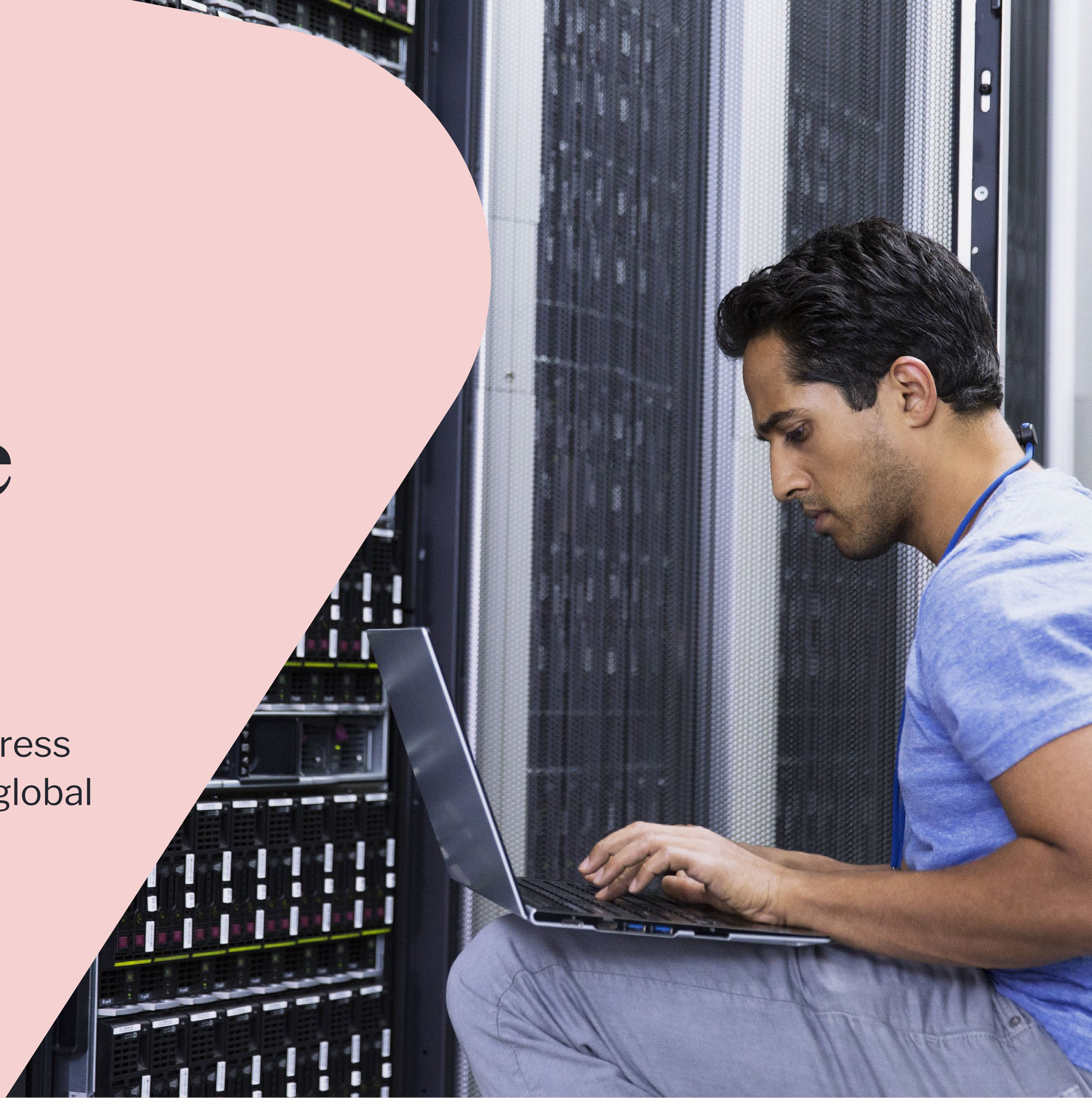
Keynote talk summary

Collaborating towards a secure digital future

Networking break

Collaborating towards a secure digital future

Panel discussion:
Engaging with industry and regulators to address specific needs and concerns using a common global approach for cryptographic module security certification. Future trends



Collaborating towards a secure digital future

Panel discussion:

Q&A

Collaborating towards a secure digital future

Summary, white paper and next steps

Collaborating towards a secure digital future

Thank you!