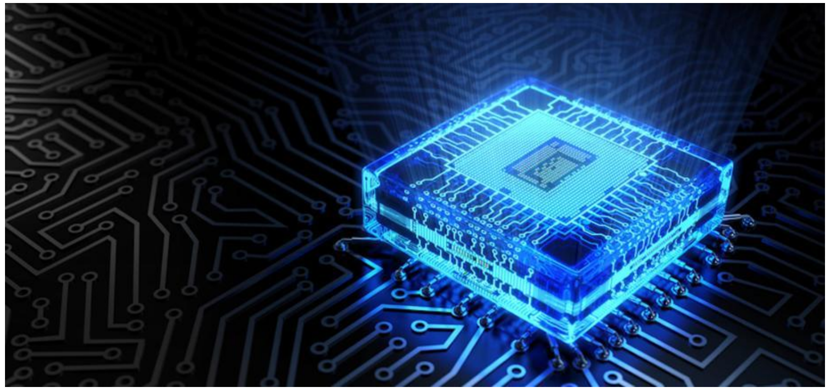
SECURE-iC
THE SECURITY SCIENCE COMPANY

The standards of embedded security



Speaker: **Prof. Sylvain GUILLEY, CTO**

7th December 2022

FIAP,

Paris, France.

Version 2

AGENDA

1. Panorama
2. Context
3. Roadmap
4. New standards

AGENDA

1. Panorama

2. Context

3. Roadmap

4. New standards

Standards in cybersecurity

- Standard Developing Organizations (SDOs)
  - NGO (neutral) vs business driven
  - National vs international

- Goal of standardization:
  - Developers: Secure investments
  - Users: Allow for comparisons

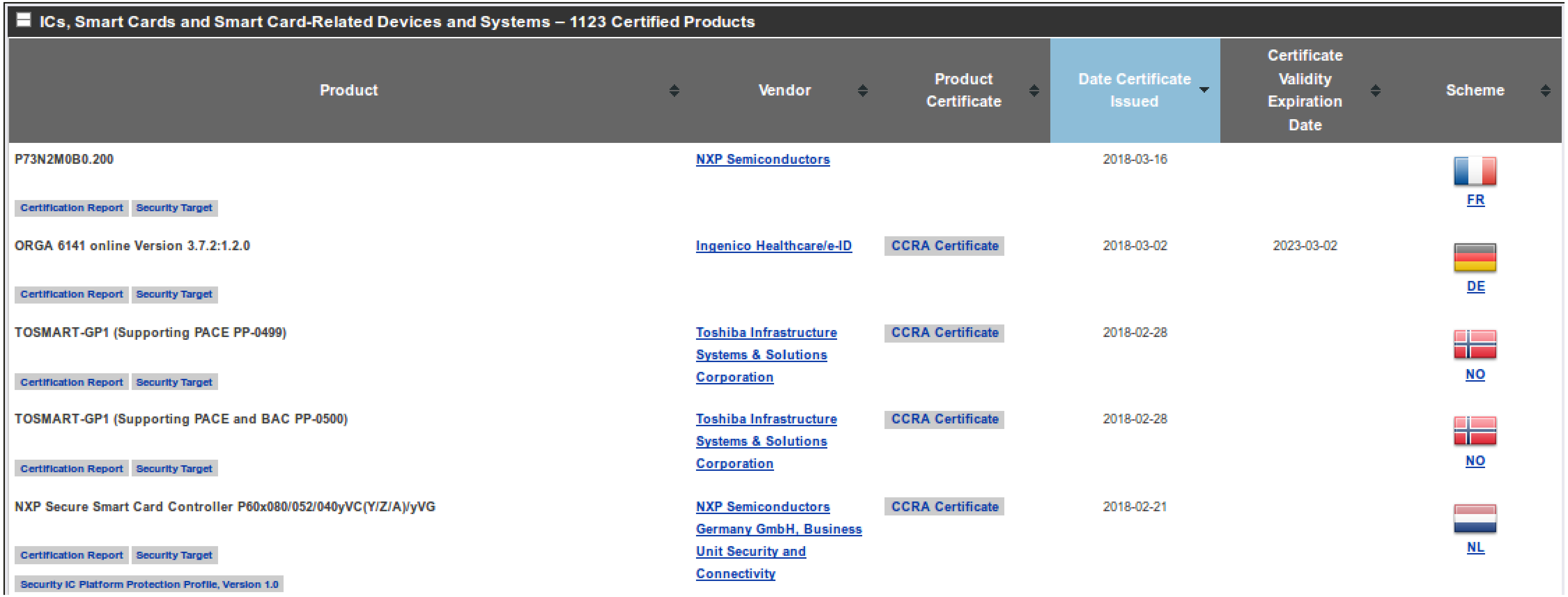
ETSI The Standards People

International Organization for Standardization ISO

afnor CERTIFICATION

Standards in cybersecurity

- Regulatory requirements
- Soft power



ICs, Smart Cards and Smart Card-Related Devices and Systems – 1123 Certified Products

Product	Vendor	Product Certificate	Date Certificate Issued	Certificate Validity Expiration Date	Scheme
P73N2M0B0.200 Certification Report Security Target	NXP Semiconductors		2018-03-16		FR
ORGA 6141 online Version 3.7.2:1.2.0 Certification Report Security Target	Ingenico Healthcare/e-ID	CCRA Certificate	2018-03-02	2023-03-02	DE
TOSMART-GP1 (Supporting PACE PP-0499) Certification Report Security Target	Toshiba Infrastructure Systems & Solutions Corporation	CCRA Certificate	2018-02-28		NO
TOSMART-GP1 (Supporting PACE and BAC PP-0500) Certification Report Security Target	Toshiba Infrastructure Systems & Solutions Corporation	CCRA Certificate	2018-02-28		NO
NXP Secure Smart Card Controller P60x080/052/040yVC(Y/Z/A)/yVG Certification Report Security Target Security IC Platform Protection Profile, Version 1.0	NXP Semiconductors Germany GmbH, Business Unit Security and Connectivity	CCRA Certificate	2018-02-21		NL

Common Criteria vs FIPS 140-3 work products

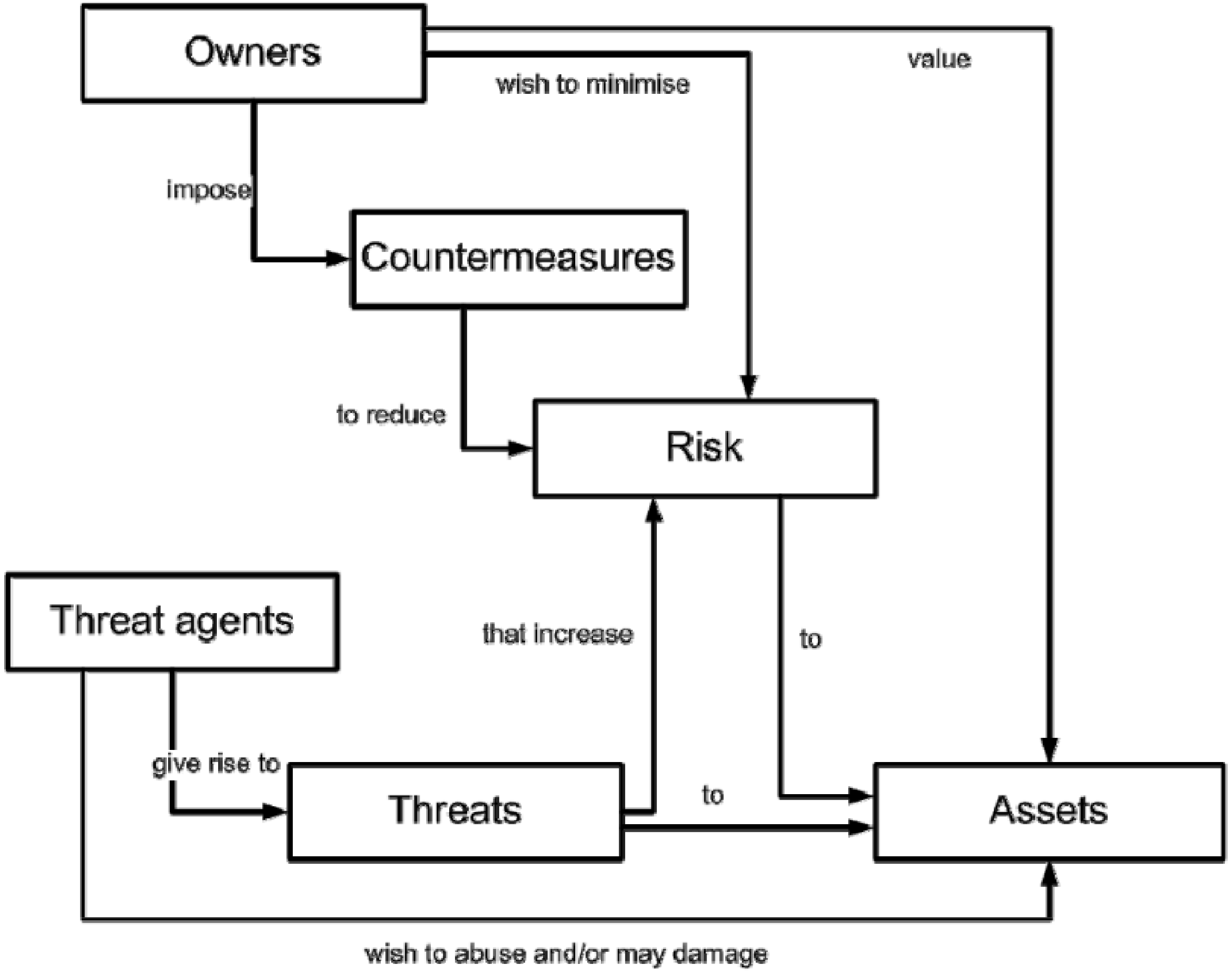
- Class ACO - Composition
- Class ADV - Development
- Class AGD – Guidance documents
- Class ALC – Life-cycle support
- Class ASE – Security Target Evaluation
- Class ATE – Tests
- Class AVA – Vulnerability assessment

- Cryptographic Module Specification
- Cryptographic Module Ports and Interfaces
- Roles, Services, and Authentication
- Finite State Model
- Physical Security
- Operational Environment
- Cryptographic Key Management
- EMI/EMC
- Self-Tests
- Design Assurance
- Mitigation of Other Attacks

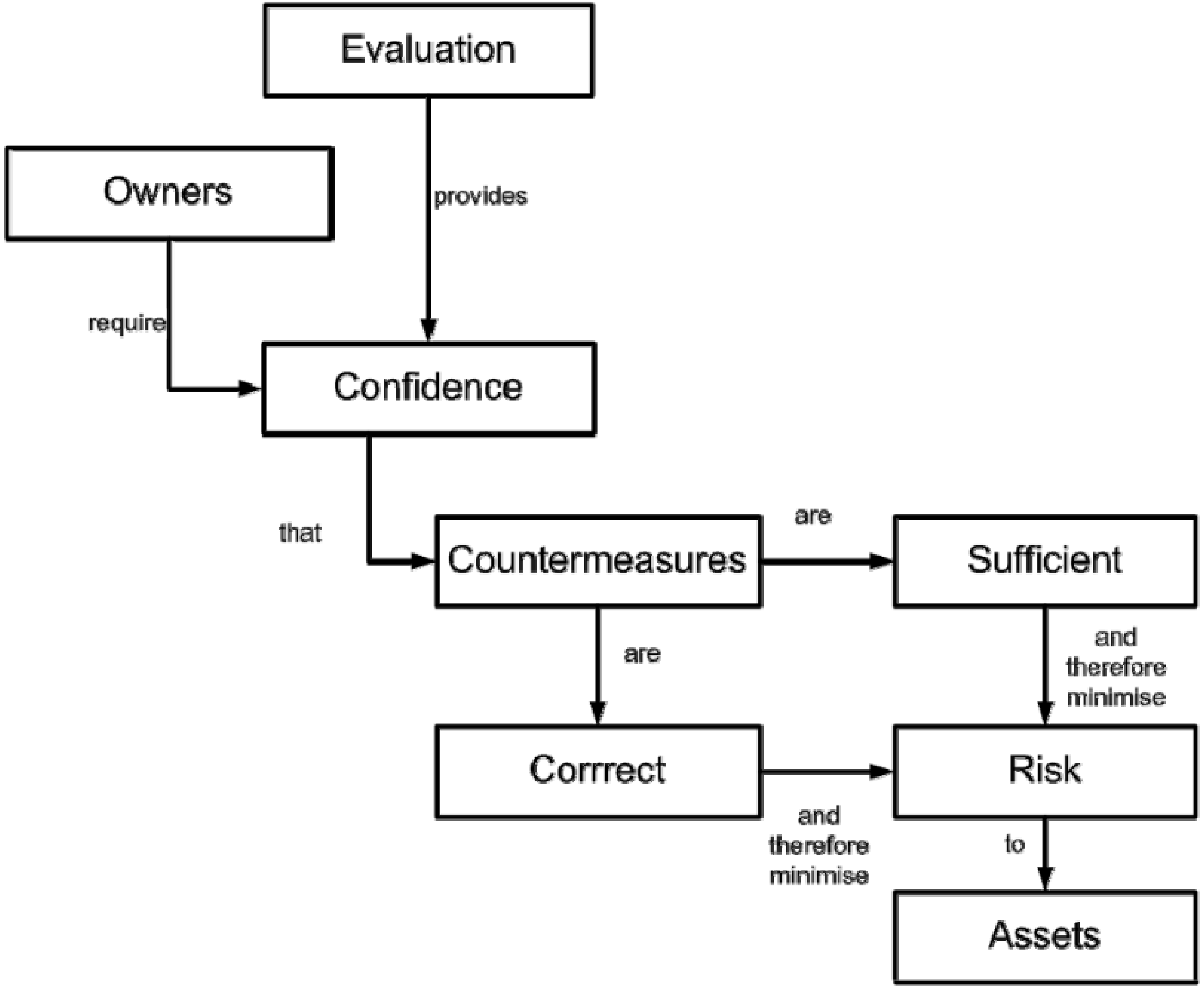
- Test: reproducible
- Evaluation: possibility to innovate, but outcome depends on the skill of the evaluator

Test	*versus*	Evaluation
CMVP Conformance through Testing FIPS VALIDATED 140-2		Common Criteria
ISO/IEC 19790:2012		ISO/IEC 15408:2009

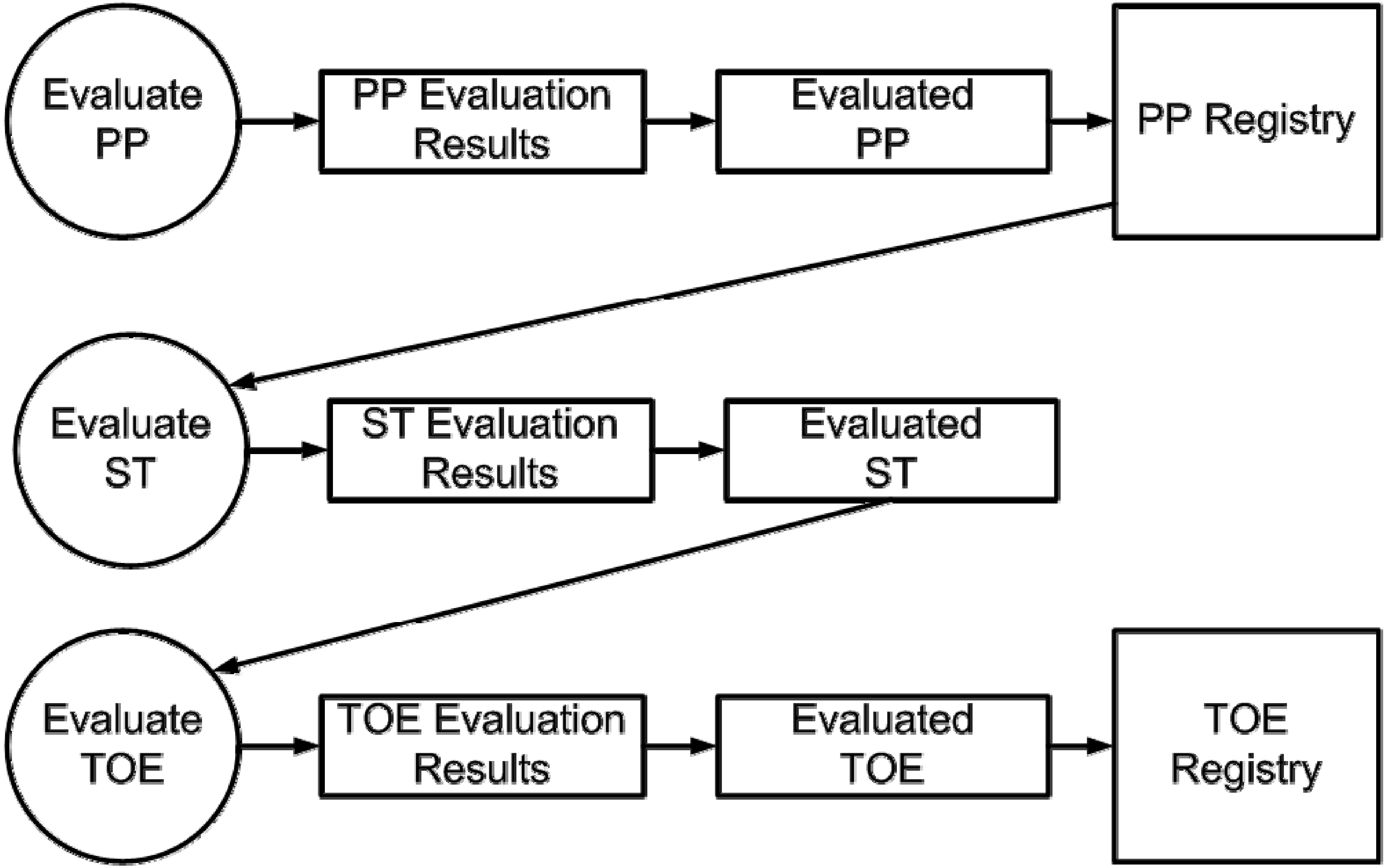
Common criteria: security concepts & relationships



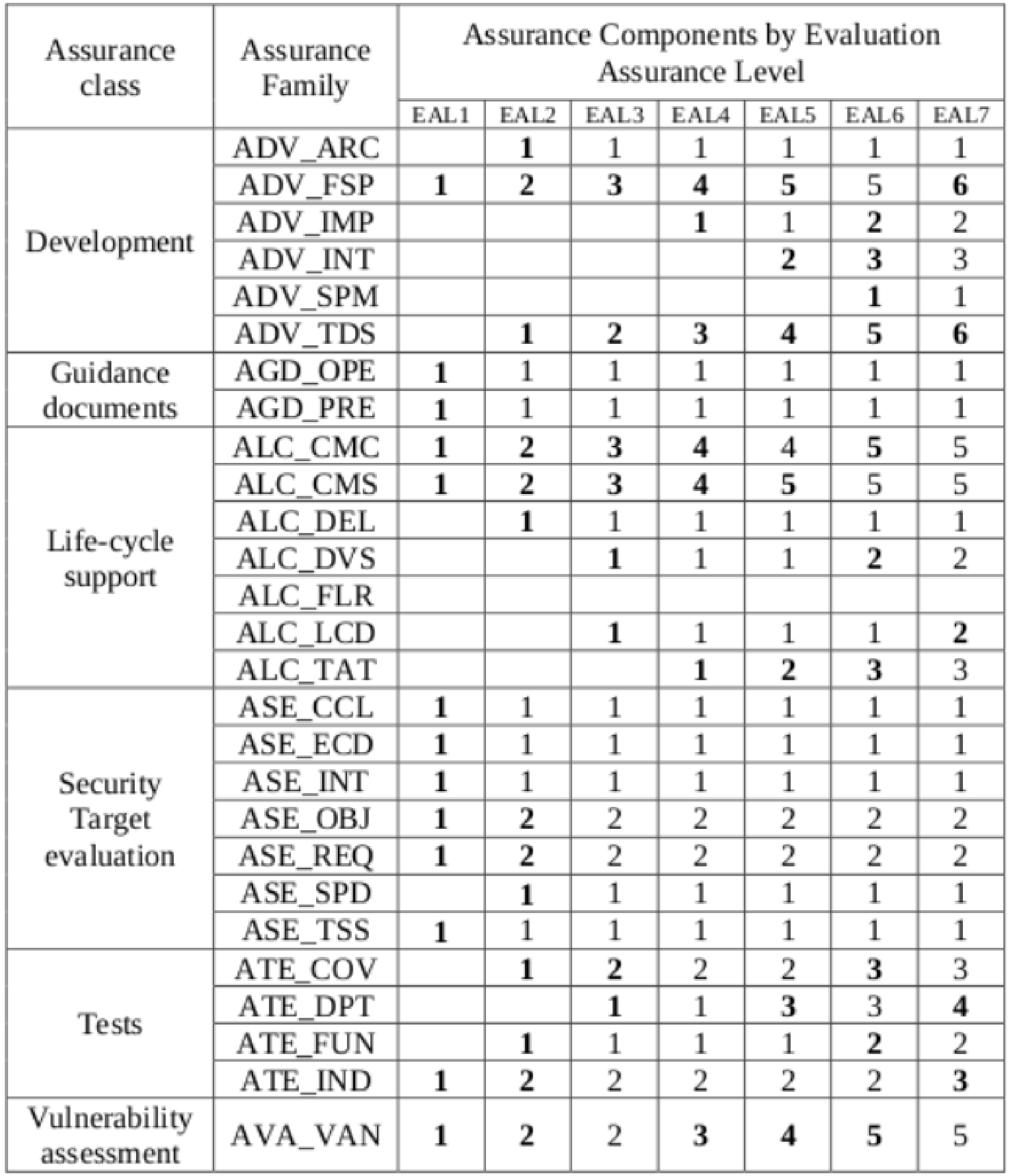
Common criteria: Evaluation concepts & relationships



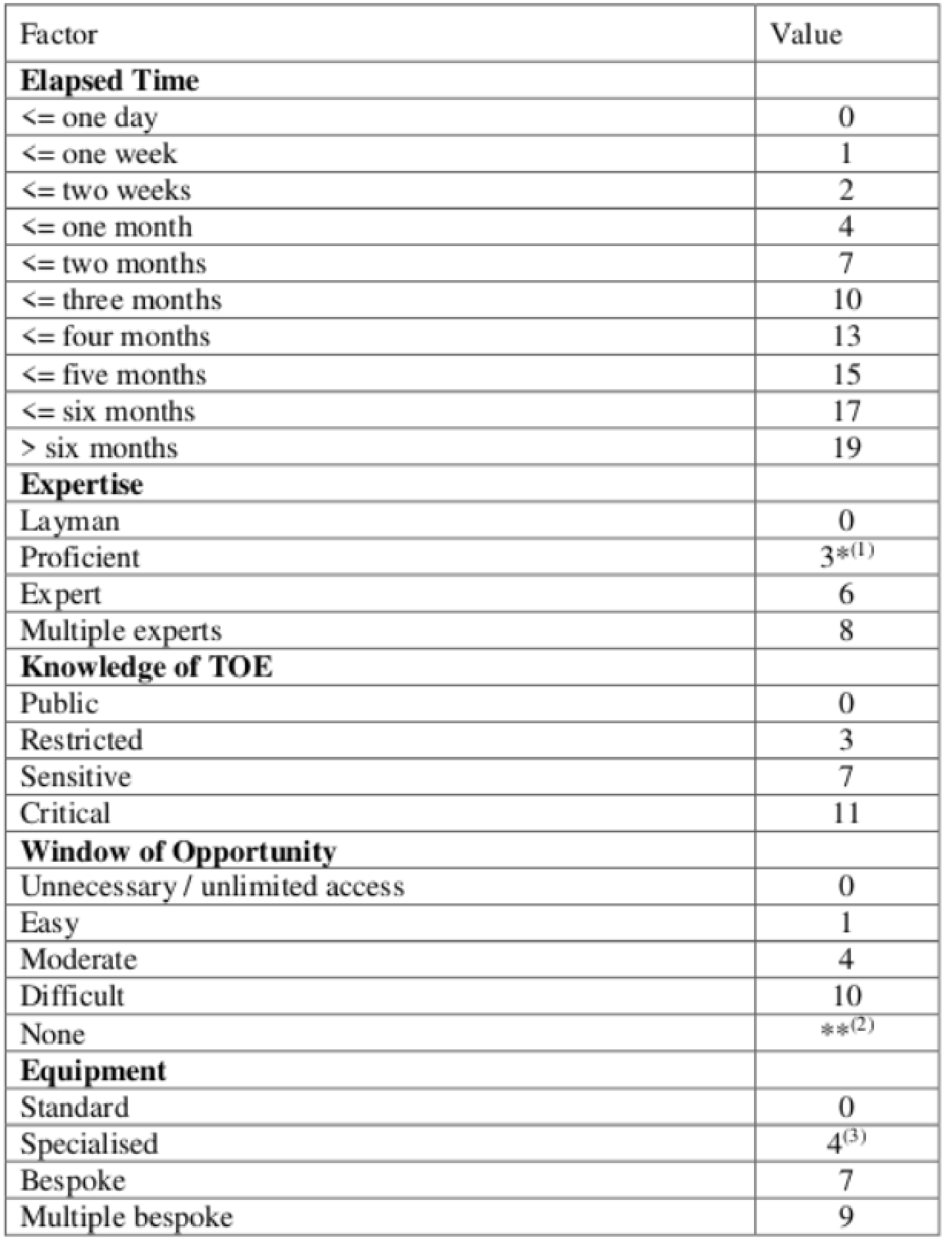
Common criteria: Evaluation results



Common criteria: table EAL

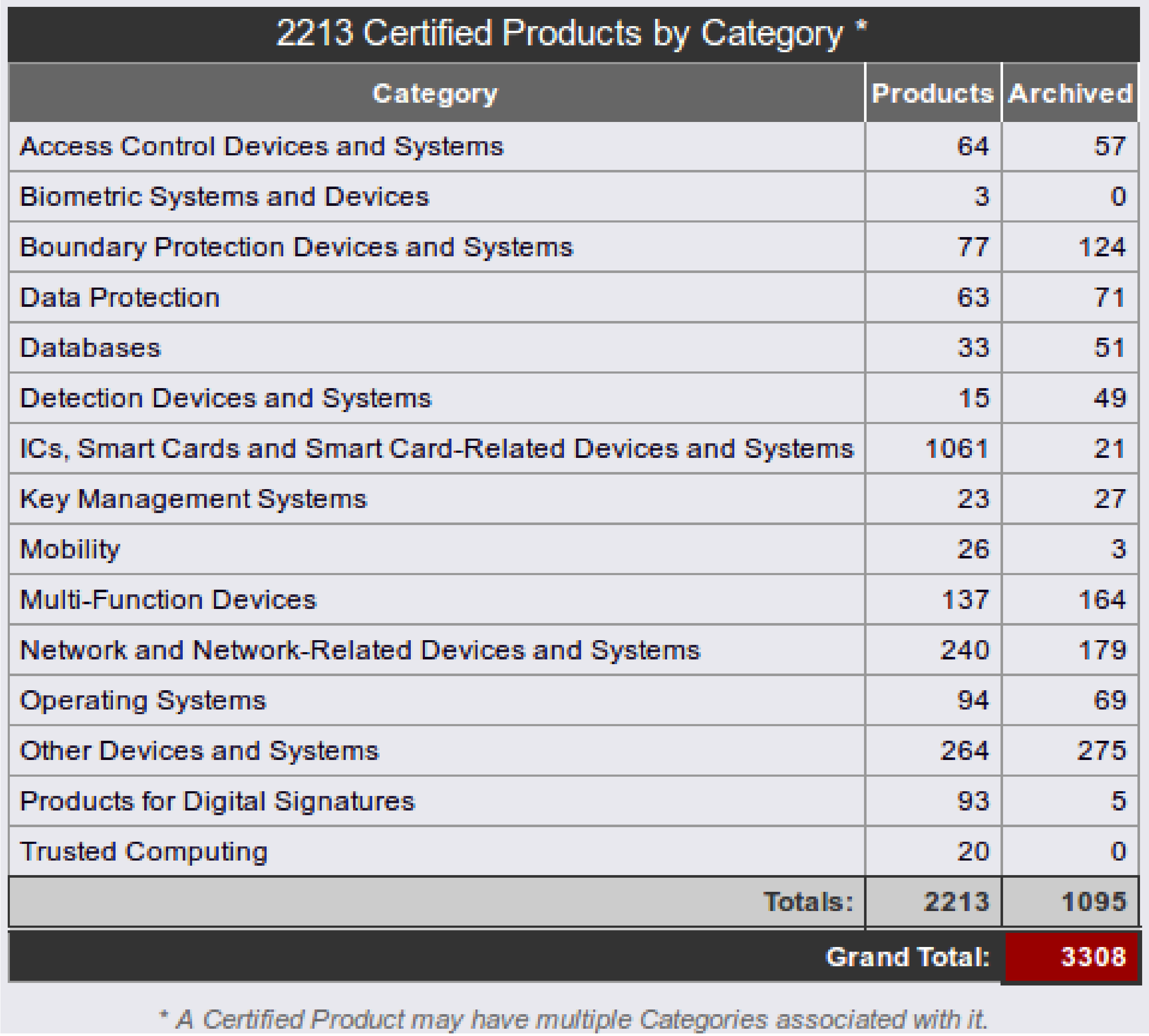


Assurance class	Assurance Family	Assurance Components by Evaluation Assurance Level						
		EAL1	EAL2	EAL3	EAL4	EAL5	EAL6	EAL7
Development	ADV_ARC		**1**	1	1	1	1	1
	ADV_FSP	**1**	**2**	**3**	**4**	**5**	5	**6**
	ADV_IMP				**1**	1	**2**	2
	ADV_INT					**2**	**3**	3
	ADV_SPM						**1**	1
	ADV_TDS		**1**	**2**	**3**	**4**	**5**	**6**
Guidance documents	AGD_OPE	**1**	1	1	1	1	1	1
	AGD_PRE	**1**	1	1	1	1	1	1
Life-cycle support	ALC_CMC	**1**	**2**	**3**	**4**	4	**5**	5
	ALC_CMS	**1**	**2**	**3**	**4**	**5**	5	5
	ALC_DEL		**1**	1	1	1	1	1
	ALC_DVS			**1**	1	1	**2**	2
	ALC_FLR							
	ALC_LCD			**1**	1	1	1	**2**
	ALC_TAT				**1**	**2**	**3**	3
Security Target evaluation	ASE_CCL	**1**	1	1	1	1	1	1
	ASE_ECD	**1**	1	1	1	1	1	1
	ASE_INT	**1**	1	1	1	1	1	1
	ASE_OBJ	**1**	**2**	2	2	2	2	2
	ASE_REQ	**1**	**2**	2	2	2	2	2
	ASE_SPD		**1**	1	1	1	1	1
	ASE_TSS	**1**	1	1	1	1	1	1
Tests	ATE_COV		**1**	**2**	2	2	**3**	3
	ATE_DPT			**1**	1	**3**	3	**4**
	ATE_FUN		**1**	1	1	1	**2**	2
	ATE_IND	**1**	**2**	2	2	2	2	**3**
Vulnerability assessment	AVA_VAN	**1**	**2**	2	**3**	**4**	**5**	5



Factor	Value
Elapsed Time	
<= one day	0
<= one week	1
<= two weeks	2
<= one month	4
<= two months	7
<= three months	10
<= four months	13
<= five months	15
<= six months	17
> six months	19
Expertise	
Layman	0
Proficient	3*(1)
Expert	6
Multiple experts	8
Knowledge of TOE	
Public	0
Restricted	3
Sensitive	7
Critical	11
Window of Opportunity	
Unnecessary / unlimited access	0
Easy	1
Moderate	4
Difficult	10
None	**(2)
Equipment	
Standard	0
Specialised	4(3)
Bespoke	7
Multiple bespoke	9

Common criteria: Statistics

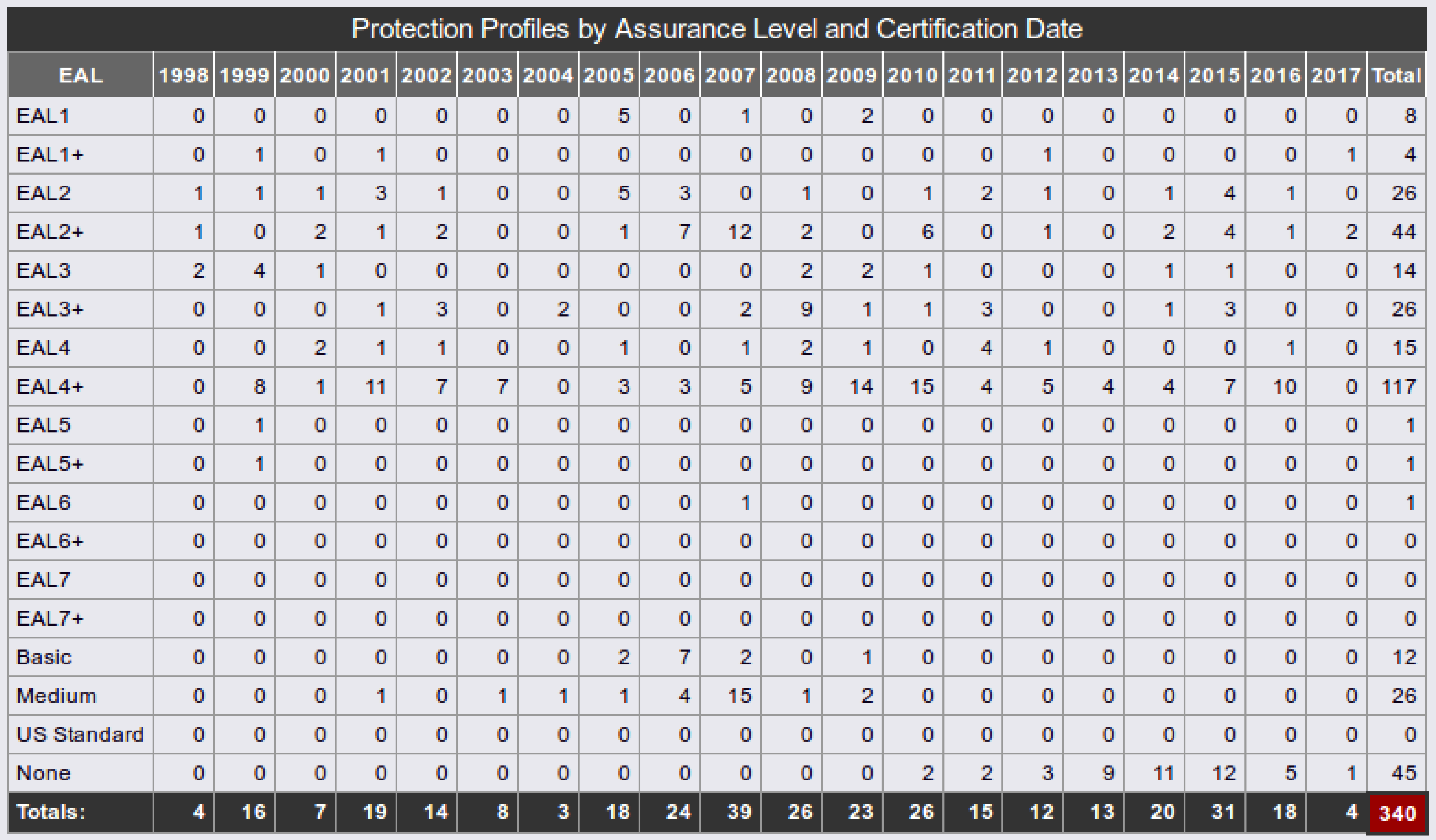


2213 Certified Products by Category *

Category	Products	Archived
Access Control Devices and Systems	64	57
Biometric Systems and Devices	3	0
Boundary Protection Devices and Systems	77	124
Data Protection	63	71
Databases	33	51
Detection Devices and Systems	15	49
ICs, Smart Cards and Smart Card-Related Devices and Systems	1061	21
Key Management Systems	23	27
Mobility	26	3
Multi-Function Devices	137	164
Network and Network-Related Devices and Systems	240	179
Operating Systems	94	69
Other Devices and Systems	264	275
Products for Digital Signatures	93	5
Trusted Computing	20	0
Totals:	2213	1095
Grand Total:		3308

** A Certified Product may have multiple Categories associated with it.*

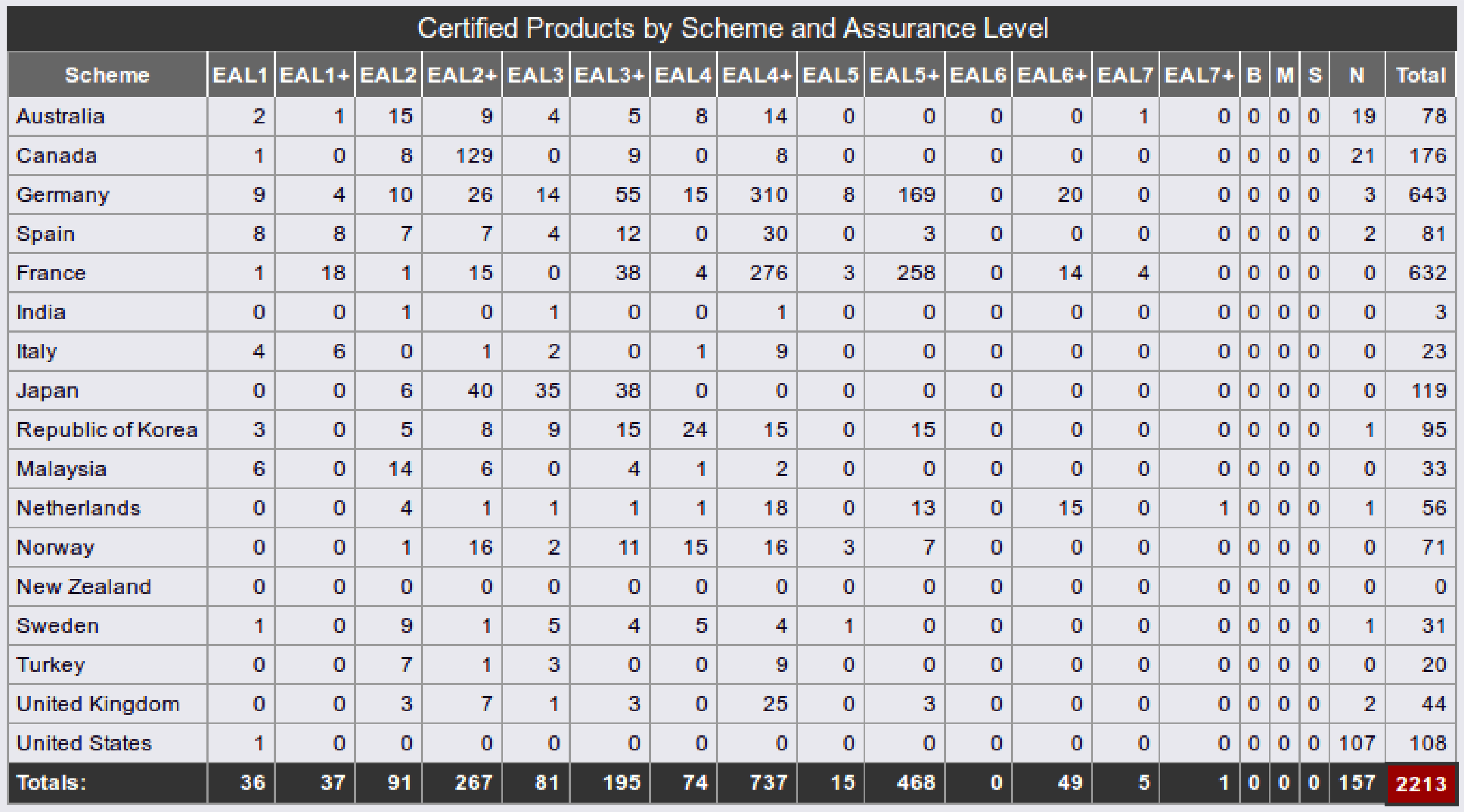
Common criteria: Statistics



Protection Profiles by Assurance Level and Certification Date

EAL	1998	1999	2000	2001	2002	2003	2004	2005	2006	2007	2008	2009	2010	2011	2012	2013	2014	2015	2016	2017	Total
EAL1	0	0	0	0	0	0	0	5	0	1	0	2	0	0	0	0	0	0	0	0	8
EAL1+	0	1	0	1	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0	1	4
EAL2	1	1	1	3	1	0	0	5	3	0	1	0	1	2	1	0	1	4	1	0	26
EAL2+	1	0	2	1	2	0	0	1	7	12	2	0	6	0	1	0	2	4	1	2	44
EAL3	2	4	1	0	0	0	0	0	0	0	2	2	1	0	0	0	1	1	0	0	14
EAL3+	0	0	0	1	3	0	2	0	0	2	9	1	1	3	0	0	1	3	0	0	26
EAL4	0	0	2	1	1	0	0	1	0	1	2	1	0	4	1	0	0	0	1	0	15
EAL4+	0	8	1	11	7	7	0	3	3	5	9	14	15	4	5	4	4	7	10	0	117
EAL5	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL5+	0	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1
EAL6	0	0	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	0	0	0	1
EAL6+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
EAL7+	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Basic	0	0	0	0	0	0	0	2	7	2	0	1	0	0	0	0	0	0	0	0	12
Medium	0	0	0	1	0	1	1	1	4	15	1	2	0	0	0	0	0	0	0	0	26
US Standard	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
None	0	0	0	0	0	0	0	0	0	0	0	0	2	2	3	9	11	12	5	1	45
Totals:	4	16	7	19	14	8	3	18	24	39	26	23	26	15	12	13	20	31	18	4	340

Common criteria: Statistics

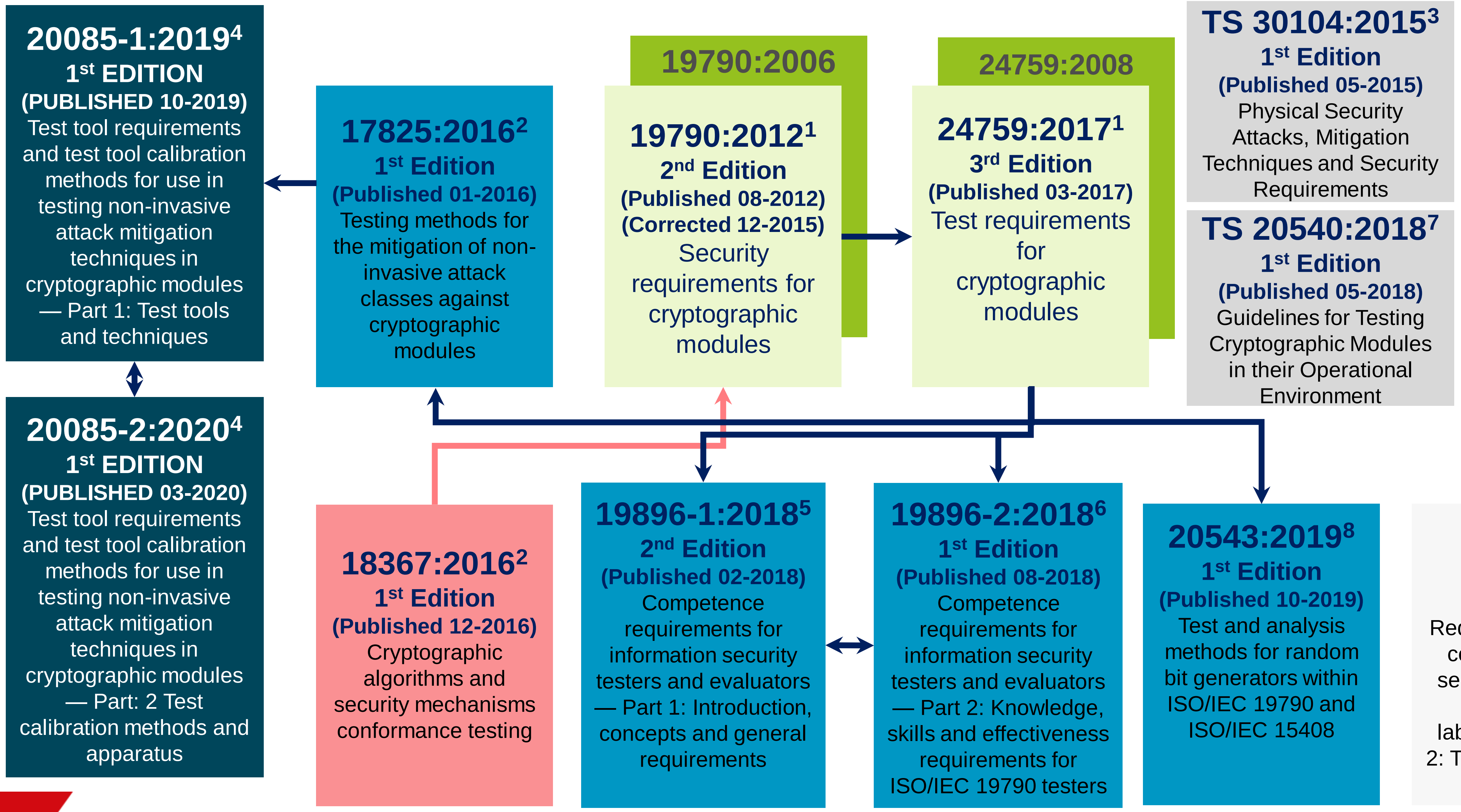


Certified Products by Scheme and Assurance Level

Scheme	EAL1	EAL1+	EAL2	EAL2+	EAL3	EAL3+	EAL4	EAL4+	EAL5	EAL5+	EAL6	EAL6+	EAL7	EAL7+	B	M	S	N	Total
Australia	2	1	15	9	4	5	8	14	0	0	0	0	1	0	0	0	0	19	78
Canada	1	0	8	129	0	9	0	8	0	0	0	0	0	0	0	0	0	21	176
Germany	9	4	10	26	14	55	15	310	8	169	0	20	0	0	0	0	0	3	643
Spain	8	8	7	7	4	12	0	30	0	3	0	0	0	0	0	0	0	2	81
France	1	18	1	15	0	38	4	276	3	258	0	14	4	0	0	0	0	0	632
India	0	0	1	0	1	0	0	1	0	0	0	0	0	0	0	0	0	0	3
Italy	4	6	0	1	2	0	1	9	0	0	0	0	0	0	0	0	0	0	23
Japan	0	0	6	40	35	38	0	0	0	0	0	0	0	0	0	0	0	0	119
Republic of Korea	3	0	5	8	9	15	24	15	0	15	0	0	0	0	0	0	0	1	95
Malaysia	6	0	14	6	0	4	1	2	0	0	0	0	0	0	0	0	0	0	33
Netherlands	0	0	4	1	1	1	1	18	0	13	0	15	0	1	0	0	0	1	56
Norway	0	0	1	16	2	11	15	16	3	7	0	0	0	0	0	0	0	0	71
New Zealand	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
Sweden	1	0	9	1	5	4	5	4	1	0	0	0	0	0	0	0	0	1	31
Turkey	0	0	7	1	3	0	0	9	0	0	0	0	0	0	0	0	0	0	20
United Kingdom	0	0	3	7	1	3	0	25	0	3	0	0	0	0	0	0	0	2	44
United States	1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	107	108
Totals:	**36**	**37**	**91**	**267**	**81**	**195**	**74**	**737**	**15**	**468**	**0**	**49**	**5**	**1**	**0**	**0**	**0**	**157**	**2213**

SECURE-IC
THE SECURITY SCIENCE COMPANY

CRYPTOGRAPHIC MODULE TESTING



20085-1:2019[4]
1st EDITION
(PUBLISHED 10-2019)
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

20085-2:2020[4]
1st EDITION
(PUBLISHED 03-2020)
Test tool requirements and test tool calibration methods for use in testing non-invasive attack mitigation techniques in cryptographic modules — Part: 2 Test calibration methods and apparatus

17825:2016[2]
1st Edition
(Published 01-2016)
Testing methods for the mitigation of non-invasive attack classes against cryptographic modules

19790:2006

19790:2012[1]
2nd Edition
(Published 08-2012)
(Corrected 12-2015)
Security requirements for cryptographic modules

24759:2008

24759:2017[1]
3rd Edition
(Published 03-2017)
Test requirements for cryptographic modules

TS 30104:2015[3]
1st Edition
(Published 05-2015)
Physical Security Attacks, Mitigation Techniques and Security Requirements

TS 20540:2018[7]
1st Edition
(Published 05-2018)
Guidelines for Testing Cryptographic Modules in their Operational Environment

18367:2016[2]
1st Edition
(Published 12-2016)
Cryptographic algorithms and security mechanisms conformance testing

19896-1:2018[5]
2nd Edition
(Published 02-2018)
Competence requirements for information security testers and evaluators — Part 1: Introduction, concepts and general requirements

19896-2:2018[6]
1st Edition
(Published 08-2018)
Competence requirements for information security testers and evaluators — Part 2: Knowledge, skills and effectiveness requirements for ISO/IEC 19790 testers

20543:2019[8]
1st Edition
(Published 10-2019)
Test and analysis methods for random bit generators within ISO/IEC 19790 and ISO/IEC 15408

23532-2[9]
Prepare for Publish
Requirements for the competence of IT security testing and evaluation laboratories — Part 2: Testing for ISO/IEC 19790

Editors/Co-Editors

1 **Randall Easter**
Jean-Pierre Quémard
Junichi Kondo
2 **Randall Easter**
Jean-Pierre Quémard
Gen'ya Sakurai
3 **Randall Easter**
4 **Hirofumi Sakane**
Sylvain Guilley
Randall Easter
5 **Fiona Pattinson**
Randall Easter
6 **Randall Easter**
Fiona Pattinson
7 **Heebong Choi**
Randall Easter
Jean-Pierre Quémard
8 **Jean-Pierre Quémard**
Randall Easter
9 **Randall Easter**
Heebong Choi
Carolyn French

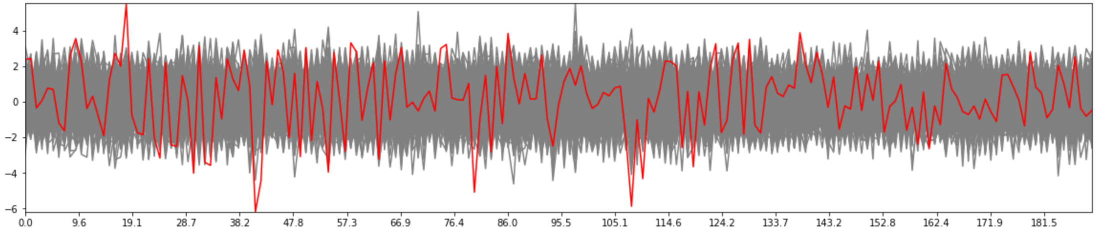
ISO/IEC 17825
Non-Invasive Analyses

- Side-channel test and evaluation is common practice:
  - Known for long (Kocher, 1997)
  - Commercial test-benches available

- But regarding the methodology in complex systems:
  - SoCs mix hardware and software
  - New side-channels:
    - MINERVA (CVE-2019-13627),
    - TPM Fail (CVE-2019-16863),
    - PLATYPUS (CVE-2020-8694), ...

- However, owing to the dissemination of SCA requirements, a formal methodology is welcomed:
  - Automotive, IoT, AI, 5G, etc.

- For the evaluations to be fair and comparable, it cannot only rely (solely) on the lab expertise



Minerva

Where FIPS prescriptive requirements do help CC

FIPS aims security warranty at the lowest cost, hence can impose design options:

- However, such prescription is always beneficial to overall security (hence to CC)
- This situation becomes complex only when performance (PPA) becomes the bottleneck

FIPS	Requirement	Advantage in CC
7.3	Cryptographic Module Interfaces	Minimal exposition
7.5	Software/Firmware Security	Secure boot helps for attacks while at rest
7.7 & 7.8	Physical Security (Environmental failure protection/testing) Non-Invasive Security	Vulnerability Analysis
7.9	Sensitive Security Parameter Management	Zeroization cuts some attack paths
7.10	Self-Test service	Allows to detect perturbation attacks
§F	Approved non-invasive attack mitigation test metrics	AVA_VAN protection

Validation of “entropy sources”

For instance, regarding True Random Number Generators (TRNGs):

- There are very detailed requirements, even *intrusive* ones (e.g., access to "raw" bits).
- Similarly, standards require tests on millions of bits generated in-a-row by the TRNG.
- The OSCCA scheme requires that several TRNGs rationales must be implemented, so as to withstand total failures. Obviously, this benefits as well for resistance to fault attacks under a CC prism.

FIPS 140-3

FIPS SP 800 90B
ISO/IEC 20543:2019

BSI AIS 31
RNG_PTG.2

COMMON CRITERIA

GM/T 0008-2012

OSCCA level	Different sources	# of rationale
1	2	1
2	4	1
3	8	2

Example of pitfalls

Now, it should be noted that some pitfalls shall be avoided as well.

- From a normative standpoint:
  - Recall for instance that EVITA secure boot is based on firmware hash,
  - which is incompatible with FIPS 140-3 requirements to leverage digital signature (from level 3 onward).
- From a functional security standpoint:
  - FIPS SP 800 90B requires that raw bits be output
  - which can be a backdoor (for attacks to analyze deeply the behavior of the TRNG under stress)

Nonetheless we see no fundamental contradiction between schemes:

- They all aim at increasing the practical security level.

AGENDA

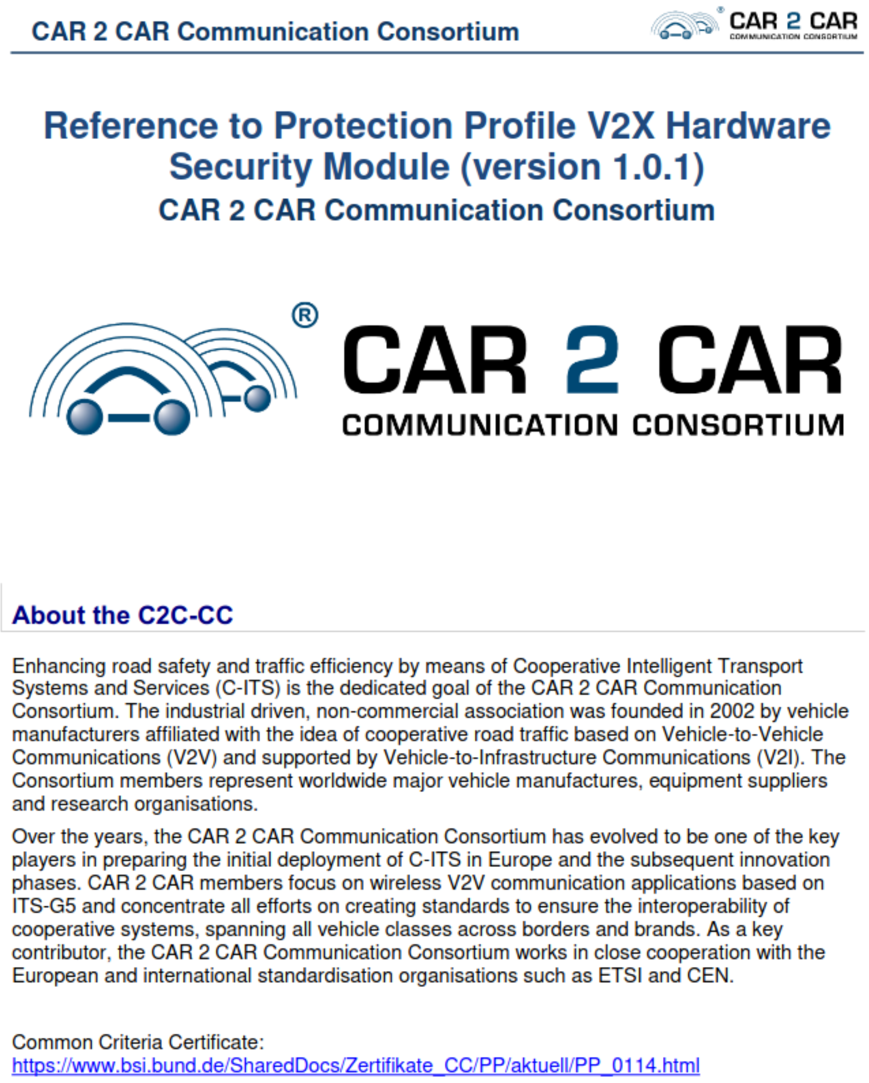
1. Panorama

2. Context

3. Roadmap

4. New standards

Multi-certification: Why?



CAR 2 CAR Communication Consortium

CAR 2 CAR COMMUNICATION CONSORTIUM

Reference to Protection Profile V2X Hardware Security Module (version 1.0.1)

CAR 2 CAR Communication Consortium

CAR 2 CAR
COMMUNICATION CONSORTIUM

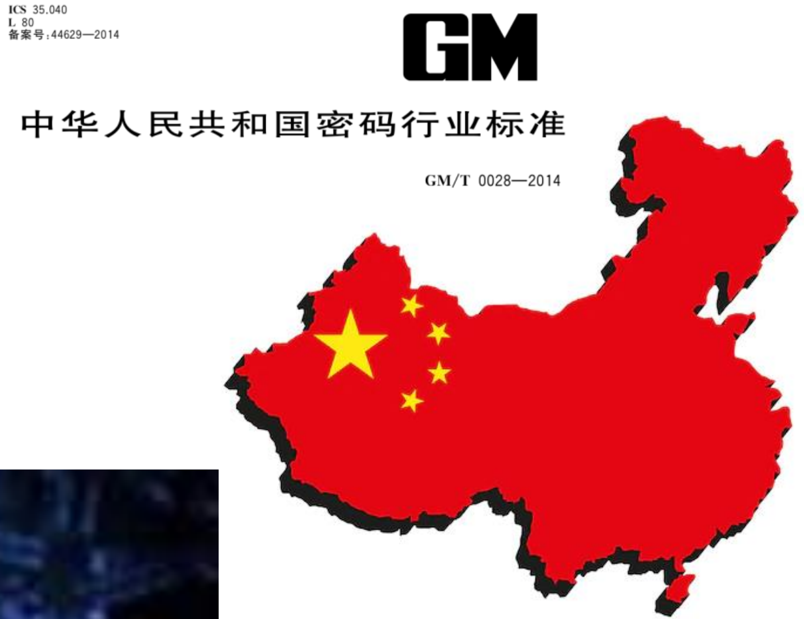
About the C2C-CC

Enhancing road safety and traffic efficiency by means of Cooperative Intelligent Transport Systems and Services (C-ITS) is the dedicated goal of the CAR 2 CAR Communication Consortium. The industrial driven, non-commercial association was founded in 2002 by vehicle manufacturers affiliated with the idea of cooperative road traffic based on Vehicle-to-Vehicle Communications (V2V) and supported by Vehicle-to-Infrastructure Communications (V2I). The Consortium members represent worldwide major vehicle manufactures, equipment suppliers and research organisations.

Over the years, the CAR 2 CAR Communication Consortium has evolved to be one of the key players in preparing the initial deployment of C-ITS in Europe and the subsequent innovation phases. CAR 2 CAR members focus on wireless V2V communication applications based on ITS-G5 and concentrate all efforts on creating standards to ensure the interoperability of cooperative systems, spanning all vehicle classes across borders and brands. As a key contributor, the CAR 2 CAR Communication Consortium works in close cooperation with the European and international standardisation organisations such as ETSI and CEN.

Common Criteria Certificate:
https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0114.html

Common Criteria



ICS 35.040
L 80
备案号：44629—2014

GM

中华人民共和国密码行业标准

GM/T 0028—2014

FIPS 140-3

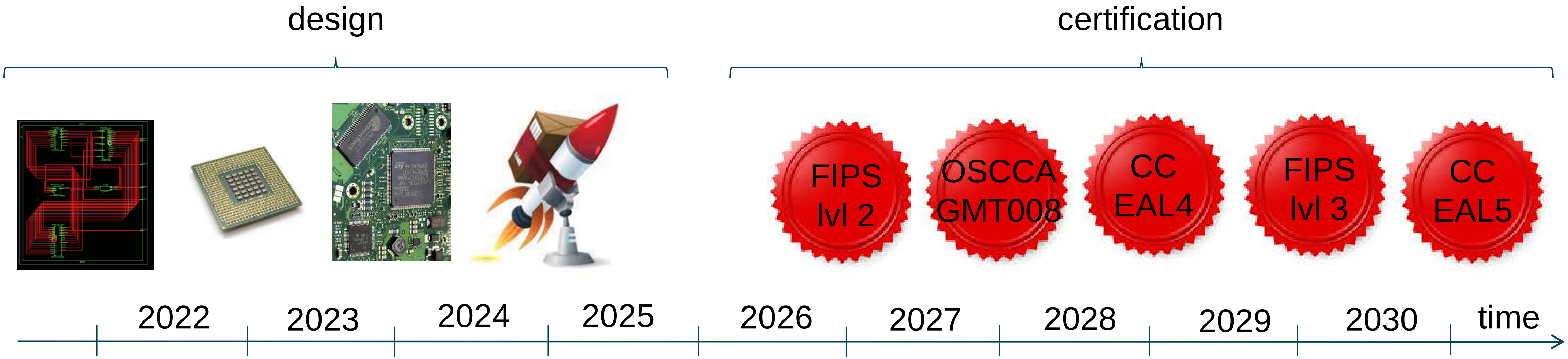
HSM:
Hardware Security Module

OASIS

PKCS #11 Cryptographic Token Interface Base Specification Version 2.40

Pre-certifiability

- Owing to time to market reduction, some chips must be ready to be deployed in markets or use-cases **unknown at design time**.
- Now each market has (or will have) its **own security schemes**.
- Hence the unavoidable need for chips to be **"pre-certifiable"** under **different schemes**.



design

certification

FIPS lvl 2

OSCCA GMT008

CC EAL4

FIPS lvl 3

CC EAL5

2022 2023 2024 2025 2026 2027 2028 2029 2030 time

- The design activity is usually tailored to a given set of security requirements.
- In the new context where multiple requirements will need to be fulfilled proactively, **design strategies** must evolve.

Multi-certifiability

Protect:

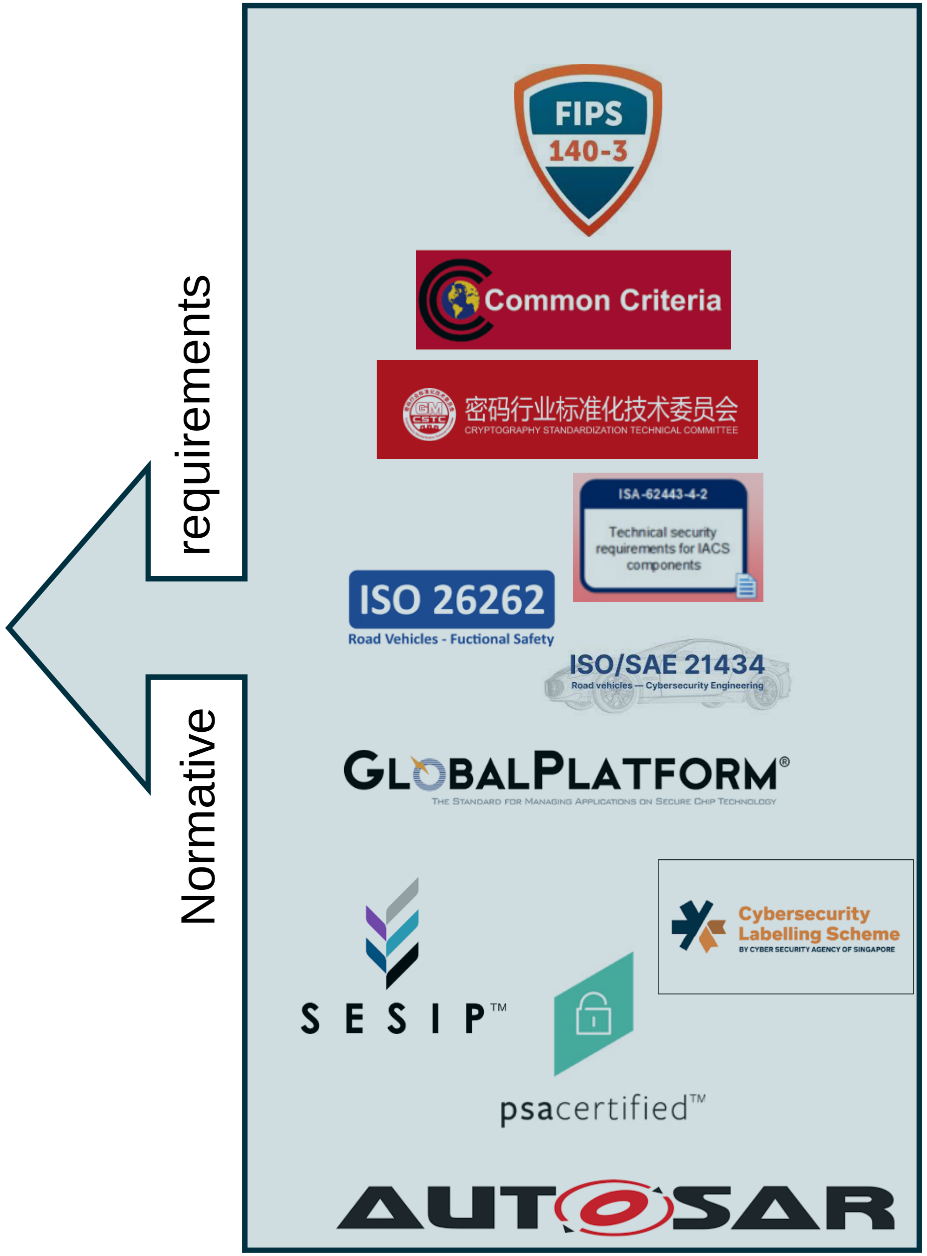
- Generic design
- Constraints

Evaluate:

- Test strategy
- Tools

Service & Certify:

- Documentation
- Evidence


Normative requirements

FIPS 140-3
Common Criteria
密码行业标准化技术委员会
CRYPTOGRAPHY STANDARDIZATION TECHNICAL COMMITTEE
ISA-62443-4-2
Technical security requirements for IACS components
ISO 26262
Road Vehicles - Fuctional Safety
ISO/SAE 21434
Road vehicles — Cybersecurity Engineering
GLOBALPLATFORM®
THE STANDARD FOR MANAGING APPLICATIONS ON SECURE CHIP TECHNOLOGY
Cybersecurity Labelling Scheme
BY CYBER SECURITY AGENCY OF SINGAPORE
SESIP™
psacertified™
AUTOSAR

Chips eligible to triple pre-certification

- Market requirements: simultaneous conformance to
  - Common Criteria,
  - NIST FIPS 140 and
  - Chinese OSCCA.
- The synergies come at three levels.
  - **First**, the documentation production is rationalized. Typically, in the newest version of FIPS 140 (the version 3), the “life-cycle assurance” requirements can be mutualized with the ADV, AGD, ALC and ATE assurance classes in CC.
  - **Second**, it is often beneficial to combine the functional requirements.
    Consider for instance the mandatory self-checks of cryptographic algorithms and/or of keys zeroization in FIPS 140: they are sound precautions that profit reducing the number of vulnerabilities in the context of CC.
  - **Third**, some specific IPs are anyhow to be analyzed more deeply in all the schemes.
    For instance, regarding True Random Number Generators (TRNGs), there are very detailed requirements, even intrusive ones (e.g., access to "raw" bits).

AGENDA

1. Panorama

2. Context

3. Roadmap

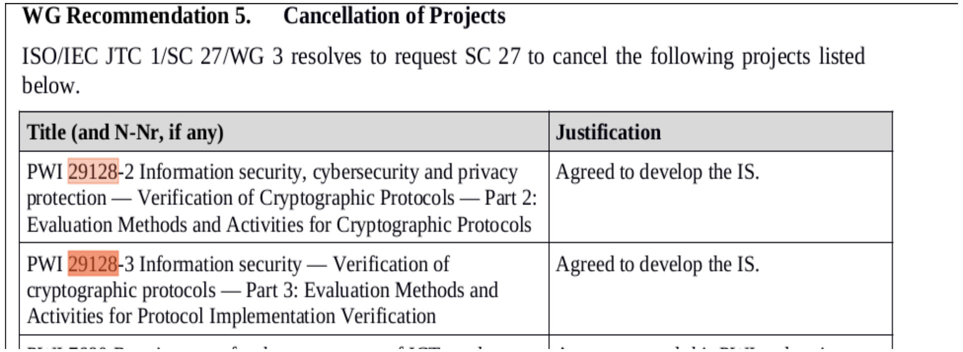
4. New standards

New CC version 4

Information security, cybersecurity and privacy protection — New concepts and changes in ISO/IEC 15408:2021 and ISO/IEC 18045:2021

European Common Criteria, European Cyber Act, ENISA

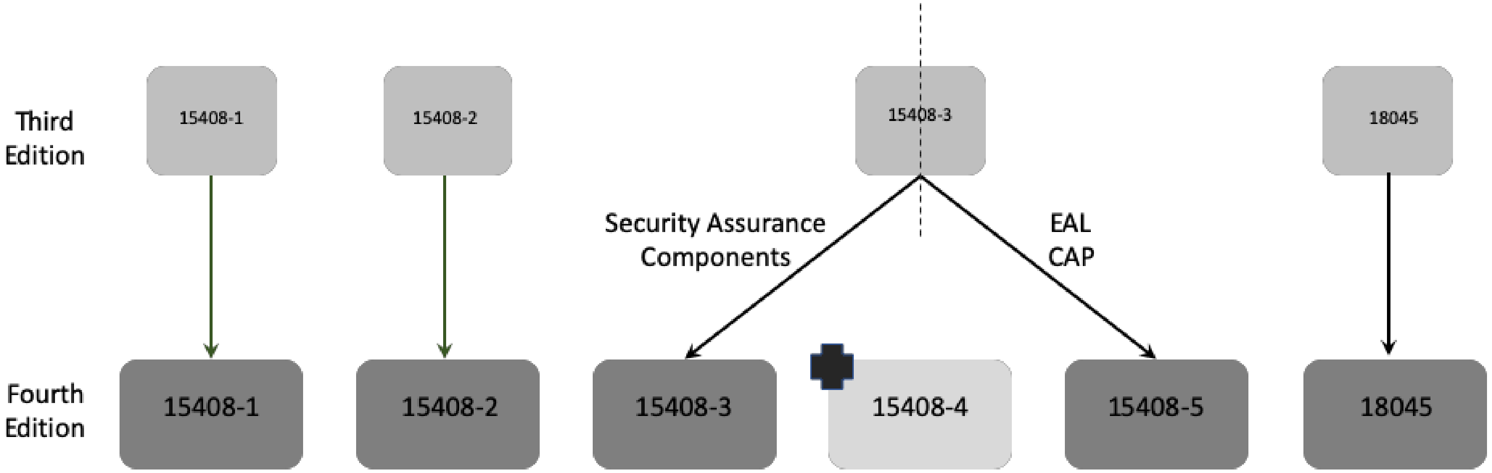
- Secure-IC is leading one exemple of use of 15408-4:
  - ISO/IEC 29128-3



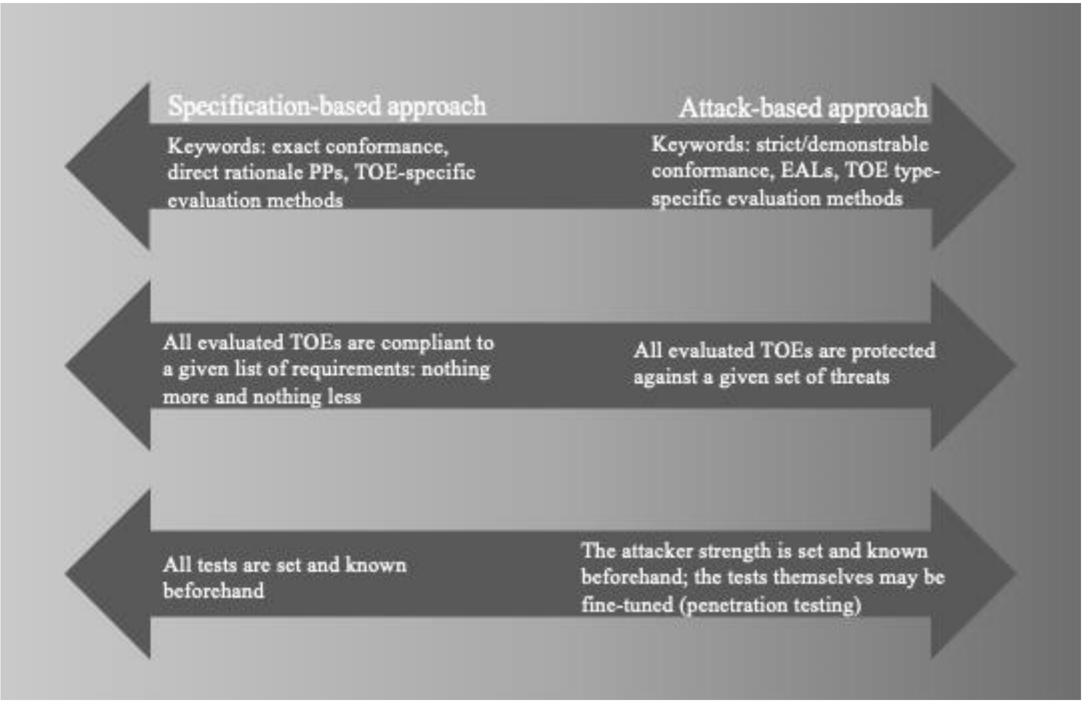
WG Recommendation 5. **Cancellation of Projects**

ISO/IEC JTC 1/SC 27/WG 3 resolves to request SC 27 to cancel the following projects listed below.

Title (and N-Nr, if any)	Justification
PWI 29128-2 Information security, cybersecurity and privacy protection — Verification of Cryptographic Protocols — Part 2: Evaluation Methods and Activities for Cryptographic Protocols	Agreed to develop the IS.
PWI 29128-3 Information security — Verification of cryptographic protocols — Part 3: Evaluation Methods and Activities for Protocol Implementation Verification	Agreed to develop the IS.



New CC version 4



Specification-based approach

Keywords: exact conformance, direct rationale PPs, TOE-specific evaluation methods

Attack-based approach

Keywords: strict/demonstrable conformance, EALs, TOE type-specific evaluation methods

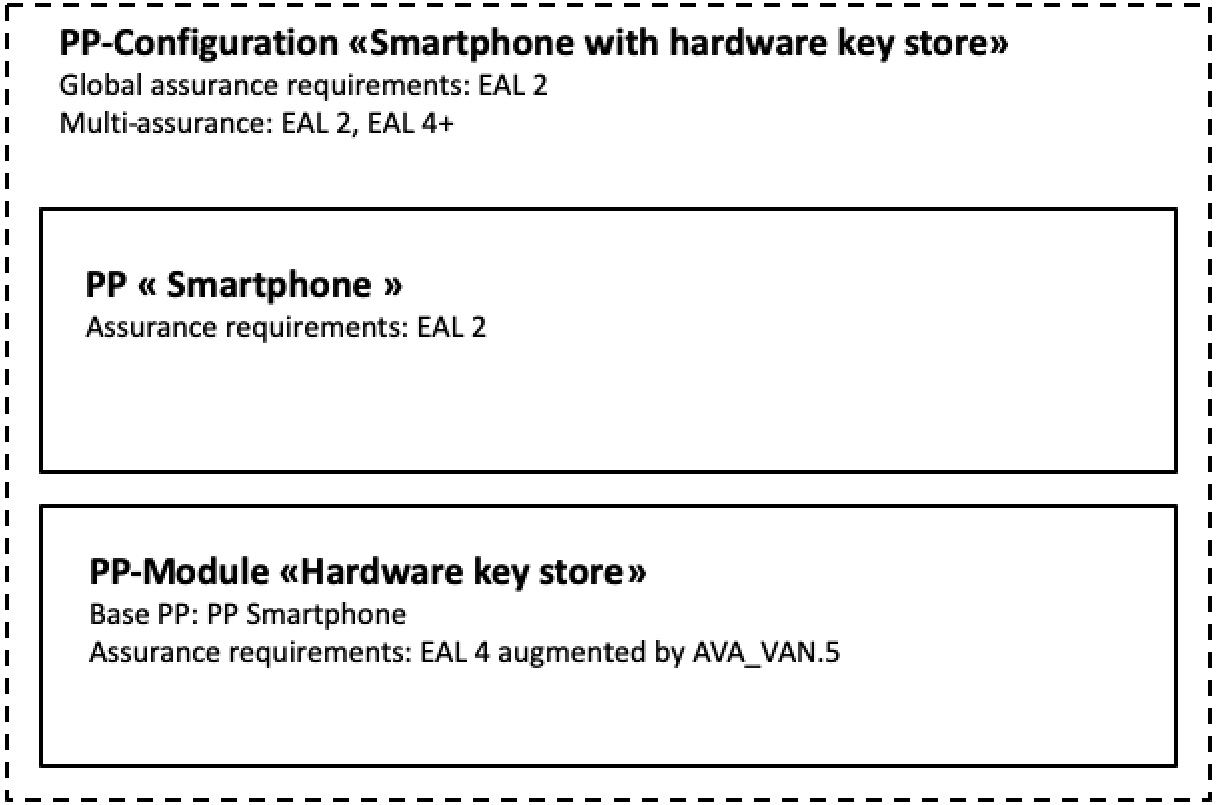
All evaluated TOEs are compliant to a given list of requirements: nothing more and nothing less

All evaluated TOEs are protected against a given set of threats

All tests are set and known beforehand

The attacker strength is set and known beforehand; the tests themselves may be fine-tuned (penetration testing)

Figure 2 — Specification-based and attack-based approaches



PP-Configuration «Smartphone with hardware key store»

Global assurance requirements: EAL 2

Multi-assurance: EAL 2, EAL 4+

PP « Smartphone »

Assurance requirements: EAL 2

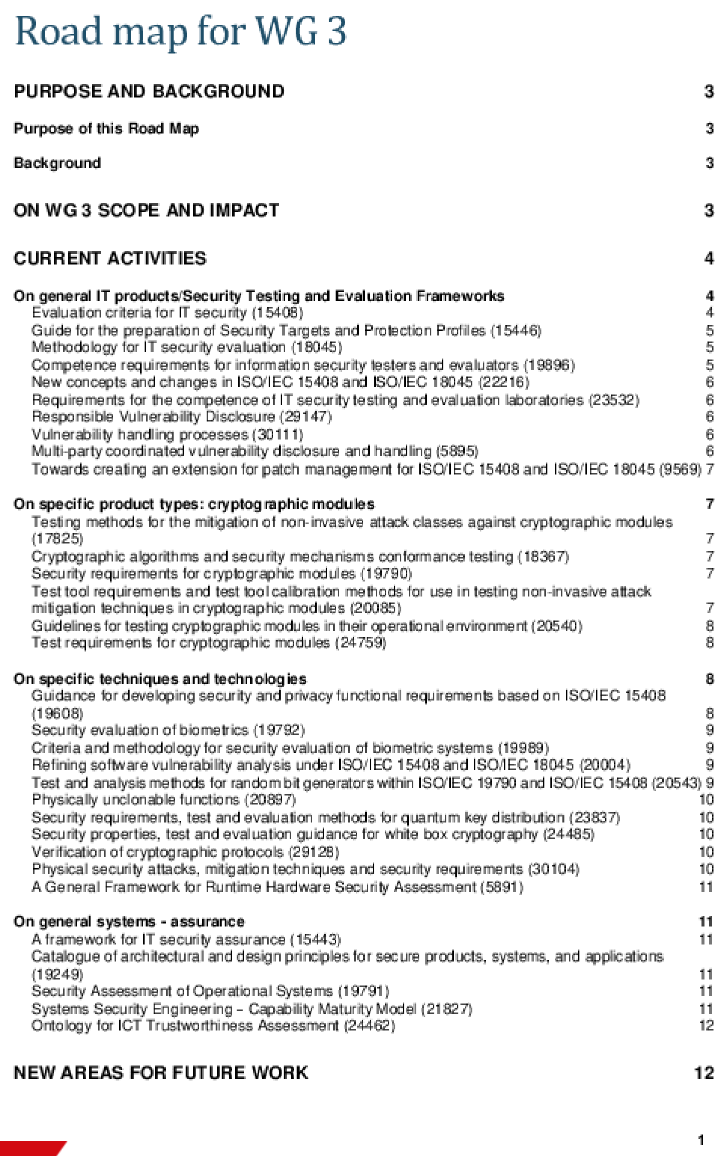
PP-Module «Hardware key store»

Base PP: PP Smartphone

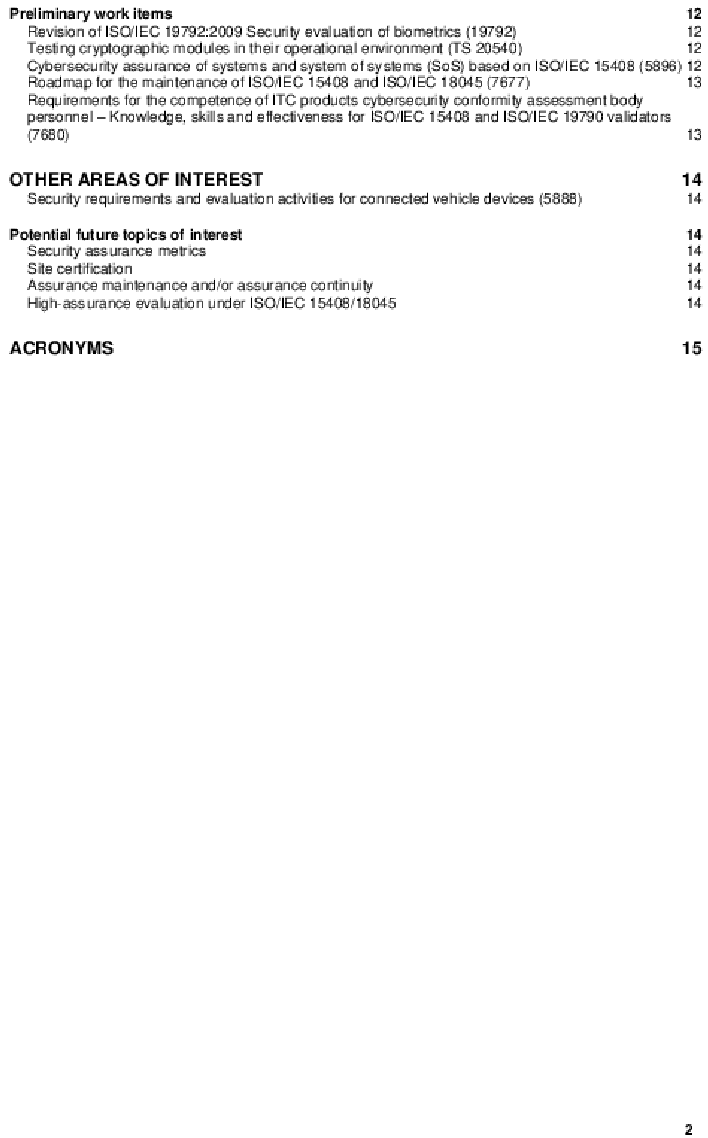
Assurance requirements: EAL 4 augmented by AVA_VAN.5

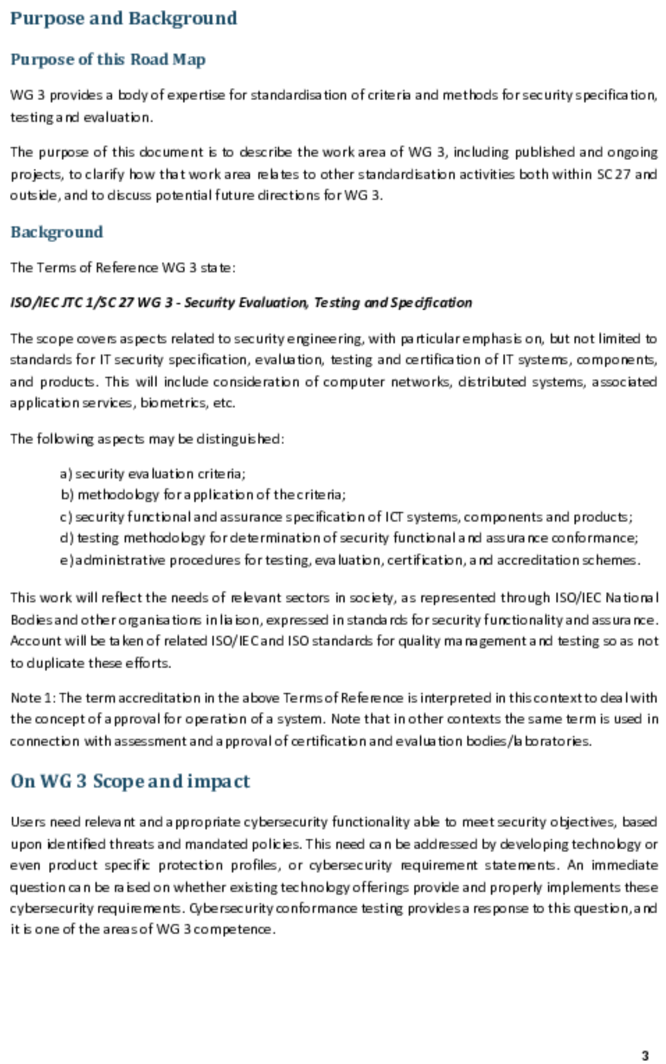
Figure 3 — Smartphone with hardware key store

ISO/IEC JTC1/SC 27/WG3 Roadmap



Road map for WG 3





Purpose and Background

Purpose of this Road Map

WG 3 provides a body of expertise for standardisation of criteria and methods for security specification, testing and evaluation.

The purpose of this document is to describe the work area of WG 3, including published and ongoing projects, to clarify how that work area relates to other standardisation activities both within SC 27 and outside, and to discuss potential future directions for WG 3.

Background

The Terms of Reference WG 3 state:

ISO/IEC JTC 1/SC 27 WG 3 - Security Evaluation, Testing and Specification

The scope covers aspects related to security engineering, with particular emphasis on, but not limited to standards for IT security specification, evaluation, testing and certification of IT systems, components, and products. This will include consideration of computer networks, distributed systems, associated application services, biometrics, etc.

The following aspects may be distinguished:

a) security evaluation criteria;
b) methodology for application of the criteria;
c) security functional and assurance specification of ICT systems, components and products;
d) testing methodology for determination of security functional and assurance conformance;
e) administrative procedures for testing, evaluation, certification, and accreditation schemes.

This work will reflect the needs of relevant sectors in society, as represented through ISO/IEC National Bodies and other organisations in liaison, expressed in standards for security functionality and assurance. Account will be taken of related ISO/IEC and ISO standards for quality management and testing so as not to duplicate these efforts.

Note 1: The term accreditation in the above Terms of Reference is interpreted in this context to deal with the concept of approval for operation of a system. Note that in other contexts the same term is used in connection with assessment and approval of certification and evaluation bodies/laboratories.

On WG 3 Scope and impact

Users need relevant and appropriate cybersecurity functionality able to meet security objectives, based upon identified threats and mandated policies. This need can be addressed by developing technology or even product specific protection profiles, or cybersecurity requirement statements. An immediate question can be raised on whether existing technology offerings provide and properly implements these cybersecurity requirements. Cybersecurity conformance testing provides a response to this question, and it is one of the areas of WG 3 competence.

New trends

Announcing the Commercial National Security Algorithm Suite 2.0
CNSA 2.0
NATIONAL SECURITY AGENCY UNITED STATES OF AMERICA
CYBERSECURITY ADVISORY

In cryptography:

- Post-Quantum Cryptography
- Lightweight cryptography
- Authenticated encryption
- White box (ISO/IEC TR 24485:2022 published this week!)
- Homomorphic encryption

AGENDA

1. Panorama

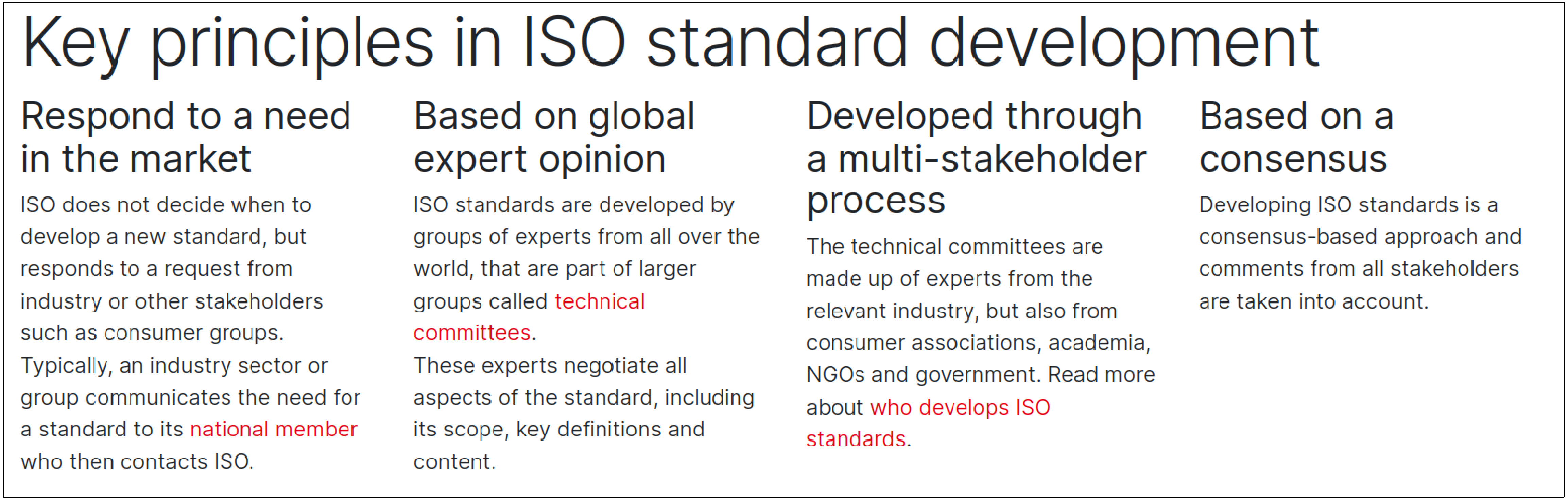
2. Context

3. Roadmap

4. New standards

Developing international standards

https://www.iso.org/developing-standards.html



Key principles in ISO standard development

Respond to a need in the market

ISO does not decide when to develop a new standard, but responds to a request from industry or other stakeholders such as consumer groups. Typically, an industry sector or group communicates the need for a standard to its national member who then contacts ISO.

Based on global expert opinion

ISO standards are developed by groups of experts from all over the world, that are part of larger groups called technical committees.
These experts negotiate all aspects of the standard, including its scope, key definitions and content.

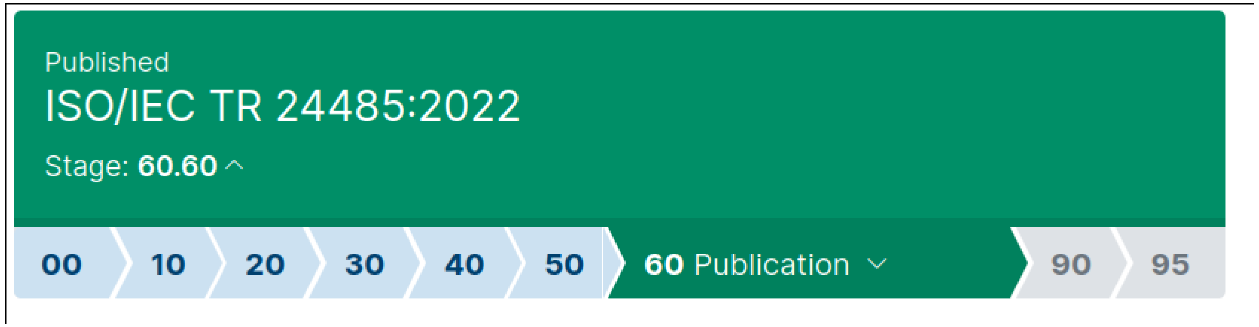
Developed through a multi-stakeholder process

The technical committees are made up of experts from the relevant industry, but also from consumer associations, academia, NGOs and government. Read more about who develops ISO standards.

Based on a consensus

Developing ISO standards is a consensus-based approach and comments from all stakeholders are taken into account.

- Example of WBC:
  - https://www.iso.org/standard/78890.html



Published

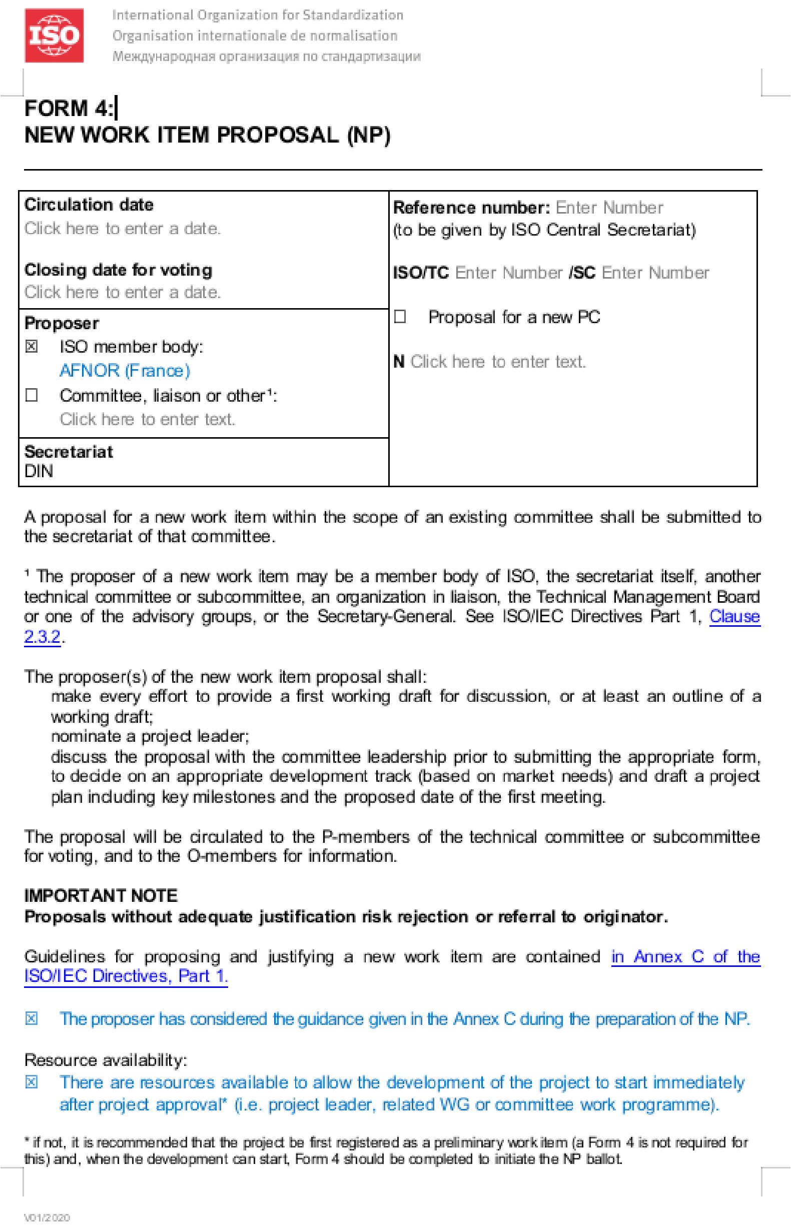
ISO/IEC TR 24485:2022

Stage: **60.60**

ISO/IEC 29128-2

Proposal:

- AFNOR
- Launched



International Organization for Standardization
Organisation internationale de normalisation
Международная организация по стандартизации

FORM 4:
NEW WORK ITEM PROPOSAL (NP)

Circulation date Click here to enter a date. **Closing date for voting** Click here to enter a date.	**Reference number:** Enter Number (to be given by ISO Central Secretariat) **ISO/TC** Enter Number **/SC** Enter Number □ Proposal for a new PC **N** Click here to enter text.
Proposer ☒ ISO member body: AFNOR (France) □ Committee, liaison or other[1]: Click here to enter text.	
Secretariat DIN	

A proposal for a new work item within the scope of an existing committee shall be submitted to the secretariat of that committee.

[1] The proposer of a new work item may be a member body of ISO, the secretariat itself, another technical committee or subcommittee, an organization in liaison, the Technical Management Board or one of the advisory groups, or the Secretary-General. See ISO/IEC Directives Part 1, Clause 2.3.2.

The proposer(s) of the new work item proposal shall:

make every effort to provide a first working draft for discussion, or at least an outline of a working draft;

nominate a project leader;

discuss the proposal with the committee leadership prior to submitting the appropriate form, to decide on an appropriate development track (based on market needs) and draft a project plan including key milestones and the proposed date of the first meeting.

The proposal will be circulated to the P-members of the technical committee or subcommittee for voting, and to the O-members for information.

IMPORTANT NOTE
Proposals without adequate justification risk rejection or referral to originator.

Guidelines for proposing and justifying a new work item are contained in Annex C of the ISO/IEC Directives, Part 1.

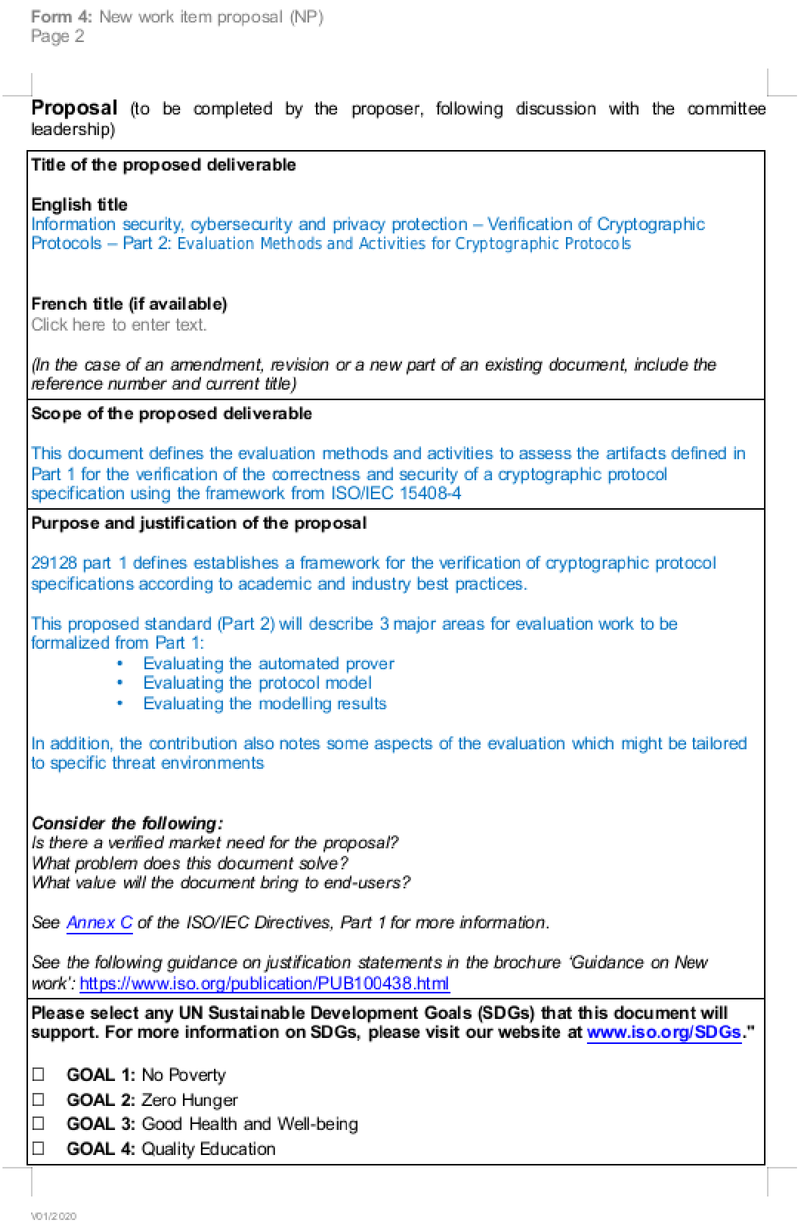
☒ The proposer has considered the guidance given in the Annex C during the preparation of the NP.

Resource availability:

☒ There are resources available to allow the development of the project to start immediately after project approval* (i.e. project leader, related WG or committee work programme).

* if not, it is recommended that the project be first registered as a preliminary work item (a Form 4 is not required for this) and, when the development can start, Form 4 should be completed to initiate the NP ballot.

V01/2020



Form 4: New work item proposal (NP)
Page 2

Proposal (to be completed by the proposer, following discussion with the committee leadership)

Title of the proposed deliverable

English title
Information security, cybersecurity and privacy protection – Verification of Cryptographic Protocols – Part 2: Evaluation Methods and Activities for Cryptographic Protocols

French title (if available)
Click here to enter text.

(In the case of an amendment, revision or a new part of an existing document, include the reference number and current title)

Scope of the proposed deliverable

This document defines the evaluation methods and activities to assess the artifacts defined in Part 1 for the verification of the correctness and security of a cryptographic protocol specification using the framework from ISO/IEC 15408-4

Purpose and justification of the proposal

29128 part 1 defines establishes a framework for the verification of cryptographic protocol specifications according to academic and industry best practices.

This proposed standard (Part 2) will describe 3 major areas for evaluation work to be formalized from Part 1:

- Evaluating the automated prover
- Evaluating the protocol model
- Evaluating the modelling results

In addition, the contribution also notes some aspects of the evaluation which might be tailored to specific threat environments

Consider the following:
Is there a verified market need for the proposal?
What problem does this document solve?
What value will the document bring to end-users?

See Annex C of the ISO/IEC Directives, Part 1 for more information.

See the following guidance on justification statements in the brochure 'Guidance on New work': https://www.iso.org/publication/PUB100438.html

Please select any UN Sustainable Development Goals (SDGs) that this document will support. For more information on SDGs, please visit our website at www.iso.org/SDGs."

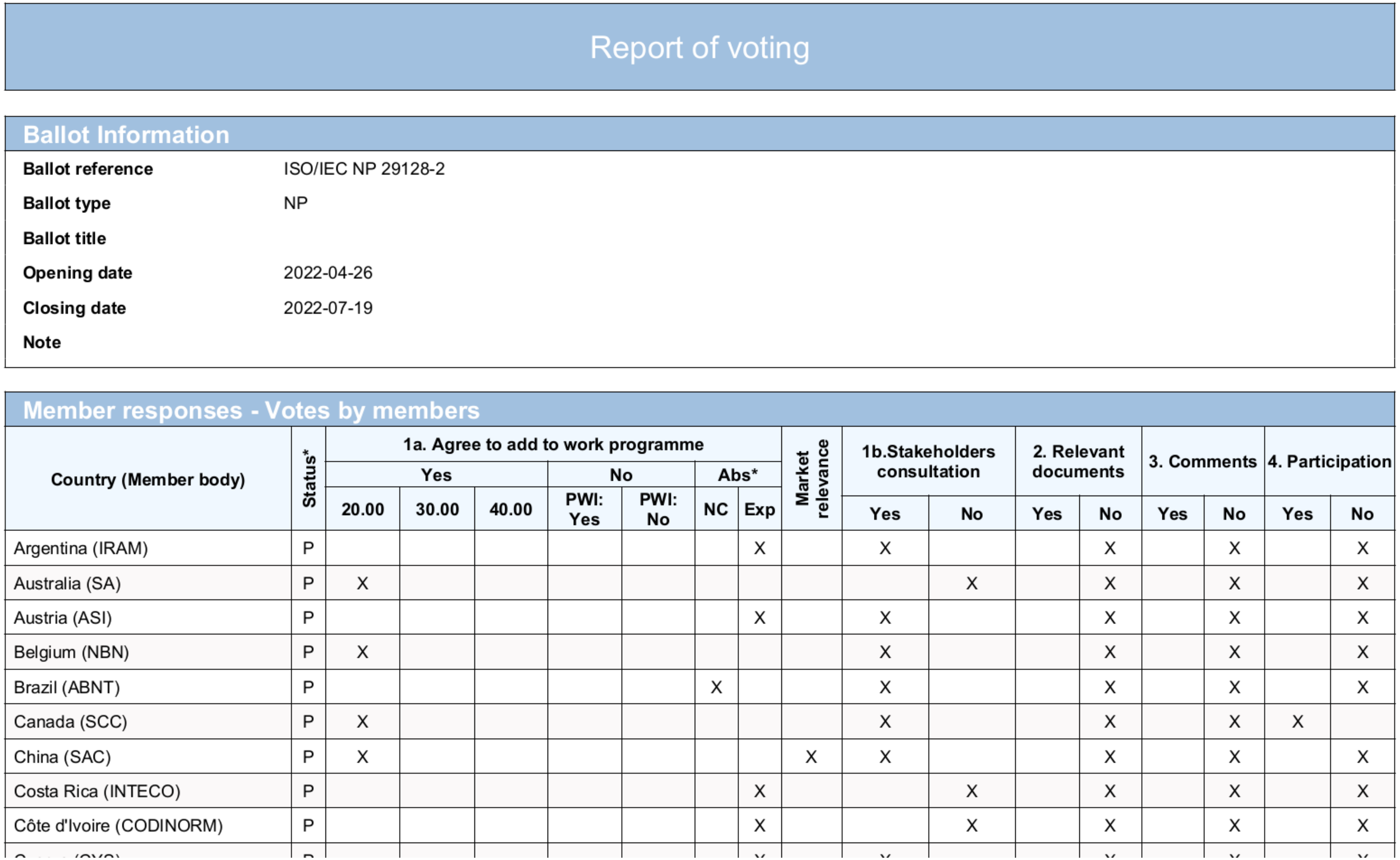
□ **GOAL 1:** No Poverty
□ **GOAL 2:** Zero Hunger
□ **GOAL 3:** Good Health and Well-being
□ **GOAL 4:** Quality Education

V01/2020

ISO/IEC 29128-2

Proposal:

- AFNOR
- Launched



Report of voting

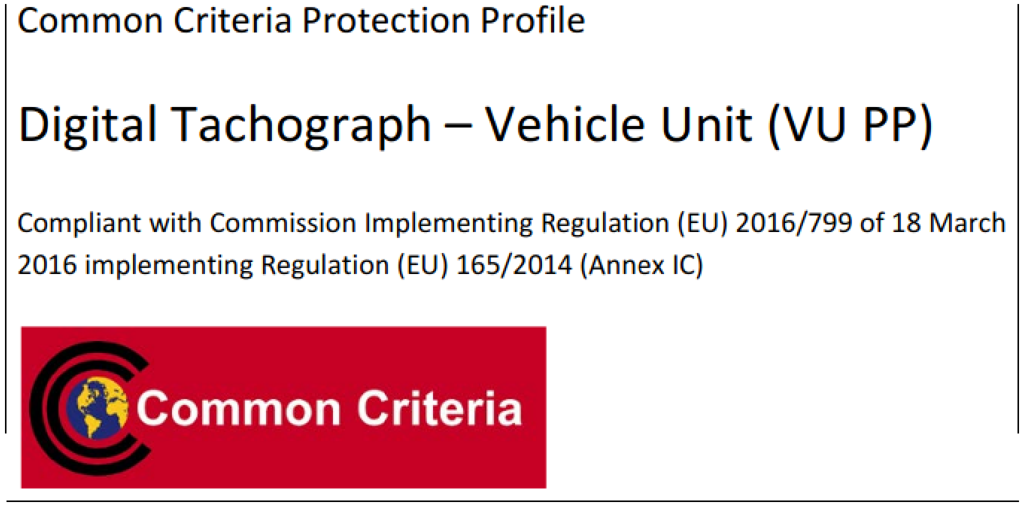
Ballot Information

Ballot reference	ISO/IEC NP 29128-2
Ballot type	NP
Ballot title	
Opening date	2022-04-26
Closing date	2022-07-19
Note	

Member responses - Votes by members

Country (Member body)	Status*	1a. Agree to add to work programme							Market relevance	1b.Stakeholders consultation		2. Relevant documents		3. Comments		4. Participation	
		Yes			No		Abs*										
		20.00	30.00	40.00	PWI: Yes	PWI: No	NC	Exp		Yes	No	Yes	No	Yes	No	Yes	No
Argentina (IRAM)	P							X		X			X		X		X
Australia (SA)	P	X									X		X		X		X
Austria (ASI)	P							X		X			X		X		X
Belgium (NBN)	P	X								X			X		X		X
Brazil (ABNT)	P						X			X			X		X		X
Canada (SCC)	P	X								X			X		X	X	
China (SAC)	P	X							X	X			X		X		X
Costa Rica (INTECO)	P							X			X		X		X		X
Côte d'Ivoire (CODINORM)	P							X			X		X		X		X
Cyprus (CYS)	P							X		X			X		X		X

TR 68

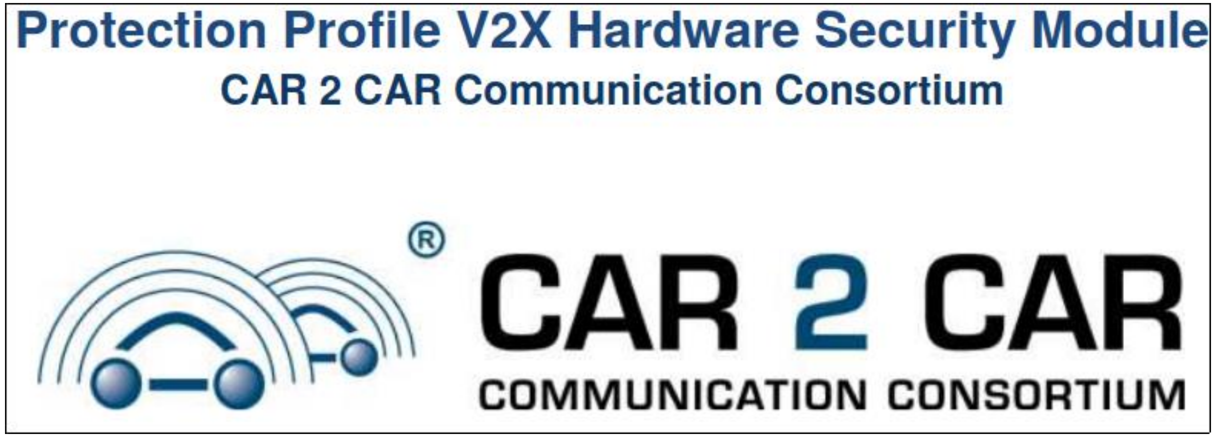


Common Criteria Protection Profile

Digital Tachograph – Vehicle Unit (VU PP)

Compliant with Commission Implementing Regulation (EU) 2016/799 of 18 March 2016 implementing Regulation (EU) 165/2014 (Annex IC)

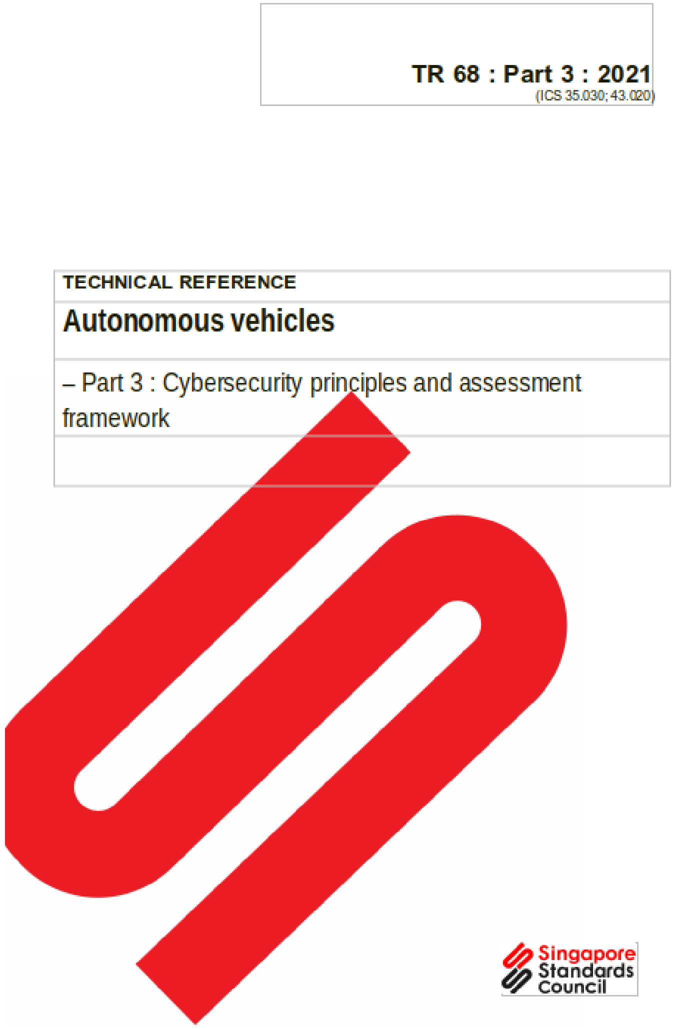
Common Criteria



Protection Profile V2X Hardware Security Module

CAR 2 CAR Communication Consortium

CAR 2 CAR
COMMUNICATION CONSORTIUM



TR 68 : Part 3 : 2021
(ICS 35.030; 43.020)

TECHNICAL REFERENCE

Autonomous vehicles

– Part 3 : Cybersecurity principles and assessment framework

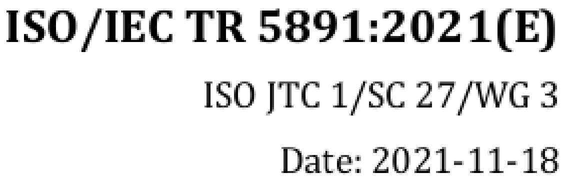
Singapore Standards Council

https://www.commoncriteriaportal.org/files/ppfiles/pp0094b_pdf.pdf

PP 0117

https://www.car-2-car.org/fileadmin/documents/Basic_System_Profile/Release_1.4.0/C2CCC_PP_2056_HSM.pdf

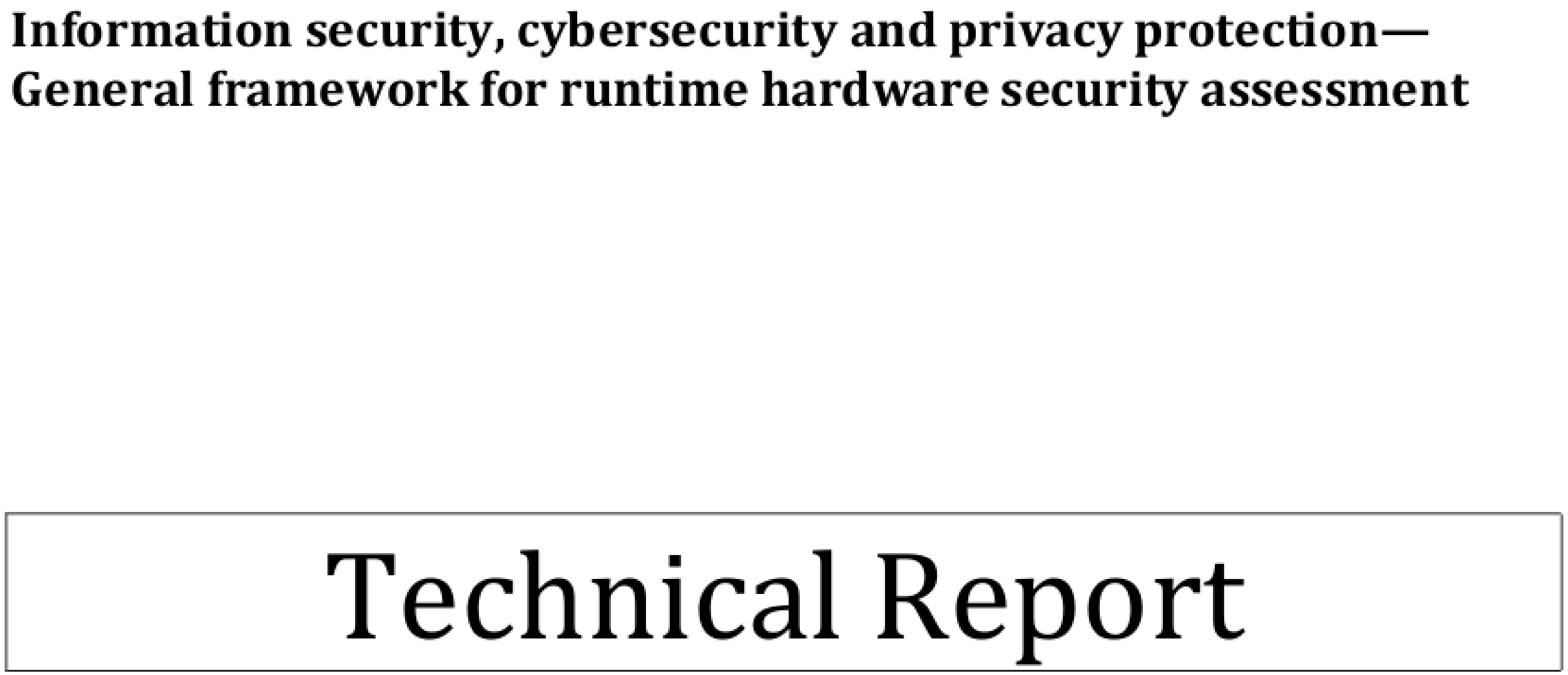
Hardware Trojans Certif.



ISO/IEC TR 5891:2021(E)

ISO JTC 1/SC 27/WG 3

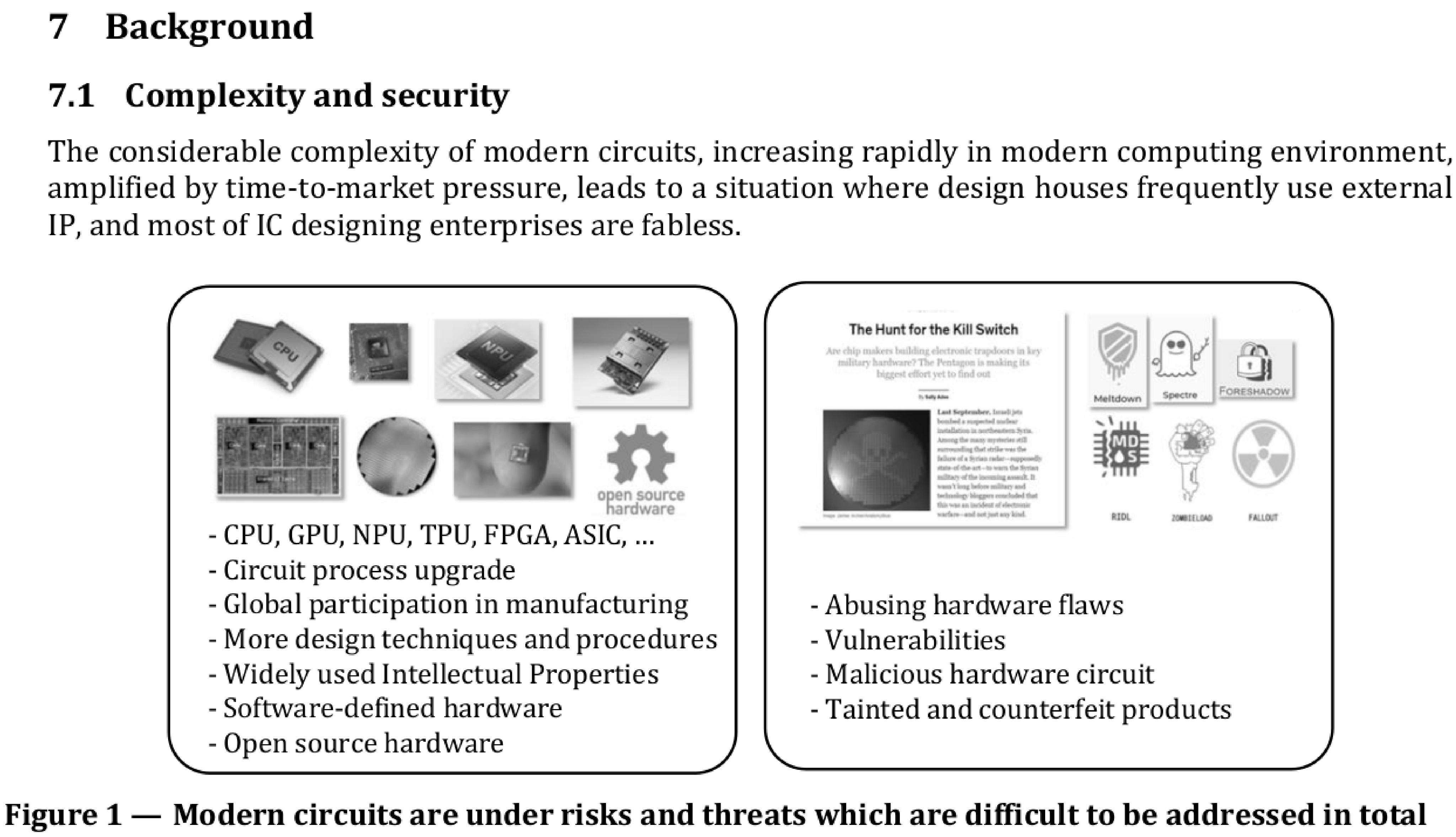
Date: 2021-11-18



Information security, cybersecurity and privacy protection—
General framework for runtime hardware security assessment

Technical Report

Hardware Trojans Certification



7 Background

7.1 Complexity and security

The considerable complexity of modern circuits, increasing rapidly in modern computing environment, amplified by time-to-market pressure, leads to a situation where design houses frequently use external IP, and most of IC designing enterprises are fabless.

CPU
NPU
open source hardware

- CPU, GPU, NPU, TPU, FPGA, ASIC, ...
- Circuit process upgrade
- Global participation in manufacturing
- More design techniques and procedures
- Widely used Intellectual Properties
- Software-defined hardware
- Open source hardware

The Hunt for the Kill Switch
Are chip makers building electronic trapdoors in key military hardware? The Pentagon is making its biggest effort yet to find out
By Sally Adee
Last September, Israeli jets bombed a suspected nuclear installation in northeastern Syria. Among the many mysteries still surrounding that strike was the failure of a Syrian radar—supposedly state-of-the-art—to warn the Syrian military of the incoming assault. It wasn't long before military and technology bloggers concluded that this was an incident of electronic warfare—and not just any kind.
Meltdown
Spectre
FORESHADOW
MDS
RIDL
ZOMBIELOAD
FALLOUT

- Abusing hardware flaws
- Vulnerabilities
- Malicious hardware circuit
- Tainted and counterfeit products

Figure 1 — Modern circuits are under risks and threats which are difficult to be addressed in total

Hardware Trojans Certification

ISO/IEC TR 5891:2021(E)

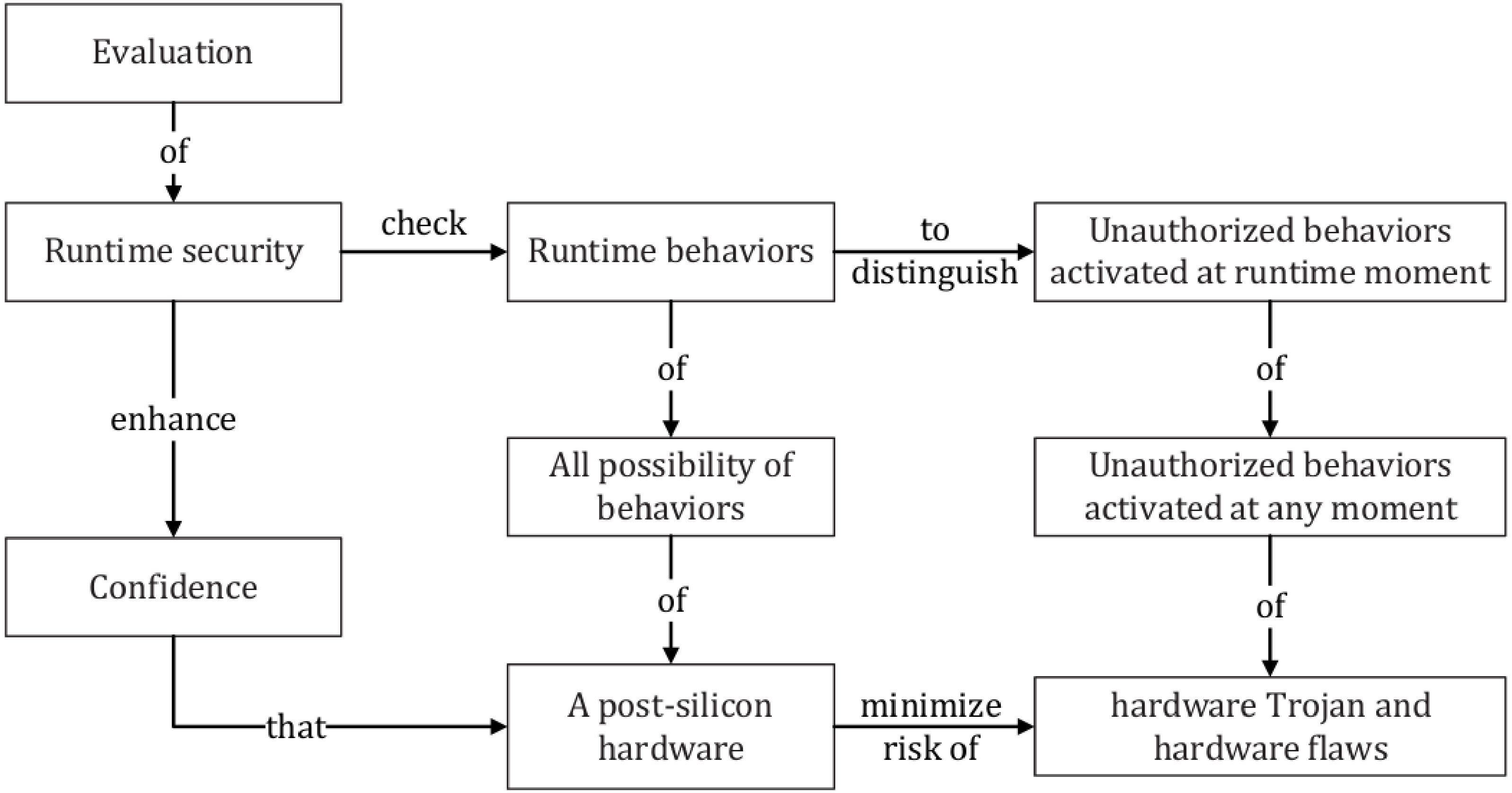

Evaluation
of
Runtime security
check
Runtime behaviors
to distinguish
Unauthorized behaviors activated at runtime moment
enhance
of
of
All possibility of behaviors
Unauthorized behaviors activated at any moment
Confidence
of
of
that
A post-silicon hardware
minimize risk of
hardware Trojan and hardware flaws

Figure 2 — Runtime hardware-behaviours-based security: concepts and relationships

Conclusions

To sum up, we have shown that **heterogeneous certification efforts** can be rationalized for a better market reach:

- with cost-saving factorization
- while designing or producing certification-related sets of evidences.

Such approach is future-proof, and based on published/patented methods:

-
  Sofiane Takarabt, Kais Chibani, Adrien Facon, Sylvain Guilley, Yves Mathieu, Laurent Sauvage, Youssef Souissi:
  Pre-silicon Embedded System Evaluation as New EDA Tool for Security Verification. IVSW 2018: 74-79
-
  Sylvain Guilley, Michel Le Rolland, Damien Quenson:
  Implementing Secure Applications Thanks to an Integrated Secure Element. ICISSP 2021: 566-571

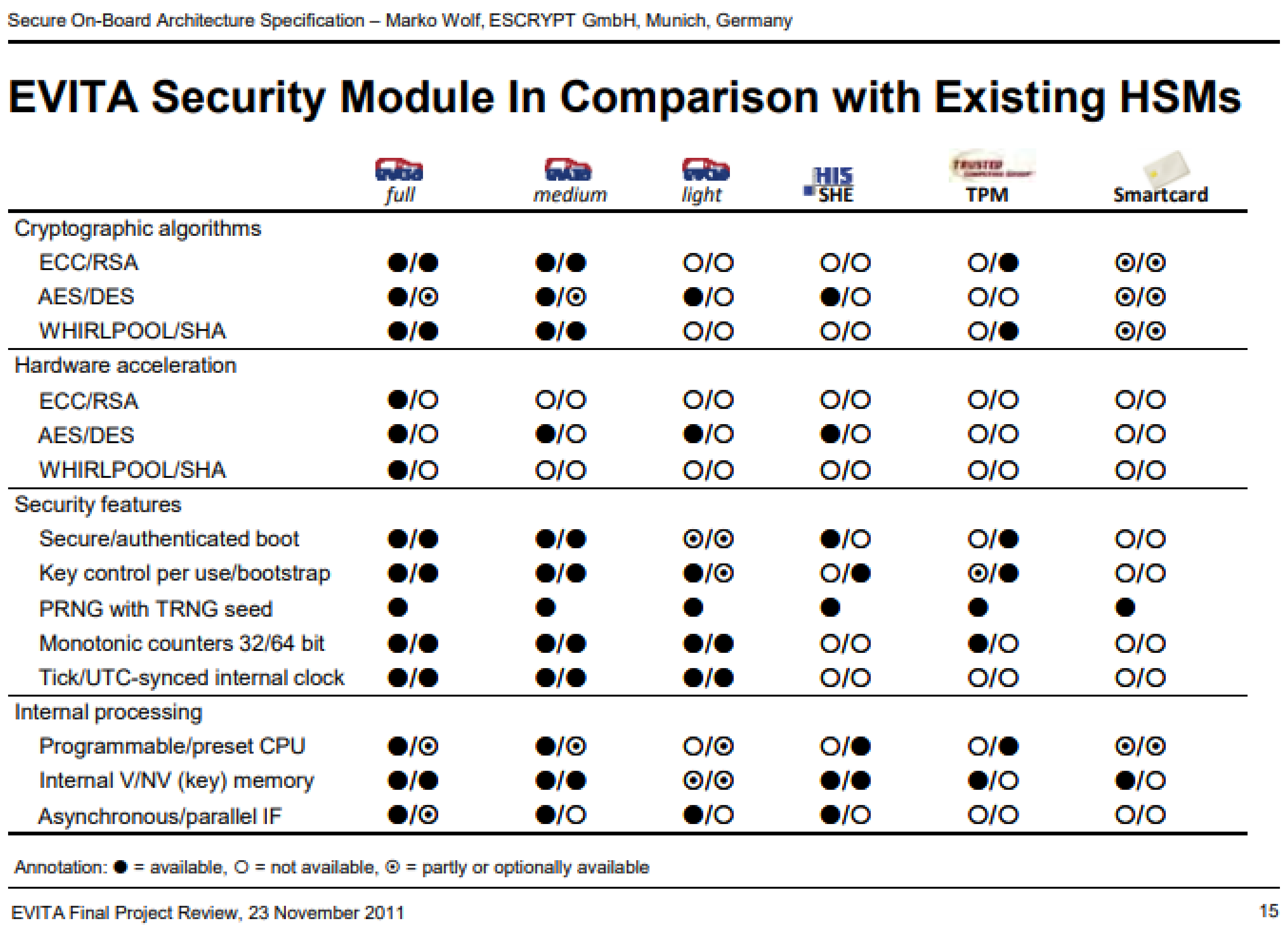
SECURE-iC
THE SECURITY SCIENCE COMPANY

THANK YOU FOR YOUR ATTENTION

CONTACTS

EMEA	sales-EMEA@secure-IC.com
APAC	sales-APAC@secure-IC.com
CHINA	sales-CHINA@secure-IC.com
JAPAN	sales-JAPAN@secure-IC.com
AMERICAS	sales-US@secure-IC.com

Automotive market



Secure On-Board Architecture Specification – Marko Wolf, ESCRYPT GmbH, Munich, Germany

EVITA Security Module In Comparison with Existing HSMs

	full	*medium*	*light*	HIS SHE	TPM	Smartcard
Cryptographic algorithms						
ECC/RSA	●/●	●/●	○/○	○/○	○/●	⊙/⊙
AES/DES	●/⊙	●/⊙	●/○	●/○	○/○	⊙/⊙
WHIRLPOOL/SHA	●/●	●/●	○/○	○/○	○/●	⊙/⊙
Hardware acceleration						
ECC/RSA	●/○	○/○	○/○	○/○	○/○	○/○
AES/DES	●/○	●/○	●/○	●/○	○/○	○/○
WHIRLPOOL/SHA	●/○	○/○	○/○	○/○	○/○	○/○
Security features						
Secure/authenticated boot	●/●	●/●	⊙/⊙	●/○	○/●	○/○
Key control per use/bootstrap	●/●	●/●	●/⊙	○/●	⊙/●	○/○
PRNG with TRNG seed	●	●	●	●	●	●
Monotonic counters 32/64 bit	●/●	●/●	●/●	○/○	●/○	○/○
Tick/UTC-synced internal clock	●/●	●/●	●/●	○/○	○/○	○/○
Internal processing						
Programmable/preset CPU	●/⊙	●/⊙	○/⊙	○/●	○/●	⊙/⊙
Internal V/NV (key) memory	●/●	●/●	⊙/⊙	●/●	●/○	●/○
Asynchronous/parallel IF	●/⊙	●/○	●/○	●/○	○/○	○/○

Annotation: ● = available, ○ = not available, ⊙ = partly or optionally available

EVITA Final Project Review, 23 November 2011

15