EUROSMART
The Voice of the Digital Security Industry

Distribution: **Public**

Eurosmart technical comments on the PwC Impact Study Analysis accompanying the Cyber Act regulation on the certification

I. Executive summary

The documents under comments are

- Impact assessment - SWD(2017)500/948161 - Part 4
- Impact assessment - SWD(2017)500/948161 - Part 5

They can be found on the website of the EU commission at https://ec.europa.eu/info/law/better-regulation/initiatives/com-2017-477_en

This document gathers comments from experienced technical experts. The list of comments presented in this document are just example and is not exhaustive.

We found a certain number of issues along the 200 pages. The main concern is that existing evaluation process and existing Certification Schemes and specifically Common Criteria appears as redundant, static, administrative burden, lengthy, costly…based on erroneous, or uncomplete information.
This study contains:

- Poor knowledge of certification process and cost leading to inconsistent conclusions,
- Shortcut in CC schemes and other initiatives leading to incorrect statements,
- Approximation in gathering certification needs,
- Over estimation in certification cost and lack of objective comparisons,
- Inconsistencies in labelling concepts,
- Surprising statement for risk and fragmentation,
- Poor understanding on the Mobile, PC, Tablet design and the associated functional bricks.

With these comments we would like to highlight that

- CC together with SOG-IS and CCRA tools is a flexible tool box which has demonstrate that it addresses the main challenges of the security evaluation and certification with constant improvement and are a legitimate ground basis for a EU certification scheme.
- Evaluation cost and time have to be adapted to the security problem that comes from risk analysis that may depend on the functionality and the expected use of the product.

This vision comes from a technical community (Eurosmart, ISCI, JHAS) who works with certification every day. The PwC “vulgarization” seems to be too hasty and leads to oversimplified statements that does not represent the certification landscape and the security need diversity.

II. Certification process

Issue 1. Page 16 - Knowledge of certification activities the editor writes "testing a given product for vulnerabilities can only produce relatively short-lived test results".

Comment on Issue 1

The editor apparently ignores that security certification includes penetration testing, which is not only "testing for [a closed list of already-known] vulnerabilities", but rather an analysis of the product itself, that grants much longer-lived results.

Assurance relies on conception and pen test.

Issue 2. Page 18 - The editor states that an EAL "simply states at what level the system was tested"

Comment on Issue 2

The editor does not measure the level of security of the system itself. It is untrue, since the penetration testing is performed considering increased attacker capabilities while the EAL is augmented. This gives assurance of a greater resistance against attacks.

EAL+ = robustness of the conception (EAL) and VAN (usually captured in +)

Maintenance and surveillance process are in place for that: it is done for all smart card product – Eg EMVCo has rules to keep banking card secure for more that 9 years.
Evolution for product that may include soft/firm-ware updates.

Life cycle of the product should be taken into account.

Issue 3. Page 20 - Levelling possibilities offered by certification, the editor states that the way energy efficiency is advertised cannot be used for security certification.

Comment on Issue 3

While a simple scale is not enough to describe the security service as a whole, there are many ways to use a scale to inform users. EALs are used, and are relevant, in Common Criteria. We could think of examples like a scale showing whether the product has been tested by a self-assessment (first-party certification), by a third-party assessment based on compliance testing, or a third-party assessment with an additional robustness assessment etc.

Issue 4. Page 21 – "Certification and competitiveness - Regulated certifications and security evaluation involve considerable costs. … It is important not to erect market barriers to smaller companies by mandating high entry costs. »

Comment on Issue 4

Misleading statement. Which are the regulated certifications?
If we are talking about cost not only certification and evaluation is to be taken into account. The cost of evaluation and certification is << than the cost of securisation and production of assurance evidences << cost of the product.
For sure a non-secure product will be less expensive, but first cost ins to implement and give a rational for security and certification provide a means to be able to compare completely proprietary solutions.

Issue 5. Page 31 - "3) In case of an internal company or a third party company evaluation, the evaluation company provides a decision on the evaluation."

Comment on Issue 5

It is an evaluation report that can be challenged by the certification body. The certification body issues the certificate. This applies to numerous evaluation scheme: CC, CSPN, EMVCo, GlobalPlatform, …

To be complete we could add delta certification.

Issue 6. Page 36 - Role of SOG-IS, the editor states that SOG-IS developed "a few protection profiles".

Comment on Issue 6

This is a misunderstanding of how SOG-IS works. SOG-IS only recommended Protection Profiles as being technically sound. Protection profiles are meant to reflect the security needs of actual risk owners, and are actually developed by:

- Risk owners and final users (e.g. banks, MNOs, payment schemes…);
- Vendors (e.g. Eurosmart, individual vendors participating in technical workgroups…);
- Associations or representing both (GSMA etc.);
- Standardization bodies (CEN, AFNOR etc.);

If we refer to the number of Protection Profiles developed in Europe, according to figure "Protection Profiles by scheme and assurance level" p 35, There 181 out of 344 that represent 52%. The rest is largely dominated by US: 136 which represents 40%.

Issue 7. Page 50 - The editor seems to understand that SOG-IS is limited to "the Common Criteria approach".

Comment on Issue 7

SOG-IS already extended their work to cryptographic assessments, and could perfectly well handle topics such as the recognition of CSPN.

Issue 8. Page 71 - The study eventually includes several offensive remarks related to SOG-IS, such as their use of « the lengthy and bureaucratic CC methodology ».

Comment on Issue 8

CC themselves may be generic and may need to be refined for a given technology. When adapted to a given technology, CC is actually not driven by bureaucracy, but rather by international technical groups sharing **practical up-to-date attack methods** between experts from **vendors, users, evaluation labs and certification bodies**. No other scheme seems to have achieved this to our knowledge.

Issue 9. Page 125 - From figure 5 Certification cost estimates: The summary of all answers also shows that costs vary widely (from 10 k to more than 1 million). In this context, the editor should probably have tried to perform a second step of analysis to understand what causes these variations.

Comment on Issue 9

The section 7.1 page 126 of the study shows how much the figures can vary depending on the context, which is something that PwC did not reflect in its conclusions.
Eventually, the figures lack crucial contextual information such as:

- The perimeter of the evaluation;
- The depth of analysis/level of assurance achieved;

- The scope of the estimate (direct cost, direct + induced cost etc.);
- The unit cost of the certified product, the amount of products to be sold/deployed and their lifespan on the field.

For sure in the case of Smart meters, CSPN and CPA are not comparable to CC EAL4+. Also perimeters are not the same.

International scheme and other initiatives

Issue 10. Page 36 and 37 - We have tables representing the certificates of 5 EU countries.

Comment on Issue 10

Why don't we have the other countries and a consolidated table?

Issue 11. Page 38 - There is a list of international (?) schemes

Comment on Issue 11

It is not clear how this list was selected. The listed schemes have different technical focused. It would have been useful to classify them. Also mentioning ITSEC is probably not any more appropriate as it has been replaced by Common Criteria and only few scheme still accept to perform evaluation under ITSEC.

Purpose and scope of cPPs under the CCRA

Issue 12. Page 59 - PwC suggests that a cPP could be used to evaluate VPNs. « For instance in the field of VPNs related network products, although VPNs are certified against a "collaborative" protection profile (cPP), meaning that the PP has been harmonized with International Mutual Recognition Arrangement, vendors wanting to access the French market have to undergo the additional CSPN certification process (and in some cases a completely new common criteria evaluation) »

Comment on Issue 12

no cPP exists for VPNs. There are cPPs for network devices, which is different. NIAP has defined extensions to this cPP in order to certify VPNs, but these extensions are only a national PP used for US public procurement, mainly because only the NIAP interests are taken into account in these extensions and their conformity to the existing CC framework has not been checked.

In practice, CC using cPPs and CSPN are very different methods, and aim at covering very different needs from the market. The first one favors comparability, while the latter favors robustness assessment. A "VPN" may be used to cover very different security needs: some are meant for home workers while others are meant for M2M communication. The level of sensitivity of transmitted data can also vary, requiring adapted depth of testing. Some may need to manage user-specific features. An analogy might be made by stating that several types of cars exist in Europe, not all of them need to have 4-wheel drive or be convertible.

National initiatives

Issue 13. **Page 20 - Recognition: the editor states that Germany and France have built national certification schemes which are not recognized by each other.**

Comment on Issue 13

France and Germany have expressed that they aim at a mutual recognition of their schemes. Note that this does not imply that schemes are identical.

Issue 14. **Page 39 - The editor describes, CSPN as a "low assurance" method.**

Comment on Issue 14

As public documentation shows, CSPN consist of compliance assessment, and a robustness assessment which is similar in attacker capabilities to the AVA_VAN.3 level of Common Criteria (as included in EAL 4). Assurance is therefore not "low". If CSPN is a "first-level" scheme, it is mostly because it is a black box evaluation with limited mandatory documentation (Security Target and Guidance. Quality and process verification are provided by a CC evaluation with an equivalent robustness assessment level.

Additionally, in their "VPN" example, the editor states CSPN is an additional step over existing certificates. Reality is that ANSSI ***forbids*** submitting a product to a CSPN evaluation if it is already certified against CC (as stated in the CSPN file on ANSSI's website).

Eventually, CSPN is supposedly required to access « the French market », which is a misleading wording. The « French market » is not regulated. CSPN can be used by private actors as well as the government qualification programs, which are related to national security interests and are out of scope of the EU certification framework.

In the CSPN process specific attention is given to the accuracy of the security target relevance for the expected use of the product.

Issue 15. **Page 39 - Qualification process is listed but not described**

Comment on Issue 15

Qualification process should either be described or removed. It relies on CSPN for basic level and on CC for standard and re-enforced level. In addition to the CSPN or CC evaluation there are 2 additional tasks: the consistency of the Security Target regarding the product functionality and cryptography evaluation in accordance to RGS.

Issue 16. **Page 40 - UK: CPA is similar to Common Criteria**

Comment on Issue 16

In other places in the document it is described as similar to CSPN, which seems a more appropriate comparison even if still vague.

With this assumption, we could deduct that French CSPN, German Low Level Evaluation, UK CPA, Dutch BSPA are quite similar.

Issue 17. Page 39 to 42 - National schemes

Comment on Issue 17

The description of the schemes is heterogeneous, for some we have the number of certification per years and per type; the cost where certification and evaluation cost are not always mentioned or distinguished, etc which make it difficult to compare.

The report forgets to mention that the SOG-IS initiative on crypto which aims at having harmonized way to evaluate cryptographic mechanism which were managed by the MS until now.

CC improvements, some improvement are done as trials in several MS: eg NSP6 in Netherlands, Collection of evidence in France, … After trials these can be adopted by SOG-IS and JIL. This is a bottom up approach that is managed by SOG-IS.

Issue 18. Page 145 - Lack of understanding of what security certification is: we could not make sense of the section 7.4.

Comment on Issue 18

This section is at times impossible to parse, and seems to rediscover issues known since the invention of Common Criteria (if not previous schemes such as ITSEC and the Orange book).

The section strikes us as particularly naive, since no practical method and organisation are opposed to the existing ones. The difficulty of building a cross-national scheme that works on a day-to-day basis is exactly what draws criticism on current certification practices in Europe.

This section mixes:

- **Disingenuous remarks**, for example the almost undecipherable « Limit in perimeter » section, which fails to show how high assurance could be obtained at no cost and no delay;
- **Misleading remarks**, such as the whole « Product distribution » chapter. The whole point of ALC_DEL requirements in CC is to ensure the integrity of the delivered product, even in conditions where the final customer does not fully trust the supply chain;
- **Outright lies**, such as “There is no homologated set of attack but what the evaluator wants to do or what he can do.”. In the smartcard domain, for example, there is such a set, whose summary can be downloaded on SOG-IS website. In other terms, whenever there is a market need for standardizing attacks, current schemes are able to provide such as standard. For other domains, the only practical way to address the issue is letting certification bodies ensure the skillset of the ITSEFs, and letting certification bodies evaluate each other through a peer review process. Fortunately, this approach is then promoted in the same section (“This choice of management facilitates the mind of initiative to create / to invent new tests. If the list of attacks was fixed as for tests of validity, it would not correspond to the reality of the reel world.”);
- **Wishful thinking** of the theoretical benefit of hypothetical evaluation methods over the limitations of actual methods (“Hence the delay between the product conception and the sale must be as short as possible.”, “the conception and the evaluation must be scheduled in parallel way.”);
- **General limitations of all regulations, laws, standards and methods** (to quote the study itself: “it is exactly the same thing that the laws”);
- **General limitations of all cross-national agreements** (« difficulties in terms of translation in the language of the country »);

- **Fundamental limitation of the notion of assurance in the IT security domain** ("Indeed, the certificate is only valid at the time of its issuance. This short delay is explained by the possibility that new attacks could have been discovered just at the time of the issuance or just after"). Certification activities could indeed be vastly simplified if attackers could stop to find and exploit vulnerabilities for a minute;
- **Fundamental issues** when trying to obtain assurance in the IT security domain. More generally, the editor does not seem to understand that increasing dynamicity and time-to-market mechanically decreases the capacity to evaluate products after they have changed. It is a trade-off, and not a flaw of the system that could be remedied by a hypothetical new scheme.

Some remarks can include several types of errors in a single sentence, rendering them nearly impossible to comment, such as "The EALs (i.e. 5, 6, and 7) are known as the higher assurance level for US and European member's countries who signed the MRA agreement, which is a challenge for new member's countries."

Challenges in EU approach

Issue 19. Page 16 - Certificate validity « Similarly, product vendors are in a dilemma. They have to choose between fixing a known issue and loose certification for the latest release of their product (at least until re-certification can be achieved) or not fixing a known but maintaining the product certification (which again points out the limited meaningfulness of product certification). »

Comment on Issue 19

In this case, no matter under which certificate scheme, the certificate is not anymore valid anyway, and any new scheme would not avoid this validity problem as well. Under CC, the maintenance process has been defined to cope with this issue.

Issue 20. Page 18 - EAL and Protection Profile « The labelling concept could be extended to cover not only the traditional levels of Common Criteria (EAL), but to address specific security functions, which can be linked to specific protection profiles. For example, labels could be defined for specific security properties like confidentiality, integrity and authentication or for a specific Security Target (ST), which is defined in the related protection profile. »

Comment on Issue 20

The proposed features have been addressed by CC, because CC allows to have

- A Security Target with an EAL that is higher than the Protection Profile it complies with. Example PP0084 is EAL4 + and numerous compliant ST are EAL5+ or even EAL6+.
- Security function at various level (see POI PP)
- Modules (see PP0084 or TEE PP) to adapt to different security needs and/or vertical markets.

Issue 21. Page 18 - Level of assurance "Level of assurance. This is the equivalent of the EAL in Common Criteria. We note that EAL level does not measure the security of the system itself, it simply states at what level the system was tested."

Comment on Issue 21

Common criteria assess conformity and robustness of security features claimed in the Security Target.

Issue 22. **Page 44 - Recertification and Patching. This require the definition of a new process or a modification of the existing approach for Common Criteria;**

Comment on Issue 22

It is already possible in the Common Criteria scheme. It requires that the patch mechanism is certified and also the new Software. It is described SOG-IS supporting document: https://www.sogis.org/documents/cc/domains/sc/JIL-Application-note-on-security-requirements-on-code-loading-v1.0.pdf. Nevertheless, we agree that CC does not address patch in an industrial way like it is done by big companies for laptops, mobile phones, …and that should be handled.

Issue 23. **Page 44 - Identified challenges**

Comment on Issue 23

The identified challenges stress on the irrelevance of Common Criteria due to "Recertification and patching, security and trust coverage, …, usability". Instead, the logical conclusion should be that Common Criteria is already a EU and even Worldwide scheme and is widely used for certain product categories. The EU scheme could rely on Common Criteria, its set of application notes and extend to other evaluation methods such as the CSPN-like schemes.

Issue 24. **Page 45 - Certification should be, in general, voluntary. Mandatory certification might be justified for some areas, or specific products, with high security requirements;**

Comment on Issue 24

Incentive for certification can be

- Regulatory most of the time
- A de-facto standard required by customers -- most of the time
- Marketing against competition

Except for the third case, it is not "voluntary" from the developer.

Issue 25. **Page 45 - During the design of the EU certification framework it should be taken into account that some Member States have national certification schemes for certain high assurance sectors, and both schemes should not be confused**

Comment on Issue 25

Does this mean that high assurance (from EAL5? / VAN.5?) should remain national?

Issue 26. **Page 45- In several items, certification is used instead of evaluation**

Comment on Issue 26

Is there a recommendation that the lab also certifies or do we keep independence between the evaluator and the certifier?

Issue 27. **Page 45 - Identification of the need to develop new underling criteria for certification;**

Comment on Issue 27

Not meaningful without complementary explanation.

Policy options

Issue 28. **Page 48 – "Option 0: The SOG-IS agreement and the CCRAs will not solve the problem in the short-medium term. The criticism towards common criteria, on which SOG-IS is based, will remain an issue as the limited geographical and substantive coverage of the agreement."**

Comment on Issue 28

Is contradictory with the paragraph in page 46: "The need to establish a practical scheme guaranteeing mutual recognition of certificates across Europe and compatible with similar requirements beyond. The current collaboration schemes like CCRA and SOG-IS could be a starting point for the establishment of a common format and semantic of the certificates."

Issue 29. **Page 50 – "Option 2: *SOGIS mandatory*. EC would make SOGIS-MRA mandatory for all MS. This solution would allow only the Common Criteria approach, so leaving out, e.g., some national approaches based on low time/cost/assurance requirements."**

Comment on Issue 29

SOG-IS in interpreted here as CC only without possibility of enlarging its scope. Rather than rejecting it, it could be considered as a tool to federate EU interpretation of EU certification scheme.

Issue 30. **Page 50 - Option 3: Reduction of adaptation costs to meet national product standards/specifications. Common EU product standards reduce the need to produce product variants adapted to meet different national standards;**

Comment on Issue 30

It is unclear whether the intention is to keep national standards reusing common EU ground or if the objective is to have identical of full recognition.

Issue 31. **Page 51 - Option 3: Negative impacts. Potentially negative impact for producers relates to the additional costs of obtaining EU certification and labelling (for products that are currently not covered by national conformity assessment and certification and labelling requirements but that will be brought within a future EU-wide system).**

Comment on Issue 31

For non-evaluated product it will be a new cost to have their product secure … and certified. Nevertheless, it is the role of certification to promote secure products.

Issue 32. **Page 51 - Negative impacts. The main identified potentially negative impact on market conditions concerns the possibility that minimum EU standards may become de facto market requirements. This may, in turn, reduce the market opportunities for products with performance levels above minimum requirements and, reduce, incentives for investments in RTD to raise product performance. Similarly, it may limit market acceptance of 'alternative' or innovative' products, particularly if they are costlier than standard products that comply with minimum requirements.**

Comment on Issue 32

Looks like there is a dichotomy between innovation and security. Apple is seen as THE Innovator and performed SOG-IS MRA certification higher than EAL4+ in Europe.

Issue 33. **Page 147 - Another study entitled "*Common Criteria: Its Limitations and Advice on Improvement*"[18] confirms the shortcomings and limitations of CC shown above. In fact, some issues are related to evaluation process. Especially, CC is criticized as being costly and time consuming. Meanwhile, there are issues in general evaluation methodology. Particularly, its limitation on vulnerability analysis is eminent: CC is not good at addressing security flaws in product implementation. The methodology of vulnerability assessment in CC is too generic, not rigorous to identify vulnerability in implementation, and does not take into account vulnerabilities specific to individual technology area.**

Comment on Issue 33

The above paragraph is nonsense. CC as a standard does not forbid to be efficient and less expensive, but things grew over time. For example, you can tune this per technology as we showed it for smart cards.

III. Certification needs

Private sector's needs

Issue 34. **Page 18 - the editor states that the security certification of a crypto-module for the road transportation may not be valid for the energy sector, and deduces the need for a "separate dimension to identify the domains".**

Comment on Issue 34

The editor seems to ignore that in most cases, road transportation and energy sectors will not use the same crypto-modules in the first place. Nowadays, a component for IoT typically includes not only security features but also communications stacks or other functional features that are generally proper to a given sector. The energy sector may use energy-specific components, which may or may not be certified using a sector-specific PP.

Public procurement

Issue 35. **Page 29 - the editor suggests a "fragmentation between military and civilian governance."**

Comment on Issue 35

This is untrue, at least in the French market. Military applications actually rely on the "civilian" certification framework, and the associated private evaluation laboratories, for their procurement programs.

Issue 36. **Page All - Erroneous statements on the cases of SIM cards, smart metering, HSMs…**

Comment on Issue 36

These products are bought by private entities (MNOs for SIM cards, banks, for HSMs, and so on), and these private entities have different needs and different appreciations of the risk.

National schemes offer users a possibility to use CC or CSPN for different certification needs, but ultimately the choice lies in the hands of *users*. The editor describes the case of HSMs as an example of double certification, but misses the fact that an HSM having passed both certifications usually aims at different markets (for example a banking customer requiring FIPS, and a governmental customer requiring CC).

But of course, this happens frequently and certification bodies are concerned with this. Therefore, evaluation laboratories are welcome to reuse, as much as possible, evaluation results when they perform both evaluations on the same product. For example, in France, all the ITSEF are licensed to perform CSPN and CC evaluations and can reuse their test results.
Most of them are also licensed by payment, DRM, … schemes. The segregation lies more on area of expertise.

IV. Cost estimates for certification bodies

Oversimplified cost estimate of joining a recognition agreement such as SOG-IS for a MS

Issue 37. Page 62 - According to the study, « The extension of SOG-IS agreement to all MS is not a valid policy option to be considered since there are Member States which are too small and for which the start-up and maintenance of a Certification Authority may be too costly. »

Comment on Issue 37

As it is the case for CE marking, a Member State may rely on another Member State's certification body if needed. Moreover, the cost of maintaining a certification body is not high if the MS intends to stay a certificate consuming member. Today, SOG-IS includes all cases, from MS who heavily invested so that they can issue high-level certificates to MS who did not invest at all and only intend to be consumers.

Issue 38. Page 63 - IT Certification Authority costs

Comment on Issue 38

Before entering in the detail of the cost it would be worth defining the mission of this EU certification authority and the way it relies (or not) on existing schemes and national certification bodies.
Having estimation of the workforces at each CB would have been also useful.

Issue 39. Page 66 - First occurrence in price for an expert at 450 €/day

Comment on Issue 39

It is a good news for EU if it is able to find experts at this rate. As a comparison the public price that the Dutch scheme invoices for its external certifiers is 175E per hour which makes 1400€ for 8 hours.

V. About labelling

Issue 40. Page 16 - However, there are multiple points often criticized about security certification and the criteria against which certification happens, among them are lack of publicly accessible, standardized certification criteria and processes, meaningfulness of the results (or rather lack thereof) and cost of certification.

Comment on Issue 40

For CC it is rather clear form CC portal.

Issue 41. Page 17 - §1.2, Figure 5 (SOURCE IDC 2009). The editor makes wrong analysis using too old data (source IDC 2009)

Comment on Issue 41

The editor considers IDC trust and confidence Gap Indicator to provide an analysis. The source is a quite old source (2009) to be considered as accurate. Plenty of events (malware, ransomware and massive network disruption) arise recently changing deeply the user rating of fear of security threats.

Issue 42. Page 18 to 26 - Mix of disparate notion in labelling section

Comment on Issue 42

Intermediate conclusion such as: "Labelling, therefore, creates the very real risk of a false sense of security";

Description of food, energy, healthcare…it would had been useful to identify criteria to characterize the adoption … these are example extracted from rather static criteria as opposed to security where the threat landscape constantly evolves. Not so helpful.

At the end of the study there is probably a distinction to make between several categories:

- Regulated business
- Standard B2B actors
- B2C

Issue 43. Page 18 - §1.3 Labelling concept.

Comment on Issue 43

The editor defines "different dimensions for which the label can be defined": Level of assurance = EAL, Protection profile, mean to achieve certification. Moreover, several concepts are mixed (security evaluation, certification, certification scheme and qualification).

Issue 44. Page 18 – About dimensions

Comment on Issue 44

It would be interesting to think about dimensions that should appear in a Label. Nethertheless even if EAL, Protection Profile and certification means could contribute to it, they are technical tools that are too complex to be handled in a label:

- EAL is a set of assurance evidences among a predefined scale comprising about 30 components for the highest levels. It allows to specify without ambiguity which level of correctness and robustness requirements a product has to fulfil to be eligible to get a certificate.
- A Protection Profile specifies the scope, the threats and the security requirements for a type of product. The number and type of functional requirements defined in protection profile may be considered as a dimension to determine level of protection by a product versus defined threats.
- Certification means are also numerous: self, by third a private party, by regional, sectorial, MS or EU Certification body, …

Issue 45. Page 19 - The editor makes wrong statements about labelling concept

Comment on Issue 45

Mean to achieve certification using IACS scheme

The scale refers to 2 criteria: which entity validates result of evaluation and a link with level of criticality of system to obtain assurance.

The level of independency for a given entity contributes to the level of assurance of a label.

- Self-declaration has a low level of independency, therefore assurance if accuracy in result of evaluation may be considered as low.
- When third party is used for evaluation, we can consider that the level of independency is higher, but if third party performing evaluation is directly paid by vendor, it remains a bias and accuracy in result of evaluation may be considered as medium.
- When an impartial entity (governmental agency, private autonomous agency) is used to check results of evaluation provided by a third party selected amongst agreed entity, then accuracy in result of evaluation may be considered as high.

The second criteria is criticality of a system.
The link between accuracy of level and criticality of a system is a shortcut.
Indeed, high accuracy that system has a low level of robustness is probably not appropriate.

To summary: it is better to split this topic in 2 different items:

- Security evaluation is performed to demonstrate that a product fulfils security objectives (including protection against a set of defined threats), using security features with a given strength of function and they cannot be bypassed. This statement is assessed by assurance methods linked to correctness and robustness requirements.
- Labelling is a way to assess the accuracy of the security evaluation results with key properties as:
  a) well defined levels, recognized by actors,
  b) independency of issuer providing trust in accuracy of evaluation results,
  c) level of expertise of issuer and lab assuming repeatability of evaluation results.

Find here proposal of definition for such concept.

Security Evaluation is an assessment that an item is compliant against defined security criteria. Assessment is performed by an entity [third party or item provider (then it is named self-assessment)].

Certification is an approval from an independent authority that inspection of evaluation findings demonstrates that evaluation results are compliant against defined security criteria.

Qualification demonstrates conformance to a set of requirements defined by a security national agency or a community associated to a dedicated technical domain.

Certification scheme is an administrative and regulatory framework under which the certification criteria are applied by an authority within a given community.

Issue 46. Page 19 - The editor makes strange statement about "ITC certified quality" The editor writes "Unlike common certification, the product quality and safety information reach directly the final consumer through the new "ITC certified quality" mark".

Comment on Issue 46

We agree that any user has to go on www.commoncriteriaportal.com to know if a product is certified against Common Criteria, but this page is well known by people aware about product security when "ITC certified quality" mark is quite unknown. Editor should clarify how the final user is better reached with such mark.

The editor writes "An excessively narrow and static certification and labelling system may actually restrict the range of technical security solutions…". "This prevents innovation and market diversity".

Objective of security certification is not to block innovation or diversity but to check that security requirements are fulfilled. Diversity is not necessary an objective if it may introduce weaknesses in product.

Issue 47. Page 21 - The editor makes strange statement about "labelling and benchmarking" The editor writes "Component/product labelling could potentially lead to a false sense of security for end-users in the consumer market. Benchmarking cybersecurity practices, on the contrary, would allow both consumers and organizations to compare situations and form an idea of the cybersecurity state-of-the-art".

Comment on Issue 47

We consider that benchmarking practices may also introduce false sense of security if context of execution is not considered which it is a current way to proceed in benchmarking.

Issue 48. Page 24 - The editor makes strange statement about "visibility of label and rigor of testing from outside organization" The editor writes "When consumer's see a third-party certification is displayed or visible on a product, customers believe that specific standards have been met because an outside organization has verified findings through an audit or a rigorous testing process".

Comment on Issue 48

As already mentioned upper in the document, outside organization allows to achieve higher level of confidence than self-assessment but only an independent authority can really assess without doubt the evaluation work. Third party testing is not by default a rigorous approach if it is not controlled at all.

This is why we promote organization with a third-party evaluation is validated by an official & independent authority (public or private).

By the way, we consider that a sticker on a product is no more the accurate solution for IT product. We suggest that any IT certificate may be translated in an electronic format (example of letter of approval from Global platform) to be recognized by IT equipment.

Issue 49. Page 18 to 28 - The editor makes strange comparison about "IT security and eco-label or food label". The editor compares label for environmental or food purposes with label for security IT product.

Comment on Issue 49

Such comparison is not fully accurate without considering attacker potential and motivation evolving in the time. This is why Robustness scale must evolve and label could be stated for a product for a given period of time, requiring a surveillance process to master the level of risk among the time.

VI. Fragmentation

Issue 50. Page 29 - The editor makes wrong statement about "Fragmentation" The editor states that "One of the key drivers of increasing cybersecurity risk is fragmented industry"

Comment on Issue 50

Such statement is completely false when you consider key technologies (as OS, mobile, server, Internet access, internet services…) where few actors represent major part of market. With such position, dominant actors are not so motivated to spend time and money to demonstrate effectiveness of the security of their product, system and services. Only when regulation imposes evaluation as FIPS-140-2, then providers perform security evaluation.

Issue 51. Page 29 - Shortage of EU companies that … are able to absorb the talent on the market" P30: The European cybersecurity firms cannot absorb the newly skilled professionals produced by European academic institutions

Comment on Issue 51

It seems that Labs, CBs and Industrial Companies are struggling to hire people with the right skills.

Issue 52. Page 96 - Fragmentation is related to the existence of multiple national and sectorial certification schemes not mutually recognized especially in reference to National programs and regulations. The Italian health care cards are completely different from French health care cards, because they have different data, different functions and different type of certifications.

Comment on Issue 52

This is first the fragmentation the functional specification.

VII. Smart-metering

Issue 53. Page All - The editor assumes that different "Smart Meters" have the same security problem in the French, German and UK context

Comment on Issue 53

From the document it is difficult to understand why the evaluation of the same smart meter could cost from 25KE to more than 1ME.
Infrastructures deployed by energy providers differ widely from one country to another. Hence the risks they face are not the same; in particular, they require different threats to be addressed by components such as meters, resulting in different scopes/perimeters for the evaluations and possibly different levels of assurance (EAL4+ in the DE case, first level assurance in FR).
Example: a meter taking a measure every ten minutes would face privacy threats (the end-user power usage allows deducing personal information) while a meter taking a measure every other day would not.

Issue 54. Page All - The editor assumes that all products called "smart meters" are similar in architecture and functionalities

Comment on Issue 54

The editor could have explained that products have different roles within their respective architectures: they are functionally different and it is therefore not possible for manufacturers to address these "markets" with a single product. A single certification scheme with EU wide recognition would not in the least solve that equation.
Example: The German program evaluates gateways and their security modules, while the French program validates meters and hubs. Physical interfaces vary widely between these programs (Ethernet, PLC, 3G/4G etc.). Evaluations are different, mainly because products are different.

Issue 55. Page All - The editor mistakes private actor's procurement requirements with a national certification requirement

Comment on Issue 55

In France for example, Enedis had a regulatory requirement to use certified products, but Enedis was free to define their own security target and could choose any certification framework.
Example: if German gateways had been compatible with Enedis infrastructure, and if they had been answering Enedis security needs, they would have met the regulatory requirement set upon Enedis. Enedis did not use these products because they needed different functionality, different physical interfaces and had different threats to address – not because of the certification scheme.

Issue 56. Page All - The editor assumes that vendors carry the burden of addressing the three markets

Comment on Issue 56

Certification frameworks separate the role of sponsor and the role of developer because they do not always match. The vendor does not necessarily pay for the evaluation.
Example: in France smart metering program, Enedis was the user/risk owner; they decided to sponsor the evaluations, so the direct cost of the certification did not weigh on the developers' shoulders.

Issue 57. Page 99 - The editor produces wrong certification cost estimates Q6: "In France, the cost of certification is something between Germany and UK. The cost it is similar to the UK, so it is about 150K euro or more. »

Comment on Issue 57

In the case of CSPN, the information was available on ANSSI's website. An evaluation requires between 25 and 35 men-days in workload (with waivers to 50 for some technologies), which converts to approx. 25-50K€.It is also mentioned in several places in the document: in p39 see section 1.1-France. Also in section 7.1 p 128.

By mentioning the unitary cost and number of meters deployed, the editor could have discovered that the cost of the CSPN is marginal.

VIII. First Conclusion

The editor (PwC) seems convinced of the limitations of current schemes, but does not provide any practical alternative, except for a few mentions to self-evaluation.

We would have expected the editor to use elements from other schemes to provide an actual contribution, or at least alternatives perceived as viable (e.g. proprietary schemes such as EMVCo, CSA STAR, ISO/IEC 27001, security evaluation "checklists" such as OWASP, secure development methodologies such as MS SDL…).

May be the solution cannot be found in a unique scheme but through a meta-scheme including several schemes to be applied for different types of items (product, system, service, process, site…) and dedicated to a technical domain (automotive, energy, web application, health, banking…).

The ECSO Meta Frame that have been approved by the ECSO Board is based on this concept. ECSO represents the complete EU Cyber Security; National Security Agency EU research laboratory, CAB and user ecosystem.

Although smart cards, secure elements and HSM don't represent the full ICT market, it is already a good achievement in terms of mutual recognition, labelling and reuse of results.

They are considered as Cyber Security strategic tools to protect personal data and M2M data. It could have been worth to make a status on the other kind of products.

We are also conscious that CC has been designed for product evaluation and is not straightforwardly applicable to systems and services even if there are on-going work on these topics.

CC should be seen as a tool box and may need to be adapted like it is already the case but does not need to be reinvented and of course could be complement by other existing methods used in other general or dedicated schemes. Numerous schemes are listed in the document, some important may be missing.

Certification cost are repeatedly presented as enormous but are not related to the cost of the product, its lifetime or to the risk that is associated to its usage. Of course it does not prevent to rationalize the evaluation and certification efforts to avoid testing overlaps.

Of course we remain at your disposal to explain and extend the comments if needed.

To move forward, we are convinced that improvement of cybersecurity at level of Europe is a key challenge to be addressed by several means and several levels.

A unique organization applying a unique solution for any topic is certainly a dream but may become a nightmare very fast when trying to address several issues as:

- Specification of security needs for several types of items and different technical domains,
- Refinement of security needs in security requirements, levels of assurance and evaluation schemes,
- Setup organization to manage and maintain evaluation schemes through Europe,
- Assessment of common security assurance through homogenous evaluation for different items and technical domains,
- Performing follow-up of security risk and maintaining security level of ICT through reassessment and continuous assurance,
- Setup security measures to prevent malicious events and
- React to security incidents and learn from them.

Eurosmart experts are available to discuss these items in a workshop and are ready to contribute on the future technical discussions regarding European Certification Framework.

IX. About us

Eurosmart, the Voice of the Digital Security Industry, is an **international non-profit association located in Brussels**, representing the **Digital Security Industry** for multisector applications. **Founded in 1995**, the association is committed to expanding the world's Digital secure devices market, developing smart security standards and continuously improving the quality of security applications.

X. Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, security evaluation laboratories, High Security Hardware, Biometric technology providers, terminals, system integrators, application developers and issuers who work in dedicated working groups (security, electronic identity, communication, Cybersecurity, marketing). Members are largely involved in research and development projects at European and international levels.

Eurosmart members are companies (Fingerprint Cards, Gemalto, Giesecke & Devrient, GS TAG, Idema, Imprimerie Nationale, Infineon Technologies, Inside Secure, Linxens, Nedcard, NXP Semiconductors, +ID, Real Casa de la Moneda, Samsung, Sanoïa, STMicroelectronics, Toshiba, Trusted Objects, WISekey, Winbond), laboratories (CEA-LETI), research organisations (Fraunhofer AISEC), associations (SCS Innovation cluster, Smart Payment Association, Mobismart, Danish Biometrics).

XI. Press contact:

Pierre-Jean VERRANDO
Director of operation
Mobile: +32 471 34 59 64