Contribution ID: a9732940-3290-4da8-95c4-19ec8df869c3
Date: 19/05/2017 15:46:13

ICT Security Certification 2017

Fields marked with * are mandatory.

Files

*
1. Type of organisation:

- [ ] National authority / Agency
- [ ] Manufacturer / provider of ICT of ICT products (both hardware and software) and services
- [ ] User / Customer / Consumer of ICT products (both hardware and software) and services
- [ ] Manufacturer of testing equipment
- [ ] Security certification laboratory
- [x] Other (Please specify)

If other, please specify:

DIGITALEUROPE is a Brussels based industry association representing the digital technology sector in Europe. DIGITALEUROPE is a membership based organisation and our members include some of the world's largest IT, telecoms infrastructure providers and consumer electronics companies as well national associations from every part of Europe. More specifically, DIGITALEUROPE's members include 61 corporate members and 37 national trade associations.

*2. Are you aware of the existence of multiple ICT security certification schemes across EU Member States for the same product/service?

- (•) Yes (Please answer question 2a)
- ( ) No (Please answer question 2b)
- ( ) Don't know

2a. If yes, please add further details concerning product/scheme/country/mandatory-voluntary nature, etc.:

DIGITALEUROPE acknowledges the existence of multiple ICT security certification schemes across Member States and encourages ENISA and the European Commission to consult the material produced by Working Group 1 of the European Cyber Security Organisation ("ECSO"), for a comprehensive overview. Some noteworthy examples include certification for 'smart meter gateways' as different schemes exist across the EU (Smart Meter Protection Profile – DE, Dutch Smart Meter Requirements – NL, Intelligente Essgeräte-Anforderungs-Verordnung – AT, and Commercial Product Assurance – UK).

DIGITALEUROPE also wishes to stress that the existence of multiple schemes across Member States does not inherently mean that there is a problem that needs to be 'solved'. The focus of any scheme should be on the 'risk assessment' that the security certification aims to address. Each 'risk analysis' depends on the specific context and in many instances different approaches are needed based on the objective. Voluntary schemes may help to achieve minimum security baselines within a more rapid timeline.

2b. If not, do you see the emergence of multiple national or sectorial certification schemes as a likely scenario in the future, especially in view of the growing cybersecurity risks?

- ○ Yes (please answer question 2c)
- ○ No
- ○ Don't know

2c. If yes, please add detail on type of product/service/sector:

*3. Have you encountered any of the following problems when dealing with ICT security certification procedures? Please thick box(es) as appropriate (more choices possible):

- ☑ Lack of mutual recognition of certificates across Member States
- ☑ Cost
- ☑ Duration of the process
- ☐ Lack of transparency
- ☐ Lack of a dedicated scheme to cyber -certify a specific product/service
- ☐ Lack of certification support for the lifecycle of the product (e.g., incremental certification for software and hardware changes/updates)
- ☐ Other (Please add detail)

If other, please add detail:

DIGITALEUROPE members stress that the majority of the problems they encounter when dealing with ICT security certification relate to the cost and the duration of the process. We would caution against any view that the 'lack of a dedicated scheme to certify products or services' should be viewed as a problem as product certification is usually ill suited to platforms or applications, as well as those services which have integrated development systems. All of these need different approaches and as such a 'catch-all' certification scheme cannot be the solution. When it comes to the issue of 'security life-cycle', DIGITALEUROPE wishes to stress that products require constant and flexible updates and patches. A certification schemes built around the life-cycle of a product, service, platform or application must remain flexible as constant re-certification of patches will further slowdown the process and not lead to greater cybersecurity. We continue to stress that the focus should be on processes rather than the components/end product and ensure that it remains flexible to apply to products and services with the consumer and enterprise customer in mind.

*

4. Currently, there is no EU-wide ICT certification framework allowing for mutual/cross recognition of national schemes. Do you see the need for a mutual recognition mechanism of certificates across all MS? Please thick box(es) as appropriate (more choices possible):

- [ ] The current situation is satisfactory
- [x] Mutual recognition is desirable at European level
- [ ] Don't know

*

5. Do you think that certification and labelling can be effective tools to increase transparency about the level of security assurances of ICT products/services, and enhance trust across the digital single market?

- ( ) Yes
- (•) No
- ( ) Don't know

Please explain, if needed:

Although well intentioned, DIGITALEUROPE believes that inflexible certification and static labelling risks creating a false sense of security for consumers and enterprises, increases costs, and does little to actually improve cybersecurity. The existence of certification and labelling will likely not lead to increased transparency, since such tools will not provide meaningful information about security and the customer is thus not well informed. Whilst in the enterprise sector, customers may well be better informed about risks posed, and as such take necessary measures, in the consumer space, a labelling scheme is far more likely to give a false sense of security.

Instead of a blanket labelling scheme, we suggest that voluntary market actions and/or self-regulation should be facilitated that can enable a set of good IoT security practices including: (i) ensuring users/consumers are aware of security settings and can take appropriate actions (for instance change them as necessary through adequate display settings/user interface with warnings about settings) (ii) ensuring IoT devices are not shipped with default security settings (many IoT devices share default user names and passwords that are well known and can be found with a quick search engine query) (iii) ensuring IoT devices are 'secure-by-design' and security is not left as an afterthought (which includes an ability for IoT devices to be patched so that vulnerabilities can be remediated).

We believe that the European Commission and ENISA should also work with industry to collect security 'best-practices' while looking towards organisations such as the Global Certification Forum ("GCF") as examples of successful voluntary testing and self-certification platforms. The GCF successfully brought entities from the device and operators side together to secure validation prior to market launch due to recall and brand risks. Such a system should be explored further.

DIGITALEUROPE also wishes to note that the discussion of a 'label' continues to incorrectly be held as an extension of the product 'certification' discussion. There instead should be a distinction between the two. Certification schemes tend to focus on the protection of critical infrastructure and governments, whereas labels focus on the consumer market by providing transparent information to the customer at the point of sale. While DIGITALEUROPE believes that greater harmonisation of certification schemes may positively contribute to an overall higher level of security across the EU, we continue to express our doubts that a labelling scheme can effectively achieve such a goal for consumers.

We note that consumer products are unlikely to have the same level of security functionality due to their inherently lower level of risk. Furthermore, the nature of security fluctuates. As such, the ever-changing threat landscape may render a device insecure regardless of whether it has a 'label' attached to it. Due to this, we believe that a labelling scheme will lead to a false sense of security.

*

6. Do you consider that recourse to certification and labelling in the ICT sector are sufficiently widespread or rather that it should be further encouraged or supported? Do you believe that greater effort to promote ICT security certification is needed in specific sectors?

- (●) This is a pure market issue and there is no need for additional support
- ( ) No, greater efforts are required in specific sector
- ( ) Don't know

Please explain, if needed:

DIGITALEUROPE would once again stress that the focus of any future activity should be on the associated risk. If there is a high level of risk, as is often associated with critical infrastructure, there will be higher levels of customer requirements. DIGITALEUROPE supports the idea that in those specific sectors where the risk is high, the promotion of ICT security certification should follow. However, the IoT sphere, at least in the area of B2C, is generally not associated with the 'high-risk' scenarios which require the same level of scrutiny. A 'one-size-fits-all' model should be avoided and voluntary schemes may help to achieve, more rapidly, a minimum security level for IoT consumer devices.

The IoT industry has anticipated the current and futures needs of end users' privacy and security and is working on industry-led initiatives for standardisation at an international level through actions such as the Open Connectivity Foundation ("OCF") (https://openconnectivity.org). The OCF is creating specifications and sponsoring open source projects to enhance interoperability and security for IoT business.

Furthermore, as mentioned in question 5, the discussion of a 'label' continues to incorrectly be held as an extension of the product 'certification' discussion. There should be a distinction between the two. Certification schemes tend to focus on the protection of critical infrastructure and governments, whereas labels focus on the consumer market by providing transparent information to the customer at the point of sale. While greater harmonisation of certification schemes may positively contribute to an overall higher level of security across the EU, we doubt whether that a labelling scheme can effectively achieve such a goal for consumers.

*7. Do you see a specific role for certification and labelling in the Internet of Things-domain?

- ( ) Yes
- (●) No
- ( ) Don't know

Please explain, if needed:

As previously mentioned, applying a similar level of assessment that exists for critical infrastructure and government to 'light weight' IoT products should be avoided. Such action will simply lead to increased cost, market access limitations and a false sense of security for end-users. It is important to note that even a device that is deemed 'secure', can be installed in an insecure way, thereby eradicating any certification or labelling. Moreover, the development of a single simple label or certification scheme for the entire spectrum of IoT products would be difficult as the variance of products is vast. While it is true that some verticals in an IoT ecosystem (eHealth, smart agriculture, industrial automation) may expose individuals and businesses to distinct threats and consequences, approaching the entire sphere of IoT with these vertical in mind should be avoided. DIGITALEUROPE therefore continues to express an openness to the concept of a voluntary IoT Trust Charter allowing the industry ecosystem to sign up to a set of principles that elucidate their approach to security. Such a voluntary approach could be applicable for certain IoT device verticals, where the validation could be based on having the minimum set of security, like basic access control and some form of trusted computing measures to ensure only proper code can execute, that is required to avoid such un-managed devices from causing major harm if hacked, to e.g. privacy and other services though forming botnets.

*

8. Do you see a specific role for certification and labelling in Industrial Control System (ICS)-domain?

- ○ Yes
- ◉ No
- ○ Don't know

Please explain, if needed:

To address the need of certification of industrial products, several international standards already exist, such as IEC62443 which specifically focuses on functional security and provides certification for products and product life-cycle processes. Such certification schemes have gained acceptance across different industrial sectors (ICS, power installation, etc.), proving that security development life-cycle ("SDL") frameworks are effective at improving security.

*9. Which of the following actions do you consider appropriate and proportionate to achieve the objective of reducing internal market fragmentation and improving trust in the security of ICT products and services in the EU?

- (●) "Soft law approach", encouraging, supporting and to the extent possible coordinating the adoption and use of certification initiatives at European level
- ( ) Extending the SOG-IS MRA to all Member States: legislative proposal making MS participation to the SOGIS agreement mandatory
- ( ) Creating a European certification general framework, laying down the essential rules for mutual recognition of certificates issued in accordance with the framework
- ( ) Regulating the security of ICT products and services, specifying essential security requirements for such products to be placed on the market
- ( ) None of the above (Please explain)

If "none of the above", please explain:

As pointed out in the European Commission's staff working document (SWD(2016) 216 final), market inefficiencies could arise with regulated certification schemes, particularly for national or regional schemes that define standards and evaluation methodology and only recognise certain certification bodies within their own territory. Harmonising only within Europe, or beginning the existing frameworks anew, will only continue to hurt European companies. Therefore, DIGITALEUROPE strongly believes that the 'soft law approach' should be pursued, however, it should not only focus on coordinating certification initiatives at European level, but efforts should instead be directed to strengthening global approaches.

*10. Do you think that the current SOG-IS MRA could be a basis to build an EU-wide certification framework?

- ( ) Yes
- (●) No
- ( ) Don't know

If yes, please explain if the current SOG-IS MRA model should be improved/modified and how?

DIGITALEUROPE believes the EU could explore the extension of SOG-IS to other Member States. However, we would caution against pursuing this through a legislative proposal making Member State participation in SOG-IS mandatory as SOG-IS participation is closely linked to available Member State resources. Instead, it should be encouraged with an emphasis placed on resource and capacity building so that participation can be met with added-value. Moreover, we wish to stress that SOG-IS cannot be a 'catch-all' solution as it is specifically tailored towards 'Common Criteria' and this approach cannot apply to the majority of products, particularly consumer facing products and industrial products.

We also wish to reiterate that SOG-IS today has a focus on higher level security requirements typically appropriate for products for which security is the primary function as in the public sector and critical infrastructure (and not industrial systems or consumer products). Those are sectors where the cyber risk is highest and is very resource heavy. Given the continued contraction of product development cycles and life spans, such requirements would not be appropriate for the consumer sphere as these require more dynamic and 'lightweight' solutions. Instead, agile self-assessment schemes and test automation environments will need to be created to ensure ICT products have minimum security capabilities appropriate for the context where they are used.

We reiterate the importance of a globally harmonised approach. The transaction costs and uncertainty of a non-coordinated, technically questionable and fragmented procedure would be much greater and should be avoided.

*11. Do you think that self-certification schemes could be considered a viable option to boost the level of cyber-security for selected product' domains?

- (●) Yes
- ( ) No
- ( ) Don't know

Please explain, if needed

As previously mentioned, DIGITALEUROPE believes that self-certification schemes must be considered as a tool to boost the level of cybersecurity for selected products. Such schemes would be able to properly take account of the evolving nature of products and services and would also be able to adapt to the context in which the products are used. While 'Common Criteria' effectively cover critical infrastructure and government, self-assessment would allow a wider range of products to be assessed across 'non-critical' environments. Any self-certification scheme would also be able to correctly take into account international standards.

DIGITALEUROPE wishes to stress that market dynamics play a significant role in driving cybersecurity. Market forces reward reliable operators offering solid security-by-design processes and transparent self-assessment actions, while allowing industry to freely develop products and services with the highest degree of innovation.

The UK's Cyber Essentials programme, which defined requirements involving self-certification for basic cyber hygiene practices for enterprises, or GSMA's IoT Security self-assessment framework are good examples where self-certification is able to address, in a more rapid manner, the need for harmonised solutions.

As previously mentioned, the IoT industry has anticipated the current and futures needs of end users' privacy and security and is working on industry-led initiatives for standardisation at an international level including through the OCF. The OCF is creating specifications and sponsoring open source projects to enhance interoperability and security for IoT business.

*12. Do you think that the processes and tools used for security certification should be improved to ensure the required flexibility to adapt to different market situations, particularly by allowing different level of assurances according to market needs (e.g. more stringent testing/assessment standards for more sensitive products/applications and less stringent for less sensitive products/applications)?

- (●) Yes
- ( ) No
- ( ) Don't know

Please explain, if needed

As per our previous responses, DIGITALEUROPE supports the concept of allowing different levels of assurances according to market needs as this provides the necessary flexibility to meet the given risk assessment. There must be adaptation to the market with different standards references (see ENRCIP proposal). This broadly represents the way market regulation exists today as duty of care for utility is passed down the supply chain. This also includes coordination across various market regulators to address any problems raised by aggregate customer demand.

*

13. Would you be in favour of the introduction of a common label signalling that the products have been certified within a certification scheme in accordance with EU rules?

- Yes
- (•) No
- Don't know

Please explain, if needed

Similar to our answer to question 5, the introduction of a common label signalling that products have been certified will likely lead to a false sense of security for customers. The discussion of a 'label' continues to be held as an extension of the product certification discussion, while there instead should be a distinction between the two. Labelling, tends to focus on the 'quick-to-digest' consumer market, whereas certification schemes tend to focus on the critical infrastructure and public sector section of the market. The distinct difference in characteristics means that both spectrum's of the market are highly unlikely to have the same level of security functionality and therefore consumers are not likely to support the cost premium attached to an extensive and independent evaluation of the vast array of products on the market.

Additionally, security is not static. While a product may achieve a top rating at the point it is put on the market, after a certain time frame the threat landscape will change and the label will now be rendered 'insecure'. This will, as previously mentioned, lead to false security and a widening of the 'trust gap' without adequate consideration of the life-cycle and business models of IoT products and services.

*14. Do you see a role for existing EU Commission's bodies and agencies (e.g. JRC, ENISA, ACER) in a possible future certification and labelling framework?

- Yes (Please explain)
- (•) No
- Don't know

If yes, please detail agency/body and possible tasks:

As pointed out in DIGITALEUROPE's response to the public consultation on the evaluation and review of ENISA, we believe that harmonised standards and the implementation of globally common ICT security standard frameworks have become more pressing issues to tackle in order to help European businesses meet their commitments when it comes to cybersecurity and regulatory compliance.

Although DIGITALEUROPE does not believe that EU agencies such as ENISA should lead on the development of EU wide standards or possible future certification and labelling frameworks, ENISA could play a role in 'keeping track' of Member State developments in an effort to point out where divergence between Member States and with international standards and activities occur. As a second step, ENISA could work with Member State authorities to create a set of non-binding guidelines with a view to harmonising practices across the EU, in accordance with internationally agreed upon standards and frameworks. Only an EU framework that is compatible with international standards and frameworks will enable European industry to expand and become competitive on the global market. Therefore we do not believe EU institutions shall take any actions on defining standards and certification schemes but leave this to industry driven global standards.

Contact

Florian.Pennings@enisa.europa.eu