Home Appliance Europe

Bld. Brand Whitlock 114
B-1200 Brussels
+32 2 738 78 10

Sanne Goossens
sanne.goossens@applia-europe.eu

Michał Zakrzewski
michal.zakrzewski@applia-europe.eu

Position Paper | 5/07/2018

APPLiA's Feedback on the Proposal for a European Certification Scheme on ICT Products and Services

As more and more home appliances become connected, online activities and services increase, and the digitisation of the home appliance industry develops, cybersecurity is a crucial issue for APPLiA. For our members, ensuring cybersecurity, from the design, development and production stages of the appliances to the connection of the appliances to the digital home ecosystem and security maintenance until end of support, it is imperative to ensure the trust that consumers have in our appliances and in our industry. Thus, our industry is committed to "security by design".

Therefore, we want to work with the European policy-makers to deliver a Cybersecurity Act that can truly protect European consumers. At the same time, we feel that it is important to promote innovation and stimulate growth for the industry in Europe. We take the opportunity to provide our input to the challenges and opportunities we see for the proposed Cybersecurity Act, most notably:

- The proposed cybersecurity certification framework must be voluntary, and schemes should be dynamic to certify the ability to react to new challenges and risks.
- The proposed framework should allow for self-declaration as a default, while only introducing third-party certification for critical requirements. In addition, strong market surveillance is a must.
- Establishing and optionally certifying the appropriate development, test and monitoring processes are regarded as more effective compared to product certification.
- The proposed framework should ensure an EU-wide scheme.
- The standards and practices behind each certification scheme will be crucial. They should be industry-led and developed in an open, transparent and consensus-based way.

1. Voluntary Approach

APPLiA believes that the creation of a European cybersecurity framework could be beneficial, but only if the framework enables specific, voluntary, dynamic, industry-relevant and affordable certification schemes. In addition, the international recognition and compatibility of such schemes should be kept in mind due to the global relevance of the home appliance market.

Also, the framework should recognise that different groups of products and services will require a different approach. Although some capabilities to react to cyber threats can be standardised, there is no one-size fits all solution that can be attributed to the assortment of current and future IoT technologies and the potential risks that belong to them. Therefore, different approaches are needed for different sectors. Furthermore, the elements to include should be guiding and not pre-prescribe or direct any scheme. It should be decided on the basis of stakeholder input, for each scheme at hand.

Still, the current proposal may already have unintended consequences of making certain schemes mandatory by default. As the proposal enables ENISA to determine schemes through referencing other Union or international standards, any reference made to "state of the art" (e.g. in privacy by design), could automatically warrant it mandatory in practice. While this may not be the intention of this proposal, legal certainty should prevail.

Additionally, fragmentation of national cybersecurity rules have proliferated and can represent single market barriers, particularly in areas where they are used to enable market access. Therefore, we support the Commission's proposal that once a specific EU scheme and the related certificate is adopted, a national scheme covering the same area falls away. Otherwise, a legally uncertain and confused market for these technologies would exist.

2. Self-declaration

We believe that the Cybersecurity Act should include self-declaration as the default option.

Self-declaration, without the involvement of a third party, is a well-established and effective approach in the home appliance industry. It allows for necessary flexibility, speed, available resources and doesn't put any unnecessary administrative and financial burdens on manufacturers and authorities.

Products and applications that are certified by a third-party are not necessarily more secure or more trustworthy than self-declared products, because a declaration corresponds to a test made according to pre-determined rules and requirements at a specific time. This means that dynamic changes – which are always present in the cybersecurity environment – and parameters not provided for in the test procedures cannot be detected by a third-party certification of a prototype. On the other hand, the manufacturer self-declaration procedure enables a prompt and flexible reaction to the changing conditions and can provide the relevant, updated information on cybersecurity. When combined with strong market surveillance, the self-declaration ensures reliable and legally effective information. It can therefore achieve at least the same degree of transparency and trust as third-party certification, but above all it can provide for the fulfilment of the technical requirements that are needed for the security of the end customer.

We therefore propose that under the certification framework proposed in the Cybersecurity Act, self-declaration will remain a recognised principle, while third-party certification will be an exception for critical areas only. In case of third-party certification, the laboratories that will test the critical products should be recognised at a European level and assessed by an accredited body.

3. Labelling and Market Surveillance

The proposed framework may introduce or further develop labelling practices for companies in order to demonstrate voluntary compliance. However, the presence of a label does not guarantee the (ongoing) security of the product. In addition, any label will only be as useful as the market surveillance that follows it, because the companies that are investing in labelling need to be able to do this within a level-playing field and without the threat of being undercut by unfair companies that may be seeking to apply labels to non-conforming technologies.

This will require substantial Member State investment in order to police the market. Our extensive experience has shown that market surveillance creates a level-playing field and ensures the reliability of the information provided on the market (e. g. manufacturer's declarations of conformity). To ensure effective evaluation of cybersecurity of products, market surveillance authorities need significantly more resources, meaning more budget and staff, since evaluating cybersecurity requires comprehensive and deep knowledge as well as effective testing procedures.

The Cybersecurity Act does not currently provide a strong role for market surveillance and relies primarily on the activities of the conformity assessment done by third-parties, which will likely not be able to take the appropriate or effective actions against misuse and violations of the law, while market surveillance authorities would be able to provide this.

4. Standardisation

When designing the certification schemes under the cybersecurity framework as proposed under the Cybersecurity Act, we should take into account that 100% security is simply not possible. Therefore, the schemes and the requirements included in the schemes should reflect that an acceptable marginal risk will exist.

Defining requirements is typically the role of standards developing organisations. European standardisation organisations like CEN/CENELEC and ETSI and international standardisation organisations like ISO and IEC have vast experience in developing technical specifications at European and international level, which is why they – together with the industry – should be at the heart of developing the cybersecurity standards considered under the certification schemes. Since IoT technologies are developing and proliferating at a rapid pace, we believe that it is necessary to have sector specific standards, on top of industry wide base security standards, that are industry-led and developed in an open, transparent and consensus-based way.

Annex I

5. Suggested amendments to the Proposal for a Regulation of the European Parliament and of the Council on ENISA, the EU Cybersecurity Agency (Cybersecurity Act), (COM(2017) 477 final)

Article	European Commission proposal	Proposal for amendment
43	A European cybersecurity certification scheme shall attest that the ICT products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems	A European cybersecurity **conformity and** certification scheme shall attest that the ICT Products and services that have been certified in accordance with such scheme comply with specified requirements as regards their ability to resist at a given level of assurance, actions that aim to compromise the availability, authenticity, integrity or confidentiality of stored or transmitted or processed data or the functions or services offered by, or accessible via, those products, processes, services and systems
44 (1)	Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity Certification Group (the 'Group') established under Article 53 may propose the preparation of a candidate European cybersecurity certification scheme to the Commission	Following a request from the Commission, ENISA shall prepare a candidate European cybersecurity conformity and certification scheme which meets the requirements set out in Articles 45, 46 and 47 of this Regulation. Member States or the European Cybersecurity **Conformity and Certification** Group (the ‚Group') established under Article 53 may propose the preparation of a candidate European cybersecurity **Conformity and Certification** scheme to the Commission
44 (2)	When preparing candidate schemes referred to in paragraph 1 of this Article, ENISA shall consult all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary	When preparing candidate schemes referred to in paragraph 1 of this Article, **ENISA shall work closely together with the industry stakeholder group and consult** all relevant stakeholders and closely cooperate with the Group. The Group shall provide ENISA with the assistance and expert advice required by ENISA in relation to the preparation of the candidate scheme, including by providing opinions where necessary
44 (4)	The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with	The Commission, based on the candidate scheme proposed by ENISA, may adopt implementing acts, in accordance with

	Article 55(1), providing for European cybersecurity certification schemes for ICT products and services meeting the requirements of Articles 45, 46 and 47 of this Regulation	Article **5 of Regulation (EU) No 182/2011, providing for European cybersecurity conformity and certification schemes for ICT products and** services meeting the requirements of Articles 45, 46 and 47 of this Regulation. **The implementing acts shall contain information based on the council decision (768/2008/EC) about what type of conformity assessment should be chosen for the scheme. The type of conformity assessment shall be chosen in accordance with the criteria given in Article 4 of Council Decision 768/2008/EC**
46 (1 and 2)	A European cybersecurity certification scheme may specify one or more of the following assurance levels: basic, substantial and/or high, for ICT products and services issued under that scheme.	A European cybersecurity certification scheme may specify one or more ~~**of the following**~~ assurance requirements based on the risks and threats determined by the context in which the product, process, or service is to operate ~~**levels: basic, substantial and/or high, for ICT products and services issued under that scheme.**~~ **Delete 2.**
47 (b)	Detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by reference to Union or international standards or technical specifications	Detailed specification of the cybersecurity requirements against which the specific ICT products and services are evaluated, for example by reference to Union or international standards or technical specifications. **In relation to the technical requirements and evaluation procedures, the schemes shall, whenever possible, make use of existing standards and shall not develop the technical standards themselves. A process based approach might provide better cybersecurity results compared to product specific objectives.** **Note: In the case of referencing European standards, these are**

		published by the European standardisation organisations and endorsed by the European Commission by publication in the Official Journal (see Regulation 1025/2012)
47 (c)	Where applicable, one or more assurance levels	Where applicable, one or more assurance levels **and type of conformity assessment**
47 (d)	Specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved	Specific evaluation criteria and methods used, including types of evaluation, in order to demonstrate that the specific objectives referred to in Article 45 are achieved. **Whenever possible for criteria and methods, the schemes shall make use of existing standards and shall not develop the criteria and methods themselves**
48 (3)	A European cybersecurity certificate pursuant to this Article shall be issued by the conformity assessment bodies referred to in Article 51 on the basis of criteria included in the European cybersecurity certification scheme, adopted pursuant to Article 44	A European cybersecurity **conformity and certification** certificate pursuant to this Article shall be issued by **manufacturer or** the **bodies** referred to in Article 51 on the basis of criteria included in the European cybersecurity **conformity and** certification scheme, adopted pursuant to Article 44
48 (6)	Delete	The certification scheme will determine conditions under which the issued certificate may no longer be valid and actions to be taken to regain the certificate.