EU's Cybersecurity Certification Scheme
Workshop Protocol — 11th October 2017

The following is a summary of central aspects of the discussion at the workshop *EU's Cybersecurity Certification Scheme* from October 11th, 2017. The workshop is part of a series about IoT security and was organized and moderated by Jan-Peter Kleinhans, *Project Director IoT-Security*. At the workshop were participants from civil society, ministries, private companies and academia. It was held under the Chatham House Rule. For questions about the workshop or feedback, please contact jkleinhans@stiftung-nv.de

The workshop consisted of two sessions. The first brainstorming session explored central aspects and indicators for an effective and efficient (EU-wide) IoT security certification scheme. In the second session, the participants discussed the European Commission's proposal for a cybersecurity certification scheme (part of the Cybersecurity Package) based on the aforementioned indicators. Goal of the workshop was to better understand the Commission's draft, identify its weaknesses and brainstorm ideas how to fix these from the perspectives of different stakeholders.

Since IoT security is a vast topic, one of the presumptions for the workshop was, that there will be an EU-wide certification scheme for IoT-devices in the near future. Thus, other regulatory tools to improve the security of IoT-devices, like software/distributor liability or capacity building measures, were not discussed. The focus was solely on the certification ecosystem. Like the workshop, this protocol first summarizes the brainstorming session and focuses in the second part on the discussion of ideas to improve the EU's proposed certification scheme.

SESSION #1 — BRAINSTORMING

Q: What are characteristics of an effective and efficient (EU) IoT-security certification ecosystem?
Following the initial brainstorming session the group together identified 7 categories and roughly clustered the ideas and indicators around these categories. The following section will describe and summarize the ideas for every category.

Certification Scheme

- It's based on (extending) existing, functioning certification schemes (Common Criteria/SOG-IS, CE, etc.)
- Transparency: There should be clear rules who needs a certificate and how to get it
- The certificate scheme should work with trade rules (WTO)
- The scheme should avoid the possibility for "light" (meaningless) certification and encourage re-certification — instead of "certificate-stacking"
- Consumer oriented: participation of consumer organizations, funding for consumer representatives (like ANEC)
- Consumers need a trustworthy system: responsibility → liability → sanctions → fines
- Escalating certification model: mandatory (basic) requirements → samples are tested on a regular basis → external review
- Enforceable at EU-level against backdrop of standards

- Allow for both security AND privacy certification
- Enforcement mechanism for Non-EU manufacturers
- Prioritization of products that have to be certified needs to be justified (based on safety aspects?)

Proportionality

- Cost, time and length of validity of certification should be proportionate to cost of the product certified.
- There should still be the possibility for companies to have a competitive advantage through “high-end” cyber certification alongside “basic” EU requirements.
- Mandatory requirements (baseline) should just focus on protecting third parties against negative external effects like botnets (DDoS attacks, etc.)
- Meaningful sanctions if a product violates or has no certification

Label

- Should be developed separately from certification scheme and should not be conflated.
- Transparent and understandable: clear definition what consumers might expect (level of security, update time, etc)
- Makes informed choice for consumer possible and makes buying decision easier (precise information)
- Avoids consumer reactance, rebound effects
- Purely physical labels might be too static for today’s IoT-devices.

Evaluation

- Effective monitoring and keeping certification up-to-date
- Ensuring consistency and equivalence of evaluation methods and costs across member states for the same certificate: what are we doing if “certified in Germany” becomes more valuable / trustworthy than “certified in Austria”? → oversight of certification bodies to ensure equal playing field across EU!
- Allow for 1st and 3rd party assessment
- Comparability of certification across countries and conformity assessment bodies

Technical Standards

- Based on Industry and/or International standards → ideally developed by a multi-stakeholder group
- Standard should focus on meaningful “default values” (strong authentication, end-to-end encryption, etc.)
- Scalability: for high-end security and for general purpose consumer products
- Standard should cover: operational environment + physical security + device → network → cloud
- Risk classification needs to go beyond device itself → some devices can trigger cascading risks
- Usability is important aspect of security

Division of Responsibility

- What's the responsibility of the consumer, the original manufacturer, the vendor, the distributor, the cloud operator… ?
- Requirements should apply to entire supply chain not just the OEM
- Clear legal responsibilities of certifier / conformity assessment body

Market Economics

- Interrelation of certification with insurance (high certification level → low insurance policy)
- If the certification is voluntary, there needs to be a clear economic incentive for manufacturers to apply for certification → should not conflict with business interests / strategies
- Manufacturers need a system that works with large scale / large number of consumer products → low day-by-day economic impact on the production & quick certification

SESSION #2 — SHORTCOMINGS OF THE PROPOSAL AND IDEAS HOW TO FIX THOSE

Following is a summary of the discussion in the second session to identify potential shortcomings of the proposal and brainstorm ideas how to fix those.

The certification schemes…

- Following the discussion about proportionality of the certification, the group agreed that the intensity / depth of certification should consider the context of a product and vary based on different parameters. The EU proposal seems to do that by introducing three levels of certification (basic, substantial, high). But the question is how those levels are differentiated. Risk of physical safety should definitely play a role.
- The group discussed that fixed risk or product categories might be too static for today's IoT world. An alternative could be the introduction of tags that describe a product (Wifi, 230V, physical risk = 3, or similar) Every tag is connected to certain requirements for the certification. This modular approach creates flexibility and might make the certification more meaningful for a specific device.
- It was discussed to which extend the operational environment / context might ask for different levels of certification for the same product? An Internet router that is used in a SOHO environment might need a lower certification than the same Internet router that is used in a doctor's practice.
- Because of the aforementioned relevance of context it was stressed that there should be more expert forums consisting of a variety of stakeholders to talk about and develop future certification schemes. ENISA's role should be to give guidance on how (!) to develop those certification schemes.

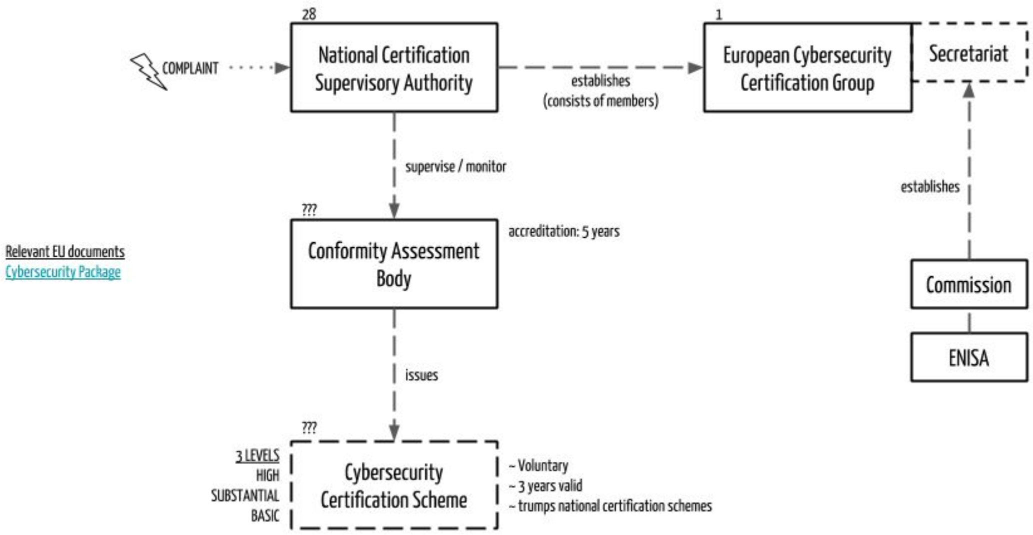
Enforcement…

- Even though the EU's proposal references the CE mark (a "static" safety mark), future certification schemes should have clear language about enforcement over the entire product lifecycle: period and frequency of guaranteed updates; sanctions if a company does not comply; etc. This would make certification more meaningful in a (dynamic) IT security context.
- Market surveillance plays a critical role in the current proposal. The question is if the current ecosystem of assessment bodies and national authorities are up to the task once they are supposed to take care of many of the consumer IoT devices. Quick response

mechanisms, clear single points of contact and easy re-certification and transparency are key.

- A database that tracks certified devices might help market surveillance. Similar to the approach the new EU Energy Efficiency Label is taking, a QR-Code on the product linking to a product database might also be helpful for enforcement. The database could contain: history of software updates; status of certification; reported vulnerabilities...

EU Cybersecurity Certification Scheme


28
COMPLAINT
National Certification Supervisory Authority
establishes (consists of members)
1
European Cybersecurity Certification Group
Secretariat
supervise / monitor
establishes
???
Conformity Assessment Body
accreditation: 5 years
Relevant EU documents
Cybersecurity Package
Commission
ENISA
issues
???
3 LEVELS
HIGH
SUBSTANTIAL
BASIC
Cybersecurity Certification Scheme
- Voluntary
- 3 years valid
- trumps national certification schemes