EUROSMART
The Voice of the Digital Security Industry

Feedback on the preliminary report on sector inquiry into consumer IoT

16 August 2021

Eurosmart reviewed the preliminary report related to the sector inquiry into consumer internet of things (C-IoT). C-IoT is the largest IoT market in Europe with around 510 million potential buyers. Our association would like to highlight the following:

Cybersecurity as important differentiating factor

In the connected world, for each device, the security functions of connected products and a security certification should cover protection against cyber-attacks, even for products where the use does not include confidential data or security usage since they could serve as an entry point for hackers to attack the network and other connected devices. The need for cybersecurity is horizontal to all IoT segments, included the C-IoT sector.

The threats faced by connecting devices to the network put the whole environment exposed to attacks. Thereby exposing the consumers to privacy loss, data theft, monetary loss, and, in some cases, harm to life.

In the report, cybersecurity was identified as a differentiating factor in section 4.2. However, recommendations are missing regarding the need for a trustworthy cyber-resilient smart device ecosystem based on cybersecurity by design and a robust cybersecurity evaluation process.

Recommendations

Eurosmart's feedback to this report is focused on three aspects of security that we, as European Industry experts in IoT security, think should be part of the report.

1) EU law to ensure that C-IoT products, systems and services on the market are cyber secure designed.

2) Security certification for devices placed on the European market should be based on compliance assessment by third party labs that is performed by security professionals to make security certifications trustworthy for the C-IoT devices and services.

3) Security standards within Europe should include protection against – and resilience to – the latest cybersecurity threats by making security testing standards "dynamic" so it is able to evolve as the hackers' abilities evolve.

- Section 5.7 - CERTIFICATION PROCESSES, presents functional compliance testing. Cybersecurity certification should be mentioned as well for covering the protection of the devices, of their connectivity to the internet and of the users' assets and data.
- Section 6 - STANDARDS AND THE STANDARD-SETTING PROCESS presents mainly compliance testing for fulfilling the security aspects of the device/platform. When products are offered which are supposed to be secure, there is a strong need to build trust between the buyer/user and the vendor. Trust increases when product security evaluation is being done by an external lab rather than by self-assessment (ex – what will you trust more? A door lock which was self-tested or one which was tested in a lab by security professionals?)

The following security standards for C-IoT should be used:

- ETSI EN 303 645
- ETSI TS 103 701
- ENISA Baseline Security
- ISO/IEC 27402 (in progress)

Some national authorities in the EU have published specific security recommendations on critical C-IoT devices. One example is BSI in Germany with TR 03148 on broadband router for smart home and building application.

Also, cybersecurity testing should be dynamic and performed by professional entities as the hackers' capabilities evolve. With respect to it, we recommend mentioning currently existing cybersecurity evaluation methodologies, those could be useful to build trust in smart devices:

- ISO15408 – Common Criteria std which is the most comprehensive std for security evaluation with a time-tested methodology. This methodology is currently used for security certification for devices in critical infrastructure, personal identity and other cyber-secure sectors.
- GlobalPlatform organization which hosts SESIP methodology for "Security Evaluation Standard for IoT Platforms". This Methodology addresses both platform and devices and provides solution for composite evaluations, as required by the IoT industry. SESIP is a methodology of security evaluation that applies well to C-IoT evaluation.

Pursuant to the Cybersecurity Act and according to the Union Rolling Work Programme, ENISA will soon launch an ad-hoc expert group for an IoT certification scheme. It is expected that the scheme would also address the C-IoT sector.

About us

Eurosmart, the Voice of the Digital Security Industry, is a **European 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.

Our members

Members are designers or manufacturers of secure elements, semiconductors, smart cards, systems on chip, High Security Hardware and terminals, biometric technology providers, system integrators, secure software and application developers and issuers. Members are also involved in security evaluation as laboratories, consulting companies, research organisations, and associations.

Eurosmart members are companies (**BCA, Bureau Veritas, CYSEC**, **Fingerprint Cards**, **G+D Mobile Security**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **NXP Semiconductors**, **PayCert**, **Prove & Run**, **Qualcomm**, **Real Casa de la Moneda**, **Samsung**, **Sarapis**, **SGS**, **STMicroelectronics**, **Synopsys, Thales**, **Tiempo Secure, Trusted Objects, TrustCB, WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom - IMT, ISEN - Institut Supérieur de l'Électronique et du Numérique Toulon**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart**, **Danish Biometrics**).

Eurosmart is a member of several European Commission's groups of experts: Radio Equipment Directive, eCall, Multistakeholder platform for ICT standardisation, and Product Liability.

Eurosmart and its members are also active in many other security initiatives and umbrella organisations at EU-level, like CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, GlobalPlatform, ISO, SIA, TCG, Trusted Connectivity Alliance and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Square de Meeûs 35 | 1000 Brussels | Belgium
Tel +32 2 895 36 56 | mail Contact@eurosmart.com