EUROSMART
The Voice of the Digital Security Industry

Brussels, 26th February 2019

ETSI TC Cyber's Technical Specification
"Cybersecurity for Consumer Internet of Things"
Is this enough to secure IoT consumer devices?
ETSI TS 103 645 V1.1.1 (2019-02)

On the 19th of February ETSI's TC Cyber issued new technical specification entitled: "Cyber Security for Consumer Internet of Things". Eurosmart welcomes this publication that makes provisions for an increase in the security level of connected consumer devices, network infrastructure, home network and associated services.

This new TC Cyber technical specification intends to tackle a wide range of IoT devices, such as connected children's toys, wearable health trackers, smart home appliances, smart home assistant which all deserve high security standards to ensure a high level of security, data protection and privacy to the consumer.

Eurosmart supports the valuable works of the European Standardisation organisations (ESOs) in the development of qualitative European standards. These European standards are in the best position to ensure Europe's digital autonomy and to raise consumers' confidence in the Digital Single Market.

This approach shall foster the upcoming development of European cybersecurity certificates. As stated by the European Commission in its communication on 13th September 2017: a key aspect is the lack of cybersecurity certification schemes recognized across the EU to build higher standards of resilience into products and to underpin EU-wide market confidence.

The development of European standards by ESOs will help both the European legislator and manufacturers to improve the temper resistance of connected devices, the protection of user's data and privacy. Eurosmart strongly encourages the European regulatory and standarisation trend which helps people trust the devices they use every day because they can choose between products, which are cyber secure.

The new technical specification from the TC Cyber provides a common-sense guidance for the development of connected devices.

Eurosmart considers the technical specification's requirements from the TC Cyber, as the good practices' summary for IoT devices' security hygiene. These requirements may perfectly be used to performed Corporate Binding Rules.

Moreover, the new technical specification is a good first step to avoid the basic security mistakes which could be made by IoT manufacturers. The provisions laid down in the technical specification set out far-sighted recommendations.

However, these introductory recommendations which aim to **make systems resilient to outages but** cannot be considered as a comprehensive secure approach. Interactions of the device and its environment (network and infrastructure) are regrettably missing. Moreover, borders between critical infrastructures and consumer's personal network are more and more blurred. This is particularly true for smart home environment where a smart appliance can connect to a network operator (phone, TV, Web etc.) which is considered as critical infrastructures in Europe. When it comes to wearables health trackers, they can be connected to hospitals infrastructures, that fall under the NIS directive.

A reference architecture of smart home, the identification of possible risks in this architecture and the definition of minimum IT-security function of connected devices in smart homes are key pillars to sustain **"security by design"** for the producer of connected smart home devices. These building blocks are needing to protect more than 500 million consumers in EEA in the future.

- **As regards the privacy of personal data**, nothing is said about the way the consumers should be informed about the manner their personal data are processed. Such a technical specification would have benefit from a more consistency approach with GDPR requirements. When it comes to the removal of personal data, the technical specification foresees a simple recommendation and targets data stored in the device, nothing is specified for data or meta-data that could embedder personal information and which could have been processed by a service outside the device. As a complement to the first technical specification, Eurosmart encourages a more comprehensive approach including clear mandatory requirements.
- **Vulnerability reports and software updated** is an entry point to ensure basic secure IoT, however the standard make simple recommendation for a "timely manner" for acting on vulnerability and the that coordinated vulnerability disclosure should be implemented.
- **End-to-End encryption for communication and anonymisation of personal (privacy) and telemetry data** should be mandatory principles. The new technical specification should enhance the recommendations of the GDPR and ePrivacy Directive. All these principles are only optional but are the only way to guarantee a suitable data protection for the users.
- **Software and Hardware resistance to potential attacks** is missing. The technical specification points out optional provisions to minimize the exposed attack surface for software only. Eurosmart has been advocating for years to identify the vulnerability for hardware and software. Penetration testing is key to limit risks and narrow exposures to potential attacks.

Euromsart and its members believe that such an initiative along the digital transformation and the cybersecurity topics in the European Economic Area (EEA) (i.e. NISD, eIDAS, CSA, PSD-2 etc.) requires a more consistent and comprehensive approach.

As a conclusion, Eurosmart welcomes the general trend that makes Europe's cyber resilience stronger, and the first efforts of ETSI - TC Cyber to provide an overview of good practices for security requirement. However, Eurosmart enjoins ESOs and specifically CEN CENELECT JT13 to work on even safer standards which may be referenced by the upcoming European cybersecurity certification schemes. The certification framework built upon the Cybersecurity Act, is expected to quickly raise the security requirements for consumer IoT devices from assurance levels Substantial to High.

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.

Our members

Members are manufacturers of secure element, semiconductors, smart cards, secure software, High Security Hardware and terminals, biometric technology providers, system integrators, application developers and issuers.

EUROSMART members are companies (**BCA**, **Cabinet Louis Reynaud**, **Fingerprint Cards**, **Gemalto**, **Giesecke+Devrient**, **GS TAG**, **IDEMIA**, **IN GROUPE**, **Infineon Technologies**, **Inside Secure**, **Internet of Trust**, **Linxens**, **Nedcard**, **NXP Semiconductors**, **+ID**, **Real Casa de la Moneda**, **Samsung**, **Sanoïa**, **STMicroelectronics**, **Toshiba**, **Trusted Objects**, **WISekey**, **Winbond**), testing, inspection and certification (TIC) companies (**SGS, Bureau Veritas, Trust CB**), laboratories (**Brightsight, CEA-LETI**, **Keolabs**, **SERMA**), research organisations (**Fraunhofer AISEC, ISEN**), associations (**SCS Innovation cluster**, **Smart Payment Association**, **Mobismart**, **Danish Biometrics**).

EUROSMART and its members are also active in many other security initiatives and umbrella organisations on EU-level, like CEN, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA, TCG and others.

EUROSMART
The Voice of the Digital Security Industry

www.eurosmart.com @Eurosmart_EU @Eurosmart

Rue de la Science 14b | B-1040 Brussels | Belgium
Tel +32 2 880 3635 | mail eurosmart@eurosmart.com