EUROSMART
The Voice of the Digital Security Industry

Internet-connected radio equipment and wearable radio equipment

Eurosmart's answer to the European Commission Public Consultation

Eurosmart, the voice of the digital security industry welcomes the European Commission (DG GROW) proposal to strengthen the security approach of internet-connected radio equipment and wearable radio equipment.

Reaching a trustworthy and secure IoT market is paramount for the achievement of the European Digital Single Market. By 2025, the projected IoT connections are expected to exceed the 25 billion of units' threshold[1]. In the meantime, consumer IoT devices will account for over half of these connections. However, Europe will only represent the 3rd IoT market with 4.9 billion units, far behind the Asia-Pacific (10.9 billion units) and the U.S.-Canada ones (5.8 billion units). In this context the challenge for Europe is to place on the market consumer IoT devices which has not been specifically designed for its own market, but which respect the European philosophy and exigences in terms of security, privacy and safety. Throughout the evolution of the Digital Single Market, Eurosmart has been advocating for the strengthening of the digital security as an essential precondition for consumer confidence and the European digital industry growth in a global market where Europe doesn't hold the balance of power.

Hence, in this context, Eurosmart and its members pay a particular attention to the security of the IoT devices placed on the European market, which must respect our fundamental values of data privacy and resistance to potential attacks (Cybersecurity).

Eurosmart highlights the fact that than an IoT device is not expected to act in an isolated manner. Due to its dynamical nature, and the way the device adapts to its environment, security should be understood in a more compressive sense. The cybersecurity of the device has an impact on its whole environment (network, other devices) and even on critical infrastructures in the meaning of the NIS directive. For instance, a smart wearable such as a cardio activity tracker, which is not a medical device, can relate to both individual's home network and to Hospital network.

Until now, there are no strong and mandatory cybersecurity requirements for placing a consumer IoT device on the market. The Radio Equipment Directive manly focuses on essential requirements for safety and health while ensuring electro-magnetic compatibility. As laid down in the Radio Equipment Directive, Eurosmart supports the idea of incorporating safeguards to ensure that the personal data and privacy of the user are protected, and to take measures to prevent from fraud, but on the condition that real cybersecurity measures, instead of a safety-based approach, would be incorporated into a potential delegated act.

[1] Source GSMA

Eurosmart acknowledges the benefits in terms of safety of the New Legislative Framework (NLF) approach, and the 2014 recast of the Radio Equipment Directive which keeps flexibility for manufacturers and set out level-playing-field between manufacturers and importers. However, Eurosmart does not support the idea that the NLF will fit in with cybersecurity requirement level. NLF was built to support safety requirements when placing a product on the market and not to assess a resilience level of a product to potential cyber-attacks.

The Inception Impact Assessment suggests the idea of baseline security requirements, to comply with the rules set out by the GDPR and the ePrivacy Directive which do not concern access market to products. Eurosmart fears that this option may lead to the sole principle of "cyber hygiene" based on a self-declaration or a check list to the manufacturer or the importer. This is not clearly enough to reach a trustfully Digital Single Market and will put Europe's digital sovereignty at risks: how could the potential backdoors be identified? How to make sure that European citizens' personal data and credentials are securely stored and processed?

For these reasons, Eurosmart strongly recommends a cybersecurity approach for the potential Delegated act of the Radio Equipment directive. The NLF-Safety approach is designed to assess static targets whereas cybersecurity is a matter of anticipation and moving security target. The European Cybersecurity Certification Framework as defined by the Cybersecurity act, has been designing to evaluate cybersecurity resistance level of products, it is the only viable process to fulfil this task. Due to the interconnected and sensitive nature of a consumer IoT device and as stated by the Inception Impact Assessment, Eurosmart urges the European Commission to propose a certification scheme at the level "substantial" for "Internet-connected radio equipment and wearable radio equipment", and thus, based on trustworthy European Standards to be defined. This adopted certification scheme shall be referenced in the foreseen Delegated Act of the Radio Equipment Directive to support the intended purposes pursuant both Articles 3(3)(e) and (f).

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 36 00 | mail eurosmart@eurosmart.com