Digital Security Industry affected by global chip shortage

A Silicon shortage, initially hitting the automotive industry and widely covered by the media over the last months, is now spreading to consumer electronics, as more and more household goods use computer chips. First announcements have already been made by smartphone manufacturers, reporting difficulties due to this semiconductor shortage. It is expected that this effect will continue at least into the second quarter of 2022, as reported by market analysts, such as GARTNER.

Eurosmart, as the voice of the digital security industry, would like to emphasize that security chips, which are used as secure elements in smart cards or smart devices are also affected by the current chip shortage. These security chips are implemented in products that are crucial for enabling secure payment (e.g. in payment cards), secure mobile communication (e.g. in SIMs/eSIMs), secure IoT, and the secure identification of people (e.g. in national ID cards and passports). In 2020, the overall market amounted to more than 9 billion security chips. Furthermore, despite and partly driven by the Covid-19 crisis, security chip demand has increased, and is likely to increase once the pandemic has been overcome.

While the magnitude of the shortage is not yet predictable, it will affect the smart security industry this year and beyond. Eurosmart would therefore like to encourage **all stakeholders to consider the potential impact of the silicon shortage and to engage with relevant industry actors to set the right way to deal with this challenging situation.** Notwithstanding this difficult situation, the smart security industry is fully committed to do its best to provide products to the market so that people can continue to benefit from trusted services such as secure payment, mobile communication, IoT, and identification of persons.

Eurosmart emphasizes that the security chip is the only tamper resistant technology that guarantees that user data, cryptographic keys and the applications handling them remain protected at rest and during execution. They provide the highest level of security and privacy, which are key concerns in any governmental or private domain (payment, industry, telecommunication, law enforcement, digitalization). Today's challenges and priorities of the European Commission cover security, cybersecurity and privacy as shown by initiatives such as the addition of biometric authentication (fingerprints and face) performed within a security chip in all identity documents as well as the proposed revision of the eIDAS regulation.

Eurosmart calls all stakeholders to keep in mind the challenges of security, cybersecurity and privacy that are ahead of us, and for which citizens expect nothing but the highest level of trust and protection. Security chips are, and will remain the cornerstone of these expectations. The current and temporary chip shortage shall therefore not divert stakeholders from these objectives.

Eurosmart appreciates the European strategy[1] to support and invest in the European semiconductor industry. This will strengthen Europe's technology sovereignty and will help the European economy to be more resilient in the future. Also, Eurosmart encourages the European Commission to set up dedicated actions in this strategy considering the security chip industry.

---

1 Joint declaration on processors and semiconductor technologies - Joint declaration on processors and semiconductor technologies | Shaping Europe's digital future (europa.eu)

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 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**, **Synospys**, **Thales**, **Tiempo Secure, Trusted Objects**, **WISekey**, **Winbond, Xilinx**), laboratories (**Brightsight**, **Cabinet Louis Reynaud, CCLab, CEA-Leti, Jtsec, Keolabs**, **Red Alert Labs**, **Serma**), consulting companies (**Internet of Trust, Trust CB**), research organisations (**Fraunhofer AISEC, Institut Mines-Telecom – IMT, ISEN – Institut Supérieur de l'Électronique et du Numérique Toulon**), and associations (**SCS Innovation cluster**, **Smart Payment Association**, **SPAC, Mobismart, Danish Biometrics**).

Eurosmart is a member of several European Commission's expert groups: 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 the EU level, such as CEN-CENELEC, ECIL, ETSI, ECSO, ESIA, ETSI, GP, ISO, SIA and TCG.

EUR⊘SMART
The Voice of the Digital Security Industry

www.eurosmart.com   @Eurosmart_EU   @Eurosmart