Study on Trusted Electronics – Executive Summary

An overview over requirements, technologies and initiatives towards more trusted electronics

Written by Matthias Hiller and Johanna Baehr, Fraunhofer AISEC
November 2023

EUROPEAN COMMISSION

Directorate-General for Communications Networks, Content And Technology
Directorate A — Artificial Intelligence and Digital Industry
Unit A3 — Microelectronics and Photonics Industry

Contact: CNECT-A3@ec.europa.eu

European Commission
B-1049 Brussels

EUROPEAN COMMISSION

Study on Trusted Electronics – Executive Summary

An overview over requirements, technologies and initiatives towards more trusted electronics

Directorate-General for Communications Networks, Content And Technology

2024 EN

Manuscript completed in November 2023

1st edition

Luxembourg: Publications Office of the European Union, 2024

PDF ISBN 978-92-68-09400-6 doi : 10.2759/572679 KK-02-23-221-EN-N

Developing, deploying and operating trusted electronics in Europe is a prerequisite for Europe's technological sovereignty and foundation for secure and trustworthy applications of all kinds. The supply chains of electronics involve a large number of specialised partners around the world and contain a large number of steps from specification, design, manufacturing and assembly to operation and end of life. This poses several options for introducing vulnerabilities in form of unintended weaknesses or intentional backdoors. In addition, unreliable ICs originating from the grey market may be introduced into the supply chain. Work on trusted electronics addresses these vulnerabilities and thus facilitates the foundation for the cybersecurity of the devices.

Typical issues that hinder the adoption of trusted electronics are an increased complexity, implementation overhead, verification overhead, compatibility, lack of specialised expertise, gap between research and real-world products, availability of design tools, incorporating trust into the supply chain, access to technology and conflicts in regulatory compliance.

Even if trusted electronics rarely contributes new features to a product, intrinsic and extrinsic market drivers motivate companies to increase the trustworthiness of their devices and systems. Intrinsic drivers that internally drive the transition to trusted electronics are differentiation in the market, reputation of the company, and protection of the business, whereas extrinsic drivers address external requirements imposed through regulation, standardisation, or by insurance companies. In addition, there is the geopolitical and strategic dimension that the sovereignty of today's societies heavily relies on the availability of trusted electronics and their integration into critical infrastructures. When addressing intrinsic and extrinsic drivers, there is a distinction in motivation. While companies strive to address intrinsic drivers to the best of their ability, extrinsic drivers must simply be met, and exceeding the requirements only offers little benefit. This makes it important to define extrinsic drivers clearly to achieve the desired impact.

To fulfil the market drivers, requirements need to be met by these technologies and products. A first, general set of requirements are basic requirements that apply to every company in every market and address the affordability, scalability, accessibility of technology, integrability, and robustness of the solution. Horizontal requirements are common across many industries and sectors but, their relative importance may vary between companies. In general, platforms need to be generic and a tooling, design and verification ecosystem needs to be provided in addition to the technology. Sectorial requirements apply to particular industries or markets. For instance, time to market may be of utmost importance for basic consumer goods, but it may not play a significant role in high-security military applications. These requirements are accountability, time to market, lifetime of a device, and also security requirements of the data.

Distilled from roadmaps, workshops, literature study and communication with stakeholders, the following list discusses relevant technologies that can lead to

more trusted electronics and increase the cybersecurity of embedded devices, and also open challenges to bring them into practice.

- Secure Designs cover topics such as open-source hardware, and in particular RISC-V, roots of trust / secure elements, cryptographic implementations, and integration technologies such as chiplets and advanced heterogeneous integration.

- Supply chain security requires a chain of trust, cross-manufacturer trustworthiness, and technologies for counterfeit detection, mitigation and fingerprinting.

- Analysis also plays a critical role for trusted electronics and requires research on metrics for trustworthiness, test, analysis and verification during design, manufacturing, operation and post-mortem, verification through open-source electronic design automation, and digital twins.

- Cross-technical challenges complement the technical ones such that, involvement of real-world products and training and teaching also play a critical role for the deployment of trusted electronics.

Research on trusted electronics is carried out and funded in a combination of dedicated initiatives and programs, as part of programs with a wider scope, and funding of individual projects. While the focus of this study is on dedicated initiatives, the latter can be part of e.g. cybersecurity and semiconductor chips research programs and be carried out through bottom-up research funding for individual researchers and groups. European initiatives on cybersecurity and semiconductor chips often provide funding for a wide range of topics, without specifically focusing on trusted electronics in general. In Europe, currently a sizable part of the publicly funded initiatives is carried out in Germany whereas few initiatives exist at national or European level.

The opportunity to establish a dedicated program for trusted electronics holds the potential to attract specific funding for initiatives in this field, enabling focused efforts towards securing and advancing trusted electronic technologies. An important goal is the transfer of research outcomes into applied research and tangible products, which reflects the importance of bridging the gap between scientific results and their practical implementation in real-world applications. Ensuring adequate support and funding for applied research, technology development, and the commercialization of innovative ideas is becoming increasingly crucial.

The large number of funded initiatives in the United States shows that major research advances require large strategic investments to develop technologies for governmental and military applications. Transferring the results into more cost sensitive commercial technologies will require an even larger effort.

Standardisation activities help to foster trusted electronics driven by end users, industries, and governmental actors. There exists a wide range of work on cryptographic and information security standards driven by governmental agencies or industrial standardization bodies. Standardisation is also a foundation to collect and harmonise requirements in a broad scale and foster the adoption of technologies that are researched in other initiatives, by research facilities or by industrial players.

As it is not feasible to develop and manufacture all electronics in trusted environments, technologies are needed to support neuralgic points and provide trust anchors. This requires researching and deploying technologies for trusted electronics. They cover secure designs for hardware or cryptographic implementations, supply chain security to maintain trust and detect counterfeits, and analysis techniques.

Initiatives supporting bottom-up and broad activities are a first step but require more specific funding for fundamental research and the transfer into the applications with a focus on real-world applications. In addition, trusted electronics can only be achieved in depth and breadth when the research is accompanied by training and teaching programmes and, most importantly, followed up by companies deploying and using the technology and methods in large scale.

Strengthening the European design and manufacturing ecosystem through the European Chips Act is an important step towards European technological sovereignty. However, complementing this effort and improving the trustworthiness of electronics beyond existing standards will benefit from dedicated security-focused funding. Looking to the United States shows that researching trusted electronics in a broader scale requires strategic funding that goes widely beyond individual calls on the topic and establishing centres that bring together a critical mass of competencies and equipment.

GETTING IN TOUCH WITH THE EU

In person

All over the European Union there are hundreds of Europe Direct information centres. You can find the address of the centre nearest you at: https://europa.eu/european-union/contact_en

On the phone or by email

Europe Direct is a service that answers your questions about the European Union. You can contact this service:

– by freephone: 00 800 6 7 8 9 10 11 (certain operators may charge for these calls),

– at the following standard number: +32 22999696 or

– by email via: https://europa.eu/european-union/contact_en

FINDING INFORMATION ABOUT THE EU

Online

Information about the European Union in all the official languages of the EU is available on the Europa website at: https://europa.eu/european-union/index_en

EU publications

You can download or order free and priced EU publications at: https://publications.europa.eu/en/publications. Multiple copies of free publications may be obtained by contacting Europe Direct or your local information centre (see https://europa.eu/european-union/contact_en).

EU law and related documents

For access to legal information from the EU, including all EU law since 1952 in all the official language versions, go to EUR-Lex at: http://eur-lex.europa.eu

Open data from the EU

The EU Open Data Portal (http://data.europa.eu/euodp/en) provides access to datasets from the EU. Data can be downloaded and reused for free, for both commercial and non-commercial purposes.

KK-02-23-221-EN-N

Publications Office
of the European Union