December 2016

Infineon – NXP – STMicroelectronics – ENISA
Common Position On Cybersecurity

1 Preamble

The internet and mobile revolution have transformed our world. Today 2.9 billion people--40% of the world's population--are online. By 2020, market analysts expect between 20 and 50 billion connected devices to be in the market. With all the benefits from the use of connected devices, also come a range of threats from data manipulation, data theft, and cyberattacks – and these are increasing. In 2015, European enterprises had at least a one-in-five chance of losing data through a targeted cyber-attack[1]. As a result, they have high concern regarding the availability and integrity of their systems.

Today we are seeing a **market failure for cybersecurity and privacy**: trusted solutions are more costly for suppliers and buyers are reluctant to pay a premium for security and privacy. This weakness creates a severe risk that the European economy is falling behind in its ability to tap into the promising emerging IoT markets. The lack of trust in smart and connected devices from businesses and consumers is a barrier to growth and jobs.

The smart card world already knows the relevance and risks of physical attacks when devices are physically accessible to an attacker. With the rise of the Internet of Things (IoT) enabling cars, critical infrastructure, and health applications using the same pipes and systems to communicate, **attacks will get even more risky and threatening**.

SOG-IS[2] member states, including the respective accredited evaluation labs, have built **high expertise** for the evaluation and certification of smart cards and similar devices to **high assurance levels**. We highly recommend building on this unique expertise, scaling it to more member states, and optimizing its mutual recognition within the EU to equalize the demand which is going to come with the rise of IoT (from low to high assurance levels depending on the application needs).

Currently there is **no basic level, no level zero defined for the security and privacy of connected and smart devices**. There are also no legal guidelines for trust of IoT devices and services and no precautionary requirements in place. This is why we recommend effective baseline requirements for security and privacy in the networked architecture and value chain as a whole: from simple IoT devices up to complex IoT-systems like connected cars and factories. Stakeholders need an equal and level playing field to implement trust into connected devices and services.

We believe it necessary to **define the European Baseline Requirements for Security and Privacy** that minimizes risk, is neutral in technological terms, and remains open to innovation. Currently a set of draft baseline requirements is being developed and discussed within **AIOTI**[3] by defining technical gaps.[4] It

---

[1] http://quocirca.com/content/least-1-5-europe-enterprises-lose-data-through-targeted-cyber-attacks
[2] http://www.sogis.org/
[3] Companies involved: https://docbox.etsi.org/SmartM2M/Open/AIOTI/!!20160616AIOTIWorkshopOnSecurity/
[4] Report available at: https://docbox.etsi.org/SmartM2M/Open/AIOTI/!!20160616AIOTIWorkshopOnSecurity/TICKEDv2%20List%20of%206

includes the request for third party evaluation and certification for connected devices and services. The **introduction of an EU Trust Label,** based on various security levels and on a related risk assessment, as discussed during an AIOTI workshop on Security and Privacy in the hyper-connected world in Sophia Antipolis at ETSI recently, should also be evaluated by the European Commission.

Ideally, the use of the label should be mandatory as a symbol of trust of citizens, consumers and businesses in the connected world. An obligatory reference framework and an associated label would ensure appropriate levels of security for products and services. This would further lead to a level playing field for the entire industry. As a second step, higher, sector- or application-specific security levels can be developed building on and extending the baseline requirements.

2 Challenges and recommendations

2.1 Standardisation and certification – priority 1

- Any existing and new regulation should take **standards** developed and / or strongly supported by EU stakeholders (EU industry, EU governmental agencies) into account (related good examples: PSD2, eIDAS, GDPR, NIS).
- So called **baseline requirements** for IoT security and privacy that cover the essentials for trust, e.g. rules for authentication / authorization, should set **mandatory reference levels for trusted IoT solutions.** Simple ones for products like smart thermostats and more sophisticated ones for complex devices like a smartphone.
- The framework for **interoperability testing** needs to be adapted to new requirements related to IoT
- The EU-standardisation process can be time-intensive, potentially causing delays in application of necessary standards and interoperability. This situation needs to be improved. Solutions include the **support of European industry** and **best practices** as precursors. industry standards could become recognised by European Standard Development Organisations and integrated into their work
- Future standards for **scalability of security controls** have to anticipate and meet the needs of different risk levels. Some market sectors, such as industrial internet, have already defined and standardized four security levels on cyber physical systems (IEC 62443). This approach should be evaluated to determine if it could be used as a reference for other sectors.
- A currently well-established certification of security products is **Common Criteria** (CC, ISO/IEC 15408). It has been implemented in many EU Member States and other countries and benefits from a dedicated mutual recognition agreement (SOG-IS MRA) between 13 EU member states. This should be extended ideally to all Member States. Also SOG-IS MRA covers high assurance security levels, a key asset on which the EU should build. The MRA and the way CC is applied require adjustments in order to stay attractive for the development of modern applications and agile development methodologies. In addition, for customers/applications not requiring full CC certification or those willing to accept lower security levels while maintaining the vulnerability assessment of the security solutions, a **baseline security certification**

1%20Registered%20(53%20ticked%20on%20site)%20Participants%20to%2016%20June%202016%20AIOTI%20Workshop%20on%20Security%20and%20Privacy%20in%20the%20hyper-connected%20world.pdf

(essentially a "lightweight" certification) for ICT products should be developed and agreed by all MSs, addressing IoT, Commercial of-the-shelf (COTS) and products with short life cycle. Certification should use standardized security requirements for connected devices as reference.

- The introduction of a **European trust label for connected devices** should be built on defined baseline security requirements and existing internationally recognized certification schemes. Such a European trust label should make the underlying certification transparent, also including the targeted security need. This should be supported by a **European Certification Framework**.

> **The European Commission should define a policy framework for ensuring minimal security requirements for connected devices. The development of European security standards needs to become more efficient and/or adapted to new circumstances related to IoT. Based on those requirements a European** scheme for certification and the development of an associated **trust label should be evaluated.**

2.2 Security processes and services – priority 1

- **Existing high assurance-level security processes and services that come with SOG-IS need to be evaluated and adapted to new challenges related to IoT.**
- **Evaluation of security processes** and services (delivery, testing, life cycle management etc.) should lead to certification.
- Framework solely for **interoperability testing** is not sufficient with regard to the requirements. Speed and cost of third party **security testing** should be improved by considering application specific attack scenarios (e.g. by proper application of user guidance, testing in live environments in the course of certification).
- **There is a lack of awareness when it comes to security and privacy in IoT. Industry, especially SME, needs to be provided with information about existing security features** such as encryption, appropriate key storage, strong authentication, privacy and identity management systems.
- Existing approaches to **Industrial Internet** (i.e. Cyber-Physical Systems, Internet of Things, Cloud Computing) should be promoted and studied further.

> **The European Commission should ensure that reliable security processes and services are being developed and should support industry in implementing security features in their products (e.g. through providing information and training about state-of-the art security solutions).**

2.3 Security requirements and implementation – priority 2

- **Baseline requirements for security and privacy** must become effective in the networked architecture and value chain as a whole: from components of simple IoT-devices up to complex IoT-systems like connected cars and factories. A mandatory reference level for any trusted IoT solution must be set. In future revisions of existing legislation, scalable technical security requirements and **common principles** should be made **mandatory** (e.g. **NIS Directive**). These common principles shall be based on scalable robustness requirements (including security controls and mechanisms), reference security architectures, basic functionalities, and security certification of embedded security services.

- **Synergies across various sectors** (e.g. energy, health care, transport, finance) should be used to a larger extent to reduce the amount of standards for similar certification and service approaches.
- **Convergence of safety and security** is important especially where human lives are endangered, e.g. in Automotive or in Industry 4.0 (IEC 62443).
- Privacy should be correctly perceived. **Appropriate training** should be mandatory in schools, universities (through all disciplines) and industry, in order to exercise certain functions.

> **The European Commission should encourage the development of mandatory staged requirements for security and privacy in the IoT, including some minimal requirements. These common principles should be considered in future revisions and new legislative initiatives.**

2.4 Economic dimensions – priority 2

- A **level playing field** with the same rules and requirements on security to all stakeholders will support cost benefits and provide legal certainty.
- Insurance companies and policies could define a **'Digital Security Bonus'** as reward for implementation of security solutions, particularly in non-regulated sectors, such as industrial internet, smart homes or smart living. A mandatory cybersecurity insurance for connected devices might stipulate this approach.
- **Risk management practices**, including certifications, (like that defined by Basel II accord) should be promoted, e.g. by granting insurance premiums for assessing cybersecurity risks.
- To set a good example, national public authorities should integrate appropriate security standards into their **sectoral public procurement policies**.
- An enforceable set of penalties should be defined for dealing with **vendors** of security products and services that abuse established practices on certification and/or deliver counterfeit products.

> **The European Commission should create an equal level playing field for cybersecurity and look into incentives similar to the Digital Security Bonus in order to reward the use of good security practices.**

3 About us

Infineon Technologies is a world leader in semiconductor solutions that make life easier, safer and greener. Barely visible, semiconductors have become an indispensable part of our daily lives. Chips from Infineon play an essential role wherever energy is generated, transmitted and used efficiently. They safeguard data communication, reduce harmful emissions produced by cars and are paving the way for driverless vehicles. Microelectronics from Infineon is the key to a better future.

NXP Semiconductors enables secure connections and infrastructure for a smarter world, advancing solutions that make lives easier, better and safer. As a technology developer with decades of expertise for secure connectivity solutions in embedded applications, NXP is driving innovation in the secure connected vehicle, end-to-end security & privacy and smart connected solutions markets.

STMicroelectronics is a global semiconductor leader delivering intelligent and energy-efficient products and solutions that power the electronics at the heart of everyday life. ST's products are found everywhere today, and together with our customers, we are enabling smarter driving and smarter factories, cities and

homes, along with the next generation of mobile and Internet of Things devices. With a 20-year presence in security, ST supplies the market's most advanced technologies and solutions and is committed to contributing to a more secure connected world. By getting more from technology to get more from life, ST stands for life.augmented.

ENISA assists the European Commission, the Member States and the business community to address, respond and especially to prevent network and information security problems. The Agency is a body of expertise, set up by the EU, to carry out very specific technical, scientific tasks in the field of information security.