



January 10, 2014

United States Federal Trade Commission  
Office of the Secretary  
600 Pennsylvania Avenue, NW  
Washington, DC 20580  
<http://www.ftc.gov/os/publiccomments.shtm>  
RE: "Internet of Things, Project No. P135405"

Dear Commissioners:

Thank you for inviting comments on the security and privacy concerns emerging with the increasingly networked world. Infineon Technologies is deeply experienced in securing digital devices through secure microcontrollers and integrated circuits (ICs) and we welcome the opportunity to highlight some key elements of protecting data and devices in the Internet of Things.

Infineon is a global semiconductor company with core competencies in the fields of security, wireless communication and embedded control. Our microcontrollers and ICs are facilitating security in an increasingly connected world. For example, secure chips enable mobile payment systems security, local network security, cloud security, and electronic ID documents. As the market leader in hardware-based security, Infineon believes a hardware root of trust (HRoT) is fundamental to securing sensitive information, transactions and devices.

In the emerging IoT, the consumer becomes more widely and deeply connected to the Internet through intelligent machines that anticipate needs, facilitate transactions and promote safety – all strong benefits to consumers. At the same time, many of these devices and applications provide information about consumer behavior that may be considered private, and so should be secured.

Laying the groundwork for defined categories of data and devices to be secured, and the protection protocols to do so, is important at this early stage of the IoT. It is critical for consumers to have trust in these technologies, and critical for innovators to build upon accepted standards and principles for privacy, security, and safety.

Infineon addresses the question of security technology posed in your RFI on the Internet of Things (IoT).

**What existing security technologies and practices could businesses and consumers use to enhance privacy and security in the Internet of Things?**

The IoT needs a fundamental ubiquitous security layer based on international standards, rooted into hardware for safety and security applications. ISO, IETF, Trusted Computing



Group and Global Platform are standards organizations who provide building blocks for the HW and SW security layer.

Security must be built into devices and networks to prevent harm and build consumer trust in the IoT. Security is the underlying layer in the IoT network and needs to be integrated in the communication layer as well as in the lower layers of the TCP/IP stack, even down to silicon.

The key elements hardware security can provide to the IoT are:

- Support **system integrity** which means the user can see and analyze the health of a IoT system
- **Secure authentication** and attestation of endpoints and subsequent secured data exchange
- **Secure storage** of key material as the foundation for trust establishment between IoT sensors and nodes
- **Foundation for trusted operating systems and application software** for mission critical systems to ensure availability and continuity of service

A HRoT is fundamental to securing devices and data in the IoT, especially when safety is paramount such as in vehicles, public transport systems, critical infrastructure systems or even home automation equipment.

The many IoT endpoints will become autonomous operators on the Internet, therefore they are potential entry ways for attacks. These endpoints need to be protected against counterfeits, software attacks and hardware manipulation. The HRoT facilitates monitoring the “health” of the system and allows secure software updates based on signature-based schemes already used in the PC and App environments for mobile phones.

Looking toward the future, it is foreseeable that intelligent end points supporting web services or virtual objects (avatars) will act independently and interact depending on context, circumstances or environments. Ambient intelligence, where embedded electronics interact with people, is estimated by researchers to become a reality by 2020. With this innovative and productive future in mind, it is important to focus now on building security standards, protocols, and best practices for the Internet of Things.

Sincerely,

Joerg Borchert  
Senior Vice President, Chip Card and Security ICs  
Infineon Technologies North America Corp.