Whitepaper on Certified Security in the Internet of Things

List of Contents
I. Executive Summary p. 1
II. Introduction p. 2
III. Starting Point p. 3
   1. What is the “Internet of Things”? p. 3
   2. Opportunities – But Risks As Well p. 3
   3. Risks Insufficiently Heeded to Date p. 4
IV. Imperative Measures p. 5
V. Summary p. 7
VI. Sources p. 8

I. Executive Summary

The Internet of Things (“IoT”) – meaning the all-embracing networking of smart devices interconnected with each other via the Internet – is on the rise and will already become reality within the next five years. The decisive change accompanying the IoT will be its ubiquity: networked devices are everywhere. Like any technological progress, this development offers social and economic opportunities, but at the same time it also harbours risks:

- In the IoT, every networked device is currently a potential target for hackers. Almost every day there are reports of networked devices being hacked, ranging from control being taken over a car’s steering to interference with the functioning of an anaesthesia device. In by far the majority of cases, it is at weak points in the software that hackers manage to gain unauthorised access.
- No user of a networked device – be it a business or a consumer – can be absolutely sure that the device only features those functions and only executes those dataflows that have been specified by the persons or bodies authorised to do so. Thus for devices in the IoT, it is not possible to trace the dataflows and functions actually carried out.

In order to ensure that data is protected and guarantee the security of networked devices in future, thereby strengthening trust in our networked day-to-day and commercial life, regulatory precautions are called for that minimise risk, are neutral in technological terms, and remain open to innovation. They need to relate to all sectors and to cover the entire components of the networked devices for one thing as well as the overall system architecture for another, in order to enable the devices to communicate in a manner that ensures data security and privacy to common standards. The purpose of certification is to ensure that the networked devices marketed in the EU meet the following minimum requirements:

- Communication with other IoT devices and data processing are standardised and are always done using an integrity-secured or where necessary encrypted channel.
- Proper authentication of the communication partners is required.
- The functions with which each device is equipped, the type of data processing that is done, and the devices to which data are transmitted are all clearly stated.
- Only authorised persons may modify the communication and function settings.
In compliance with data protection law, a space should be provided where authorised persons only can optionally specify the purpose for which authorised third parties are allowed to use certain data from the networked device. At the same time, networked devices should constantly meet the latest technical standards. In order to guarantee these measures for protecting users and their data, a regulatory framework needs to define **basic minimum requirements**. Exactly how the arrangements take into account the state-of-the-art in technology, or the needs of specific sectors or lines of business, should be left up to tried and tested self-management processes, such as standardisation.

In this context, independent inspection agencies provide a guarantee – along the lines of a “security TÜV” – of compliance with the uniform minimum requirements yet to be defined. Other approaches, such as exclusive self-regulation or the creation of merely internal group standards, fail to produce the regulatory framework urgently required for this important technological development. A ban on marketing technical devices that do not satisfy certain minimum standards and an order to protect internal IT infrastructure from attack are already laid down in European and German law. Nonetheless, the statutory regulations in force (e.g. IT Security Act; Energy Management Act) are aimed only at certain business sectors and special areas of use. With the phenomenal increase in the number of networked devices, however, risks are not restricted merely to these few areas; on the contrary, they ensue from the very existence of the devices and their networking in itself. The minimum requirements therefore need to apply irrespective of the walk of life or area of business that is concerned. Right now, fixing minimum standards for a highly networked world that is both secure and trustworthy offers a unique opportunity for creating safer and more reliable systems right from the beginning.

**II. Introduction**

In the networked world of the Internet of Things (“IoT”), the main challenges pinpointed by the German Government in its Digital Agenda are the protection of users, security, and system controllability. According to current estimates, at least 50 billion devices and things will be networked with each other by the year 2020. Data protection and the safety of information and communication technology (“ICT”) are prerequisites for trust in digital services and in new business models. Secure networked devices must exist as a matter of principle, so that the data created in the Web is better protected and to enable safe communication.

The current legal environment in Germany and Europe only provides partial answers – restricted to certain fields of use and lines of business – to questions regarding data protection as well as IT security for the IoT infrastructure. However, cross-sector specifications are required that fully protect all devices and their data.

An important aim of the German Government’s Digital Agenda, namely “to ensure a high level of security in digital transformation by means of **statutory requirements** or **generally binding standards**”, thereby “taking measures to safeguard the trustworthiness of digital infrastructures”, can only be achieved if the EU – or in a first step, Germany – pushes ahead with uniform cross-sector specifications for **security in the Internet of Things**, regulating the admissibility and marketability of IoT devices and at the same time implementing the principles of “**Security by Design**” and “**Privacy**
by Design”, and moreover guarantees verifiable minimum security requirements by means of an independent inspection agency – a kind of “security TÜV”.

III. Starting point

1. What is the “Internet of Things”?

In the Internet of Things, all kinds of electronic devices will be interconnected with other electronic devices in future. In principle, that can apply to any object at all (e.g. motor vehicles, household appliances, production machinery).

This has relevance not only for each individual person, who will be able in future to use an App to set the heating on his way home or his smart watch to send medical data to his health insurer, but also for products as well as for development, production and marketing processes in trade and industry – for instance, when robots used in automotive manufacturing exchange data with one another.

2. Opportunities – But Risks As Well

The Digital Agenda defines “smart cities” as the components needed for a modern and efficient infrastructure, comprising elements such as “automatic identification in inland waterway transport; digital planning in the construction industry; smart and efficient house connections and networking amongst buildings; and other ways of achieving integrated sustainable civic development for urban areas”. In this example of actual uses, the German Government sees a huge opportunity for all concerned in the Internet of Things: citizens can reduce their energy consumption, have their health checked by requesting a remote diagnosis of their medical data, or reduce the accident risk in a smart city by driving connected cars. Businesses can save costs in production processes, improve the data basis for their development projects and optimise services for their customers.

Nonetheless, it is agreed that networking in the Internet of Things involves a significant increase in security risks. Over 50% of medium-sized businesses see IT security risks as a threat, and thus they are reluctant to join the so-called fourth industrial revolution (“Industrie 4.0”).

- There will be more weak points prey to attack, because more points of contact with the Web itself will exist. On top of which, devices and connections will have to be secured that has not been possible to secure to date, or that have not previously needed securing because no networking previously existed.
- With more parties networking, the probability of identity theft and misuse will significantly increase, and the consequences of such incidents will potentially be much more serious.
- The increasing number of networked devices – and above all the fact that in future, a large number of devices with IoT connectivity will carry out functions without them being consciously controlled by human beings, depending on the individual circumstances – will increase the level of protection needed for each device’s actual functions, also against attacks launched internally. If adequate technical solutions are not employed right from the start to ensure that a device really does only carry out those functions for which it is intended, only collects and processes those data that it is meant to collect and process, and exclusively processes data obtained from a trustworthy party, then the time and cost of controlling and security will no longer be affordable.
The volume of data will be bigger, and there will be far more information that can be gleaned from the data. On top of which there will be the possibility of correlating data, and this will enable new insights that were not previously possible to be obtained from highly sensitive confidential data (“Big Data”).

These risks are real and can become life threatening.

- For instance, an IT specialist succeeded recently in hacking into an anaesthesia device. From the laptop used on that occasion, it was possible to take over control of the medical device, to halt the breathing apparatus and even to block the device’s entire functions. Hackers have also managed to take over an infusion device, which would mean that they could modify the dosage of the medication being administered.
- Security experts in Vienna have managed to access networked light bulbs and even door locks.
- In the USA, IT researchers have succeeded in de-activating the brakes of a Corvette sports car from a smartphone. They gained access through a weak point in the telematic device of an American insurance company.

From IT security risks, further related risks ensue – namely risks that threaten the protection of personal data on the one hand and of business know-how and trade secrets on the other, not to mention operational safety. The success of the Internet of Things and a positive response from society and business alike will decisively depend on security in this hyper-networked environment being guaranteed at a structural level. If this is to be achieved, **uniform minimum requirements are needed for security in the Internet of Things.**

### 3. Risks Insufficiently Heeded to Date

The risks for devices networked in the Internet of Things are not adequately addressed in legislation:

- Laws on data protection aim exclusively to regulate the handling of personal data; IT security only plays a secondary role.
- Current laws (or bills) on data protection do not specifically focus on the Internet of Things and do not aim for a given level of IT security to be achieved generally.

In terms of legislation on IT security, the IT Security Act does not serve any general purpose – although the name of the statute might suggest that it does – instead of which it is protective legislation for selected critical infrastructures: the legislator rightly acknowledges that the IT infrastructures of economic sectors of particular importance for public welfare (electricity, atomic power, transport, health, water) merit protection. In order to ensure vital uniform protection of the overall IT infrastructure of this whole area of fundamental importance for society, the operators of such critical infrastructures undertake to implement special protective measures – after all, the state’s ability to function depends on the availability of its infrastructure. So metaphorically speaking, it is a matter of not leaving half the country sitting in the dark or unable to phone or without any water supply, simply because of some IT security issue.
In view of their specific objective, it is logical that the statutory regulations on taking technical security measures in practice are only implemented in a limited area of daily or business life. In keeping with its very structure and objective, the IT Security Act makes no provision for more general rules that prescribe minimum standards for the protection of devices, people or data networked in the Internet of Things.

However, the risks inherent in the Internet of Things are rather different, because the Internet of Things is ubiquitous. In future, networked devices will be found in all spheres of life. The decisive issue will be the safety of all users of networked devices, no matter whether use takes place at a manufacturer’s production plant (“Industrie 4.0”) or when IoT products are being put to practical use (connected driving, networked household appliances, etc.).

Consequently, both existing laws and proposed legislation lack the basic approach vital for regulating the Internet of Things, namely an approach that is generally applicable technologically and does not favour any particular interests, and which focuses at a structural level on the protection of IoT devices and on the secure generation and transmission of data in a networked world in all walks of life. The diversity and randomness of the areas affected by the Internet of Things should therefore be reflected in the generally binding nature of minimum requirements laid down for marketing secure devices. In view of the ubiquity of the IoT and the pace of change, a mere “snapshot” for differentiating between infrastructures that are of greater or lesser importance for the public welfare cannot be allowed to play a part when it comes to protecting networked devices.

IV. Imperative Measures

For efficient and sustainable development of the IoT in Germany and Europe that is built on trust, transparency, and planning and legal certainty, cross-sector obligations are still lacking that demand certified standards of security at the networked devices’ structural and technical level. This is a matter of creating trust in the integrity and confidential handling of data, trust in the functions of the networked devices, and trust in the way they communicate with other connected appliances. In order to achieve this, measures need to be taken.

The following measures are proposed:

- **“Security by Design”**

  An essential starting point is a certified security structure by default. This includes the obligation to safeguard the integrity and where necessary ensure the encryption of information as well as of transmission channels. Effective reciprocal authentication of the IoT devices must be made possible. These default settings should be designed without technological or application restrictions to avoid lock-in effects.

  Building on the minimum requirements, the devices must also allow the security level to be fixed that is required for the respective purpose. Moreover, it must be ensured that all concerned can trust in the standards thus specified and in their compliance. Only allowing networked devices to carry out specifically defined functions that can be determined only by authorised persons or bodies must already be implemented as a matter of course.
In short: security must be firmly rooted in the devices ex works, and its implementation at product level must be tested and confirmed in existing and proven certification procedures that are recognised as being state-of-the-art. This aims to ensure that a uniform minimum degree of security is fixed for all IoT devices.

- “Privacy by Design”

Everyone acting in the Internet of Things – no matter whether individual persons or business entities – must be able to decide for themselves what happens with the data they produce and for what purposes this may be done. The most important prerequisites for this are transparency and technical protection against misuse.

Thus, manufacturers of IoT devices, whilst complying with technical security obligations, should also make sure that only the actual user of a device has authority to modify the device’s parameters as fixed by the manufacturer. Here, in contrast to common DRM, the user has control over the data of the IoT device. This would mean that it is possible to decide flexibly in future which device has to satisfy which requirements.

All devices connected to the Internet of Things should only communicate those data which are required in the specific case in hand, or which has consciously been decided to disclose to others (need-to-know principle). In technical terms, if devices are designed with a view to data safety, this can also contribute directly towards protecting the purposes of data collection and data processing as laid down in data protection law.

Defining IT security as a structural issue opens up a big opportunity for furthering the aims of data protection (data minimisation, limiting data processing to the degree appropriate to the processing activity being carried out and its objectives, control, transparency and options for data subjects). “Privacy by Design” will also be an essential obligation for data processing that is imposed on controllers under the forthcoming EU General Data Protection Regulation (cf. Art. 23 of the proposal).

Thus for instance, only the entity responsible for billing should be able to decode accounting data from smart services. Similarly, a production machine should only be able to use the data needed for its particular stage in production. The technologies required for implementing such requirements already exist: they are almost always based on use of cryptographic protocols in combination with secure hardware, e.g. as for vehicle-to-vehicle and vehicle-to-infrastructure communication under the IEEE 1609.2 Standard.

- Independent Inspection Agencies

These principles of “Security by Design” and “Privacy by Design” lay down a binding minimum dimension for security and trust in the networked world. The technical rules and standards that are required can be established and certified afterwards by the responsible bodies or competent authorities, many of which already exist.
One example of such an agency is the Federal Office for Information Security (Bundesamt für Sicherheit in der Informationstechnik, “BSI”), which in the field of networked systems already performs comparable tasks for RFID technology (access control, smart meter gateway security modules). Agencies that have the relevant qualifications and the necessary experience also exist in other EU Member States, e.g. the Agence nationale de la sécurité des systèmes d’information (“ANSSI”) in France, as well as at a European level, e.g. the European Union Agency for Network and Information Security (“ENISA”) based in Greece.

In addition, private bodies can by all means check compliance with technical specifications, provided these bodies are duly officially certified. A qualified electronic signature is just one example here: the Federal Network Agency (Bundesnetzagentur) inspects private providers of certification services, and providing the results are positive, it awards a quality seal indicating that the service provider’s technical and administrative security have been fully tested and approved. The service provider then in turn issues the secure certificates to private individuals and to business enterprises.

V. Summary

Our society has reached a disruptive technological turning point. It is hard to forecast now what the hyper-networking of our everyday and business world will mean for the interaction of players in the legal field. But one thing is clear: rules are needed that still remain viable in the future. Because the Internet of Things as an open architecture of networked systems can no longer be protected in the manner that has worked to date for analogue systems or closed networks. Taking a structural approach with “Security by Design” and “Privacy by Design” is the right path to take. It offers a unique opportunity now to build safe and more reliable systems from the start.

From areas of law regulating specific sectors, such as the Energy Management Act and the appurtenant Metering System Ordinance, the German legislator is already acquainted with the basic concept of making networked devices secure and with the measures needing to be taken:

> “An efficient smart grid therefore calls for secure IT and telecommunications technologies, even at the early stages of data input and initial transmission at the smart meter gateway, which as a communication unit assumes the key role in the security structure of a smart metering system.”

This approach can be applied to all networked devices in the all-embracing Internet of Things which the future holds. If uniform minimum requirements for secure and trustworthy networked devices are to succeed, this whole issue will have to be tackled and implemented quickly. This is because technological development is progressing at a tremendous speed and is currently promoted almost exclusively by Big Data corporations, who implement IT security in their own interests but are barely concerned about basic standards that might protect individuals or the economy as a whole. The de facto standards thus brought about, once they have become established, can scarcely be influenced subsequently. Uniformly fixed minimum security requirements can not only prevent the emergence of these de facto standards that are hardly geared towards the public welfare: instead, they can even create a separate and thriving market for innovations that further privacy and security.
One of the strong points of the German security industry lies in the development and implementation of systems that – based on special solutions certified for security purposes – offer protection against attacks e.g. for payment transactions, smartphones or secure gateways. Thus, Germany is well equipped for introducing security standards, and the pan-European economy would have a head start in the competition for innovative products.

Not only individual members of the public and businesses developing security technologies, but also this country’s economy generally, would stand to gain from basic IT security in the Internet of Things. German companies in particular are a constant target of industrial espionage at the hands of both private individuals and other countries. Against this background, the IoT and the networking of manifold devices that it implies pose a risk for both business and society. Generally binding security standards are a well-proven remedy here. Thus, the structural approach can be not only an innovation driver, but also for numerous companies a prerequisite for introducing new technologies:

- Smart integrated cryptographic **security architecture** will enable Germany and Europe to set their own control points and curb the unwanted outflow of data. The German Government’s Digital Agenda also states that we need “further extend our technological systems expertise and reduce dependencies”.
- **System controllability** is indispensable when it comes to working with new technologies – right from the start as an innovation driver, not just once the technologies have become established elsewhere. Trust cannot be created without system controllability.
- The technical architecture and dataflows must be made **transparent**.
- **Legal certainty**: if at all possible, the legal system – if it is to retain its relevance at all, and if the impression of an emerging “cyber-Western” is to be avoided – must regulate reality right from the start.
- If businesses take security precautions in future that follow minimum standards laid down by law, this will **save costs** for the general public. So far, society has had to balance losses sustained when companies fail to invest in digital security.
- **Control** over the data they have generated can be returned to consumers.

VI. **Sources**

1 For the successful hacking of a Jeep in the USA, see ([http://www.faz.net/aktuell/feuilleton/medien/wie-zwei-hacker-vom-sofa-aus-einen-jeep-ubernnehmen-13715866.html](http://www.faz.net/aktuell/feuilleton/medien/wie-zwei-hacker-vom-sofa-aus-einen-jeep-ubernnehmen-13715866.html)), and for the manipulation of an anaesthesia device, see ([http://www.spiegel.de/netzwelt/netzpolitik/hacker-manipuliert-narkosegeraet-a-1047258.htm](http://www.spiegel.de/netzwelt/netzpolitik/hacker-manipuliert-narkosegeraet-a-1047258.htm)).
7 Federal Data Protection Act, Telemedia Act and other German statutes specific to certain sectors, but also the EU Data Protection Regulation 1995/46/EC currently in force and the planned EU General Data Protection Regulation.
8 Particular mention should be made of the IT Security Act and the EU’s proposed Network and Information Security (NIS) Directive.
9 cf. Federal Ministry for Economic Affairs and Energy (BMWi), draft Metering System Ordinance, p. 17.