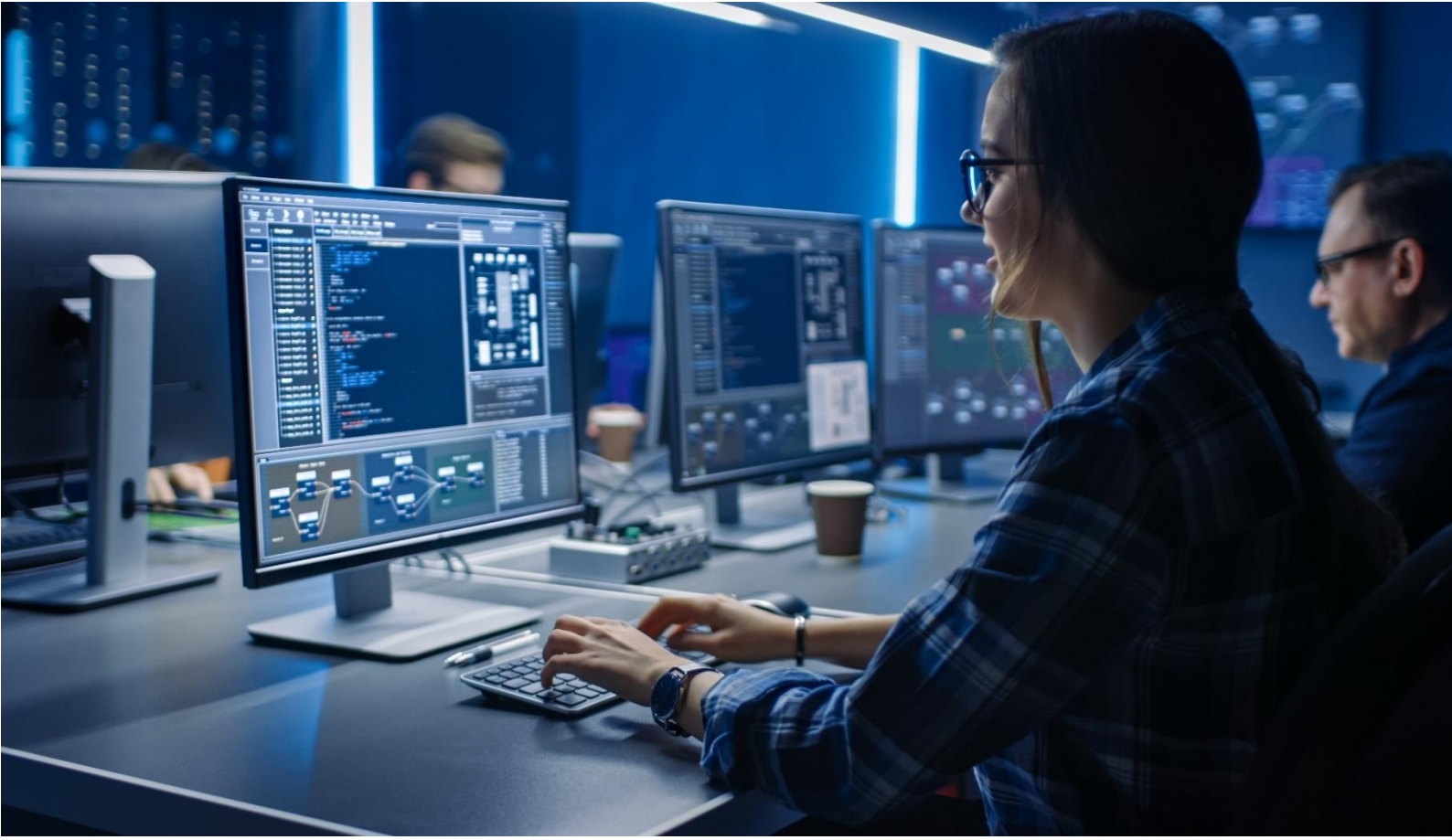

White Paper on Cybersecurity & Certification for IoT Devices

October 2021

Executive summary

28% of people who do not own a smart device will not buy one due to security concerns. Security of the devices definitely needs to evolve to reduce the user mistrust. Orange is, and wants to remain a trustworthy operator for its customers and end users. This White Paper is focused on the needs for security and certification of IoT devices for both Consumer IoT and Industrial IoT markets.

At the European level, the Cybersecurity Act started a recent evolution in regulation and other regions are also started this move.

On the security aspects, IoT ecosystems are only as safe as the weakest link in the system. At Orange, we would prefer the best practices for security being shared instead of the weaknesses. We promote the Zero Trust approach for IoT services and a security by design for IoT devices in our own security requirements.

This trust in IoT devices will come thanks to robust and clearly standardized protection mechanisms, allowing a common understanding and an efficient, shared and verifiable implementation. This is the certification process. The construction of a certification for IoT devices is the coming years challenge.

We do not see the certification as an end in itself but rather as the achievement of a common wish of the players to move forward in the same direction to enable a safer market for IoT devices supported by an appropriate future-proof regulatory framework.

orange™

Within Orange, we believe that the robustness and resilience of digitalized activities relying on connected products are critical topics for both Industry and Consumers.

User expectations move as fast as the consumer market and recent research from Consumers International and Internet Society reveals that 28% of people who do not own a smart device will not buy one due to security concerns. Security of the devices needs to evolve to reduce the user mistrust.
Orange is, and wants to remain a trustworthy operator for its customers and end users. The world of IoT opens up the market to a myriad of objects with technologies, designs and purposes that are so heterogeneous that the network operator cannot be in a position to fully control all the devices. It is necessary to have a minimum of guarantees about the security of the device by itself, regardless of the network it will be attached to.

This White Paper is focused on the security of IoT devices for both Consumer IoT and Industrial IoT markets. It deals solely with the device itself, without making any assumptions about the security mechanisms implemented within the network or the IoT service platforms it is connected to.

The Cybersecurity Act started a recent evolution in regulation.

Adopted by the EU (European Union) in June 2019, the Cybersecurity Act established a new European cybersecurity framework and granted ENISA a permanent mandate to establish the certification framework facilitating the preparation of EU certification schemes to be recognized in all EU countries. According to the Cybersecurity Act, strategic priorities for future European cybersecurity certification schemes are provided by EC (European Commission) in consultation with the ECCG and SCCG groups.

The EU has also a legal instrument provided by the RED (Radio Equipment Directive): 2014/53/EU. Indeed, the RED establishes a regulatory framework for placing radio equipment on the market by setting essential requirements for safety and health, electromagnetic compatibility, and the efficient use of the radio spectrum. The RED also provides the basis for further regulation for the protection of privacy, personal data and against the fraud.

On its side, ECSO (European Cyber Security Organization) has positioned itself as a key actor in the European standardization and certification institutional landscape by contributing to the EC via the SCCPG and ENISA. In its task, ECSO is also collaborating with CEN CENELEC JTC13 and ETSI.

In a first analysis, the Cybersecurity Act foresees three assurance levels for the future European certificate: Basic, Substantial and High and suggests that the assignment to the assurance levels will be based on a vulnerability assessment (or risk assessment).

In the updated EU Cybersecurity Strategy of December 2020, the EC highlighted the need for developing standards of cybersecurity for connected devices, certification of devices and services, as well as responsibility of manufacturers for maintenance and updates of their products.

An important point that we see in the whole picture is to avoid the geographical fragmentation of requirements and to eliminate duplicated (country and regional) certification schemes.

IoT ecosystems are only as safe as the weakest link in the system.

IoT devices are often singled out as being a source of vulnerabilities. Some of those risks are intrinsic to the device capabilities like the ability to interact with the real world through actuators which can create new opportunities for malicious operations. Many examples exist: taking control of a connected lock to facilitate a robbery or stealing personal data and intellectual property through a compromised camera. Some attack scenarios can even endanger lives, like a hack of a connected pacemaker, the modification of a car trajectory, or compromise a whole company through a hack of a single device (e.g. taking control of industrial systems in an automated factory).

Today, it is unfortunately not very complicated to perform an attack to an IoT device. The wide variety of hacking tools (development kits repurposed as attacks tools, open source programs…) that are easy to obtain, and the increasing number of devices sharing a common code base or hardware components may lead to huge impacts caused by a single vulnerability**.** Multiple IoT devices serving different functions are based on the same software component.

At Orange, we would prefer the best practices for security being shared instead of the software weakness.

One of the key questions is how to be able to quickly fix the vulnerabilities as soon as are identified (e.g. when they are made public in CVEs - Common Vulnerabilities and Exposures database). Fixing vulnerabilities may also be limited by the technological choices made by device manufacturers. For instance, a very low power protocol is typically not meant to exchange more than a few hundred bytes per day, thus downloading a new firmware of a few Kb/s is tricky and, as a consequence Over The Air (OTA) firmware update features are sometimes not implemented at all or are optional.

The sheer number of inter-connected devices increases the attack surface, makes it easier for a vulnerable device to be “within reach”, then finally causes a chain reaction (eg. Retrieve the Wi-Fi key from a connected doorbell).

The security of a system should always be considered as a whole and even technologies designed with security, if misused may be irrelevant for the overall product security. As an example, using encryption for a proprietary radio protocol may be totally useless if there is no anti-replay mechanism in place and an attacker could simply record and replay the radio signals using a Software Defined Radio tool. Even standardised protocols used with an improper configuration, may be a source of vulnerability (e.g. security not enabled in configuration, use of a default and publicly known encryption key…).

In terms of global security, the hacking of a device may be used as an entry point to attack a device management platform. In a successful attack the whole fleet of devices could be taken over through the configuration and update orders. Since it is almost impossible to

guarantee that security issues will not arise at one point of time, one should always consider that other devices in a network may have been compromised. This is the zero-trust approach.
Devices may implement measures to protect against this, such as only accepting signed firmware images and proposing a way to reset the device to a known good configuration. Secure elements like a (e)UICC can help against cloning by keeping the authentication keys secure in a certified hardware, but the question of who (device owner, network operator X, network operator Y) should be allowed to use that secure element is still opened.

Zero Trust approach for IoT services and security by design for IoT devices.

Actors involved in designing IoT devices are globally aware of security threats related to IoT but they may not be sufficiently invested in the field of security to address all the risks. It is essential to rely on the security experts at every step: design of the radio protocol, network applications, operating system, bootloader, hardware, user interface…

The impact of a vulnerability in an IoT device are summarised below:

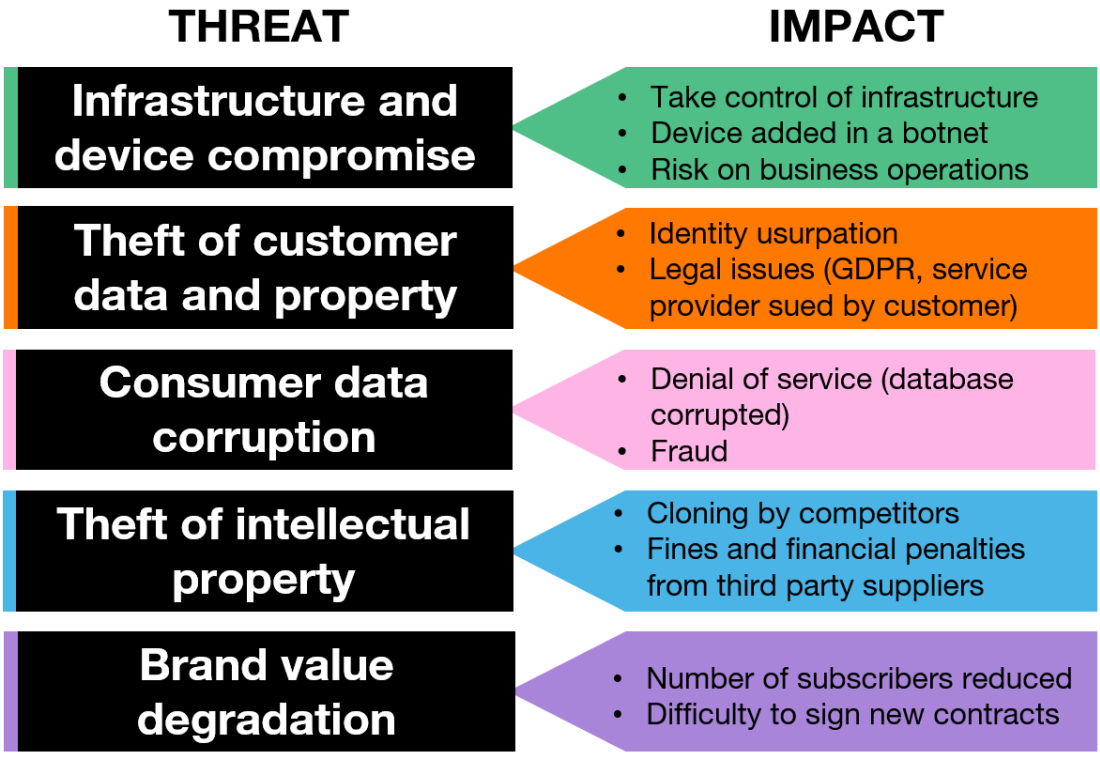

Figure 1 Common vulnerabilities impact

Orange is vigilant about the security risks of all objects being offered through our sales channels.
The certification processes need to support all kinds of Consumer IoT and Industrial IoT products such as Heath, Smart metering, Industry 4.0, Cameras, Trackers, Gateways, etc. It must also support various operating systems, form factors of products and a wide variety of connectivity interfaces such as Ethernet, Wi-Fi, LoRaWAN, Bluetooth, DECT, Zigbee, Thread, Matter, etc.

The certification processes must also take into account the operational need to deploy functional and security updates on products during their lifecycle as well as the associated constraint of the process and cost of (re-)certification which must not be a barrier to deploy such updates.

Construct a certification for IoT devices is the coming years challenge

Considering all the diversity behind IoT, a one-size-fits-all certification scheme cannot provide good security assurance to the market because it will only result in very generic and weak requirements in order to be applicable to all sets of products.
In this regard, multiple IoT security certification schemes based on different levels (Basic, Substantial and High) should co-exist.
A multi-layer approach would be a mix of:

- Certification level (based on risk assessment),
- Use cases provided for the device, and
- Category of devices (consumer, industrial, gov/state, etc.)

The certification schemes will also need to prove themselves as efficient for the industry. This would for example require evaluation performed by third parties for benchmarking the efficiency. It may take a couple of years before the different schemes will reach this level of maturity and before being fully recognized and trusted by all industry players including Orange.

Orange has already worked on defining a risk assessment evaluation, security requirements and security evaluation methodology. Security testing relies on both the conformity checks and the identification of vulnerabilities through pen-testing. Before selling a product in our channels, we verify that it has adequate security level for the targeted use case through various steps (paper assessment, security contracts, pen-testing, …)

Orange has defined its own security levels as follows:

Orange "Basic" security level

Intended to protect against simple remote attacks that do not require knowledge of credentials/keys that are only meant to be known by the end user (e.g. default WiFi key, customized admin password…). The requirements included in this level are a must have for any device.

A high-level view of what should be in the Basic level is summarised below:

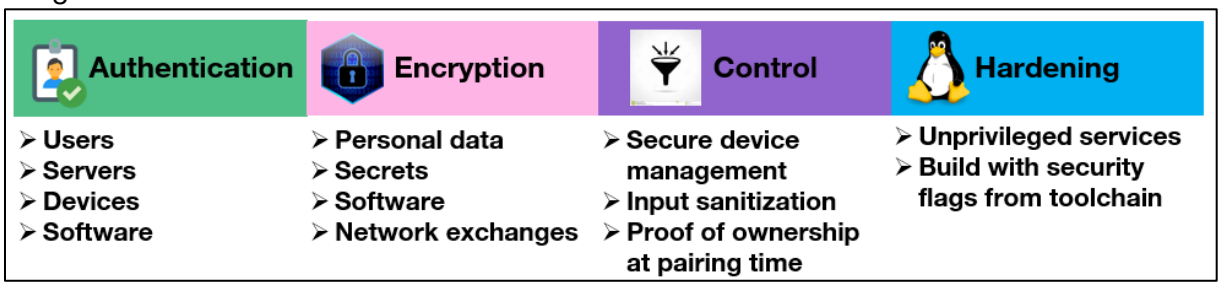

Figure 2 Building blocks for Basic level

Orange "Substantial" security level

Leverages on requirements from Basic level and adds further protection against both remote attacks with knowledge of credentials and unsophisticated hardware attacks when a direct access to the device hardware is possible (opening the device and/or connection on a hardware interface).

The Substantial certification level is required in many cases, such as:

- The device contains sensitive personal data (e.g. health information, video camera stream, payment information), or credentials giving access to a wireless network (e.g. Wi-Fi key) and is either installed in an unprotected location (e.g. doorbell in the street) or is likely to be lost/stolen due to its portable nature (e.g. drone, tracker);
- The device may be used to attack service platforms and impact the service as a whole (e.g. the platform implicitly trusts data sent by a device authenticating itself with pre-provisioned keys);
- The end-user may have a motivation to hack the device to perform fraud (e.g. smart meter, devices with paying services like VoIP);
- The device is rented to the end user and must be protected against tampering;
- The device is critical for a security service (e.g. security camera, connected lock).

A high-level view of what should be in the Substantial level is summarised below:

Mitigating HW attacks	Ensuring software authenticity	Assessing conformity
➢ Hardware debug ports locked (SWD, UART…) ➢ No logs on HW interfaces ➢ Firmware stored encrypted ➢ Data stored encrypted with device-unique key	➢ Software authentication chain relying on root of trust in chipset ➢ No permissive open source licenses (e.g. GPLv3) ➢ Hardened operating system	➢ Security tests by independent security lab

Figure 3 Main additions of Substantial level compared to Basic level

Orange "High" security level

This High level adds further hardware protections (e.g. use of a Trusted Execution Environment) and operating system hardening mechanisms (e.g. use of Linux Security Modules) but is out of scope of this document.

While having Basic assurance level will be the strict minimum for Consumer IoT market, it is also important to push for the definition of Substantial requirements that will be required in many cases (see "Substantial" cases above) and address the following problems faced with the Basic level:

- self-assessment may lead to an incorrect conformity check due to a lack of expertise;
- some devices require protection against threats other than remote attacks by an unauthenticated attacker;
- some provisions are optional in the current candidate schemes for a Basic level.

Certification is a real challenge: firstly, by the cost of the certification process which may limit the market expansion and secondly, by its geographical impact which may limit the adoption in case of multiplicity of local certifications.

For its design, a good certification process needs a clear and testable certification scheme that will be the result of well identified and specified security requirements.

Specification of security requirements is an important piece of the puzzle where standardization bodies have the first role to play. Orange is deeply involved in standardization, as well as convinced that implementing normative security rules is the best way to streamline the security design. Standardization helps to avoid non-identified loopholes or system crashes, but also to achieve multivendor interoperability and mutualize cost.

The main standards organizations (IETF, 3GPP, ITU-T…) integrate security requirements in their specifications, but they may be limited at some points when it concerns the device in particular.
IoT specific standards also include security and some of them concern the devices (LoRaWAN, OneM2M, Zigbee…). Finally, in the whole diversity of IoT standardized solutions or de facto standard, there is an heterogeneity in the way the security of the device is included (or not).

In its 2021 Rolling Plan for ICT standardization [1], the European Commission gives a panel of technical specifications that can help to achieve the EU policy objectives. With the general concern about the security of the devices that are less controlled by the service providers it has been created some dedicated initiatives. Among the standards developing IoT solutions, we can highlight the following initiatives that define requirements impacting the devices:

ETSI TC Cyber firstly worked on a set of IoT security requirements specification which became a European Norm (EN), the EN 303 645 "Consumer IoT devices security baseline" [2].
ETSI TC Cyber also set out test scenarios for assessing products against EN 303 645 with TS 103 701 "Cybersecurity assessment for consumer IoT products" [3]. TS 103 701 is intended to be used by testing labs and certification bodies that provide assurance on the security of IoT products, as well as manufacturers that wish to carry out a self-assessment.

ISO/IEC JTC 1/SC 27 provides a guidance on the basic, commonplace security features expected of all IoT devices enabling the IoT security controls with draft ISO/IEC 27402 "Cybersecurity — IoT security and privacy - Device baseline requirements" [4]. This standard is intended to be a user-agnostic baseline for both Consumer IoT and Industrial IoT requirements.

CEN/CENELEC JTC 13 is working on adoption of ISO/IEC norms at European level. JTC 13 and ETSI TC Cyber groups have created a joint working group with the objective to work on IoT certification schemes and particularly on the substantial level of EN 303 645 which does not exist yet. CEN/CENELEC JTC 13 is also consulted by EC (via ENISA) to provide horizontal standards applicable to the security requirements of RED articles.

GSMA is working on several topics related to IoT devices having a cellular connectivity (SIM, eSIM or ieUICC).

- IoT security Guidelines was one of the first workgroup on some “golden” security rules and produced "GSMA IoT Security Guidelines" [5]. These guidelines are a set of documents, describing different types of security constraints and requirements to which IoT device and IoT networks must be compliant. In addition, GSMA provided an assessment checklist to enable the suppliers of IoT products, services and components to self-assess the conformity of their products and publish the results on a voluntary basis. For its contribution, Orange was awarded as IoT Security Champion by GSMA for the adoption of GSMA IoT Security Guidelines.
- More recently, a new security standard named IoT SAFE "IoT SIM Applet For Secure End-2-End Communication" [6], proposes to use a SIM card (SIM, eSIM or ieUICC) as a tamper resistant hardware to perform some cryptographic operations and store secrets in order to secure IoT services. Orange presented a prototype of Arduino Starter Kit using IoT SAFE applet at the MWC (Mobile World Congress) in June 2021.

Standardization bodies are working to make the IoT security stronger and some of them are focusing a part of their effort on the devices. This normative work shows the common desire to move forward with more security by design for devices and not only at the network level.

In the past years, some leader device manufacturers have developed their own solutions with proprietary protocols that ensure device security including a kind of self-certification. Those spontaneous initiatives are welcomed but their effect is today limited by the small number of iconic devices concerned and the fact they cannot offer interoperability with the rest of the ecosystem on security elements.

There is a global awareness that regulation will be a key driver to create a safer market but also that we cannot force manufacturers to comply with national-level regulations for sensors having a value of a few cents per unit in a worldwide market.
While there is a general commitment, the global regulation is fragmented in several regions depending on their policy and interest to address this topic at the present time:

- The US governmental National Institute for Standards and Technology (NIST) is working on a "IoT Device Cybersecurity Capability Core Baseline";
- India and Australia both have draft Codes for national regulation;
- UK government has a Code of practices. The UK’s IoT "security by design" law; and
- At the European level, countries are joining their forces to work on the topics as members of certain EU agencies like ENISA.

One relevant indicator of the national ongoing progress with IoT device certification is to see that the ETSI standard EN 303 645 is now mentioned in several national regulation documents and official organisations in Finland, Singapore, India, UK, Australia… and some organisations have already based their products and certification schemes on EN 303 645. The US NIST has cross-referenced the ETSI standards in its IoT security guidance.

In this global trend, we can also note the Cybersecurity Tech Accord which is a worldwide initiative launched in 2018. The Cybersecurity Tech Accord is a public commitment of over 151 company signatories including Orange, which oversee important aspects of the world's communication and information infrastructure, to protect and empower civilians online and to improve the security, stability and resilience of cyberspace.

In the IoT ecosystem, several interests and constraints have to find their place and the security should be a driver as well as the business opportunity.

Looking at the IoT device certification, we are convinced that a unique type of certification is not possible and not wanted due to the diversity of the devices and the use cases.

Looking at the most advanced standard, EN 303 645, it still leaves some doors open through the use of optional provisions: critical security parameters "should" be encrypted in transit, the confidentiality of personal data transiting between a device and a service "should" be protected... This unfortunately makes this standard inferior to what Orange wants for a Basic level.
The cornerstone of an efficient certification of IoT devices is the set of security requirements on which the certification schemes are based.

In addition to the basic level, the substantial level of security seems to Orange a 'must-have' for a large number of devices that will be embedded in B2B offers or used for critical services concerning user safety and data security. We keep encouraging standardization bodies to be more demanding and stricter on the Basic level to provide real technical benefits in terms of security to the market and we also encourage the Substantial level requirements standardization. The idea is not to create standardized devices in the reduced vision of the standards, doing all the same thing the same way. The purpose is to offer a guarantee of the appropriate security protection by having standardized mechanisms against known, and unknown, threats. With this goal of common security by design, we also promote the adoption of horizontal standards, while at the same time being vigilant about the fact that such standards must not be too vague and have to establish clear recommendations for the main technologies that are typically included in IoT devices.

Having requirements specifications may not be sufficient to derive the certification schemes and therefore, an assessment document will be essential to ensure a correct interpretation of the standards in particular in case of self-assessment or declarative compliance. From our perspective, the certification of the capability for a device to perform software updates for radio chipsets will be critical. However, we believe that the risk assessment process should be rather quick (maximum 1 day) and that the risk assessment for a substantial level must be performed by an authorized security lab rather than by the company itself. In a first phase, we support the voluntary compliance to certification schemes to encourage the market adoption.

Finally, we can say that having current best practice rules shared as widely as possible (worldwide or regionally) will be the only way for customers to have trust in the device they buy, for the device manufacturer to be sure that their product is secure and for the service provider to protect the network, its users and their data. This trust in IoT devices will come thanks to robust and clearly standardized protection mechanisms, allowing a common understanding and an efficient, shared and verifiable implementation. This is the certification process.
We do not see the certification as an end in itself but rather as the achievement of a common wish of the players to move forward in the same direction to enable a safer market for IoT devices supported by an appropriate future-proof regulatory framework.

References

1. Rolling Plan for ICT standardisation 2021 https://joinup.ec.europa.eu/collection/rolling-plan-ict-standardisation/rolling-plan-2021
2. EN 303 645 (and TS 103 645) Cyber Security for Consumer Internet of Things: Baseline Requirements https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf
3. TS 103 701 Cybersecurity assessment for consumer IoT products https://docbox.etsi.org/CYBER/CYBER/05-CONTRIBUTIONS/2019//CYBER(19)018041_Commenting_Table_ETSI_TS_103_701_V_0_0_1.docx
4. ISO/IEC CD 27402 Cybersecurity – IoT security and privacy – Device baseline requirements https://www.iso.org/standard/80136.html
5. GSMA IoT Security Guidelines Overview Document https://www.gsma.com/iot/wp-content/uploads/2020/05/CLP.11-v2.2-GSMA-IoT-Security-Guidelines-Overview-Document.pdf
6. GSMA IoT.04 Common Implementation Guide to Using the SIM as a 'Root of Trust' to Secure IoT Applications v1.0 https://www.gsma.com/iot/wp-content/uploads/2019/12/IoT.04-v1-Common-Implementation-Guide.pdf