Guidelines for Privacy and Security in IoT

Pasquale Annicchino
Archimede Solutions
Geneva, Switzerland
pannicchino@archimede.ch

Simone Seminara, Francesco Capparelli
Istituto Italiano per la Privacy e la Valorizzazione dei Dati
Rome, Italy
{s.seminara, f.capparelli}@ istitutoprivacy.eu

***Abstract*— Norms and standards define the ecosystem in which IoT solutions are developed and deployed. It is often difficult for people without a legal training or an understanding of standardization dynamics to fully grasp the state of the art in this very relevant field. This contribution aims at highlighting the most relevant tools available and explaining their relevance.**

***Keywords*— Data protection; privacy; security; Internet of Things; guide-lines.**

I. Introduction: Mapping the Landscape

A. Relevance of the exercise

The mapping of international security and data protection by design guidelines is of paramount relevance in the identification of best practices in the context of IoT. With regard to the implementation and demonstration of appropriate technical and organizational measures as referred in Articles 24(1)-(3), 25, and 32(1)-(3) of the General Data Protection Regulation (GDPR) [1], the literature on data protection is extensive, ranging from regulations to privacy-enhancing technologies and rules that are general. Without any objective of completeness, which would be outside the scope of this contribution, we briefly introduce below some of the best-known approaches to data management and data protection from a technical perspective (among those freely available online) which might be useful also for researchers with no previous legal training.

First of all, the European Union Agency for Cybersecurity (ENISA) in the eminent document *Privacy and Data Protection by Design* [2] declares eight general strategies for implementing the principle of "privacy by design" as defined in the GDPR: minimise, hide, separate, aggregate, inform, control, enforce and demonstrate.

Another important approach to formulate general principles for the protection of personal data and cybersecurity is the one developed by the Information & Privacy Commissioner of the State of Ontario, Canada. This work [3] proposes seven general principles: Proactive not Reactive (Preventative not Remedial); Privacy as the Default Setting; Privacy Embedded into Design; Full Functionality (Positive-Sum, not Zero-Sum); End-to-End Security (Full Lifecycle Protection); Visibility and Transparency (Keep it Open); Respect for User Privacy (Keep it User-Centric).

It should also be noted that there are several non-legal frameworks resulting from the application of international cybersecurity standards and, therefore, the present document is useful to provide a mapping of the actual international standards, guidelines and best practices regarding IoT.

B. Regulations

Almost all the articles of the GDPR provide the European interpretation of the concept of personal data protection, specifying several rights for citizens with regard to the processing of their personal data. Rights such as access and limitation are well detailed in the Regulation, which therefore gives control over the data primarily to the individual to whom the data are related. To complement this, there are three articles referring to cybersecurity, without which data protection would inevitably be compromised. Article 32 outlines the security measures, while Articles 33 and 34 the notification obligations in case of data breach.

In relation to the focus on the IoT systems in this document, however, it should be noted that the GDPR is not entirely explicit on how an IoT device should protect data. The manufacturers are therefore obliged to supply products that comply with the Regulation and to ensure that the companies that will (acquire and then) use them can operate in accordance with the Regulation. Finally, Article 25 outlines provisions on data protection by design and by default, i.e. already by design and by default, taking over the concepts outlined in Articles 5 (on "data minimization") and 32 (on security measures, mentioning in particular "pseudonymization"). However, it is completely implicit what characteristics an application must have in order to be considered GDPR-compliant.

The processing of personal data within the IoT framework often sees the interaction between the system and its operator, the latter being authorised to the specific processing possible through the use of the given IoT device. In particular, the authorisation to the processing – as mandated by the GDPR – details the areas of the processing itself, i.e. what and how the authorised person is allowed to process personal data. There is then a so-called *ceremony* between device and operator, i.e. a protocol distributed and enacted between machines and human beings. Sometimes such a protocol may involve several persons or even none: the GDPR defines the latter case as *automated processing*.

The articles of the GDPR can be interpreted as a set of requirements, aimed at achieving the general objective of personal data protection, for the participants in the ceremony/protocol mentioned above.

This work has been partially supported by NGIoT [52], a Coordination and Support Action funded by European Union's Horizon 2020 research and innovation programme (H2020-EU.2.1.1.) under grant agreement ID 825082.

II. Relevant guidelines

In this paragraph we detail general guidelines, reviews and mappings which can be applied to the world of the Internet of Things as a whole. Each subsection details one of the organisations involved in such publications.

A. OWASP

The Open Web Application Security Project (OWASP) [4] is a nonprofit foundation that works to improve the security of software through its community-led open source software projects. One of its flagship projects is the *OWASP Top 10* [5], a standard awareness document for developers and web application security; it represents a broad consensus about the most critical security risks to web applications.
Here are two of its publications about IoT.

1) OWASP IoT Top 10, 2018 (previous version in 2014)

Along the lines of the widely known Top 10 for web apps, the *OWASP IoT Top 10* [6] focuses on things to avoid when building, deploying or managing IoT systems. The list is:

1) *Weak, Guessable, or Hardcoded Passwords.* Use of easily brute forced, publicly available, or unchangeable credentials, including backdoors in firmware or client software that grants unauthorised access to deployed systems.
2) *Insecure Network Services.* Unneeded or insecure network services running on the device itself, especially those exposed to the internet, that compromise the confidentiality, integrity/authenticity, or availability of information or allow unauthorised remote control.
3) *Insecure Ecosystem Interfaces.* Insecure web, backend API, cloud, or mobile interfaces in the ecosystem outside of the device that allows compromise of the device or its related components. Common issues include a lack of authentication/authorization, lacking or weak encryption, and a lack of input and output filtering.
4) *Lack of Secure Update Mechanism.* Lack of ability to securely update the device. This includes lack of firmware validation on device, lack of secure delivery (un-encrypted in transit), lack of anti-rollback mechanisms, and lack of notifications of security changes due to updates.
5) *Use of Insecure or Outdated Components.* Use of deprecated or insecure software components/libraries that could allow the device to be compromised. This includes insecure customization of operating system platforms, and the use of third-party software or hardware components from a compromised supply chain.
6) *Insufficient Privacy Protection.* User's personal information stored on the device or in the ecosystem that is used insecurely, improperly, or without permission.
7) *Insecure Data Transfer and Storage.* Lack of encryption or access control of sensitive data anywhere within the ecosystem, including at rest, in transit, or during processing.
8) *Lack of Device Management.* Lack of security support on devices deployed in production, including asset management, update management, secure decommissioning, systems monitoring, and response capabilities.
9) *Insecure Default Settings.* Devices or systems shipped with insecure default settings or lack the ability to make the system more secure by restricting operators from modifying configurations.
10) *Lack of Physical Hardening.* Lack of physical hardening measures, allowing potential attackers to gain sensitive information that can help in a future remote attack or take local control of the device.

2) OWASP IoT Top 10 2018 Mapping Project

This project [7] provides mappings of the OWASP IoT Top 10 2018 [6] to industry publications and sister projects, such as:

- OWASP IoT Top 10, previous version (2014) [8];
- GSMA IoT Security Assessment Checklist [9] (see also § 2.3.2);
- Department for Digital, Culture, Media & Sport (UK Government), *Code of Practice for Consumer IoT Security* [10] (see § 2.2.1);
- ENISA Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures, 20 November 2017 [11] (see § 2.4.1);
- CTIA Cyber-security Certification Test Plan for IoT Devices [12][13] (see § 2.5);
- CSA IoT Security Controls Framework [14][15] (see § 2.5);
- ETSI Technical Specification (TS) 103 645 V1.1.1 (2019-02), *CYBER; Cyber Security for Consumer Internet of Things* [16].

Since this Mapping Project, ETSI published an updated version of the above standard [17] and its European counterpart [18].
From this starting point, in the following subsections we will explore these publications.

B. UK Government, Department for Digital, Culture, Media & Sport

The Department for Digital, Culture, Media & Sport (DCMS) [19] helps to drive growth, enrich lives and promote Britain abroad. Among other activities, the DCMS commissioned the *PETRAS IoT Research Hub* [20], a consortium of universities and research institutions that work together to explore critical issues in privacy, ethics, trust, reliability, acceptability and security of the IoT to conduct two literature reviews: on industry recommendations for government to improve IoT security; on the current international developments around IoT security. The two aims to these reviews, jointly published in [21], were to identify the key themes emerging from the literature and to identify international consensus around core Security by Design principles for the IoT.

1) Code of Practice for Consumer IoT Security, 14 October 2018

The DCMS, in conjunction with the UK National Cyber Security Centre (NCSC) [22] and following engagement with industry, consumer associations and academia, has developed this Code of Practice [10] (see § 2.1.2) to support all parties involved in the development, manufacturing and retail of consumer IoT with a set of guidelines to ensure that products are secure by design and to make it easier for people to stay secure in a digital world. The Code of Practice brings together, in thirteen outcome-focused guidelines, what is widely considered good practice in IoT security. The Code was first published in draft in March 2018 as part of the *Secure by Design* collection of reports [23].

An indication is given for each guideline as to which stakeholder is primarily responsible for implementation. Stakeholders are defined as Device Manufacturers, IoT Service Providers, Mobile Application Developers and Retailers. The thirteen guidelines are:

1) *No default passwords.* All IoT device passwords shall be unique and not resettable to any universal factory default value.
2) *Implement a vulnerability disclosure policy.* All companies that provide internet-connected devices and services shall provide a public point of contact as part of a vulnerability disclosure policy in order that security researchers and others are able to report issues. Disclosed vulnerabilities should be acted on in a timely manner.
3) *Keep software updated.* Software components in internet-connected devices should be securely updateable. Updates shall be timely and should not impact on the functioning of the device. An end-of-life policy shall be published for end-point devices which explicitly states the minimum length of time for which a device will receive software updates and the reasons for the length of the support period. The need for each update should be made clear to consumers and an update should be easy to implement. For constrained devices that cannot physically be updated, the product should be isolatable and replaceable.
4) *Securely store credentials and security-sensitive data.* Any credentials shall be stored securely within services and on devices. Hard-coded credentials in device software are not acceptable.
5) *Communicate securely.* Security-sensitive data, including any remote management and control, should be encrypted in transit, appropriate to the properties of the technology and usage. All keys should be managed securely.
6) *Minimise exposed attack surfaces.* All devices and services should operate on the 'principle of least privilege'; unused ports should be closed, hardware should not unnecessarily expose access, services should not be available if they are not used and code should be minimised to the functionality necessary for the service to operate. Software should run with appropriate privileges, taking account of both security and functionality.
7) *Ensure software integrity.* Software on IoT devices should be verified using secure boot mechanisms. If an unauthorised change is detected, the device should alert the consumer/administrator to an issue and should not connect to wider networks than those necessary to perform the alerting function.
8) *Ensure that personal data is protected.* Where devices and/or services process personal data, they shall do so in accordance with applicable data protection law, such as the GDPR. Device manufacturers and IoT service providers shall provide consumers with clear and transparent information about how their data is being used, by whom, and for what purposes, for each device and service. This also applies to any third parties that may be involved (including advertisers). Where personal data is processed on the basis of consumers' consent, this shall be validly and lawfully obtained, with those consumers being given the opportunity to withdraw it at any time.
9) *Make systems resilient to outages.* Resilience should be built in to IoT devices and services where required by their usage or by other relying systems, taking into account the possibility of outages of data networks and power. As far as reasonably possible, IoT services should remain operating and locally functional in the case of a loss of network and should recover cleanly in the case of restoration of a loss of power. Devices should be able to return to a network in a sensible state and in an orderly fashion, rather than in a massive scale reconnect.
10) *Monitor system telemetry data.* If telemetry data is collected from IoT devices and services, such as usage and measurement data, it should be monitored for security anomalies.
11) *Make it easy for consumers to delete personal data.* Devices and services should be configured such that personal data can easily be removed from them when there is a transfer of ownership, when the consumer wishes to delete it and/or when the consumer wishes to dispose of the device. Consumers should be given clear instructions on how to delete their personal data.
12) *Make installation and maintenance of devices easy.* Installation and maintenance of IoT devices should employ minimal steps and should follow security best practice on usability. Consumers should also be provided with guidance on how to securely set up their device.
13) *Validate input data.* Data input via user interfaces and transferred via application programming interfaces (APIs) or between networks in services and devices shall be validated.

2) Mapping of IoT Security Recommendations, Guidance and Standards to the UK's Code of Practice for Consumer IoT Security, 14 October 2018

This document [24], and the open data files and graphs provided in its companion website [25], maps the Code of Practice for Consumer IoT Security against published standards, recommendations and guidance on IoT security and privacy from around the world. Around 100 documents were reviewed from nearly 50 organizations. Whilst not exhaustive, it represents one of the largest collections of guidance available to date in this area.

The purpose of the mapping is to serve as a reference and tool for users of the Code of Practice. Manufacturers and other organisations are already implementing a range of standards, recommendations and guidance and will seek to understand the relationship between the Code of Practice and existing material from industry and other interested parties.

C. GSMA

The GSM Association (GSMA) [26] represents the interests of mobile operators worldwide, uniting more than 750 operators with almost 400 companies in the broader mobile ecosystem, including handset and device makers, software companies, equipment providers and internet companies, as well as organisations in adjacent industry sectors.

1) GSMA IoT Security Guidelines, version 2.2, 29 February 2020

The goal of the Internet of Things Security Guidelines document set [27][28][29][30] is to provide the implementer of an IoT technology or service with a set of design guidelines for building a secure product. The set of guideline documents promotes a methodology for developing secure IoT Services to ensure security best practices are implemented throughout the life cycle of the service. The documents provide recommendations on how to mitigate common security threats and weaknesses within IoT Services.

2) GSMA IoT Security Assessment

The GSMA IoT Security Assessment [31][32] (see § 2.1.2) provides a flexible framework that addresses the diversity of the IoT market, enabling companies to build secure IoT devices and solutions as laid out in the *GSMA IoT Security Guidelines* (see § 2.3.1), a comprehensive set of best practices promoting the secure end-to-end design, development and deployment of IoT solutions.

D. ENISA

The European Union Agency for Cybersecurity [33] has been working to make Europe cyber secure since 2004. The Agency works closely together with Members States and other stakeholders to deliver advice and solutions as well as improving their cybersecurity capabilities. It also supports the development of a cooperative response to large-scale cross-border cybersecurity incidents or crises and since 2019, it has been drawing up cybersecurity certification schemes.

1) ENISA Good practices for IoT and Smart Infrastructures Tool

This website [34] intends to provide an aggregated view of the ENISA Good Practices for IoT and Smart Infrastructure [35] that have been published the last years. This link comprises the above-mentioned *Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures* [11] (see § 2.1.2) and then other publications about cars, hospitals, airports, public transport and Industry 4.0.

E. Other sources and references

In this subsection we mention other miscellaneous sources about privacy and security in IoT.

CTIA [36] represents the U.S. wireless communications industry and companies throughout the mobile ecosystem and has organised a certification programme for the cybersecurity of IoT devices [12, 13] (see § 2.1.2).

The Cloud Security Alliance (CSA) [37] is an organization dedicated to defining and raising awareness of best practices to help ensure a secure cloud computing environment, including the Internet of Things with specific security controls [14, 15] (see § 2.1.2).

The Internet of Things Security Foundation (IoTSF) [38] is a collaborative, nonprofit, international response to the complex challenges posed by cybersecurity in the expansive hyper-connected IoT world. Among its publications, listed in [39], we can cite [40][41].

The World Wide Web Consortium (W3C) [42] is an international community that develops open standards to ensure the long-term growth of the Web. It is led by Tim Berners-Lee, the inventor of the Web. Its *Web of Things* (WoT) section [43] seeks to counter the fragmentation of the IoT through standard complementing building blocks (e.g. metadata and APIs) that enable easy integration across IoT platforms and application domains; to date, two W3C Recommendations have been published about WoT [44][45].

Of course, international standards developing organisations (SDOs) – whose members are governmental bodies, agencies or committees, one per member economy – have published IoT-related standards. We can cite the ITU-T Y.4000 series from the International Telecommunication Union (ITU) [46][47] and a few of those jointly published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) [48][49][50].

Lastly, we show a glimpse of other relevant international standards, under development or just finished. This list is taken from the outcome of the 2020-04-10 webinar *Integrating privacy in the IoT ecosystem* [51], organised by the Horizon 2020 project *Next Generation Internet of Things* (NGIoT) [52], with the participation of Antonio Kung:

- ISO/IEC TR 20547-1, *Information technology — Big data reference architecture — Part 1: Framework and application process*, first edition published August 2020
- ISO/IEC TR 20547-2:2018, *Information technology — Big data reference architecture — Part 2: Use cases and derived requirements*, first edition published January 2018
- ISO/IEC 20547-3:2020, *Information technology — Big data reference architecture — Part 3: Reference architecture*, first edition published March 2020
- ISO/IEC 20547-4, *Information technology — Big data reference architecture — Part 4: Security and privacy*, first edition published September 2020
- ISO/IEC TR 20547-5:2018, *Information technology — Big data reference architecture — Part 5: Standards roadmap*, first edition published February 2018
- ISO/IEC CD 23751, *Information technology — Cloud computing and distributed platforms — Data sharing agreement (DSA) framework*
- ISO/IEC CD 27400.2, C*ybersecurity – IoT security and privacy – Guidelines* (formerly known as ISO/IEC CD 27030, *Information technology — Security techniques — Guidelines for security and privacy in Internet of Things (IoT)*)
- ISO/IEC CD TS 27101, *Information technology — Security techniques — Cybersecurity — Framework development guidelines*

- ISO/IEC CD 27556, *Information technology — User-centric framework for the handling of personally identifiable information (PII) based on privacy preferences*
- ISO/IEC WD 27557, *Organizational privacy risk management*
- ISO/IEC WD TS 27560, *Privacy technologies — Consent record information structure*
- ISO/IEC AWI 30149, *Internet of things (IoT) — Trustworthiness framework*
- ISO/AWI 31700, *Consumer protection — Privacy by design for consumer goods and services*

III. Conclusion

Guidelines are important tools for different stakeholders involved in the deployment of IoT solutions. They offer key basic points and requirements to enhance the trust of end-users and facilitate deployment. The documents highlighted in this contribution show that an important amount of work has been already done by several organisations and deserves to be taken into account.

Following the recommendations provided by the mapped international standards, therefore, allows to respect the principles of the GDPR: for example, the international standards referred to the development phase are useful to respect the "privacy by design" principle set in Article 25 GDPR; the standards on the security of personal data processing are functional to the respect of Article 32 GDPR.

As a side note, the application of the principles of the GDPR is not sufficient in cases where such processing of personal data should concern Law Enforcement Agencies (LEAs). According to the provisions of Article 29 of Directive (EU) 2016/680 [53], in fact, the data controller may use an accountability mechanism in the evaluation and adoption of technical-organisational measures. In any case, the aforementioned measures must be suitable to guarantee an adequate level of security in order to avoid the risk of personal data violation.

In general, it is useful to use all international standards as guidelines and to deduce the best practices necessary to achieve a level of security that can generate trust in end-users and simultaneously achieve compliance with the main regulations. All the mapping efforts across different security controls and publications show that the amount of redundancies is very high: we can then state that a consensus, a "common sense" has emerged in the field of IoT cybersecurity and privacy. Moreover, from a broader perspective, we can say that IoT security measures overlap consistently with cybersecurity frameworks and standards already in place for "traditional computing": consider, for instance, ISO/IEC 27001:2013 [54] and the *Common Criteria for Information Technology Security Evaluation* [55][56][57][58][59][60].

It is paramount at legislation level to properly address the need to go beyond what the GDPR and the NISD (Network and Information Security Directive) [61] today represent. With the progress of technology, is obvious that lawmakers have the duty to follow rapidly the new challenges that arise from the evolution in the societal and economic global landscape. In this sense, the integration of IoT in homes, cities and industries gives the legislators the opportunity (or necessity?) to build a new legal framework to comply with ethical requirements, to better protect freedoms and rights of citizens, at an increasingly supranational and intergovernmental level. A "GDPR of Things" is therefore urgent, with an expanded scope from previous laws, in order to establish stricter rules and norms for information security and personal data protection in World that moves fast towards "ubiquitous computing" (IoT, 5G, wearables, etc.).

In parallel with new legislative frameworks, it would be preferable a consolidation of standards and best practices carried forward by SDOs and the private sector in an open and interoperable way, before the proliferation of "walled gardens" that may compromise freedoms and rights of citizens worldwide.

References

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of per-sonal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance); current consoli-dated version (2016-05-04) available at https://eur-lex.europa.eu/eli/reg/2016/679/2016-05-04

[2] European Union Agency for Cybersecurity (ENISA), Privacy and Data Protection by Design – from policy to en-gineering, 12 January 2015; PDF available at https://www.enisa.europa.eu/publications/privacy-and-data-protection-by-design/

[3] Information & Privacy Commissioner (Ontario, Cana-da), Ann Cavoukian, The 7 Foundational Principles. Im-plementation and Mapping of Fair Information Practices; PDF available at https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-implement-7found-principles.pdf

[4] OWASP Foundation, Inc.; https://owasp.org/

[5] OWASP Top 10; https://owasp.org/www-project-top-ten/

[6] OWASP IoT Top 10, 2018; https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=IoT_Top_10

[7] OWASP IoT Top 10 2018 Mapping Project; https://scriptingxss.gitbook.io/owasp-iot-top-10-mapping-project/ and https://wiki.owasp.org/index.php/OWASP_Internet_of_Things_Project#tab=OWASP_IoT_Top_10_2018_Mapping_Project

[8] OWASP IoT Top 10, 2018; https://wiki.owasp.org/index.php/Top_10_IoT_Vulnerabilities_(2014)

[9] https://www.gsma.com/security/resources/clp-17-gsma-iot-security-assessment-checklist-v3-0/

[10] https://www.gov.uk/government/publications/code-of-practice-for-consumer-iot-security/

[11] https://www.enisa.europa.eu/publications/baseline-security-recommendations-for-iot/

[12] CTIA, IoT Cybersecurity Certification Program Manage-ment Document, version 1.1, May 2019; PDF available at https://api.ctia.org/wp-con-tent/uploads/2019/05/ctia_IoT_cybersecurity_pmd_ver-1_1.pdf

[13] CTIA, IoT Cybersecurity Certification FAQ, version 1.0, 28 March 2019; PDF available at https://api.ctia.org/wp-content/uploads/2019/03/CTIA-Certification-FAQ-Ver-1.0-28-March-2019.pdf

[14] CSA, IoT Security Controls Framework, 5 March 2019; https://cloudsecurityalliance.org/artifacts/iot-security-controls-framework/

[15] CSA, Guide to the IoT Security Controls Framework, 5 March 2019; https://cloudsecurityalliance.org/artifacts/guide-to-the-iot-security-controls-framework/

[16] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/01.01.01_60/ts_103645v010101p.pdf

[17] https://www.etsi.org/deliver/etsi_ts/103600_103699/103645/02.01.02_60/ts_103645v020102p.pdf

[18] ETSI European Standard (EN) 303 645 V2.1.1 (2020-06); https://www.etsi.org/deliver/etsi_en/303600_303699/303645/02.01.01_60/en_303645v020101p.pdf

[19] https://www.gov.uk/government/organisations/department-for-digital-culture-media-sport/

[20] https://petras-iot.org/

[21] PETRAS IoT Hub, Summary literature review of industry recommendations and international developments on IoT se-curity, 7 March 2018; https://www.gov.uk/government/publications/summary-literature-review-on-iot-security/

[22] https://www.ncsc.gov.uk/

[23] https://www.gov.uk/government/collections/secure-by-design/

[24] https://www.gov.uk/government/publications/mapping-of-iot-security-recommendations-guidance-and-standards/

[25] Copper Horse Ltd. on behalf of DCMS, Mapping Securi-ty & Privacy in the Internet of Things; https://iotsecuritymapping.uk/

[26] GSM Association; https://www.gsma.com/

[27] GSMA, IoT Security Guidelines Overview Document; https://www.gsma.com/iot/iot-security-guidelines-overview-document/

[28] GSMA, IoT Security Guidelines for IoT Service Ecosystem; https://www.gsma.com/iot/iot-security-guidelines-for-iot-service-ecosystem/

[29] GSMA, IoT Security Guidelines Endpoint Ecosystem; https://www.gsma.com/iot/iot-security-guidelines-for-endpoint-ecosystem/

[30] GSMA, IoT Security Guidelines for Network Operators; https://www.gsma.com/iot/iot-security-guidelines-for-network-operators/

[31] GSMA, IoT Security Assessment Checklist, version 3.0, 30 September 2018; .zip file available at https://www.gsma.com/iot/iot-security-assessment/

[32] GSMA, IoT Security Assessment Process, version 2.0, 30 September 2018; .zip file available at https://www.gsma.com/iot/iot-security-assessment/

[33] https://www.enisa.europa.eu/

[34] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/good-practices-for-iot-and-smart-infrastructures-tool/

[35] https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/

[36] https://www.ctia.org/

[37] https://cloudsecurityalliance.org/

[38] https://www.iotsecurityfoundation.org/

[39] https://www.iotsecurityfoundation.org/best-practice-guidelines/

[40] IoTSF, IoT Security Compliance Framework, Release 2.1, May 2020; .zip file available at https://www.iotsecurityfoundation.org/wp-content/uploads/2020/05/IoTSF-IoT-Security-Compliance-Framework-Questionnaire-Release-2.1.zip

[41] IoTSF, Mapping the IoT Security Foundation's Compliance Framework to ETSI TS 103 645 Standard, February 2019; PDF available at https://www.iotsecurityfoundation.org/wp-content/uploads/2019/02/Mapping-the-IoTSF%E2%80%99s-Compliance-Framework-to-ETSI-TS-103-645-Standard.pdf

[42] https://www.w3.org/

[43] https://www.w3.org/WoT/

[44] W3C, Web of Things (WoT) Architecture, W3C Recom-mendation, 9 April 2020; https://www.w3.org/TR/wot-architecture/

[45] W3C, Web of Things (WoT) Thing Description, W3C Rec-ommendation, 9 April 2020 (link errors corrected 23 June 2020); https://www.w3.org/TR/wot-thing-description/

[46] ITU-T Recommendation Y.4000/Y.2060 (approved in 2012-06-15); SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS AND NEXT-GENERATION NETWORKS; Next Generation Networks – Frameworks and func-tional architecture models; Overview of the Internet of things (former ITU-T Y.2060 renumbered as ITU-T Y.4000 on 2016-02-05 without further modification and without being republished); https://www.itu.int/rec/T-REC-Y.4000

[47] https://www.itu.int/ITU-T/recommendations/index.aspx?ser=Y

[48] ISO/IEC 21823-1:2019, Internet of things (IoT) — Interop-erability for IoT systems — Part 1: Framework, February 2019; https://www.iso.org/standard/71885.html

[49] ISO/IEC 21823-2:2020, Internet of things (IoT) — Interop-erability for IoT systems — Part 2: Transport interoperabil-ity, April 2020; https://www.iso.org/standard/80986.html

[50] ISO/IEC 30141:2018, Internet of Things (loT) — Reference Architecture, first edition published August 2018 (sec-ond edition pending); https://www.iso.org/standard/65695.html

[51] https://www.ngiot.eu/event/ngiot-webinar-integrating-privacy-in-the-iot-ecosystem/

[52] https://cordis.europa.eu/project/id/825082

[53] Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of per-sonal data by competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penal-ties, and on the free movement of such data, and re-pealing Council Framework Decision 2008/977/JHA; current consolidated version (2016-05-04) available at https://eur-lex.europa.eu/eli/dir/2016/680/2016-05-04

[54] ISO/IEC 27001:2013, Information technology — Security techniques — Information security management systems — Requirements; https://www.iso.org/standard/54534.html

[55] ISO/IEC 15408-1:2009, Information technology — Securi-ty techniques — Evaluation criteria for IT security — Part 1: Introduction and general model, December 2009 (cor-rected version January 2014); https://www.iso.org/standard/50341.html

[56] ISO/IEC 15408-2:2008, Information technology — Securi-ty techniques — Evaluation criteria for IT security — Part 2: Security functional components, August 2008 (corrected version May 2011); https://www.iso.org/standard/46414.html

[57] ISO/IEC 15408-3:2008, Information technology — Securi-ty techniques — Evaluation criteria for IT security — Part 3: Security assurance components, August 2008 (corrected version May 2011); https://www.iso.org/standard/46413.html

[58] ISO/IEC DIS 15408-4, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities, under development; https://www.iso.org/standard/72913.html

[59] ISO/IEC DIS 15408-5, Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements, under development; https://www.iso.org/standard/72917.html

[60] ISO/IEC 18045:2008, Information technology — Security techniques — Methodology for IT security evaluation, Au-gust 2008 (corrected version January 2014); https://www.iso.org/standard/46412.html

[61] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and in-formation systems across the Union; https://eur-lex.europa.eu/eli/dir/2016/1148/oj