ETSI SR 003 680 V1.1.1 (2020-03)

SmartM2M;
Guidelines for Security, Privacy and Interoperability in IoT System Definition;
A Concrete Approach

Reference
DSR/SmartM2M-003680

Keywords
interoperability, IoT, IoT platforms, oneM2M
privacy, SAREF, security, semantic

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Special Report (SR) has been produced by ETSI Technical Committee Smart Machine-to-Machine communications (SmartM2M).

Modal verbs terminology

In the present document "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

IoT systems are often seen as an extension to existing systems created by the (potentially massive) addition of networked devices to an existing system to enlarge its capabilities. However, in a growing number of ICT systems, the IoT part becomes the core of the overall system and the place where a large part of the value is created.

Though many of the characteristics of IoT systems may be found in other ICT-based systems, the main challenge with IoT systems is that they should address simultaneously a number of high-level issues like e.g. stakeholders' involvement, technology choices, deployment model, and integration with/of legacy.

The complexity of these challenges for IoT raises a very large range of questions that should be addressed across the whole lifecycle of any IoT system (from its inception to its development, deployment and even de-commissioning). The approach to IoT systems specification, development and deployment taken in the present document is based on the analysis of typical examples (Use Cases) which have been selected in order to cover a broad panel of sectors and to answer some of the most pressing questions of the readers from a strategy, management and technology perspective.

The present document focuses on questions related to privacy, security, platforms interoperability and semantic interoperability that are addressed from different angles and not just from a simple technical perspective. Tables present "Frequently Asked Questions" with the intent to illustrate major questions in IoT, and their solutions in an easily digestible form.

The present document offers some strategic, operational and technical guidelines, which intend to fix the issues addressed in it.

Annexes of the present document contain representative Use Cases (eHealth, Smart Buildings, Industrial IoT, IoT-based Mission Critical Communications) relating to the issues addressed in the present document and contain material and references for further reading as short descriptions of the Technical Reports already produced by ETSI, technical material and others.

1 Scope

1.1 Context for the present document

The design, development and deployment of - potentially large - IoT systems require to address a number of topics - such as security, interoperability or privacy - that are related and should be treated in a concerted manner. In this context, several Technical Reports have been developed that each address a specific facet of IoT systems.

- ETSI TR 103 533: "Security; Standards Landscape and best practices" [i.1].
- ETSI TR 103 534: "Teaching Material: Part 1 (Security) [i.2] and Part 2 (Privacy)" [i.3].
- ETSI TR 103 535: "Guidelines for semantic interoperability in the industry" [i.4].
- ETSI TR 103 536: "Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms" [i.5].
- ETSI TR 103 537: "Plugtests™ preparation on Semantic Interoperability" [i.6].
- ETSI TR 103 591: "Privacy study report; Standards Landscape and best practices" [i.7].

In order to provide a global and coherent view of all the topics addressed, a common approach has been outlined across the above Technical Reports (TRs) concerned with the objective to ensure that the requirements and specificities of the IoT systems are properly addressed and that the overall results are coherent and complementary.

The present document has been built with this common approach also applied in all of the TRs listed above.

1.2 Scope of the present document

The present document intends to be a high-level document for the general public and is not specifically addressing a technical audience (e.g. designers, developers, etc.). It is introducing, in a relatively non-technical manner, to some of the main issues that individuals and organizations should address when they face the development of an IoT system. A strong emphasis is put on interoperability, security, privacy and standards in support.

Based on the analysis of representative Use Cases (eHealth, Smart Buildings, Industrial IoT, IoT-based Mission Critical Communications), which are documented in Annex A, and relating to (and updating) the guidelines developed in the TRs listed in clause 1.1, it provides guidelines for Security, Privacy and Interoperability in IoT System Definition.

The present document is structured as follows:

- Clauses 1 to 3 set the scene and provide references as well as definition of terms, symbols and abbreviations, which are used in the document on hand.
- Clause 4 explains the approach to IoT systems specification, development and deployment taken in the present document. This approach is based on the analysis of typical examples (also termed as Use Cases) which have been selected in order to cover a broad panel of sectors (e.g. eHealth or Smart Buildings) and to answer some of the most pressing questions of the readers from a strategy, management and technology perspective. The clause also suggests how the rest of the document should be read in order to maximize the findings for the readers.
- Clause 5 focuses on questions related to **privacy, security and interoperability (platforms interoperability and semantic interoperability)** that are addressed from different angles and not just from a simple technical perspective. The text in this clause is mostly presented in the form of a "Frequently Asked Questions" (FAQ) information sheet with the intent to illustrate major questions in IoT, and their solutions, in an easily digestible form. The questions also refer to the associated Technical Reports (detailed in Annex B) and the use case examples (detailed in Annex A).
- Clause 6 offers some strategic, operational and technical guidelines, which intend to fix the issues addressed in clause 5.
- Clause 7 provides observations and lessons learned from the addressed issues and analysis of Use Cases.

- Annex A documents representative Use Cases (eHealth, Smart Buildings, Industrial IoT, IoT-based Mission Critical Communications) relating to the issues addressed in clause 5 and guidelines provided in clause 6.
- Annex B contains short descriptions of the Technical Reports listed in clause 1.1, as well as technical material and others for further reading.

2 References

2.1 Normative references

Normative references are not applicable in the present document.

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long-term validity.

The following referenced documents are not necessary for the application of the present document, but they assist the user with regard to a particular subject area.

[i.1] ETSI TR 103 533: "SmartM2M; Security; Standards Landscape and best practices".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103533/01.01.01_60/tr_103533v010101p.pdf.

[i.2] ETSI TR 103 534-1: "SmartM2M; Teaching material; Part 1: Security".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/10353401/01.01.01_60/tr_10353401v010101p.pdf.

[i.3] ETSI TR 103 534-2: "SmartM2M; Teaching material; Part 2: Privacy".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/10353402/01.01.01_60/tr_10353402v010101p.pdf.

[i.4] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103535/01.01.01_60/tr_103535v010101p.pdf.

[i.5] ETSI TR 103 536: "SmartM2M; Strategic/technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103536/01.01.02_60/tr_103536v010102p.pdf.

[i.6] ETSI TR 103 537: "SmartM2M; Plugtests™ preparation on Semantic Interoperability".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103537/01.01.01_60/tr_103537v010101p.pdf.

[i.7] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103591/01.01.01_60/tr_103591v010101p.pdf.

[i.8] ETSI TR 103 582: "EMTEL; Study of use cases and communications involving IoT devices in provision of emergency situations".

NOTE: Available at https://www.etsi.org/deliver/etsi_tr/103500_103599/103582/01.01.01_60/tr_103582v010101p.pdf.

[i.9] 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 personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), OJ 2016 L 119/1.

[i.10] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, OJ L 303.

[i.11] Directive 2011/24/EU Of The European Parliament And Of The Council of 9 March 2011 on the application of patients' rights in cross-border healthcare, OJ L 88.

[i.12] 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 information systems across the Union (NIS Directive).

[i.13] AIOTI WG03 Release 4.0, 2018: "High Level Architecture (HLA)".

NOTE: Available at https://aioti.eu/wp-content/uploads/2018/06/AIOTI-HLA-R4.0.7.1-Final.pdf.

[i.14] ETSI TS 118 112: "oneM2M; Base Ontology (oneM2M TS-0012)".

[i.15] GDPR & Public Safety, EENA and Bird & Bird, August 2019.

NOTE: Available at https://eena.org/document/gdpr-public-safety/.

[i.16] ISO/IEC 29147: "Vulnerability Disclosure".

[i.17] ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.18] Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).

[i.19] ETSI TS 118 103: "oneM2M; Security Solutions (oneM2M TS-003)".

[i.20] "Privacy Code of Conduct on mobile health apps".

NOTE: Available at https://ec.europa.eu/digital-single-market/en/privacy-code-conduct-mobile-health-apps.

[i.21] ETSI TR 103 305 (all parts): "CYBER; Critical Security Controls for Effective Cyber Defence".

[i.22] ETSI EN 303 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.23] ISO/IEC 27000:2018: "Information technology -- Security techniques -- Information security management systems".

[i.24] BS 10012:2017: "Data protection - Specification for a personal information management system".

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the following terms apply:

denial of service type attacks: cyber-attack in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by temporarily or indefinitely disrupting services of a host connected to the Internet

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

AI	Artificial Intelligence
AIOTI	Alliance for the Internet of Things Innovation
API	Application Programming Interface
BMS	Building Management System
CCTV	Closed Circuit Television
CEO	Chief Executive Officer
CTI	Centre for Testing and Interoperability
CTO	Chief Technical Officer
CXO	Chief eXperience Officer
DCMS	Department of Culture, Media and Sport (a UK Government body)
ECSO	European Cyber Security Organization
ENISA	European Network Information Security Agency
ER	Emergency Room
ETSI	European Telecommunications Standards Institute
EU	European Union
GDPR	General Data Protection Regulation
GSMA	GSM Association (a trade body)
HMI	Human Machine Interface
HVAC	Heating, Ventilation, and Air Conditioning
ICT	Information and Communications Technology
IEA	International Energy Agency
IIoT	Industrial IoT
IoT	Internet of Things
IoT-EPI	IoT-European Platforms Initiative
JSON	Java Script Object Notation
NIS	Network Information Security
NIST	National Institute of Standards and Technology
OCF	Open Connectivity Foundation
PoC	Proof-of-Concepts
PPM	oneM2M Privacy Policy Manager
PSAP	Public Safety Answering Point
SAREF	Smart Applications REFerence ontology
SIM	Subscriber Identity Module
SSN	Semantic Sensor Network
TCG	Trusted Computing Group
TR	Technical Report
TVRA	Threat Vulnerability Risk Analysis
UML	Unified Modelling Language
W3C	World Wide Web Consortium
XML	eXtensible Markup Language

4 Role based analysis of IoT systems

4.1 Challenges

IoT systems are often seen as an extension to existing systems created by the (potentially massive) addition of networked devices to an existing system to enlarge its capabilities. However, in a growing number of ICT systems, the IoT part becomes the core of the overall system and the place where a large part of the value is created.

Though many of the characteristics of IoT systems may be found in other ICT-based systems, the main challenge with IoT systems is that they are required to address simultaneously a number of high-level issues amongst which:

- **Stakeholders involvement:** during the life-cycle (e.g. definition, design, development, deployment) of an IoT system, a large variety of stakeholders with a wide range of roles should be associated in order to ensure that their - potentially conflicting - requirements (regarding e.g. economics, technology, usage) can be considered, discussed and resolved in a concerted manner.

- **Technology choices:** by nature, all IoT systems should integrate potentially very diverse technologies, very often for the same purpose (e.g. communication protocols) with a risk of overlap. A critical aspect is the balance between proprietary and standardized solutions which should be carefully managed, with a lot of potential implications on the choice of the supporting platforms.

- **Deployment model:** a key aspect of IoT systems is that they emerge at the very same time where Cloud Computing and Edge Computing have become mainstream technologies. All IoT systems are facing the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.

- **Integration with/of Legacy:** many IoT systems are requested to deal with legacy (e.g. existing connectivity, back-end ERP systems). The challenge is to deal with the requirements of the legacy part without compromising an "IoT centric" approach which may, as much as possible, favour the demands of the IoT part.

4.2 Issues to address

Given the complexity of the challenges outlined in clause 4.1, a very large span of issues needs to be addressed during the whole lifecycle of an IoT system (from its inception, to its development, deployment and de-commissioning). The present document is addressing issues such as:

- **Interoperability:** there are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc. These requirements also have an impact on the selection of the platform(s) that are expected to concretely support and implement them.

- **Privacy:** in the case of IoT systems that deal with critical data in critical applications (e.g. e-Health, Intelligent Transport, Food, Industrial systems), privacy becomes a make or break property.

- **Security:** as an essential enabling property for Trust, security is a key feature of all IoT systems and needs to be dealt with in a global manner. One key challenge is that it is involving a variety of users in a variety of Use Cases.

Though these issues are rather technology-oriented in nature, they raise questions that cannot be resolved from a simple technical perspective.

4.3 Guidelines

Based on the identified set of issues, the present document is proposing **guidelines** regarding strategy (e.g. how to make choices that globally impact the structure in charge of the IoT system), technology (e.g. what are the main choices to guaranty the development and evolution of the IoT system) and operations (e.g. how to ensure that the choices made can be supported by the structure and the stakeholders involved).

These guidelines are generic in nature. They have been developed by using two complementary sets of information:

- The guidelines developed in the associated set of Technical Reports developed concurrently with the present document (listed in clause 1.1) and relating to the following topics:

  - Privacy Standards and Best Practices

  - Security Standards and Best Practices

  - Teaching Material for Security

  - Teaching Material for Privacy

- Guidelines for using Semantic Interoperability in the Industry
- Preparation of Plugtests™ on Semantic Interoperability
- Interoperability and interworking of existing IoT Platforms

- The generalization of the guidelines and recommendations coming from a set of detailed examples.

4.4 Stakeholders and roles

The present document intends to provide support to a large variety of "stakeholders" involved across the IoT system lifecycle, not only those with a technical role. Examples of the stakeholders concerned by the guidelines are:

- CXOs (e.g. CEO, CTO) involved in the high-level choices related to the IoT system inception;
- System Designer, System Developer, System Deployer;
- End-user;
- Device Manufacturer.

4.5 Detailed examples

Examples from different sectors have been chosen to illustrate the generic (cross-sector) guidelines. The sectors chosen are illustrative of the large span of situations: eHealth, Smart Building, Industrial IoT and Critical Communications.

The analysis made in the detailed examples allows not only to illustrate the generic guidelines in a specific context, but reversely - when significant - to explain how the view from a specific sector can highlight the relevance of a guideline: for example, the privacy aspects are an important element for all use cases, and the analysis of the eHealth example will bring a very important clarification whichever is the reader's sector of interest.

5 Questions to address

5.1 Introduction

The complexity of the challenges for IoT (outlined in clause 4.1) raises a very large range of questions that should be addressed across the whole lifecycle of any IoT system (from its inception to its development, deployment and even de-commissioning). The present document focuses on questions related to **privacy, security and interoperability (platforms interoperability and semantic interoperability)** that are addressed from different angles and not just from a simple technical perspective.

The text in this clause is mostly presented in the form of a "Frequently Asked Questions" (FAQ) information sheet with the intent to illustrate major questions in IoT, and their solutions, in an easily digestible form. The questions also refer to the associated Technical Reports (detailed in Annex B) and the use case examples (detailed in Annex A).

5.2 Privacy

Two associated Technical Reports (ETSI TR 103 591 [i.7] and ETSI TR 103 534-2 [i.3]) and a set of teaching slides have addressed privacy within IoT. The key aspects are that there should be a clear allocation of responsibilities regarding the protection of personal data between the series of entities involved in the provisioning of IoT services.

Table 1 provides examples of possible questions and answers from interested stakeholders.

Table 1: Questions and answers for privacy

Question	Answer	Reference for further information
What are the main challenges facing Privacy in IoT?	The key challenges for privacy in IoT can be summarized as follows: • the high risk of profiling, for example, of a user of an IoT device or for a resident of a smart home; • the lack of transparency resulting from hyper-connectivity hindering individuals to exercise their rights; • increased dependencies raise concerns on the acquisition of a *freely* given and well-informed consent Overall, it seems less likely for the individual to be able to exercise control over the information concerning him and to be able to retain his anonymity within an IoT environment, while the large amounts of data collected create stakes not only at an individual but also at a societal level.	ETSI TR 103 591 [i.7]
Is IoT privacy different from existing privacy concept?	In general, the concept of privacy is broader than privacy in IoT. Privacy in IoT should be rather perceived as closer to the concepts of informational privacy and data protection.	ETSI TR 103 591 [i.7] ETSI TR 103 534-2 [i.3] (Teaching material)
Are there any existing examples of implementation of privacy for IoT systems?	A relevant example of practical implementation of Privacy policy for IoT is the oneM2M Privacy Policy Manager (PPM) architecture. This simple architecture describes the implementation of GDPR principle for IoT.	ETSI TR 103 591 [i.7] ETSI TS 118 103 [i.19]
What is the most important concept to consider when considering Privacy for an IoT system?	Privacy by design is an approach that aims to build privacy and data protection up front, into the design specifications and architecture of information and communication systems and technologies, in order to facilitate compliance with privacy and data protection principles.	ETSI TR 103 591 [i.7]
Which data are affected by privacy?	The concept of privacy refers to personal data. Under EU law personal data are defined as: "Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person."	ETSI TR 103 591 [i.7] ETSI TR 103 534-2 [i.3] (Teaching material)
Does GDPR apply to IoT systems?	GDPR applies to all processing of personal data, irrespective of the technology used. It, therefore, applies to IoT systems.	ETSI TR 103 591 [i.7]

Question	Answer	Reference for further information
What are the key principles when it comes to GDPR?	The key principles of the GDPR are listed below: • Lawfulness, Fairness and transparency: Personal data should be processed lawfully, fairly ad in transparent manner in relation to the subject. • Purpose Limitation: Personal data should be collected for specified, explicit and legitimate purposes and not for further processing in a manner that is incompatible with those purposes. • Data minimization: Personal data should be adequate, relevant and limited to what is necessary in relation to the purpose for which they are processed. • Accuracy: Personal data should be accurate, kept up to date if not they should be rectified. • Storage Limitation: Personal data should be kept in a form that permits identification of data subjects for no longer than it is necessary for the purpose for which the personal data is processed. • Integrity and Confidentiality: Personal data should be processed in a manner that ensures appropriate security including protection against unauthorized or unlawful processing against accidental loss, destruction or damage. • In addition, the principle of accountability requires organizations acting as data controllers that they are in the position to be able to demonstrate that they comply with all the above principles.	ETSI TR 103 534-2 [i.3] (Teaching material)
How is it possible to ensure that an IoT system is GDPR compliant?	In essence, compliance with the key principles of the GDPR entails compliance with the GDPR; hence meeting the GDPR principles ensures that a system is somewhat GDPR compliant.	ETSI TR 103 591 [i.7]
How does the notion of consent apply?	Consent in the IoT context is particularly relevant for the users of IoT devices. Users of IoT devices should be in the position to give their clear consent to the processing of their personal data either by a statement or by a clear affirmative action. Consent should be freely given, specific and well-informed. Notably, under the GDPR, organizations acting as data controllers are requested to, also, provide for data subject's withdrawal of consent.	ETSI TR 103 534-2 [i.3] (Teaching material)
Once a network has been secured, can it be assumed that privacy is also covered?	Privacy and security are separate concepts in the sense, for example, that privacy can be perceived independently of security. But they are complementary, given that in reality security is an enabler of privacy. It can be stressed that security is a basic requirement for the effective protection of privacy.	ETSI TR 103 534-2 [i.3] (Teaching material)
Are there specific standards available for IoT privacy?	Most of the standards relevant to privacy are combined with security standards however current standards on privacy are usually separated from security standards. Standardization bodies are gradually recognizing the hyper-connectivity and interconnectivity related developments, including IoT, example include: "BS 10012:2017: Data protection. Specification for a personal information management system" [i.24].	ETSI TR 103 591 [i.7]
Is there any missing standard that needs to be developed for IoT privacy?	There are no obvious missing gaps in standardization but there is a significant gap in application of privacy protection capability in general, and of standards based on privacy protection capability specifically.	ETSI TR 103 591 [i.7]

Question	Answer	Reference for further information
Can a stakeholder in IoT find out what type of Privacy issues are directly pertaining to his role in the IoT supply chain?	Yes, Privacy issues is different depending on the stakeholder that is impacted and for IoT this can be complex because of the various stakeholders involved. This includes: • Device Manufacturers • Professionals designing IoT products (Social Network) • Professionals using IoT products (Third Party Application developers) • IoT Platforms • Individuals as Data Subjects: Subscribers, Users, Non-Users The teaching TR and Slides have reviewed some of the areas and some of typical issues that should be considered.	ETSI TR 103 534-2 [i.3] (Teaching material)
Is there a tool that could help identify which type of privacy risks need to be considered in IoT system design?	Data Protection Impact Assessment -is a tool to help identify, assess and mitigate the data protection risks of new projects. They are part of your accountability obligations under the GDPR.	ETSI TR 103 534-2 [i.3] (Teaching material)
Are emergency services requested to comply with GDPR?	Emergency services should comply with the GDPR at all times. In particular, the GDPR allows for the collection and further processing of personal data for the protection of the vital interests of the individual to whom these personal data relate to, which is of direct relevance for the provisioning of emergency services. Nevertheless, once the service is terminated, the processing of the same personal data is allowed, provided only that there is another legal ground allowing it (e.g. acquisition of consent from the individual).	EENA [i.15]

5.3 Security

The intent in this clause is to illustrate security concerns in IoT, and their solution, in an easily digestible form. Two associated Technical Reports (ETSI TR 103 533 [i.1] and ETSI TR 103 534-1 [i.2]) and a set of teaching slides have addressed security within IoT.

In some cases, there are provisions of the Cyber Security Act (CSA) [i.18] that will require devices on the market to be certified with respect to their security claims. Thus, the guidance offered below should always be verified against current best practice and regulatory constraints.

Table 2: Questions and answers for security

Question	Answer	Reference for further information
How is security supported by IoT platforms?	This is a somewhat moot question as it appears to request an answer that not all IoT devices and platforms have to support security. This is not the case. In all IoT instances security of the entire system should be considered. All elements of the IoT system, i.e. devices, hubs, networks, have to be net contributors to the overall system security goals. Thus IoT devices in general should verify that when connected that they are connected to a known element - this requires authentication, in addition if data is involved then the element receiving the data (either as a sensor or as an actuator) should verify that it is from a trusted source. In all cases if the data is sensitive the transmission should be protected from eavesdropping (e.g. by encrypting all connections).	ETSI TR 103 533 [i.1]

Question	Answer	Reference for further information
Are all IoT devices a security concern?	No. The security concern of IoT generally applies to the entire system and the way in which each IoT device interacts with the wider system determines its role either as benign or worrisome as regards security. For example a window-sensor on a domestic window may appear benign in itself, as it contains no personal data, has no processing capability other than the ability to detect if a window is open or not, but if it the sensor is part of an anti-theft system then it becomes an "object of interest" to a thief. So if the thief can disable the sensor from sending a message or force it to send the wrong message then this has the potential to introduce a security issue by ensuring the opening of the window is not picked up. The strategy of Defence-in-Depth would not rely on just a window sensor to detect a break in, rather it will rely on motion sensors, perhaps floor pressure sensors, and even physical locking of jewel boxes and money boxes in order to protect the home.	ETSI TR 103 533 [i.1]
Are all IoT devices constrained devices?	No. The term constrained device is somewhat of a misnomer. A programmable device with a reasonable expectation of being updated over its lifetime will have some memory, processing and I/O overhead designed in such that it can be updated. There will be some point in a device's lifecycle where irrespective of the originally designed overhead it will be insufficient. This would indicate end-of-life if updates cannot be maintained. A device may be constrained by design though if it cannot have new functionality added - i.e. it is limited to provide only the functionality necessary to perform its designed for function. It is difficult to consider this as constrained if it achieves its primary function over its planned lifetime.	ETSI TR 103 533 [i.1]
Where are the security threats from IoT?	IoT devices present a threat in part due to their ubiquity but in particular they may act as vectors to confidentiality, integrity or availability of the overall system.	ETSI TR 103 533 [i.1]
Is there a difference in terms of security between professional IoT devices and mass market IoT devices?	Not really, although the expectation and management of devices in a controlled sector may require more configuration flexibility than would be expected in a mass market device where there is no expectation of professional installation and configuration. What security is required of an IoT device should always be determined by an evaluation of the risks. Managing the risk introduces the concept of security in depth. An IoT device without embedded security functions of its own can be used in an otherwise secure IoT environment if its functionality is not introducing vulnerabilities into the wider system. In general, the concept of defence in depth is to avoid a single point of failure in the overall system.	ETSI TR 103 533 [i.1]
Once an IoT system has been considered as secured, how often is it necessary to reassess its potential vulnerability?	Every manufacturer and the supply chain should operate a vulnerability disclosure policy. This is addressed at some length in ETSI TS 103 645 [i.17] and in the update in ETSI EN 303 645 [i.22]. In undertaking such a policy there is a core requirement to continuously assess vulnerability.	ETSI TS 103 645 [i.17] ISO/IEC 29147 [i.16]

5.4 Platform Interoperability

The IoT is expected to support the massive deployment of a very large range of devices within new or existing systems and allow the development of associated services. IoT systems are required to deal with a (potentially very) large number of (potentially very) heterogeneous IoT devices with very fast evolving underlying technologies. Secondly, the main expectation of IoT is that it will allow for the fast and cost-effective development and deployment of new applications and services. In this perspective, an IoT platform is not just an execution environment specialized in IoT devices.

The expectations for an IoT platform are high: it is supposed to mask the heterogeneity of devices, to handle and simplify communication, to support (end-to-end) data flows, and to provide generic services to the applications built on top of it. IoT applications will see an IoT platform as a framework that connects devices, gateways and machines, applications, and users; and potentially spans the entire value chain of an end-to-end IoT system.

Beyond the provision of a very large number of individual solutions in the early days of IoT, the notion of IoT platform has emerged as a key building block to better support the development of IoT systems, in particular as a "mediation" between the needs of the IoT devices and those of the applications and services supported by corresponding architectural layers.

Given the complexity of issues related to IoT platforms, a number of questions should be addressed, in particular regarding the choice of the different supporting platforms and how they can be integrated in a highly interoperable manner.

The rest of this clause presents a list of generic questions regarding IoT platforms. More details can be found, in particular, in the associated Technical Report ETSI TR 103 536 [i.5] and in the example on Industrial IoT in clause A.3.

Table 3: Questions and answers for platform interoperability

Question	Answer	Reference for further information
What kind of IoT platforms are available?	There is a lot of platforms (actually hundreds) available on the market in support of IoT developments. Most of these platforms are proprietary and, for the most successful, try to offer the broadest possible set of features and services in a relatively closed ecosystem. Other platforms are developed by communities that aim at proposing open (i.e. non-proprietary) solutions developed in a transparent manner. This is, in particular, the case for standardized platforms.	ETSI TR 103 536 [i.5] clause 5.3
What are the pros & cons of proprietary platforms?	A major announced goal of commercial IoT platforms is to provide users with "full experience", i.e. a broad offer of services that range from connectivity up to data visualization, analytics, processing and rule-based actions (and more). In addition, dedicated APIs are provided that enable access to third party applications and systems. The packaging of the platform is done so that users should be able to use it from for all the most common tasks, with well-integrated and optimized functionalities. The trade-off is that the various components available on the platform are tightly coupled with its internals, so that attempting to use them with other platforms may prove infeasible or, at the very best, extremely impractical.	ETSI TR 103 536 [i.5] clause 5.2.2.4
Is it possible to use only one IoT platform?	Many of the available platforms have been developed with a certain scope (e.g. support to connectivity; usage within a given sector) and struggle to expand to a larger set of features (e.g. data analytics) or business domain (e.g. in Smart Cities). When the IoT system is complex enough, it becomes difficult to use only one platform and the interworking of different platforms becomes an issue.	ETSI TR 103 536 [i.5] clauses 6.3 and 7.1.4
What is a standardized platform?	A standardized platform is referring to a set of standards that is integrated by an open community with specifications that can be subject to different implementations. Such platforms can be developed by Standards Developing Organizations (formal SDOs) or by Standards Setting Organizations (SSOs or Fora).	ETSI TR 103 536 [i.5] clause 5.3
Which standardized platforms exist and how to use them?	There is only one relevant example of standardized IoT platform, the oneM2M standard developed by the oneM2M Partnership Project. It is a full IoT solution offering a very complete service platform layer. It is the only full IoT platform currently available with a few actual implementations. Other platforms have been developed by SSOs, often addressing a specific aspect (e.g. connectivity protocols, API, data model) but not offering a global platform, thus requiring further integration.	ETSI TR 103 536 [i.5] clause 5.3
What is the place of generic cloud-based platforms in IoT?	The place and role of the cloud infrastructure is varying depending on the use case and the business domain, in particular because of the security and data protection concerns. However, the flexibility offered by IoT Virtualization is making the role of the cloud-based platforms more and more central in the provision of IoT systems. The Cloud Service Providers (in particular the large ones) are offering more and more integrated platforms, offering a large variety of APIs and built into complete ecosystems.	ETSI TR 103 536 [i.5] clause 7.2.4

Question	Answer	Reference for further information
How can big data be supported by IoT platforms?	In the context of IoT, Big data refers to IoT analytics, i.e. the usage of data analysis tools and procedures to extract value from the huge volumes of data generated by IoT devices. A very large range of new data analytics offerings specifically aimed at IoT use cases (e.g. for Industrial IoT and manufacturing) has emerged, be it as global offering for verticals (e.g. energy) as well as more specialized offerings applying analytics models and machine learning to specific problems.	ETSI TR 103 536 [i.5] clause 7.2.5
What are the main interoperability issues due to the use of heterogeneous IoT platforms?	Interoperability issues may be experienced at all the four levels identified by IERC AC4: • Technical, concerning heterogeneous hardware and/or software (e.g. communication protocols heterogenicity). • Syntactical, concerning data formats (e.g. JSON vs XML); even when data is represented in similar ways (e.g. both in JSON), the layout and data content of messages exchanged are often incompatible between two platforms. • Semantical, concerning the meaning of content. It impacts the human rather than machine interpretation of the content. • Organizational, concerning the heterogeneity of the digital infrastructures of different service providers. These issues may lead to a broad range of interoperability difficulties, ranging from total impossibility of exchanging data to being able to exchange messages that cannot be understood, up to not being able to assign the correct meaning to data that has been exchanged. The very fact that two or more heterogeneous platforms are involved may lead to administrative and security problems. From an operating point of view, at least some in the operating and design staff needs to have a good knowledge of both platforms.	ETSI TR 103 536 [i.5] Annex A especially clause A.3 on Platforms
What needs to be done to enable interoperability between two heterogeneous platforms?	Information needs to be transferred from one platform to the other and interpreted and used correctly by both. This goal can be achieved in more than one way, according to the level of heterogenicity (see question above) and to the characteristic of the platforms involved. If at least one of the platforms allows for the installation of interoperability modules, a common way to overcome technical, syntactical and sometimes semantical heterogenicity involves the design and development of those interoperability modules: they will take care of extracting (or receiving) data from one of the platforms, decode and "understand" it, then create data items carrying the same information and injecting it into the other platform. These modules incorporate (possibly very detailed) knowledge about the internal structure and semantics of both platforms at once.	ETSI TR 103 536 [i.5] clauses 6.4, 6.5 and 7.2

Question	Answer	Reference for further information
What to do when none of the platforms involved support interoperability modules?	Sometimes, none of the involved platforms lend themselves to the installation of interoperability modules (or their internals are not accessible, for whatever reason): in such cases it is not uncommon to use an application, external to both platforms, to execute the operations that are needed to achieve the intended degree of interoperability. In many occasions, it is convenient to base said application on a third IoT platform, different from all the others, which offers the needed support for implementing the needed functionality. From the organizational point of view, several activities are involved: • A design team is put in place, and the usual activities of a project development are performed: from formalizing requirements and determining the extent of the desired interoperability (maybe only a portion of the information needs to be exchanged between the platforms involved), up to design, installation, configuration an d testing • Special care is needed to ensure that the functionalities that are put in place for the sake of interoperability do not adversely impact on the larger system that is formed by the original platforms plus the interoperability modules (or external applications) It is to be expected that, during the life of this complex system, changes will happen. They will range from simple changes in the configuration of one platform, that should be reflected into the other and therefore impact also the interoperability modules/applications to bigger changes. This translates to the need to retain over time the knowledge and capability to perform the activities that are required.	ETSI TR 103 536 [i.5] clause 7.2.2
What are the advantages of a standardized platform?	A standardized platform may allow the growth of an ecosystem where multiple providers compete between themselves while at the same time offering users a standard way of accessing their services. At the time of purchasing, this allows an easier way of comparing multiple offers. Over the life of the platform, it can help the user to limit the effort needed to change providers, without having to completely redo the installed project. This helps to protect investments that are intended to stay in place for a long time.	ETSI TR 103 536 [i.5] clause 5.2.2.7

5.5 Semantic Interoperability

The semantic interoperability complements the platform interoperability. When implemented, the semantic interoperability allows any IoT application to understand and use the data produced by different applications developed by different vendors and by different IoT devices provided by different manufacturers. The levels of interoperability may be more or less high (e.g. understanding measurement units for platform sensors, or being able to map an abstract comfort temperature requirement at a given interval depending on the context) depending on the data representation techniques (e.g. json/xml descriptions or ontologies) and models (e.g. a generic cross-domains ontology such as oneM2M Base Ontology, or a rich domain-enabled ontology such as ETSI reference ontology for smart applications SAREF). Multiple criteria can be considered depending on the objectives behind the implementation of the semantic interoperability. For a given vertical domain (e.g. eHealth, energy), a rich domain-specific data model can be elaborated using data structure notations (e.g. json model), and a more elaborated domain-specific ontology-like description (e.g. OWL model) can be considered [i.5]. For cross-domain applications, subsets of existing data models or ontologies may be combined to achieve the desired goal. This leads to different levels of interoperability [i.5] needing more or less processing resources and giving more or less automation and reasoning capabilities that application developers may reuse.

The rest of this clause presents a list of generic questions regarding Semantic interoperability. More details can be found, in particular, in the associated Technical Reports ETSI TR 103 535 [i.4] and ETSI TR 103 537 [i.6].

Table 4: Questions and answers for semantic interoperability

Question	Answer	Reference for further information
How is semantic interoperability supported by IoT platforms?	Semantic interoperability proceeds by extending the platforms interworking by providing a common data (and resources) representation model allowing platforms and associated applications to have an unambiguous understanding of the meaning of produced/exchanged/stored data (and the underlying resources such as the sensors/actuators producing/consuming such data).	ETSI TR 103 535 [i.4] clauses 6.1, 6.3.2
Is semantic interoperability needed in IoT platforms?	Semantic interoperability in IoT platforms is considered as a step towards further global interoperability as required for different domains including: industrial IoT, and smart cities. These requirements of interoperability are considered as priorities in Europe.	ETSI TR 103 535 [i.4] clauses 6.4, 7.2.3
What are the benefits of implementing semantic interoperability in IoT platforms?	The benefits of implementing interoperability in IoT platforms encompass extending the technical interoperability at the communication level and allow efficient operations on data at the level of platforms and intelligent exploitation by applications. Depending on the data model description richness (ontologies vs JSON data models), the benefits can go beyond interoperability and help machine-level decisions by automated reasoning based on inference rules.	ETSI TR 103 535 [i.4] clause 6.3.3
To what extent semantic interoperability can be implemented in IoT platforms?	The choice of the level of interoperability to be adopted and the technique to be implemented can be constrained by the computation and the communication capacities. A trade-off between the richness of the model and the constrains of its implementation should lead to the choice of the appropriate approach and technique to be adopted.	ETSI TR 103 535 [i.4] clauses 6.5, 8.3.2
Can semantic interoperability be implemented for any IoT platform?	Semantic interoperability can be implemented for any IoT platform with more or less powerfulness in the exploitation depending on the constraints of the platform and the requirements behind implementing semantic interoperability. Different levels of interoperability are considered, and different solutions are associated.	ETSI TR 103 535 [i.4] clause 6.5 on interoperability dimensions
Is there a reference model for semantic interoperability?	Several initiatives are addressing this point. Some of them high level rich models such as oneM2M Base ontology and ETSI SAREF ontology. Others provide more basic models for REST APIs such as the IPSO data model.	ETSI TR 103 535 [i.4] clause 6.5
What are the main interoperability issues due to the lack of a common semantic data model in IoT platforms?	There is no common method to share, process, analyse the huge amounts of datasets generated by IoT devices. This hinders generating useful information and sharing valuable knowledge for different vertical domains and cross-domains applications.	Annex A in particular "Smart Buildings" (A.3) and "eHealth scenarios" (A.2)
How can semantic interoperability between two IoT devices, platforms or applications be assessed?	The assessment of semantic interoperability should be based on the adopted interoperability approach. For each case, ranging from schema-based to ontology-driven approaches, a specific assessment model is to be implemented. There is no common universal model for this purpose.	ETSI TR 103 537 [i.6]

6 Guidelines for practical implementation

6.1 Introduction

On the basis of the questions addressed in clause 5 (and the detailed support of the examples of Annex A), some generic (cross-domain) guidelines can be provided in order to address the questions. Those guidelines are targeting different kind of stakeholders and have been grouped to address different angles:

- strategy (e.g. how to make choices that globally impact the structure in charge of the IoT system),

- operations (e.g. how to ensure that the choices made can be supported by the structure and the stakeholders involved); and
- technology (e.g. what are the main choices to guaranty the development and evolution of the IoT system).

Strategy and operations guidelines are rather generic whereas technology guidelines are more domain specific. More detailed guidelines can be found in the associated ETSI Technical Reports described in clause B.1.

6.2 Strategic guidelines

Prepare for massive innovation and disruptive changes in the value chains

The introduction of IoT technologies and the resulting development of new offerings from incumbents or new entrants are creating enormous changes in the established value chains. The emergence of new entrants is largely facilitated, in particular with the massive virtualization of IoT currently taking place and allowing for the creation of new ecosystems based on the emergence of new, potentially dominant, platforms proposed by Cloud Service Providers to a large number of new specialized start-ups. Hence, the introduction of IoT should be considered as a major strategic challenge and treated as a priority by the organization impacted. Though this has been already the case for some organizations (in particular the large ones), a large number of them still should articulate clear strategies beyond the development of initial prototypes or Proof-of-Concepts.

NOTE 1: This guideline will be of major importance for the CEO and, in general, the CXO level in the company.

NOTE 2: See ETSI TR 103 536 [i.5] on "Platforms Interoperability" for more details.

Advertise and operationalize the decisions made and the resulting successes

Even though strategic decisions to adopt new technologies (e.g. data analytics or semantic interoperability) are made, further efforts are necessary to clarify their impact and ease their diffusion and full adoption in the organization. A staged model of technology diffusion (consisting of initiation, adoption and acceptance, adaptation, routinization, and infusion) should be followed. An increased investment budget for extending systems based on the chosen technologies may offer resulting effective and sustainable services that demonstrate positive results. The strategy decisions should be taken and made clear to the entire (technical) organization and the resulting successes to be advertised (and even rewarded explicitly).

See notes 1 and 2.

Promote success and expand diffusion

Even if the decision to adopt a new technology (such as semantic interoperability) is made, further efforts will be necessary to make it easier for the system to get diffused in an organization. A stage model of technology diffusion consists of initiation, adoption and acceptance, adaptation, routinization, and infusion. The level of services in terms of both quantity and quality should not only reach a critical mass, but ontologies should also be shared to be cost-effective. An increased investment budget for extending systems based on semantic enables such systems to offer sustainable services that demonstrate positive results, such as service improvement and productivity.

See note 1.

NOTE 3: See ETSI TR 103 535 [i.4] on "Semantic Interoperability" for more details.

6.3 Operational guidelines

Decide adoption and promote it

Absorptive capacity is the ability of companies to recognize the value of new, external information, assimilate it, and apply it to commercial ends. It means the ability to evaluate, accept, and apply innovation to achieve organizational objectives and depends on knowledge source and prior knowledge, and it influences innovation adoption. When dealing with semantic, proactive attitude in analysing trends or technological features and a determined will for a successful introduction is required for semantic adoption. In addition to efforts in analysing technological trends, experts need to persuade internally their department heads and resolve any conflict with managers who have a negative opinion of the semantic.

NOTE 1: This guideline will be of major importance for the CTO and the technical community in the company.

NOTE 2: See ETSI TR 103 535 [i.4] on "Semantic Interoperability" for more details.

Outline expectation upfront

There is a significant discrepancy in expectations between suppliers and users. Users expect that many more things will be possible through the adoption of semantic, while suppliers recognize that it is difficult to reveal demonstrable effects that would match user expectations. In other words, there is a gap between the user perspective expecting substantial performance and that of supplier recognizing some limitations due to the early stage nature of semantic. Some developers believe that their services would improve with the semantic without considering whether the semantic is appropriate for their services. The gap resulted from the frequent promotion that the reasoning engine can enable fantastic services that are not possible with existing technologies such as database and data mining.

See notes 1 and 2.

Invest in communication and training

Once they have made the choices regarding the selection of platforms, organizations need to provide educational programs for designers, developers, integrators and deployment teams who may not have enough understanding or knowledge of the new technologies required and make sure that they participate in the training programs. The efforts of the organization to communicate with its engineers and train them is essential to overcome the knowledge gap and can align the technical capability of the organization with the needs of customers.

In the case of emerging technologies (such as Semantic Interoperability), the degree of academic knowledge is higher than that of company organizations. Under such environment, company efforts to communicate with their developers and train them is essential to overcome their knowledge gap and can align the capability of the semantic with the needs of customers.

See notes 1 and 2.

NOTE 3: See ETSI TR 103 536 [i.5] on "Platforms Interoperability" for more details.

6.4 Technical guidelines

6.4.1 Generic Guidelines

Enough standards to start with

A large number of standards are available. It is currently possible to use them on many aspects of the IoT system development. Examples are:

1) the integration of devices using communication protocols for which a very large set of protocol adaptation solutions exist (e.g. with oneM2M);

2) the integration of new and more dynamic information models such as the ones promoted by Semantic Interoperability (e.g. with SAREF [i.14]);

3) the development of secure-by-design solutions for which all the required standards exist (see [i.1]).

In summary, there is no reason to wait for the standards gaps to be filled.

NOTE 1: This guideline will be of major importance for the CTO and the technical development community.

NOTE 2: See ETSI TR 103 536 [i.5] on "Platforms Interoperability" for more details.

Clearly outline the scope of the IoT (sub-) system and its integration

The introduction of the IoT system should be clarified upfront from the point of view of the organization's technical strategy. This is in particular true regarding the place of the IoT system in the overall organization offering (e.g. as a sub-system integrated in legacy versus as a new central system to which remaining legacy elements should be integrated). Once this initial approach is followed and completed, it will be easier to understand the implication of the introduction of new technologies (such as Semantic Interoperability) and make the best trade-off between the expected substantial efficiency and performance improvement and the limitations due to the adoption of technologies that may be still at an early stage of the maturity evolution and the difficulty of working together with more mature existing technologies such as data management or data mining.

See notes 1 and 2.

6.4.2 Privacy

Proposed guidelines on meeting GDPR principles

The following elaborates on the above principles and suggest guidelines needed to meet these principles in practice:

1) No personal data by default principle: avoid personal data collection or creation by default, except where, when and to the extent required.

2) Provide a Short Contextual Privacy Notice at the point of collection.

3) If relying on consent, provide granular choices - do not bundle consent - and ensure individuals are aware of the persistency of consent and how to revoke it.

4) Capture and retain evidence of consent revocation.

5) Identify the legal basis for processing special categories of personal data such as biometrics.

6) Use language that can easily be understood by target audience.

7) Place a hyperlink in the short Privacy Notice to the more detailed company Privacy Statement.

More:

- 'As-If' principle: design and engineer IoT ecosystems as-if these will process personal data, now or in a later phase.
- De-Identification by default principle: de-identify, sanitize or delete personal data as soon as there is no longer any valid legal basis.
- Data minimization by default: only process data where, when and to the extent required, and delete or de-identity other data.
- Encryption by default principle: encrypt personal data by default and include digital rights and digital rights management thereto.

NOTE 1: This guideline will be of major importance for all IoT stakeholders. Compliance with these guidelines does not guarantee compliance with the entire set of GDPR principles governing lawful processing of personal data.

NOTE 2: See ETSI TR 103 591 [i.7] on "Privacy" for more details.

Privacy by design

Privacy by design is a sub-domain in some respects of "secure by default" and shares many of the same attributes in the provision of countermeasures. For example, it can be argued that data minimization forms an example of privacy by design. Data minimization that is also a principle of security in general - only gather what is needed and only secure what is essential. Thus, if content, say of a webpage or social media post, is intended to be public it would not be encrypted but it may have its integrity protected and the authorship authenticated. However, delivery of content may be made over an encrypted channel irrespective of the nature of the content (i.e. public content may be delivered over a private channel).

NOTE 3: This guideline will be of major importance for primarily for manufacturers, system designers, software developers. Data protection by design and data protection by default are explicitly dictated under the GDPR.

NOTE 4: See ETSI TR 103 533 [i.1] on "Security" and ETSI TR 103 591 [i.7] on "Privacy" for more details.

6.4.3 Security

Security guidance and best practices

Designing in security to any system is difficult. It is also difficult to give definitive proof of value: A successful security system will not show degradation under attack, it will not fail under attack, and it may also not be attacked. The general assumption is that if a system has a vulnerability it will be exploited and that designers will take measures to minimize the likelihood of an attack and also take the assumption that the countermeasures will fail.

There are a large number of frameworks and best practices for software developers that have been developed by the larger vendors, and most large organizations have developed in-house secure coding practices, often developed from the controls framework that has been published by ETSI as ETSI TR 103 305 [i.21], or from adaptations of the ISO 27000 [i.23] series of specifications. Examples include the following.

NOTE: See ETSI TR 103 533 [i.1] on "Security" for more details.

IoT Security

There are a large number of IoT security best practice guidelines available. Whilst many of these documents may be sector specific the general guidance has considerable overlap and focus on credential security (e.g. no default passwords), and data minimization. The intended audience of each guideline requires some review as the level of understanding of the guidance is dependent on the assumptions the authors of each guideline has regarding the level of knowledge of security technology and processes.

The identified guidelines and best practices summarized below are a small sample of a very large possible set. The reader is encouraged to take each guideline as indicative. In the core of ETSI TR 103 533 [i.1] on Security, the principles of security design outlined in clause 10 are suggested as having precedence (in addition to the arguments outlined above).

See note.

6.4.4 Platforms

Start Small on IIoT projects

Manufacturers typically begin their approach to IIoT by first starting a pilot, or PoC (Proof-of-Concepts) project. It is usually either a small plant or manufacturing line that needs to be (re)built from scratch, or an existing one that is been retrofitted with IIoT. In any case, it is not a toy demonstration project: it is a fully operational facility, intended to carry on profitable production.

The small size of the project allows for teams to be involved more directly (they have other facilities to attend to as well), so that they can experience and understand the complexity of the undertaking, thus building internal expertise that will be most valuable when the new approach gets extended to other parts of the factory. A gradual approach will ease the learning curve while reducing possible deployment issues of the newly introduced hardware and functionalities.

NOTE 1: This guideline will be of major importance for the CTO and the technical development community.

NOTE 2: See ETSI TR 103 536 [i.5] on "Platforms Interoperability" for more details.

Insert the new technologies in the overall development process

Very often, when it comes to developing larger scale IoT systems, many organizations prefer to start the project with Proof of concepts (PoC) limited in terms of technologies, data sources and scope. During the PoC phase, the need for upfront integration of critical technologies such as security or semantic interoperability is not necessarily well addressed, and their future integration becomes much costlier and sometimes extremely difficult to integrate properly. For this reason, new technologies for IoT should be inserted at an early stage in the development process to ease subsequent large-scale deployments of IoT (sub-)systems.

See notes 1 and 2.

6.4.5 Semantic Interoperability

Insert ontologies in the development process

In general, when it comes to developing larger scale IoT systems, many companies prefer to start the project with small Proof of concepts (PoC) limited in terms of technologies, data sources and scope. During the PoC phase, the need for semantic interoperability is not necessarily visible. As it often happens with security, if not initially anticipated, semantic interoperability becomes extremely costly and almost impossible to integrate properly in the future. For this reason, semantic interoperability in general and ontologies in particular should be inserted at an early stage in the development process to ease the mass scale deployments of IoT systems and avoid vendor-lock in.

NOTE 1: This guideline will be of major importance for the CTO and the technical development community.

NOTE 2: See ETSI TR 103 535 [i.4] on "Semantic Interoperability" for more details.

Agree on a trade-off for implementable Semantic Interoperability (from Platforms)

The choice of the level of interoperability to be adopted and the technique to be implemented can be constrained by the computation and the communication capacities. A trade-off between the richness of the model and the constrains of its implementation should lead to the choice of the appropriate approach and technique to be adopted. The choices can range from simple JSON data models for HVAC sensors values exchange by smart building IoT platforms, to elaborated domain ontologies for remote assistance and automated diagnosis using wearable sensors for internet of medical things platforms. Modularity of the design may help easier transformation and evolving of the model within the different levels of interoperability and for the different modelling techniques.

See note 1.

NOTE 3: See ETSI TR 103 536 [i.5] on "Platforms Interoperability" for more details.

General guidelines for a semantic interoperability Plugtest™

The initial preparation activity for a semantic interoperability Plugtests™ is to choose with interested stakeholders the objective and purpose of the test among the possible situations described in clause 6.1 of ETSI TR 103 537 [i.6], together with the event date and venue.

At this stage, it is important to identify the relevant specifications and ontologies to be tested and the corresponding test configurations, from the configurations defined in clause 7.

From the results of ETSI TR 103 535 [i.4], it appears that the number of standardized semantic-enabled frameworks is limited. Such an event should then have to choose whether the tests are run inside one framework, using specifications from the same origin (for example, like the semantic interoperability that were organized by oneM2M in December 2017) or across different frameworks and set of specifications (for example, mixing SAREF and SSN implementations), allowing more platforms and implementations to be involved in the test.

Once the purpose of the event is agreed, dedicated test specifications that describe unitary test scenarios need to be written, to support the interoperability test. Each scenario will test one specific feature (e.g. part of ontology management or data management capabilities of the devices) in a specific configuration and permit to declare whether interoperability is achieved for that feature, based on specific validation criteria which can be human observable (e.g. an application shows the successful reception of a measured value on an HMI) or obtained through logging tools in the implementations. The detailed testing scenarios are written using the flows of the applicable generic scenarios as a baseline.

See note 1.

NOTE 4 See ETSI TR 103 537 [i.6] on "Plugtests™ Preparation for Semantic Interoperability" for more details.

7 Observations and Lessons Learned

Many issues related to IoT adoption are cultural

The adoption of and integration of IoT in organizations (enterprise, cities, public sector, etc.) is not just related to the resolution of technical problems. Non-technical, human related factors have to be considered as well, since the adoption of new technology paradigms also change the way people work or interact with complex systems. This means that the stakeholders concerned (e.g. managers, professionals) have first to evaluate, choose and apply innovations to achieve their organizational objectives, including the satisfaction of the end-user's needs.

Once this is done, those in charge of the IoT systems should develop educational programs for the actors involved (designers, developers, data specialists, etc.) who do not have enough understanding or knowledge of the new technologies required (e.g. privacy, security, semantic interoperability) and make sure that they actively participate to the associated training programs.

Privacy and data protection require organizational adaptation

With respect to the IoT environment, the effective protection of privacy and (personal) data protection requires appropriate technical and organizational measures. The implementation, monitoring and optimization of those measures should be planned, prepared in advance as well as during the related data collecting, data processing and data management pertaining to the life cycle of the respective IoT ecosystem.

Considering that the requirements set under the GDPR are mandatory and that in essence, the GDPR provides for a general and principle-based framework, the GDPR further requires organizations not only to be able to ensure, but also to deliver documented and continuous proof of appropriate levels of compliance - defined in the GDPR as accountability on a continuous basis. In this context, there is a clear role for standards and related certification schemes to play.

The task of defining security into any system is difficult

The best practices and guidelines that are available on the market from a large number of standards bodies, vendors, government agencies, industrial groupings, are very similar in their intent but often understate the difficulty in determining what has to be secured and how it is to be secured. Rather there is an assumption of knowledge of the means to apply the guidelines. One concern is that whilst in many fields there is an ability to learn "on the job", for security there is no such luxury.

A danger that is not expressed in any of the guidelines is the consequence of incomplete implementation, or of incomplete knowledge. As an example, the guidance to not allow default passwords (credentials in general) is a symptom of incomplete understanding - the need to authenticate users is good practice and the underlying mechanisms are often very well implemented. On the one hand, good practice is followed by enforcing authentication, but is then undermined by not enforcing uniqueness of the credentials that allow it to be effective.

Semantic Interoperability is a key issue and a key enabler to open platform adoption

The lack of semantic interoperability is often considered the largest market inhibitor for the uptake of IoT in the industry. Currently, companies deal with the lack of interoperability by using different approaches (amongst which semantic interoperability) depending on customer needs and internal skills. However, a lack of killer applications and successful cases, the complexity and immaturity, the uncertainty regarding scalability and performance, and the difficulties to perceive its immediate value are affecting negatively the adoption of semantic interoperability in the industry.

Semantic Interoperability can be designed and implemented following different approaches and techniques providing different levels of end-to-end interworking and understanding (in particular for IoT platforms). Protocol and service level interoperability are increasingly achieved by SDOs specifications for horizontal services and APIs, such as the oneM2M standard. An important progress is being made for rich advanced data interoperability models such as ETSI SAREF and oneM2M base ontologies. Nevertheless, the wide scope of vertical applications domains prevents the design of a unique standard data models for cross-domain Semantic Interoperability.

A growing role for standardized solutions with IoT platforms

The "Standardized approach" (originated by SDOs) to IoT platforms is gaining momentum. The approach is relying on the choice of a reference (technical) architecture with a layered model, an information and interoperability strategy, a selection of Reference Points and APIs. The resulting platform can be a combination of platforms supporting one or more of the above scenarios. These solutions are based on standards developed openly with clear and fair IPR rules, and typically are not controlled by any specific company or group of companies. In the IoT domain, oneM2M is the most prominent example.

Annex A:
Examples and associated issues and guidelines

A.1 Examples and issues addressed

In order to illustrate the issues addressed (as analysed in clause 5), four examples have been chosen. They are analysing a significant use case, each in a different business domain:

1) eHealth: Telecare and telehealth systems as for elderly people.

2) Smart Buildings: Synthetic facilities management processes regardless of existing building installations.

3) Industrial IoT: Manufacturers of complex equipment adding IoT capabilities to provide new services.

4) IoT-based Mission Critical Communications: IoT support to communication between public safety personnel.

Those examples have different focus regarding the main issues (e.g. the first one has a focus on security) and the Table A.1 below is showing which issues they are primarily addressing.

Table A.1: Main issues addressed by the examples

	eHealth	Smart Buildings	Industrial IoT	Mission Critical Communications
Privacy	Primary focus of the example			Strong focus of the example
Security	Strong focus of the example			Strong focus of the example
Semantic Interoperability		Primary focus of the example	Strong focus of the example	Primary focus of the example
Platform Interoperability		Strong focus of the example	Primary focus of the example	

The examples provide a storyline of the IoT system considered together with an analysis of why the example is relevant with respect to the current situation of IoT systems development in the associated business domain. They also provide a quick analysis of which kind of issues the IoT systems designers and developers will face and how these issues are related to the questions (as identified in clause 5) and the guidelines (as identified in clause 6).

A.2 eHealth

A.2.1 Introduction

The clause expands on a use case scenario which is dealt within ETSI TR 103 591 [i.7]. The use case scenario puts forward telecare and telehealth systems as a highly demanded solution, both by those elderly people who live alone and by their formal caregiver, namely, the Red Cross, and the family caregivers. The discussion below produces a high-level mapping of the actors in accordance with the roles provided under the GDPR [i.9] (e.g. data subject, data controller, data processor). Moreover, the clause below provides for a rough categorization of the personal data presumably collected and further processed by the IoT devices employed. Overall, the discussion surfaces the main privacy, security and interoperability related considerations that pertain to the application domain of eHealth.

A.2.2 Storyline

Ángela is 83 and she lives alone in her apartment in La Coruña. She does not have serious medical condition, but takes some chronic medication, she needs to control her blood pressure, and her mobility is not very good. She fell on the street a few weeks ago. Also, she has been losing hearing in long distances.

By installing CCTV cameras inside Angela's house, Alba - her daughter - can check at any time, through a website after signing in through a secure account, where her mother is present inside the flat. When Alba consults the information and sees that Ángela is near the phone in the living-room, she can make a call.

Additionally, a wearable blood pressure tracker will help Alba to keep a check on her mother's blood pressure. Thus, even when Ángela leaves her home to go around the neighbourhood, do some shopping and sometimes meet friends or neighbours for a cup of coffee, Alba can check her mother's blood pressure thereby feeling more confident about her health.

If, for example, Ángela falls and needs to ask for help or medical assistance, she can do so through a provision on the blood pressure tracker which will send a notification to the Spanish Red Cross, whose staff would then initiate the usual protocols to deal with such cases.

Furthermore, if Ángela during her holidays together with friends and relatives abroad (e.g. Portugal) falls and needs to ask for help or medical assistance, she can do so through a provision on the blood pressure tracker that will send a notification to the national Red Cross (e.g. Portuguese) whose staff would then initiate the usual protocols to deal with such cases, also, on the basis of the information shared by the Spanish Red Cross. Note that the wearable blood pressure tracker will send the related notifications in the local language.

A.2.3 High Level Illustration

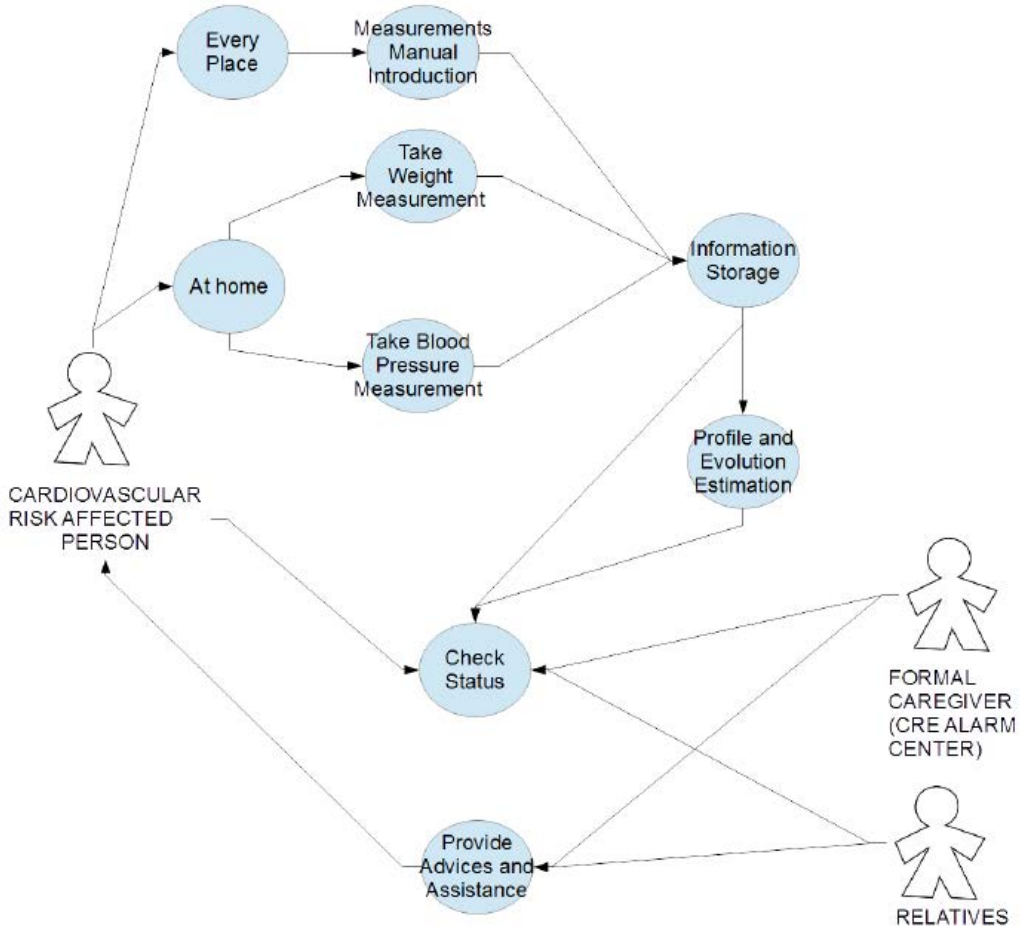

Figure A.1: UML-oriented model of the eHealth Use Case: main actors and context-aware tasks

Types of personal data collected and data protection roles

Example of Personal Data: Angela's location

Example of Health Data/Personal Data: Body Weight, Blood Pressure, Body Temperature, Blood Type

Data Subject: Angela

Data Controller: Determines the purpose and means of processing personal data:

- CCTV camera manufacturer
- Blood pressure device manufacturer

Data Processor: Processes personal data on behalf of the controller:

- Location service provider (provides Angela's location service to Alba)
- Caregiver - Spanish Red Cross company (provides staff that reviews Angela medical record)
- Relative

Joint Data Controller: Determines the purpose and means of processing jointly with the data controller. A contractual agreement should provide in a clear manner for the distribution of responsibilities between the controller and the joint controller.

A.2.4 Main stakeholders

As it is possible to see in Figure A.1, the main stakeholders are:

- Elderly people with raised cardiovascular risk: inhabitant of the home that it is the beneficiary of telecare service.
- Family caregiver: the person(s) with interest and with permission to check the status of the beneficiary. Relatives may, also, be considered as family caregivers.
- Formal caregiver: the national Red Cross that provides the 24/7 telecare and assistance service depending on the EU Member State that the incident occurs (e.g. Spanish, Portuguese).

Note that it is presumed that the relative acting in her capacity as a caregiver is not member of the Red Cross.

A.2.5 Why this Use Case is relevant

The population in Europe is ageing. Due to the demographic changes of the population, especially, in countries such as Spain and Greece, the number of people aged 65 years, or more is continuously increasing and the ratio of young persons to elderly persons is changing (fewer working people by each person older than 65). This situation is putting pressure over the public social and health care systems that will have problems in the near future to give high-quality assistance under these circumstances.

Besides, the shift of the population from rural to cities and the reluctance of elderly people to move from their homes to geriatrics is increasing the number of elderly people that live alone in their own home, without direct assistance of any person.

In this context, the use of wearable devices collecting health related data, as the one mentioned under the use case description is expected to become increasingly wide, therefore, rendering the discussion captured under this clause highly relevant for IoT stakeholders and regulators.

Furthermore, ensuring continuity of cross-border eHealth applications and services within the EU depends on the exchange of personal data concerning patients' health, in conjunction with the existing electronic healthcare information systems residing on the Member States [i.11]. In this respect, the GDPR makes explicit that Member States may impose conditions, including limitations, on the processing of genetic data, biometric data or health data. However, as stated in Recital 53 such national limitations "should not hamper the free flow of personal data within the EU when these conditions apply to the cross-border processing of such data". Note that a Code of Conduct on privacy for mobile health applications specifying the general requirements of the GDPR is currently under preparation [i.20].

This Use Case is relevant, because it illustrates certain of the issues identified in Table 1. In particular, it surfaces the challenges facing Privacy in IoT, it provides concrete example of data affected by privacy and, to an extent, points at whether emergency services are obligated to comply with the GDPR. With respect to these issues, it is inferred by the above Use Case scenario that the guidelines identified in clause 6.4.2, namely, the Proposed guidelines on meeting the GDPR principles and the Privacy by Design are applicable. As mentioned above in clause 6.4.2, the implementation of the specific guidelines does not guarantee compliance with the entire set of GDPR principles governing lawful processing of personal data.

A.2.6 Issues to address in the development of the example

Security

- Communication between IoT device and IoT gateway/application may be intercepted/penetrated, resulting in a security problem, such as false alarm, Denial of Service type attacks and interruption, usurpation or misuse by unauthorized persons that may create a significant impact on human life.

Privacy

- Consideration of the personal data protection aspects that are associated to the use of wearable devices.
- Necessity for clear determination of the data protection roles of the actors involved in the provisioning of a service.
- Consideration of additional requirements linked to the exchange of health-related information, emerging, also, from national laws of the EU Member States.

Platform Interoperability

- Definition of a future-safe strategy regarding the choice of the IoT platform, in particular with respect to the possible coexistence of proprietary, open source and standardized solutions.
- Careful consideration of the points of interoperability that should be provided by the platform.
- Alignment to standardized platforms to support the points of interoperability.
- IoT devices and subsystems not able to exchange data with service platforms and applications because they were produced by different manufacturers or providers.
- Use unified representations to avoid lack of valid data syntax and semantics to interpret data (e.g. data is out of accepted range).

Semantic Interoperability

- Necessity to provide rich resource and data description models to understand (e.g. units of measurements) and interpret data exchange and service requests (e.g. context-aware mapping of abstract to concrete data values or resource instances).
- Consider the trade-off between high-level semantic interoperability requirements and other scenario-specific NF constraints such as security and privacy enhanced by processing data close to its producers.
- Consider different levels of richness for the data representation models to be able to adapt to device constraints or cloud powerfulness during inference rules execution.
- Avoid defining models from the scratch and give priority to reuse of existing and standardized models (e.g. standardized ontologies: SAREF, oneM2M Base ontology) when defining new specialized models.

A.2.7 Questions addressed and relevant guidelines

The following "Questions to address" (see clause 5) are clearly illustrated or inferred by this example.

Privacy

- What are the main challenges regarding privacy?
- Which data are affected by privacy?
- Does GDPR apply to IoT systems?
- What are the key principles when it comes to GDPR?
- How does the notion of consent apply?

Security

- How is security supported by IoT platforms?
- Are all IoT devices a security concern?
- Where are the security threats from IoT?
- Once an IoT system has been considered as secured, how often is it necessary to reassess its potential vulnerability?

Platform interoperability

- What kind of IoT platforms are available?
- Is it possible to use only one IoT platform?
- What are the pros & cons of proprietary platforms?
- What are the advantages of a standardized platform?
- Which standardized platforms exist and how to use them?
- How can big data be supported by IoT platforms?
- What are the main interoperability issues due to the use of heterogeneous IoT platforms?
- What to do when none of the platforms involved support interoperability modules?

Semantic interoperability

- Is semantic interoperability needed in IoT platforms?
- How is semantic interoperability supported by IoT platforms?
- What are the benefits of implementing semantic interoperability in IoT platforms?
- Can semantic interoperability be implemented for any IoT platform?
- Is there a reference model for semantic interoperability?
- What are the main interoperability issues due to the lack of a common semantic data model in IoT platforms?

The following "Guidelines for practical implementation" (see clause 6) are illustrated by this example.

Strategic guidelines

- Prepare for massive innovation and disruptive changes in the value chains.

Operational guidelines

- Invest in communication and training.

Technical guidelines

- Enough standards to start with.
- Follow proposed guidelines on meeting GDPR principles.
- Enable privacy by design.
- Follow security guidance and best practices.
- Agree on a trade-off between models richness and implementability for IoT for Semantic Interoperability.
- Consider together the functional (platform and semantic interoperability) and non-functional requirements (security and privacy)

A.3 Smart Buildings

A.3.1 Introduction

Interoperability of Smart Buildings is the promise of providing a helicopter view of the facilities management processes, regardless of existing building installations. By doing so, building and facility managers can make better-informed decisions, enforce cross building policies and pave the way for automation and wider integration.

Building managers are faced with heterogeneous and vendor-specific installations. Centralized management of buildings oftentimes forces the owners to go through costly replacements to adopt mono-vendor solutions. Installation of new equipment requires costly system integration because devices are often designed to communicate with specific applications only. There is no uniform manner to access and filter the huge amounts of datasets that are generated. Huge amounts of data are generated but never get analysed and used. The buildings remain isolated from their surroundings and environment, resulting in poor or non-existing synergies with e.g. parkings, power grids, micro grids, Electrical Vehicle stations, and the city services in general.

A.3.2 Storyline

This use case assumes a facility manager working for a supermarket chain and responsible of hundreds of buildings. The management is asking to reduce costs every day. Knowing that every building has a different vendor, installation and dashboard, the facility manager job is a nightmare because he needs to connect to every building separately for monitoring and control. To solve this issue it is supposed that there is an interoperability platform that offers a standard interface to monitor and control all the buildings regardless of vendor. The facility manager could apply energy efficiency strategies to all buildings on large scale. He could for example, compare buildings to detect leaks, adjust the heat and the lighting according to forecast or predictive models, and compliant with applicable regulations.

The interoperability platform makes it possible to quickly plug and play new equipment, networks and services in a cost-efficient manner and without disturbing the ongoing building management operations. Since buildings devices generate huge amounts of data, the exposure of these data sets through modern APIs allows proliferation of new building services such as situational awareness, energy efficiency, intrusion detection, preventive maintenance and smart data. Centralized management of heterogenous buildings allows increased energy efficiency by setting global policies, quicker reactions and optimized decisions across all buildings. It also brings-down operational costs thanks to a single software set. The challenge is how to get there without retrofitting the building to a single technology/provider.

Through north bound API, wider integration of the building with the outside world is achieved to give rise to fully integrated cities. The building stops existing on its own and starts to interwork with energy grids (smart and micro grids), smart parking, Electrical Vehicle charging, waste management, etc., the ultimate goal for buildings to be considered really smart. The value resulting from wider integration goes much beyond mere energy savings to include also increased productivity, user satisfaction, greater RoI for owners and users, predictive fault detection to reduce maintenance time and ultimately increased overall value for property owners and managers.

A.3.3 High Level Illustration

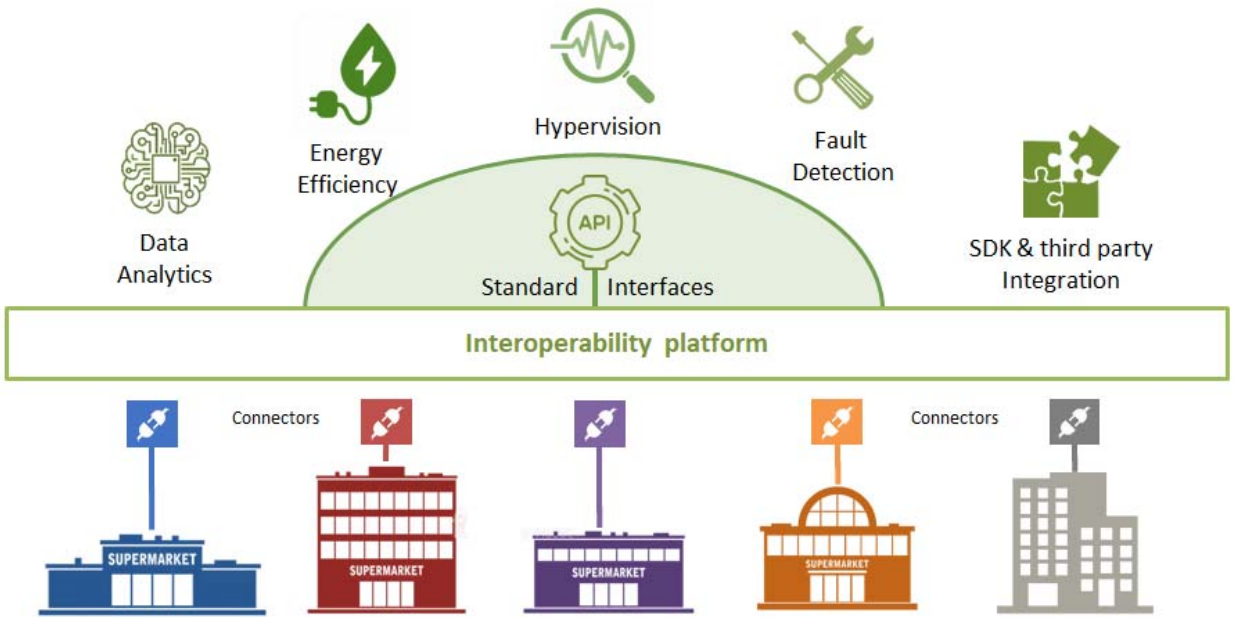

Figure A.2: Interoperability platform for Smart buildings overview

A.3.4 Why this Use Case is relevant

The worldwide buildings sector is responsible for 40 % of global energy consumption and more than 55 % of global electricity demand, according to the International Energy Agency (IEA). IEA also estimates that the global building-related CO2 emissions continue to rise by nearly 1 % per year.

Regulators worldwide are taking this problem seriously, by enforcing legislation that goes in favour of interoperability and energy savings. In Europe, the 2010 Energy Performance of Buildings Directive is the EU's main legislative instrument promoting the improvement of the energy performance of buildings. The 2018 Directive [i.10] amended the Energy Performance of Buildings Directive to introduce targeted improvements with the vision of a decarbonised building stock by 2050 and the mobilisation of investments. The revision also supports electromobility deployment and introduces new provisions to enhance smart technologies, interoperability and automation.

In the US, the Property Assessed Clean Energy (PACE) programs allow local governments, state governments, or other inter-jurisdictional authorities to fund the up-front cost of energy improvements of commercial and residential properties, which are paid back over time by the property owners.

A.3.5 Issues to address in the development of the example

Security and Privacy

- Ensure the BMS is not connected directly to the internet. Better yet, ensure the BMS is separate from the enterprise network and is separated by an air gap or firewall.
- Consider using virtual local area networks and segregated networking practices to keep BMS subnetworks separate and isolated. That way, a problem in one subnet cannot affect the other networks.
- Password controls can be a challenge with a BMS, so always change the default passwords for the BMS system, workstation and field devices.
- Train the building staff, contractors and vendors on your security expectations, policies and procedures.

- Make sure to have a security incident response plan in place. This plan should address both cyber and physical security incidents.
- Many field bus technologies are exposing building data to the cloud without any security mechanisms.
- Communication between IoT device and application may be intercepted resulting in false alarms, Denial of Service, usurpation or misuse by unauthorized persons, jamming.

Interoperability

- Building Management Systems are mainly composed of legacy equipment (Heating, Ventilation, Aeration, Colling, Lighting, Comfort, Access, etc.) using industrial field bus technologies and row data that need to be semantically enriched with missing contextual information like location, etc.
- Building Management Systems, historically composed of wired industrial field bus, are today disrupted by new wireless technologies like LPWAN that offer more flexibility for the building owner or the facility manager in terms of technological choices and use cases, however, in such hybrid environment, more data unification and semantic interoperability are required since part of the data is available locally and the other part is available in the cloud.
- Building Management Systems are not able to exchange data with a centralized platform and applications because they were produced by different manufacturers.

A.3.6 Questions addressed and relevant guidelines

Privacy

- What are the main challenges regarding Privacy?
  - the high risk of profiling
  - acquisition of a freely given and well-informed consent
- Does GDPR and its key principles apply to IoT systems?
- How does the notion of consent apply?

Security

- How is security supported by IoT platforms?
- Where are the security threats from IoT?
- Is there a difference in terms of security between professional IoT devices and mass market IoT devices?
- Once an IoT system has been considered as secured, how often is it necessary to reassess its potential vulnerability?

Platform interoperability

- What are the pros & cons of proprietary platforms?
- Which standardized platforms exist and how to use them?
- What are the main interoperability issues due to the use of heterogeneous IoT platforms?
- What to do when none of the platforms involved support interoperability modules?

Semantic interoperability

- What are the benefits of implementing semantic interoperability in IoT platforms?
- Can semantic interoperability be implemented for any IoT platform?
- How can semantic interoperability between two IoT devices, platforms or applications be assessed?

The following "Guidelines for practical implementation" (see clause 6) are illustrated by this example.

Strategic guidelines

- Advertise and operationalise the decisions made and the resulting successes

Operational guidelines

- Invest in communication and training

Technical guidelines

- Clearly outline the scope of the IoT (sub) system and its integration
- Follow proposed guidelines on meeting GDPR principles
- Enable privacy by design
- Follow security guidance and best practices
- Insert the new technologies in the overall development process
- Agree on a trade-off for implementable Semantic Interoperability (from Platforms)
- Organize semantic interoperability Plugtest

A.4 Industrial IoT

A.4.1 Introduction

Industrial IoT in general, and IoT in Manufacturing in particular, is raising additional challenges compared to other sectors (such as some of those addressed in the other use cases in the present document). In the industrial context, additional issues should be dealt with such as: the presence of Information Technologies (IT) together with Operational Technologies (OT) that require a coherent approach; the need to take into account strong requirement regarding safety; the integration with a very solid (and sometimes hard to evolve) legacy. More on this can be found in the associated Technical Report ETSI TR 103 536 [i.5].

An example of such actors of the Industrial IoT is that of Equipment Manufacturers that are addressed in the present use case. Manufacturers of complex equipment have in general understood that adding IoT capabilities to their equipment can benefit products and solutions and their customers. However, it is not often the case that this kind of manufacturers have the capabilities to develop in house an IoT solution for their production line, but the question on whether or not to do it is recurrent. The current use case addresses in particular the associated strategic and technical implications.

A.4.2 Storyline

A.4.2.1 The IoT Platform as a support to new service creation

"Smart Machines for Manufacturing" (short name: SmartM4M) is a company that manufactures packaging machines for industrial use that have a solid portfolio of customers and deliver around ten thousand of machines each year.

SmartM4M's CEO has understood the potential benefits of Industry 4.0 for the company's business. In particular, one perceived way to increase its business and to provide a more solid long-term positioning is to generate a "service" business in addition to the delivery of machines. This would involve adding additional IoT capability to the current line of products. After consultation of the high-level managers (in marketing and sales in particular), it appears that the most promising areas for the company are proactive remote service and telemetry.

IoT is not entirely new for SmartM4M since some IoT devices are already incorporated in the company's machines. In the majority of cases, those devices are dealt within the machine, but some of the data produced by the machine's sensors need to be provided to other equipment (other machines or back-end systems) and had to be integrated within the overall ecosystem of the customer's plant. This is done in general by integrating the SmartM4M machine in an already existing set of solutions, most of them proprietary.

With the decision of going towards the "service" approach comes the opportunity to have a new look at the company's technical strategy. One important aspect is that the SmartM4M machines are generating a very large amount of data and the question of Big Data becomes essential. In particular, how and where to address Big Data and how it can contribute to maximize the new revenue generated by the new services needs to be clarified as it has a large impact on the company's technical strategy.

Several scenarios are generated by the company's CTO and will require further analysis before a decision can be made, amongst which:

1) in house development;

2) partner with third parties, based on their own cloud platform plus some adaptation to interface SmartM4M's equipment; use the services of the proprietary platforms available in the customer plant's ecosystem.

It is understood by SmartM4M managers that answering the question is key for the future of the company.

A.4.2.2 The difficulty to set-up the IoT Platform

Setting-up the IoT platform require some strategic choices (e.g. cloud-based, proprietary, in-house) as well as technical solutions (e.g. alignment to an already existing platform ecosystem, integration with legacy equipment or business processes). Two scenarios are briefly addressed below, showing the hardship of future-safe decisions.

Scenario 1 Cloud-based platform

After examination of the possible solutions with the CTO and the technical managers, the CEO contracts a company offering IoT support to third parties, based on their own cloud platform plus some adaptation to interface the kind of equipment that SmartM4M makes. What looks a good deal is stricken and, after the initial tentative steps, a full year runs relatively smoothly.

At the end of that period, the solution is not entirely satisfactory. Indeed, the system is doing what is expected, and more could be done provided additional investment would be done. On one side, however, SmartM4M products do not look so unique, particularly to his own customers when they look at the provided dashboards. On the other side, even if the deal looked good at the start, once a year's worth of products has been rolling off the overall expense has grown up to a sizeable amount.

Scenario 2 In-house development

An alternative approach for SmartM4M could be to develop their own platform solution, thus getting all the desired customization up front, with a system that would exactly fit to the company requirements. This choice is made on the assumption that it would be feasible for the technical department to implement their own solution in house, with internal resources, in particular based on their experience in developing good products.

However, this assumption may prove excessive considering that, although his technicians are very good indeed, they lack the kind of knowledge that is needed to create an IoT platform that can accommodate the amount of device and traffic that will be needed to serve some years' worth of the packaging machines they will be selling. Furthermore, the technicians are also fully busy with current activities: improving current product lines and designing the next ones.

A possible way forward is the creation of an ad-hoc team. A major initial difficulty is the relationship between this team and those in charge of the development of the machines. The risk is that the new team is presented with a set of requirements and is expected to design and implement the system mostly by themselves. The approach taken is to focus on the design of a "core foundation" (with no alignment to existing standards such as oneM2M) with the objective to create a differentiating product. This approach seems adequate for some time and things seem to develop smoothly, in part because the team is able to show "visible" progress, i.e. partially usable versions of the system. However, some problems may occur, amongst which:

- Cultural and human relationships issues between the new team and the previous employees of the company.

- Focus on the technical development at the expense of associated activities such as documentation. Managers that are used to extremely detailed design and documentation for the machines that their company builds, which is largely mechanics, are unprepared to deal with complex software design.
- Difficulty to scale-up the first prototypes have been installed at friendly customers, in particular to due to significantly different IT environments at different customer premises requiring duplication of integration efforts.
- Difficulty to set-up an efficient management of bugs and minor customer adaptations.
- Consolidation of customer requirements into new development that may not fit with the "core foundation", in particular regarding interoperability with other equipment in the customers shop-floor (with difficulty to reconcile the associated information and data model).
- Overall motivation of the ad-hoc team in the long run.
- Explosion of the development costs.

The end result may be a system which is working but is difficult to maintain and almost impossible to modify in order to satisfy the growing needs of his customers.

A.4.3 Why this Use Case is relevant

Creating IoT solutions is a difficult undertaking because of the complexity of the IoT system itself and because it most often requires integration within a larger context which, for the present use case, can be substantially different from on customer to another, thus creating more options, more potential development and additional complexity.

Understanding the pros and cons to develop an "in house" solution is crucial for a company manufacturing (mostly) mechanical equipment, but similar considerations apply also to small software companies that want to offer their own proprietary platform on the market.

Customers will most likely ask for new functionalities and better interoperability. This is a fact that happened also in the past, with other technology cycles before the advent of IoT: even approaches that were performing well from a technical point of view were eventually driven out of the market because the companies that developed them could not sustain the effort involved in ensuring interoperability.

The underlying question is how to choose a technical solution taking into account the company size, investment capacity, openness of technical solutions, expertise of the technical staff, etc. Amongst the many associated considerations, the choice of a "standards-based", open platforming support of the technical choice is a very important aspect.

A.4.4 Issues to address in the development of the example

Security

- Communication between IoT device and IoT gateway/application may be intercepted/penetrated, resulting in a security problem, such as false alarm, Denial of Service type attacks and interruption, usurpation or misuse by unauthorized persons, jamming.

Privacy

- Consideration for protection of data related to the customer environment, including personal information.

Platform Interoperability

- Definition of a future-safe strategy regarding the choice of the IoT platform, in particular with respect to the possible coexistence of proprietary, open source and standardized solutions.
- Careful consideration of the points of interoperability that should be provided by the platform.
- Alignment to standardized platforms to support the points of interoperability.

Semantic Interoperability

- Lack of valid data syntax and semantics to interpret data (e.g. data is out of accepted range).
- IoT devices and sub-systems not able to exchange data with service platforms and applications because they were produced by different manufacturers or providers.

A.4.5 Questions addressed and relevant guidelines

The following "Questions to address" (see clause 5) are illustrated by this example:

Privacy

- What are the main challenges regarding Privacy?
- Does GDPR and its key principles apply to IoT systems?
- Are there any existing examples of implementation of privacy for IoT systems?
- Once a network has been secured, can it be assumed that privacy is also covered?
- Can a stakeholder in IoT find out what type of Privacy issues are directly pertaining to his role in the IoT supply chain?

Security

- How is security supported by IoT platforms?
- Are all IoT devices a security concern?
- Where are the security threats from IoT?
- Once an IoT system has been considered as secured, how often is it necessary to reassess its potential vulnerability?

Platform interoperability

- What kind of IoT platforms are available?
- Is it possible to use only one IoT platform?
- What are the pros & cons of proprietary platforms?
- What are the advantages of a standardized platform?
- Which standardized platforms exist and how to use them?
- How can big data be supported by IoT platforms?
- What are the main interoperability issues due to the use of heterogeneous IoT platforms?
- What to do when none of the platforms involved support interoperability modules?

Semantic interoperability

- Is semantic interoperability needed in IoT platforms?
- How is semantic interoperability supported by IoT platforms?
- What are the benefits of implementing semantic interoperability in IoT platforms?
- Can semantic interoperability be implemented for any IoT platform?
- How can semantic interoperability between two IoT devices, platforms or applications be assessed?

The following "Guidelines for practical implementation" (see clause 6) are illustrated by this example:

Strategic guidelines

- Prepare for massive innovation and disruptive changes in the value chains.
- Advertise and operationalise the decisions made and the resulting successes.

Operational guidelines

- Decide adoption and promote it.
- Invest in communication and training.

Technical guidelines

- Enough standards to start with.
- Start small on IIoT projects.
- Clearly outline the scope of the IoT (sub-) system and its integration.
- Follow proposed guidelines on meeting GDPR principles.
- Enable privacy by design.
- Follow security guidance and best practices.
- Insert the new technologies in the overall development process.
- Agree on a trade-off for implementable Semantic Interoperability (from Platforms).

A.5 IoT based Mission Critical Communications

A.5.1 Introduction

Mission critical communications are (multi-)point-to-(multi-)point communication between public safety personnel. They allow relationships among authorized representatives responsible for handling emergency situations as well as those between the different organizations, e.g. between emergency control centres.

IoT allows (near) real-time data gathering without human interaction. This is especially important in situations where emergency service team members are busy with critical tasks and additional reporting (e.g. via voice-based radio systems) to the team officer would cause unwanted distraction or delay. For example, smart clothing, equipped with sensors, can report in real time vital signs and temperature of firefighters involved in hazardous situations. A rescue team officer can thus warn when the situation gets too hazardous or intervene to rescue the firefighter in trouble. Such information can be used to alert other team members in real-time in order to act more carefully.

Another example is emergency service personnel equipped with wearables such as audio and video sensors or supported by a drone. The real-time audio and video transmissions can be used by other team members or the emergency control centre in order to collect more data to assess the situation.

The use case will show how IoT devices can be used in emergency situations in general and for mission critical communications in particular.

A.5.2 Storyline

This use case assumes that the communication networks and services they provide are deployed and operational; the emergency services are established and functional; the IoT devices and IoT service platforms involved in the use case are deployed and in operational condition before the event takes place.

A call is received at the PSAP (Public Safety Answering Point) that a fire has started in a mid-level apartment in the city suburb. Immediately, the operator forwards the notice to the fire station where John, Bob and Paul are on duty, together with their manager Peter. Peter is managing, coordinating and is responsible for the other members of the team. Rapidly, the emergency service team members start an emergency mission and activate their IoT devices: wearables on their firefighter outfits, wristbands, augmented reality glasses.

As they arrive on the fire scene, John and Bob enter the building looking for affected persons. They move within the building while the sensors embedded in their outfits continuously send real-time measured data to an IoT service platform located at the fire station.

Laura is an operator at the fire station. She monitors the information received from the suits, especially looking that no alarm is raised regarding John and Bob's physical condition. The data received at the fire station (from different sources, including as well sensors and cameras located in the fire engine) is also used to automatically build an enhanced view of the incident area and to be presented to the team manager Peter, helping him to make decisions. Artificial intelligence and data fusion may be used in that step. The fire engine serves as a local platform receiving the IoT data, but with a partial knowledge about the incident area only.

The automatically generated data (e.g. by AI) as well as the data that Peter decides to communicate, is published on the platform and shared between all stakeholders involved in the action. Examples include a map with meta information such as temperature values in all parts of the building, location and number of emergency responders or victims, etc. This information is used to gain extra knowledge about the incident area, the other emergency responders, and the citizens that are outside the field of vision. In this case, Peter and Laura both have a precise knowledge of the emergency situation and are kept updated in real-time. They can thus manage the emergency mission more efficiently.

When he enters the burning apartment at the core of the fire, John finds a woman, Ingrid, lying on the floor. She is still alive but requires immediate attention. This information is immediately captured by Laura who dispatches an ambulance towards the emergency scene. John and Bob manage to get Ingrid out of the building and start medical assistance, sending her vital data to the arriving ambulance, which relays it to the hospital where she will be later transported. Jack, the emergency doctor in the ambulance, monitors these data and starts preparing his medical devices.

The emergency situation has been handled efficiently thanks to the precise real-time view provided by the IoT devices to either local and remote emergency service team decision makers. Ingrid has been taken care of with the relevant treatment as soon as she has arrived at the ER.

A.5.3 High Level Illustration

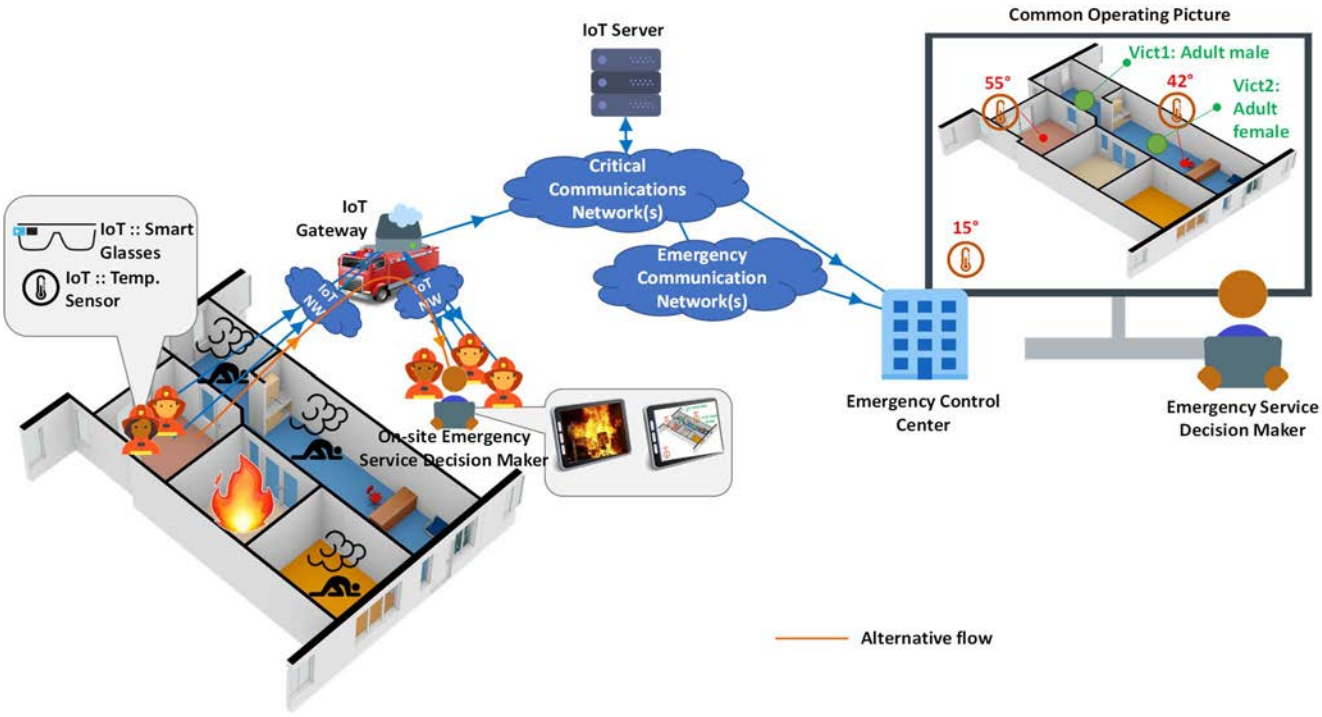

Figure A.3: Illustration of "IoT-based mission critical communications" use case

A.5.4 Main stakeholders

- Laura, at the emergency control centre: manages an emergency mission and coordinates emergency services teams. This centre may be located on-site (field emergency control centre) or off-site with regard to the incident area.
- John, Bob and Paul are members of an emergency team with an identified role in the actions of rescue and of restoration of normal conditions. They are equipped with IoT devices (e.g. wearables).
- Peter is the officer of the emergency team with responsibility for the team and a legal mandate to take decisions. He is also known as emergency services decision maker.
- Ingrid is an inhabitant of the burning apartment who has been suffocated by the smoke.
- Jack is an emergency doctor who enters the ambulance to rescue Ingrid.

A.5.5 Why this Use Case is relevant

The IoT market is developing very fast. This domain now faces the challenge of a multiplicity of standards, solutions and platforms, among which many are proprietary. This challenge reflects the fact that IoT is more than a communication technology.

Nowadays, ICT services for emergency situations start involving IoT devices. Safety organizations use it internally, e.g. for staff work suit enhanced with IoT (fire fighters, policemen, etc.) or to report about temperature, location, health risks. Such reports can be sent directly to local as well as to remote control centres. The location of an emergency can be provided directly to the remote-control centres by monitoring sensors. During medical emergencies, patient data can be transferred directly from sensors in the vehicle to medical staff in the hospital. It is thus of utmost importance that in the case of these applications, the IoT communications and systems comply with the stronger requirements of emergency services, especially for privacy, security and interoperability, and that safety organizations receive guidelines to prepare their deployments in the safest manner possible.

A.5.6 Issues to address in the development of the example

Security

- Communication between IoT device and IoT gateway/application may be intercepted/penetrated, resulting in a security problem, such as false alarm, Denial of Service type attacks and interruption, usurpation or misuse by unauthorized persons, jamming.
- IoT device is not usable because its user is not able to authenticate (password management).
- Invalid data reception and interpretation due to lack of data integrity mechanisms.
- Personal data from the emergency team members and affected persons may be disclosed in an unauthorized manner.

Privacy

- An emergency team member has access to more data than what is relevant to its function and role in the emergency scene.
- Consideration for personal information of John, Bob and the other fire responders collected through their sensors on the wearables include body temperature, blood pressure. Has their consent been obtained?
- Consideration for body camera taking pictures of people in buildings and other responders as the firemen move through the buildings to save people. Has the consent of the fire men been taken, the pictures collected are they been used to check that the people are okay? Consent on how long the information can be stored in the fire station Laura is monitoring.
- Consideration for sensors and camera on the fire engines collecting data of nearby events which include pictures of firemen or other citizens in the nearby area. Consideration for the area view of the fire engine camera, what is the coverage area of the camera and how long will be pictures be stored.

- Agreement from all team members that all their data taken during operation can be published for all members to view and also for Peter the decision maker to use them for making decisions for work related aspects only.
- Consideration about Ingrid medical data sent to the ambulance which include body temp, heart rate and pressure, should consent be required and from whom as Ingrid is found unconscious?
- The connected Ambulance contains medical instrument that can measure internal clinical data sent to the hospital to measure for example internal bleeding etc, this information also is personal data. The medical instrument should also only collect data that is necessary and only use the data for what its been required and nothing more.

Interoperability

- IoT device is not able to exchange data with service platforms and applications because they were produced by different manufacturers or providers.
- Different emergency services teams are not able to exchange information because their systems/platforms are not interoperable.
- System failure due to IoT device emergency data not being decodable/understood.
- Lack of valid data syntax and semantics to interpret data (e.g. data is out of accepted range).

Furthermore, to link this analysis with the questions to address answered in clause 5 and the related guidelines provided in clause 6, this use case has the following relevance.

A.5.7 Questions addressed and relevant guidelines

The following "Questions to address" (see clause 5) are illustrated by this example:

Privacy

- What are the main challenges regarding Privacy?
  - the high risk of profiling
  - acquisition of a freely given and well-informed consent
- Does GDPR and its key principles apply to IoT systems?
- How does the notion of consent apply?

Security

- How is security supported by IoT platforms?
- Where are the security threats from IoT?
- Is there a difference in terms of security between professional IoT devices and mass market IoT devices?
- Once an IoT system has been considered as secured, how often is it necessary to reassess its potential vulnerability?

Platform interoperability

- What are the pros & cons of proprietary platforms?
- Which standardized platforms exist and how to use them?
- What are the main interoperability issues due to the use of heterogeneous IoT platforms?
- What to do when none of the platforms involved support interoperability modules?

Semantic interoperability

- What are the benefits of implementing semantic interoperability in IoT platforms?
- Can semantic interoperability be implemented for any IoT platform?
- How can semantic interoperability between two IoT devices, platforms or applications be assessed?

The following "Guidelines for practical implementation" (see clause 6) are illustrated by this example.

Strategic guidelines

- Advertise and operationalise the decisions made and the resulting successes

Operational guidelines

- Invest in communication and training

Technical guidelines

- Clearly outline the scope of the IoT (sub-) system and its integration
- Follow proposed guidelines on meeting GDPR principles
- Enable privacy by design
- Follow security guidance and best practices
- Insert the new technologies in the overall development process
- Agree on a trade-off for implementable Semantic Interoperability (from Platforms)
- Organize semantic interoperability Plugtest

Annex B:
For further reading

B.1 Technical Reports

Seven companion Technical Reports (TRs) have been developed by ETSI, that each addresses a specific facet of IoT systems. In order to provide a global and coherent view of all the topics addressed, a common approach has been outlined across these TRs concerned with the objective to ensure that the requirements and specificities of the IoT systems are properly addressed and that the overall results are coherent and complementary.

A brief description of each TR is provided below.

- **ETSI TR 103 533 [i.1]**

  The document provides an overview of the Standards Landscape and best practices for the application of security technology to the IoT. It uses a simplified security model of IoT to describe the multi-fold purpose of security technologies: confidentiality, integrity and availability. As one of the many characteristics of IoT, the Technical Report highlights an important difference between IoT and other communication systems like e.g. cellular telecommunication: the number of IoT communicating entities is very large and the number of possible relationships per device is even larger. An IoT device, unless a specific example of a cellular enabled IoT device containing a SIM, does not have a predefined security association to a trusted entity.

  Furthermore, the document introduces the security purposes of IoT as a specialization of the generic cyber-security domain and some of the paradigms used in security analysis, design, and implementation. It gives an overview of the regulatory domain as it impacts IoT security. By adopting the "NIS Directive" [i.12] being the first EU horizontal legislation addressing cybersecurity challenges, and the General Data Protection Regulation [i.9], which addresses the topic from the perspective of security of personal data and the obligations that result on organizations that use data, EU lawmakers have been taking steps to increase cyber resilience across Member States.

  The Technical Report provides an overview of the security ecosystem as well as of the specific technologies of security that may apply to IoT, and it identifies the stakeholders in standards development and development of best practices. Finally, it gives specific security guidance and refers to best practices and guidelines for non-consumer IoT e.g. from GSMA, DCMS, ETSI, ENISA, ECSO, TCG, Global Platform and NIST.

  The document complements the overview of the Standards Landscape and best practice for privacy to be found in ETSI TR 103 591 [i.7].

- **ETSI TR 103 534-1 [i.2]**

  The document is based on the Security Report ETSI TR 103 533 [i.1]. It presents teaching material to allow readers, identified by role, to gain knowledge of the fundamentals of IoT security. The bulk of the material in the document is aimed at tutor led teaching and there is a presumption of prior knowledge to apply the material to the actual audience.

  The document starts with an introduction to security in IoT by explaining basic terms, security solutions, objects to deal with, capabilities, boundaries, technologies and principles. After presenting the standards ecosystem and an economic view on security provisions, it gives a lesson in Threat, Vulnerability and Risk Analysis (TVRA) in IoT followed by an introduction of cryptographic security basics as they apply in IoT.

  Furthermore, the document demonstrates applying best practices to IoT security including secure configuration and operation of IoT devices.

  Finally, guidance is given for programming secure IoT and for selecting a training provider.

- **ETSI TR 103 534-2 [i.3]**

  The document is based on the Privacy Report ETSI TR 103 591 [i.7]. It focuses on producing teaching material on privacy and to direct the reader to other materials that are available in order to gain a basic understanding on what is involved in the privacy concept that is especially relevant, also, for the IoT environment. Overarching objective of this teaching material is to provide learners with the necessary information, so as to gain basic knowledge on the concept of privacy, allowing them to make decisions and act in relation to the IoT environment.

  The Technical Report explains the term privacy and its relationship to personal data. It introduces the General Data Protection Regulation (GDPR) and explains the link between privacy and security.

  The document reflects upon privacy in the context of IoT, presenting a global approach of IoT systems and pointing to the challenges of privacy in IoT by means of some use case examples. It describes serious risks associated to privacy and gives some guidance how to protect from these risks.

  This teaching material is addressed to learners holding different functions in the supply chain. To this end, it provides for actors such as device manufacturers, software developers, and users benefiting from the delivery of service through the IoT supply.

- **ETSI TR 103 535 [i.4]**

  The document addresses the topic of semantic interoperability in the context of its potential usage by the industry in the development of IoT systems. The main objective of the document is to concretely foster the use of semantic interoperability in IoT by identify why it is important in industry IoT projects, to analyse the advantages and drawback of the available solutions.

  The report makes an in-depth analysis of the state-of-the-art of semantic interoperability. It defines the different approaches that are used, in particular the ontologies. The solutions from academics, standards and industry are analysed and compared. It reveals different aspects of the adoption of semantic interoperability in the industry domain as a specific case. To this extent, after analysing the approaches currently adopted in the industry to deal with interoperability, it addresses the drivers and inhibitors to market adoption. The case of ontologies is analysed in detail in order to understand what the blocking factors are and how they can be overcome.

  Finally, the Technical Report provides concrete and actionable guidelines towards those in charge of making decisions regarding the use of semantic interoperability solutions in the industry and of implementing those decisions within the overall IoT systems technical and cultural development environment.

- **ETSI TR 103 536 [i.5]**

  The document carefully outlines the nature, the role of IoT platforms and proposes elements for the identification of the most relevant ones. It also addresses detailed examples such as Industrial IoT to outline the challenges posed to generic IoT platforms. It addresses the issues related to the interoperability and interworking of IoT platforms, in particular standardized IoT platforms, and how the way they are handled can foster their adoption by the IoT community.

  The Technical Report provides an overview of the very fragmented IoT platforms landscape. At first it describes a framework for IoT platforms outlining some requirements that should be met by the main IoT platforms in order to expand their capabilities and attractiveness to IoT systems designers and developers. The impact of two major evolutions, namely Big Data and Virtualization, on these platforms is analysed. The overall objective is to better characterize what are the properties that a "standardized IoT platform" should embed in order to become a major reference to the developers of IoT solutions in various business sectors.

  Besides providing a classification of IoT platforms including advantages and drawbacks for each of them, the document introduces platforms identified by UNIFY-IoT and the IoT-EPI, platforms in the EU-funded IoT Large Scale Pilots, and the platforms standardized by oneM2M, OCF and the Open Source Software Apache platform.

  The document devotes special attention to interworking across all layers of the interoperability stack (from technical to organizational). It analyses the technical approaches in support of interoperability and outlines some criteria for best support of interoperability within and between platforms. Based on these criteria, a list of "candidate platforms" is established and an evaluation of the actual support of these criteria by the identified platforms is made.

Furthermore, the report presents Industrial IoT (IIOT) as a typical case study of the many challenges that are posed to standardized platforms. Beyond the identification of major requirements, it addresses some challenges such as the role of legacy and its impact on candidate platforms. Based on these requirements, a list of potential platforms is provided. Some of them are analysed in order to evaluate their coverage and what should be done to overcome potential limitations.

Finally, some recommendations are made towards the IoT community regarding standardization, convergence of platforms, interoperability support frameworks.

- **ETSI TR 103 537 [i.6]**

  As part of its activities towards platforms interoperability, the document aims at preparing a Plugtests™ event on Semantic Interoperability.

  For this Plugtests™ event, the interoperability will be based on AIOTI High Level Architecture [i.13], oneM2M base ontology [i.14] (linked to ETSI SmartM2M SAREF one) and oneM2M Service Layer information sharing, with the objective to demonstrate a more practical/industrial use.

  The Technical Report intends to identify the testing requirements from the semantic interoperability standards, especially those collected in ETSI TR 103 535 [i.4] and ETSI TR 103 536 [i.5]. It focuses on the test configurations and additional elements involved such as components, protocols, data models when appropriate. The document defines a set of related interoperability test scenarios based on results in these Technical Reports, but also use case documents from AIOTI, oneM2M, SmartM2M, W3C, etc. Scenarios showing interworking of semantic-unaware systems with systems supporting semantic interoperability are included as well. The scenarios are described from a user point of view. Each scenario description clarifies the different actors involved in the test, the pre-conditions, trigger, main and alternative operational flows, as well as post-conditions and test sequence.

  Finally, the TR identifies and describes the event preparation requirements like infrastructure, IT and related tools. In this step, it provides guidelines/cookbook on requirements for anonymous reporting of the Plugtests™ outcomes and results.

  The report is developed in close collaboration with the ETSI Centre for Testing and Interoperability (CTI) and delivers examples of test scenarios and testing organization.

- **ETSI TR 103 591 [i.7]**

  The purpose of the document is to demonstrate that in view of the increasingly growing number of connected objects anticipated in the near future, effective protection of privacy and data protection would require that the relevant decisions are made upfront, at the design stage of the IoT systems.

  The document focuses on privacy building on the fundamental assumption that even though it is generally considered that privacy and security are separate concepts, they are actually interconnected, and they should therefore be treated in practice in a coordinated manner. Security constitutes a prerequisite for the effective protection of privacy, as it has also been confirmed by the General Data Protection Regulation (GDPR) [i.9].

  The Technical Report elaborates on how to ensure effective protection of individuals' privacy in the IoT environment. It acknowledges the challenges for privacy and data protection, stresses the necessity for a human centred approach and highlights the role of social values in the design of IoT systems. The document provides an overview of the existing standards in the domain of privacy, reviews any potential gaps and suggests possible ways forward. The role of standards under the GDPR and the proposed ePrivacy Regulation are discussed and the role of the individual is outlined, also through a set of use cases drawn from an ongoing EU project.

  Furthermore, the document produces an overview of the main privacy and data protection challenges emerging in the IoT environment and illustrates current best practices across industrial and other organizations in the processing of personal information to meet, and in some cases exceed, the minimum requirements for compliance in view of maximizing the protection of personal information.

  Finally, it points at the fundamental shifts taking place in relation to privacy under EU Law, including the shift from rule-based frameworks to principle-based frameworks, the necessity to go beyond mere compliance to meaningful accountability and the implementation of impact-based measures, and it offers some available guidance for the safeguard of privacy in the IoT environment.

B.2 Technical material

- **ETSI TR 103 582 [**i.8**]**

  ETSI SC EMTEL has developed a Technical Report, ETSI TR 103 582 [i.8]: Study of use cases and communications involving IoT devices in provision of emergency situations with the objective to prepare the requirements for communications involving IoT devices in all types of emergency situations, including Mission Critical communications within emergency services/public safety organizations, e.g. between public safety officers and control centres, between the control centres of different public safety organizations, and between individual public safety officers.

- **ETSI TS 103 645 [**i.17**]**

  This document developed by ETSI TC CYBER specifies high-level provisions for the security of consumer devices that are connected to network infrastructure, such as the Internet or home network, and their associated services. It provides basic guidance for organizations involved in the development and manufacturing of consumer IoT on how to implement those provisions.

- **EENA [**i.15**]**

  The purpose of this document is to present the fundamental principles related to the processing of personal data, but above all to support public safety organizations in their efforts to comply with the GDPR. Using practical examples, this document is intended to present, step by step, the actions to be taken in order to comply with the regulations in force. Such steps include the different documents to be drafted, the practical way of mapping personal data, the identification of risks, the DPO governance within companies and organizations, how to choose appropriate partners offering sufficient guarantees in terms of compliance with the GDPR, etc.

Annex C:
Change History

Date	Version	Information about changes
May 2019	0.0.1	Preliminary draft with table of content and scope
June 2019	0.0.2	Following clauses filled with preliminary text: 1., 2., 3., 5.1, 5.2, 5.3, 7.1, 7.3, 8.1, 8.2, 8.4, Annex B
June 2019	0.0.3	Clauses 4 and 6 filled with preliminary text, some modifications in existing sections
June 2019	0.0.4	Early draft for providing to TC SmartM2M #50 (Milestone G3)
July 2019	0.0.5	Modified structure of the SR based on feedback from TC SmartM2M #50
August 2019	0.0.6	Adding new sub-clause 5.1 and renumbering of the following ones, new text in clauses 5.2, 5.5, 6.3 and clause B.1
August 2019	0.0.7	Clause 4 reworked
September 2019	0.0.8	Headline clause 5 modified, clause 5 cleaned up, all contributions so far contained, version serves as basis for further contributions, clause B.1 reworked
September 2019	0.0.9	Stable draft for providing to TC SmartM2M (Milestone G4)
October 2019	0.0.10	Modifications based on approved version 0.0.9
November 2019	0.0.11	Modifications based on approved version 0.0.10
November 2019	0.0.12	Clean version based on v0.0.11 (without revision marks) for final contributions inclusion
November 2019	0.0.13	New section on Smart Buildings introduced
November 2019	0.0.14	Overall consolidation for final review by STF teams before upload on SmartM2M portal
November 2019	0.9.0	Final draft proposed to SmartM2M for consensus review
February 2020	1.0.0	Final Draft reviewed by ETSI for publication pre-processing

History

Document history		
V1.1.1	March 2020	Publication