ETSI TR 103 533 V1.1.1 (2019-08)

SmartM2M;
Security;
Standards Landscape and best practices

Reference
DTR/SmartM2M-103533

Keywords
cybersecurity, IoT, oneM2M, privacy, security

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

List of figures

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 Technical Report (TR) 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.

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.

In order to provide a global and coherent view of all the topics addressed, a common approach has been outlined across the Technical Reports 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 other documents listed below (the present document is highlighted in *italic* script in the list):

ETSI TR 103 533 (the present document)

ETSI TR 103 534-1 [i.43]

ETSI TR 103 535 [i.45]

ETSI TR 103 536 [i.46]

ETSI TR 103 537 [i.47]

ETSI TR 103 591 [i.2]

1.2 Scope of the present document

The present document provides an overview of the Standards Landscape and best practices for the application of security technology to the IoT.

Existing work in mapping the landscape of security standards and best practices has been published by ETSI in both formal ETSI publications and in the review of security activity presented in the annual white paper, by ENISA through the IoT Security Expert Group (in [i.3] and [i.4]), and others but have often not addressed the particularities of IoT for the general case. In this regard the present document builds on the content of ETSI TR 103 306 [i.1] which addresses IT Security in general with a specific view to the IoT and extends and builds on the previously published work in the field.

The present document is structured as follows:

- Clause 5 provides a simplified security model of IoT.
- Clause 6 presents an introduction to the security purposes of IoT as a specialization of the generic cyber-security domain and introduces some of the paradigms used in security analysis, design, and implementation.
- Clause 7 presents an overview of the regulatory domain as it impacts IoT security.
- Clause 8 presents an overview of the security ecosystem and identifies the stakeholders in standards development and development of best practices.
- Clause 9 presents a review of the security best practices and development guidance arising from the stakeholders identified in clause 4.
- Clause 10 presents an overview of the specific technologies of security that may apply to IoT.
- Clause 11 provides a summary of the findings of the present document.
- Annex A collates a set of best practice guidelines for non-consumer IoT.

The present document complements the overview of the Standards Landscape and best practice for privacy to be found in ETSI TR 103 591 [i.2].

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 103 306: "CYBER; Global Cyber Security Ecosystem".

[i.2] ETSI TR 103 591: "SmartM2M; Privacy study report; Standards Landscape and best practices".

[i.3] ENISA: "Baseline Security Recommendations for IoT in the context of Critical Information Infrastructures", ISBN: 978-92-9204-236-3, doi: 10.2824/03228.

[i.4] ENISA: "Security and Resilience of Smart Home Environments: Good practices and recommendations", ISBN: 978-92-9204-141-0 | doi:10.2824/360120.

[i.5] Recommendation ITU-T Y.4806. "Security capabilities supporting safety of the Internet of things".

[i.6] ENISA: "Security Recommendations for IoT".

[i.7] European Data Protection Supervisor: "EDPS formal comments in response to the Çybersecurity Package' adopted by the Commission".

NOTE: Available from https://edps.europa.eu/sites/edp/files/publication/17-12-15_formal_comments_2017-0810_en.pdf.

[i.8] UK Department of Culture, Media and Sport: "Secure by Design: Improving the cyber security of consumer Internet of Things Report".

NOTE: Available from https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/775559/Secure_by_Design_Report_.pdf?_ga=2.246964045.819894548.1566555869-1475373752.1566555869.

[i.9] 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).

NOTE: Available from https://eur-lex.europa.eu/eli/dir/2016/1148/oj.

[i.10] ETSI TS 102 165-1: "CYBER; Methods and protocols; Part 1: Method and pro forma for Threat, Vulnerability, Risk Analysis (TVRA)".

[i.11] FIPS 197: "Federal Information Processing Standards Publication 197; Advanced Encryption Standard (AES)", issued by the National Institute of Standards and Technology (NIST), November 26, 2001".

[i.12] European Commission, Special Eurobarometer 460: "Attitudes towards the impact of digitisation and automation on daily life", 2017.

NOTE: Available from http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/78998.

[i.13] European Commission, Special Eurobarometer 464a: "Europeans' attitudes towards cyber security", 2017.

NOTE: Available from http://ec.europa.eu/commfrontoffice/publicopinion/index.cfm/ResultDoc/download/DocumentKy/79735.

[i.14] European Commission Cross Fertilisation Through Alignment, Synchronisation and Exchanges for IoT: "Legal IoT Framework (Initial)", Deliverable 05.05 2017.

NOTE: Available from https://european-iot-pilots.eu/wp-content/uploads/2018/02/D05_05_WP05_H2020_CREATE-IoT_Final.pdf.

[i.15] ETSI TR 103 167: "Machine to Machine (M2M); Threat analysis and counter measures to M2M service layer".

[i.16] ETSI TR 103 309: "CYBER; Secure by Default - platform security technology".

[i.17] ISO/IEC 15408: "Information technology - Security techniques - Evaluation criteria for IT security".

[i.18] ETSI EG 202 387: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method for application of Common Criteria to ETSI deliverables".

[i.19] ETSI ES 202 383: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Security Targets".

[i.20] ETSI ES 202 382: "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Security Design Guide; Method and proforma for defining Protection Profiles".

[i.21] GDPR: "General Data Protection Regulation (GDPR) (EU) 2016/679".

[i.22] ETSI TR 103 370: "Practical introductory guide to Technical Standards for Privacy".

[i.23] ETSI TS 103 485: "CYBER; Mechanisms for privacy assurance and verification".

[i.24] ETSI TS 103 486: "CYBER; Identity Management and Discovery for IoT".

[i.25] ETSI TS 102 165-2: "CYBER; Methods and protocols; Part 2: Protocol Framework Definition; Security Counter Measures".

[i.26] ETSI TR 103 305 (all parts): "CYBER; Critical Security Controls for Effective Cyber Defence".

[i.27] European Commission: "Communication from the Commission to the European Parliament and the Council: Making the most of NIS - towards the effective implementation of Directive (EU) 2016/1148 concerning measures for a high common level of security of network and information systems across the Union", 4 October 2017.

NOTE: Available from https://ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-476-F1-EN-ANNEX-1-PART-1.PDF.

[i.28] ENISA: "Good Practices for Security of Internet of Things in the context of Smart Manufacturing".

[i.29] ENISA: "Towards secure convergence of Cloud and IoT".

[i.30] TCG: "Architect's Guide: IoT Security".

NOTE: Available from https://trustedcomputinggroup.org/wp-content/uploads/TCG-Architects-Guide_2018_FC01_web.pdf.

[i.31] TCG: "IoT Security Infographic, Securing the Internet of Things".

NOTE: Available from https://trustedcomputinggroup.org/wp-content/uploads/INFOGRAPHIC-TCG-IoT-FINAL.pdf.

[i.32] AIOTI: "IoT LSP Standards Framework Concepts", Release 2.8, White Paper, 2017.

[i.33] Recommendation ITU-T X.1205: "Overview of cybersecurity".

[i.34] ISO/IEC 27032: "Information technology -- Security techniques -- Guidelines for cybersecurity".

[i.35] NIST SP800-183: "Networks of 'Things'".

[i.36] ETSI TS 103 645: "CYBER; Cyber Security for Consumer Internet of Things".

[i.37] ETSI TS 118 103: "oneM2M; Security solutions (oneM2M TS-0003)".

[i.38] ETSI TR 103 456: "CYBER; Implementation of the Network and Information Security (NIS) Directive".

[i.39] ETSI TR 103 369: "CYBER; Design requirements ecosystem".

[i.40] ETSI TR 103 331: "CYBER; Structured threat information sharing".

[i.41] ETSI EG 203 310: "CYBER; Quantum Computing Impact on security of ICT Systems; Recommendations on Business Continuity and Algorithm Selection".

[i.42] ETSI TR 103 304: "CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services".

[i.43] ETSI TR 103 534-1: "SmartM2M; Teaching Material; Part 1: Security".

[i.44] ETSI TR 103 534-2: "SmartM2M; Teaching Material; Part 2: Privacy".

[i.45] ETSI TR 103 535: "SmartM2M; Guidelines for using semantic interoperability in the industry".

[i.46] ETSI TR 103 536: "SmartM2M; Strategic / technical approach on how to achieve interoperability/interworking of existing standardized IoT Platforms".

[i.47] ETSI TR 103 537: "SmartM2M; Plugtests preparation on Semantic Interoperability".

[i.48] ISO/IEC 27000: "Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary".

[i.49] IEEE 802.11™: "IEEE Standard for Information technology--Telecommunications and information exchange between systems Local and metropolitan area networks--Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications".

[i.50] IEEE 802.15.4™: "IEEE Standard for Low-Rate Wireless Networks".

[i.51] National Security Agency (NSA): "Defense in Deph".

NOTE: Available from https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in ETSI TR 103 306 [i.1] and the following apply:

centre of excellence: educational or research & development organization recognized as a leader in accomplishing its cyber security mission

Consumer IoT: This includes consumer purchased 'off the shelf' IoT devices; IoT devices used and installed 'in the home' and the associated services linked to these devices.

NOTE: Definition from [i.8].

cyber environment: users, networks, devices, all software, processes, information in storage or transit, applications, services, and systems that can be connected directly or indirectly to networks

NOTE: Definition from Recommendation ITU-T X.1205 [i.33].

cyber security (or cybersecurity): collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets

NOTE: Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment. Cybersecurity strives to ensure the attainment and maintenance of the security properties of the organization and user's assets against relevant security risks in the cyber environment. The general security objectives comprise the following:

- Availability.
- Integrity, which may include authenticity and non-repudiation.
- Confidentiality, Recommendation ITU-T X.1205 [i.33].

Also,

cybersecurity: preservation of confidentiality, integrity and availability of information in the Cyberspace

NOTE: Definition from ETSI TR 103 591 [i.2].

cyberspace: complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form

NOTE: Definition from ETSI TR 103 591 [i.2].

Internet connected services: Allowing devices to communicate with other devices over a broad network. These connections usually involve a link occurring between devices and systems and the collection of data (definition from [i.8]).

Internet of Things (IoT): The totality of devices, vehicles, buildings and other items embedded with electronics, software and sensors that communicate and exchange data over the Internet.

NOTE: Definition from [i.8].

Secure by Design: A design-stage focus on ensuring that security is in-built within consumer IoT products and connected services.

NOTE: Definition from [i.8].

3.2 Symbols

Void.

3.3 Abbreviations

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

AES	Advanced Encryption Standard
AIOTI	Alliance for Internet of Things Innovation
ANT+™	Advanced and Adaptive Network Technology

NOTE: Trademark of Garmin.

BSIMM	Building Security in Maturity Model
CCRA	Common Criteria Recognition Agreement
CIA	Confidentiality Integrity Availability
cPP	co-operative Protection Profile
DCMS	Department of Culture, Media and Sport (a UK Government body)

ECSO	European Cyber Security Organisation
EDPS	European Data Protection Supervisor
ENISA	European Network Information Security Agency
EP	ETSI Project
ERP	Enterprise Resource Planning
ES	ETSI Standard
EU	European Union
FIPS	Federal Information Processing Standard
GDPR	General Data Protection Regulation
GSMA	GSM Association (a trade body)
HSM	Hardware Security Module
ICT	Information and Communications Technology
IoT	Internet of Things
ISM	Industrial Scientific Medical
IT	Information Technology
ITS	Intelligent Transport System
LAN	Local Area Network
M2M	Machine to Machine
NCSC	National Cyber Security Centre (a UK Government body)
NFV	Network Function Virtualisation
NIS	Network Information Security
NISD	Network Information Security Directive
NoT	Network of Things
NSA	National Security Agency
OASIS	Organization for the Advancement of Structured Information Standards
OES	Operators of Essential Services
OoT	Obligation of Trust
PII	Personal Identifying Information
RDSP	Relevant Digital Service Providers
RTS	Root of Trust for Storage
RTV	Root of Trust for Verification
SAML	Security Assertion Markup Language
SAMM	Open Software Assurance Maturity Model
SCP	Smart Card Platform
SDL	(Microsoft) Security Development Lifecycle
SE	Secure Element
SSDL	Software Security Development Lifecycle
TCG	Trusted Computing Group
TEE	Trusted Execution Environment
TPM	Trusted Platform Module
TSS	TPM Software Stack
TVRA	Threat Vulnerability Risk Analysis
UICC	Universal Integrated Circuit Card
XACML	eXtensible Access Control Markup Language

4 Security in the context of IoT

4.1 A global approach to IoT Systems

4.1.1 Major characteristics of IoT systems

IoT systems are often seen as an extension to existing systems needed because of the (potentially massive) addition of networked devices. However, this approach does not take stock of a set of essential characteristics of IoT systems that push for an alternative approach where the IoT system is at the centre of attention of those who want to make them happen. This advocates for an "IoT-centric" view.

Most of the above-mentioned essential characteristics may be found in other ICT-based systems. However, the main difference with IoT systems is that they all have to be dealt with simultaneously. The most essential ones are:

- **Stakeholders.** There is a large variety of potential stakeholders with a wide range of roles that shape the way each of them can be considered in the IoT system. Moreover, none of them can be ignored.
- **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.
- **Interoperability.** There are very strong interoperability requirements because of the need to provide seamless interoperability across many different systems, sub-systems, devices, etc.
- **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.
- **Technologies.** By nature, all IoT systems have to integrate potentially very diverse technologies, very often for the same purpose (with a risk of overlap). The balance between proprietary and standardized solutions has to be carefully managed, with a lot of potential implications on the choice of the supporting platforms.
- **Deployment.** 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 have to deal with the need to support both Cloud-based and Edge-based deployments with the associated challenges of management of data, etc.
- **Legacy.** Many IoT systems have to deal with legacy (e.g. existing connectivity, back-end Enterprise Resource Planning (ERP) systems). The challenge is to deal with these requirements without compromising the "IoT centric" approach.

4.1.2 The need for an "IoT-centric" view

4.1.2.1 Introduction

In support of an "IoT-centric" approach, some elements have been used in the present report in order to:

- Support the analysis of the requirements, use cases and technology choices (in particular related to interoperability).
- Ensure that the target audience can benefit from recommendations adapted to their needs.

4.1.2.2 Roles

A drawback of many current approaches to system development is a focus on the technical solutions, which may lead to suboptimal or even ineffective systems. In the case of IoT systems, a very large variety of potential stakeholders are involved, each coming with specific - and potentially conflicting - requirements and expectations. Their elicitation requires that the precise definition of roles that can be related to in the analysis of the requirements, of the use cases, etc.

Examples of such roles to be characterized and analysed are: System Designer, System Developer, System Deployer, End-user, Device Manufacturer. Some of these roles are specifically addressed in the present document.

4.1.2.3 Reference Architecture(s)

In order to better achieve interoperability, many elements (e.g. vocabularies, definitions, models) have to be defined, agreed and shared by the IoT stakeholders. This can ensure a common understanding across them of the concepts used for the IoT system definition. They also are a preamble to standardization. Moreover, the need to be able to deal with a great variety of IoT systems architectures, it is also necessary to adopt Reference Architectures, in particular Functional Architectures. The AIOTI High-Level Architecture (see ISO/IEC 27032 [i.34]) is the reference for the present document.

4.1.2.4 Guidelines

The very large span of requirements, Use Cases and roles within an IoT system make it difficult to provide prototypical solutions applicable to all of the various issues addressed. The approach taken in the present report is to outline some solutions but also to provide guidelines on how they can be used depending on the target audience. Such guidelines are associated to the relevant roles and provide support for the decision-making.

5 Simplified security model for IoT

Notwithstanding the discussion in clause 6 the purpose of security technologies is multi-fold:

- **Confidentiality:** Information shared by Alice with Bob is only visible to Bob and Alice. If Eve can access the information, she cannot ascertain the meaning of the content. Confidentiality is primarily achieved using cryptographic encryption (from ETSI TS 102 165-2 [i.25]).
- **Integrity:** Information shared by Alice with Bob can be proven by Alice not to have been manipulated by a 3rd party (e.g. Eve). Bob can verify this is the case. Proof and verification of document integrity is primarily achieved using cryptographic hash functions which have specific characteristics (from ETSI TS 102 165-2 [i.25]).
- **Availability:** This addresses the aim of ensuring that an authorized party (e.g. Alice) is able to access services or information when needed. In other words, that Alice has access only to those assets she is allowed to access and that they are available to Alice when legitimately demanded, and that an adversary, Eve, does not have access. The technologies that address this include Identity Management, Authentication and Access Control, in addition considerations in the availability domain include reliability and resilience which, whilst not strictly addressed by security technology, impact on availability (from ETSI TS 102 165-2 [i.25]).

One of the many characteristics of IoT is that the number of communicating entities is very large and the number of possible relationships per device is larger than, say, with cellular telecommunication.

NOTE 1: Whilst the population of cellular telecommunications devices is very large (more than 5 billion) the nature of the connection is pre-defined by the SIM containing the subscriber mobile identity and its association to a single trusted provider (holder of the symmetric key used in the network/device authentication process).

NOTE 2: 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.

As a trivial example IoT communications security may be considered as equivalent to sending presents to somebody. To ensure the recipient does not know the content before unwrapping, the sender masks the content by wrapping the gift - this makes the content confidential. The intended recipient is clearly indicated on the label as is the sender - this identifies the parties to the transaction and depending on how names are written may confer some proof of identity. Finally, in order to ensure the package is not damaged the sender adds packaging that protects it - this is some means of ensuring the integrity of the package is maintained in transit. Translating this to IoT, data from A to B the data can be encrypted to confer confidentiality, the parties A and B have to be able to prove their identity to confer authenticity to the exchange, and the parties can add data to the package that will be used to assure and verify the integrity of the package.

There are a number of complexities in IoT that arise from the nature and number of both devices and connections. The most obvious of these is key management.

6 Purpose of cyber security as it applies to IoT

6.1 Overview

The general purpose of security technology is to give confidence to the stakeholder that the risk of cyber attacks, or any other attack on the assets of a system, are mitigated. The general model given in Figure 1, adapted from ETSI TS 102 165-1 [i.10] illustrates the concept. In brief:

- A system consists of assets. An asset may be physical, human or logical. **Assets** in the model may have **Weaknesses** that may be attacked by **Threats**. A **Threat** is enacted by a **Threat Agent** and may lead to an **Unwanted Incident** breaking certain pre-defined security objective. A **Vulnerability** is modelled as the combination of a **Weakness** that can be exploited by one or more **Threats**. When applied, **Countermeasures** protect against **Threats** to **Vulnerabilities** and reduce the **Risk**.

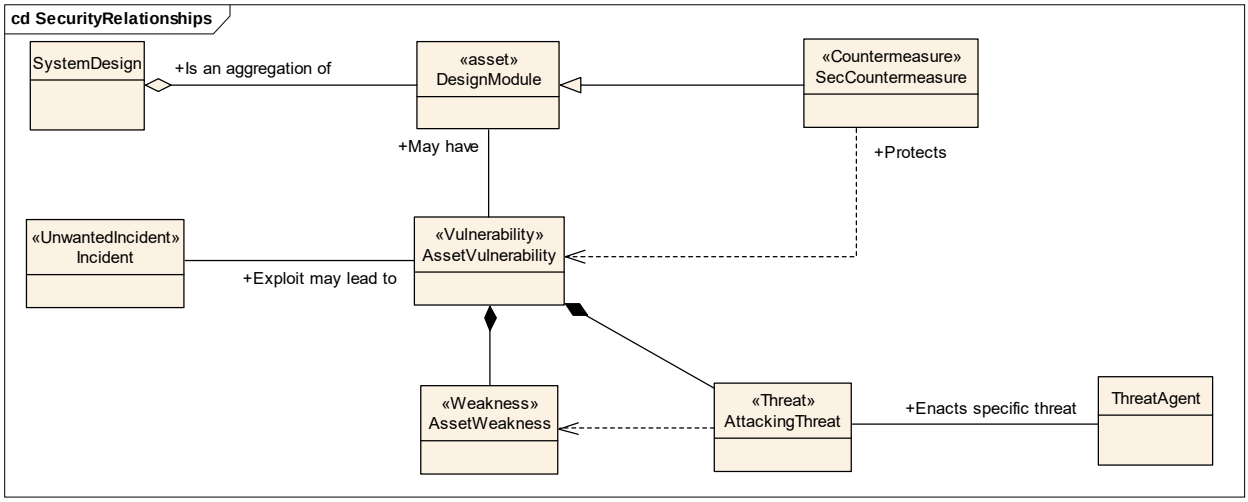

Figure 1: Generic security model for systems

One of the purposes of security design is to minimize the probability of any instance of the class "unwanted incident" being created. It should be noted that whilst some countermeasures may themselves become system assets, and as such have their own vulnerabilities, many instances of countermeasures will be considered as policies, system guidelines and, if captured early enough, system redesign.

There is a certain fashion to use the term "cyber security" to cover all aspects of security as it applies to software, to electronic hardware, and to data. In using this approach, the term "IoT Security" is an all-encompassing subset of cyber security and overlaps with Machine-to-Machine security. There is additionally a lack of precision in the term "security" as it may translate to meaning safety, or it may refer to financial instruments. For the purposes of the present document security (or IoT security) refers to the specific aspects of cyber security that pertain to the Internet of Things domain. This requires some consideration of the nature of the assets in the IoT, and in particular how those assets connect to each other in the building of systems. This is considered in more detail in clause 6.4 below.

The variation of IoT from the generic security model is very small and only deals with the definition of system as an aggregation of assets and in the identification of responsible parties. In a generic residential IoT system, the bulk of the responsibility for overall system security lies in the hands of the household. Introducing a new element to the residential system requires that the new element is recognized and configured to the residential security domain.

For security designers, with a view to mitigate threats, the IoT challenge is, as suggested above, not significantly different from any other system. The approaches towards mitigation of attacks is broadly similar: If data is at risk from capture through eavesdropping the default protection mechanism is to apply some form of confidentiality shielding most often using cryptographically strong encryption. The problem in part for IoT in achieving high system and device security is that of uncertainty: Of identity, of key management, of the deployment environment. High security often requires elimination of uncertainty and random variables which are perhaps more difficult in a generic IoT environment. For example, in an environment of Consumer IoT where devices can be purchased and installed by the consumer it is unlikely that the vendor, or manufacturer, is aware in detail of the way in which the IoT device is to be used. For such environments the "by default" capabilities and data minimization approaches that are widely recommended cannot be assured to be sufficient (i.e. the vendor or manufacturer is unlikely to be able to perform on site verification that the implemented and deployed system is consistent with their own best practice). By contrast in an industrial IoT environment devices may be subject to strict control before being installed and operated, at least this would certainly be expected of any organization that has followed the recommendations of the ISO/IEC 27000 [i.48] series of controls, or adopted the controls recommended in ETSI TR 103 305 [i.26].

6.2 The Security Cycle

As identified in the introduction of ETSI TR 103 306 [i.1] cyber security consists of a continuing cycle of structured actions to:

- Identify:
  - Requires gaining an understanding of the system that allows the owner to state the risks to systems, assets, data, and capabilities.
  - Requires understanding of the nature of attacks and the nature of change on the system.
- Prevent (also termed as protect):
  - The application of countermeasures.
  - At design time, at update time.
- Prepare (also termed as detect):
  - Being able to react - measuring how the security of the system is performing.
- Respond:
  - Implement resilience and restoration of impaired capabilities resulting in an update of the system and return to the start of the cycle.

All of these activities rely on the trusted, timely sharing of related structured information as illustrated in Figure 2.

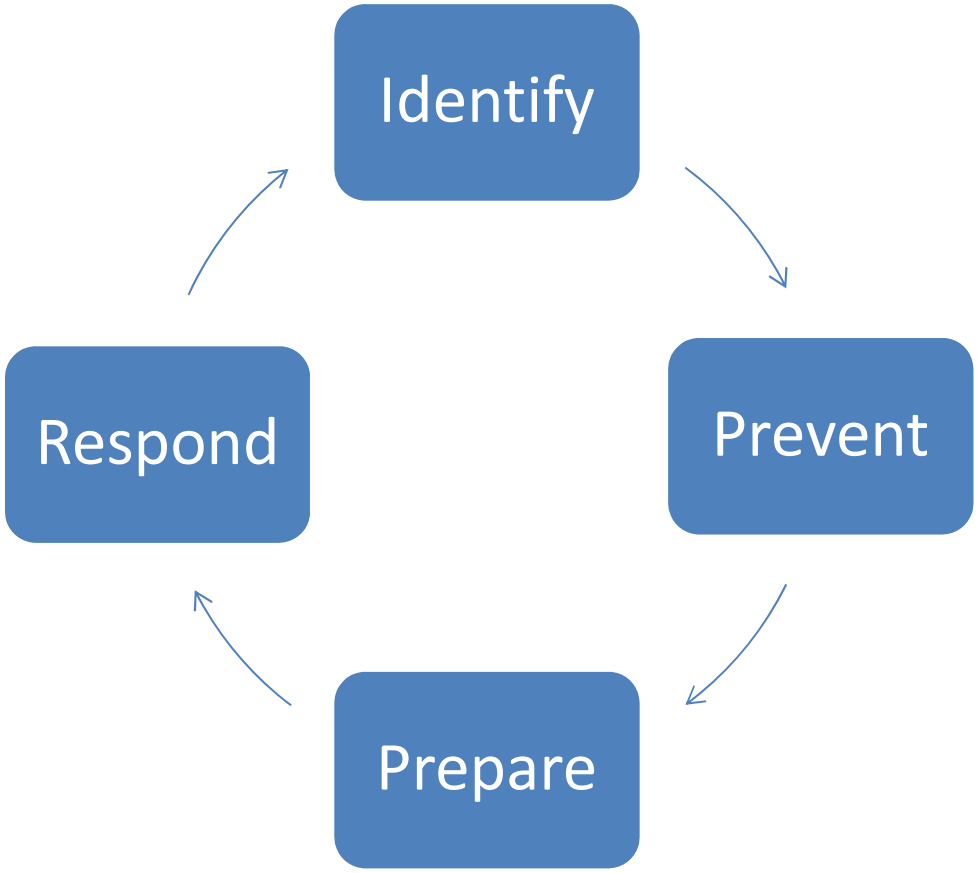

Figure 2: Basic activities of the cyber security ecosystem

As also identified in ETSI TR 103 306 [i.1] effective cross sector security requires the sharing of knowledge. This has been summarized as a requirement for interoperability across each of the syntactic, semantic, mechanical and process domains.

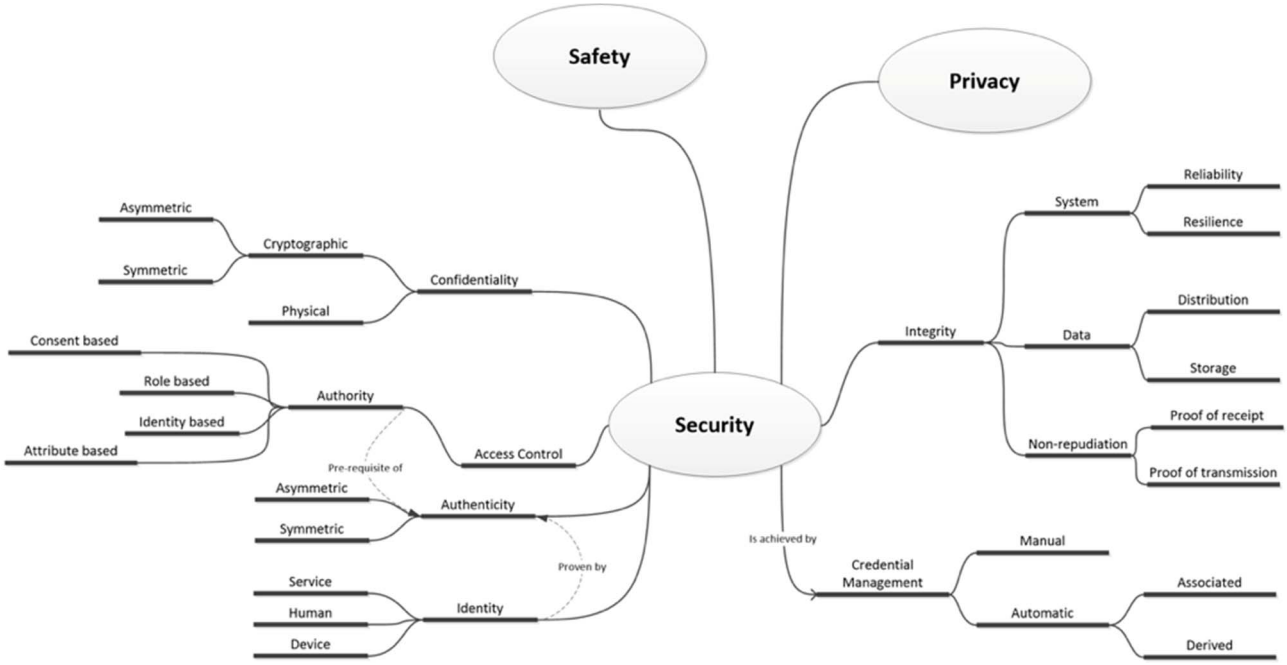

Figure 3: Mindmap of concepts and functions associated to security

The extension of security to concepts and functions as shown in Figure 3 is illustrative of the overall complexity of achieving security in systems. For IoT, there are many unknowns that have to be resolved prior to overall security being achieved. As an example, the form and function of an IoT device, its identity, its set of security credentials, the algorithms it deploys to assure each of confidentiality, identity and integrity, the means by which it interacts with peers and other systems, all of these have to be known.

The nature of the system determines to some extent the difficulty of each of these elements of security. For instance, in a simple view of the home connected IoT device that needs to connect to an external cloud server for data storage, but also has to be associated to the residential system for access, identity management and credential management are obviously key concerns. Many current standards exist for each of the concepts and functions in Figure 3 to allow the problems to be resolved.

6.3 The CIA Paradigm

The core technical work in much of security focusses on the application of the CIA paradigm: Confidentiality; Integrity; Availability. However where to apply techniques that give assurances of each of the CIA dimensions is not a trivial exercise and should be rooted in a risk analysis that identifies the threats, the threat agents, the weaknesses and vulnerabilities in the system. Methods for performing a risk analysis and identifying the assets of any system are described in the following core documents from ETSI:

- ETSI TS 102 165-1 [i.10].
- ETSI TR 103 305 [i.26].

It is strongly recommended that any application of security technology adopts the risk analysis approach and the cataloguing of the system identified in the documents cited above.

The root of the CIA paradigm is the view that threats can be classified as one of 5 types:

- interception;
- manipulation;
- denial of service;
- repudiation of sending, and
- repudiation of receiving.

NOTE: A more general case may be repudiation of involvement in an action, for communication this can be stated as repudiation of sending or receiving, but may be any other action such as editing or deleting a file (where such actions themselves are considered under manipulation threats).

Similarly, security objectives can be classified as one of 5 types (commonly referred to as "CIA" types):

- Confidentiality.
- Integrity.
- Availability.
- Authenticity.
- Accountability.

A consequence of the CIA model is to consider security in broad terms as determination of the triplet {threat, security-dimension, countermeasure} leading to a triplet such as {interception, confidentiality, encryption} being formed. The threat in this example being interception which risks the confidentiality of communication, and to which the recommended countermeasure (protection measure) is encryption.

The application of the CIA model (paradigm) to the IoT is strongly recommended best practice. The perceived difficulty in IoT is identifying the nature of the threat. This is particularly well considered in the DCMS report [i.8] and is somewhat closely associated to some of the peculiarities of IoT described in clause 6.4 of the present document, but include poor default configuration, ability to be repurposed (i.e. to run programs not commensurate with the base operation of the device), inability to report change of purpose and such. If the device itself can be repurposed, for example to act as a node in a botnet, this is often by masquerade of the attacker as a legitimate user, an attack that is simplified if all devices of a particular type have the same credentials to access and modify their functionality. Countering such attacks requires acceptance that the attack is possible and in many respects is the application of traditional security thinking in which access control credentials (say username and password) are managed to be unique (the simplest statement of this guidance is to encourage no default passwords).

6.4 Peculiarities of IoT

6.4.1 IoT characteristics

It is probably true that IoT is not a distinct security problem. However, in IoT, in the general case, there may be more uncertainties to be resolved than in conventional centrally managed security systems. The mechanics of protection for IoT are broadly similar to those of any other ICT system:

- Confidentiality may be preserved using encryption.
- Masquerade may be countered by authentication.
- Manipulation may be countered by integrity assurance.

In each of these, whilst the core mechanisms for IoT are either identical or very similar to non-IoT systems the primary difficulty in IoT, as with all security systems, is key management.

6.4.2 Resource limitation

The range of devices that makeup the IoT are such that there can be no simple generalizations. However, for certain classes of device there is limited processing and memory overhead to perform complex cryptographic operations. In addition, where a device may be required to digitally sign data it may be required to perform as a trusted signature creation device and have access to a hardware root of trust, this latter may be provided in the form of a trusted platform module. It should be noted in the risk analysis any constraints on hardware or software processing that will impact an IoT device being used as a component of a cryptographic security operation.

The memory constraint of AES is identified in FIPS 197 [i.11] and theoretically for a 128-bit key size requires 316 Bytes of memory for encryption operations and 320 Bytes for decryption operations. Practical implementations expand the memory requirement depending on both the compiler used and the language in which AES is implemented and may be an order of magnitude greater than the theoretical guidance.

For authentication and encryption based on asymmetric cryptography, the resource requirement is often much greater than for symmetric cryptography. The rule of thumb in non-IoT systems to move any secured relationship from reliance on resource hungry asymmetric cryptography to the relatively resource light symmetric cryptography. This rule of thumb applies equally to IoT.

NOTE: For devices with no retained memory of a connection the establishment of a resource light secured connection may not be readily achievable.

6.4.3 Connectivity modes

In like manner to the discussion of resource limitation the way in which IoT devices connect to each other and to other system elements needs to be considered. In conventional security design there is a convention to minimize, or to eliminate, uncertainty regarding relationships between assets. This means that asset-A is generally constrained to have a relationship with asset-B and any other asset is identified as an adversary. In some security systems the restriction is absolute, i.e. a specific instance of an asset is constrained in the relationships it can hold, whereas in the IoT such constraints are either not viable or not allowed.

6.4.4 Radio considerations

Whilst there is some lack of agreement it appears to be a widely held view that IoT will use low power radio connectivity in license free spectrum (primarily the Industrial Scientific Medical (ISM) bands). The dominant radio technologies in what may be termed as IoT are Bluetooth™ and some forms of IEEE 802.11™ [i.49] and IEEE 802.15.4™ [i.50] (Zigbee™) with a number of proprietary technologies including ANT+™ (from Garmin). One characteristic of the connectivity is that each of range (10 s of metres) and power (not exceeding 100 mW) are low.

7 Regulatory context of IoT Security

7.1 Overview

In the period to approximately mid-2016, the EU regulatory landscape related to cyber security was relatively fragmented with legal obligations and principles scattered across numerous legal acts. Due to recent technological advancements and increased connectivity, the risk of becoming a victim of a cybercrime has also increased. Thus, EU law-makers been taking steps to increase cyber resilience across Member States by making the respective regulatory landscape more concise, among others. In this respect, they have adopted Directive (EU) 2016/1148 [i.9] (commonly referred to as the "NIS Directive"), being the first EU horizontal legislation addressing cybersecurity challenges, and the General Data Protection Regulation [i.21], which addresses the topic from the perspective of security of personal data and the obligations that result on organizations that use data.

7.2 GDPR

NOTE 1: In the text below reference is made to both Articles and Recitals of the GDPR. The Recitals are linked to each article and depict the rationale for why the articles of the GDPR have been adopted.

Unlike the NIS Directive discussed in clause 7.3, GDPR approaches the topic of cybersecurity from the data perspective, prescribing obligations and responsibilities on organizations processing data related to natural persons.

There are several provisions that the GDPR makes which suggest security solutions. Article 24, for example, introduces concrete obligations assigned to controllers to "*implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation. Those measures shall be reviewed and updated where necessary*". The measures that are expected should consider in their design and implementation the nature, scope, context and purposes of the processing and the risk to the rights and freedoms of natural persons. This is a subtle deviation from the CIA paradigm in security design where there is greater concentration on the application of security technology to counter specific forms of attack. Thus, in a purely security context where there is a threat of eavesdropping a reasonable counter measure will be the provision of encryption to thwart the eavesdropper. The security model, in its risk analysis, will consider the impact of the eavesdropping by consideration of the content of an eavesdropped communication, i.e. if knowledge of the content by an adversary has mild, major or critical impact on the attacked parties, and take into account this impact assessment with an assessment of the likelihood of an attacker gaining access to the communication. Thus, from a security perspective communication in a trusted environment is at less risk than the same communication in an untrusted environment, even if the impact is identical.

NOTE 2: The GDPR references a need for Data Protection Impact Assessment and not for a Data Protection Risk Assessment whereas the security perspective is to determine both impact and likelihood, with the general understanding that it is difficult to modify impact, but it is difficult to modify the likelihood of an attack.

In the GDPR context it is the data controller that defines what data is collected and thus it is the responsibility of the Data Controller to document, and be able to demonstrate, the proportionality of measures taken to appropriate authorities. The GDPR adopts a risk-based approach which is consistent with the risk-based analysis to determine appropriate security provision that are recommended across most SDOs. In this respect Recital 75 identifies examples of data that when exploited by an adversary may give result in physical, material or non-material damage, and clarifies, by example, the forms of damage that should be considered. This is consistent in concept, although not in detail, to the methods used in many security risk analysis approaches, where risk is seen as a combination of the likelihood of an adversary mounting an attack, and the impact of the attack when it succeeds. The outline in Recitals 75 and 76 of GDPR are somewhat closer to consideration of the impact element of risk analysis methods such as those found in ETSI's TVRA (ETSI TS 102 165-1 [i.10]) and the ISO/IEC Common Criteria domain (ISO/IEC 15408 [i.17]) rather than to combinational product of the evaluation of likelihood of an attack and assessment of the impact of an attack which is the foundation of most security risk analysis.

Overall, as highlighted by the European Data Protection Supervisor (EDPS) in their report responding to the cybersecurity package [i.7], "applicable data protection law, including the General Data Protection Regulation, considers information security as an enabler to the protection of individuals through the protection of their personal data. Information security is among the data protection 'principles' laid down by the law (Article 5(1)(f))."

It should be noted that a general security guideline, consistent across all security practice, is that only essential data is collected and this principle of data minimization is consistent in GDPR. This is explicitly identified in Article 25 of the GDPR which calls for privacy-by-design, privacy-by-default by means of "Data protection by design and by default" which refers to Recital 78 requiring "Appropriate technical and organisational measures". A further strong link between GDPR and security design practice is found in GDPR Article 32 for security of processing which addresses the suite of risks normally considered in security design (i.e. to address mechanisms to minimize the likelihood of an adversary accessing and exploiting data). It is made clear in GDPR that privacy is a qualified right and Recitals 19 and 49 when properly considered across a system have similar impact to the provisions made for Lawful Interception in telecommunications by ensuring proper provision of security and privacy protection and lawful exception in all parts of the system.

A general caveat to consideration of the GDPR is that the GDPR assumes central processing and consent from edge to middle, i.e. the IoT device or its user agrees consent to processing. However, a wider reading of Article 6 of GDPR, "Lawfulness of processing" makes it clear that consent is only one route to lawful processing. In GDPR, the scope of data gathering and data processing is set by a visible data controller. The general architecture of GDPR is not consistent with all IoT application models although the obligations are expected to apply to them. In addressing the scope of the GDPR for IoT the device has to act in concert with other elements in the system to ensure that data processing and data controller roles are clearly visible on demand to the end user. It may not be clear to the IoT device who the data controller is, and a single IoT device may be used in more than one context where more than one data controller exists.

7.3 Network Information Security Directive

7.3.1 The objectives of the Directive

While almost three quarters of Europeans believe that digital technologies have a positive impact on our economy, society and quality of life [i.13] a vast majority of them believe that the risk of becoming a victim of cybercrime is increasing. In this regard, it is propitious that EU law makers have begun addressing the issue of cyber security, starting with the introduction of the NIS Directive. The NIS directive is the first EU horizontal legislation addressing cybersecurity challenges, aiming to increase the overall level of cybersecurity resilience and cooperation in the EU and to prevent far-reaching consequences of cyber-attacks within the bloc [i.14]. Recognizing the important role of network and information systems and services in the society (which IoT devices and ecosystems are an inseparable part of), the Directive acknowledges that their reliability and security are essential to economic and societal activities, and in particular in Recital 1 to the functioning of the internal market. In doing so, it aims to put forward measures promoting a culture of risk management and preventing or mitigating the effects of the most serious incidents capable of having a significant disruptive effect on these systems and services. These can result in an impediment of the pursuit of economic activities, substantial economic loss, undermining of user confidence and major damage caused to the economy of the Union as stated in Recital 2 of the NIS Directive.

7.3.2 Scope of the NIS Directive

Aiming to achieve high common level security and improve functioning of the internal market, the NIS Directive puts into place measures concerning security of *network and information systems*, encompassing a wide domain of network, infrastructure, devices as well as data (defined in Article 4 of the NIS Directive). By doing so, the NIS Directive appears to address all elements and stakeholders of the connected ecosystem but focusses on a restricted range of operators and providers, and thus of the underlying services. This approach explicitly excludes many of the device and edge of network services and operations that will be within the scope of IoT.

To promote a culture of risk management and ensure that the most serious incidents are reported (as cited in Recital 4 of the NIS Directive) it is required that specific security and incident notification requirements apply to *operators of essential services* (defined in Article 14) and *digital service providers* (defined in Article 16). While the Directive clearly states that hardware manufacturers and software developers should not be considered as operators of essential services, nor digital service providers, it contains a fairly broad definition of *cloud computing services*, being "services allowing access to a scalable elastic pool of shareable computing resources". It is reasonable to expect that many IoT devices will interact through facilities and services offered by operators of essential services, and by digital service providers, thus whilst IoT devices may not be directly impacted by NIS the services enabled by them they may be. This therefore has to be addressed on a case by case basis and is not viewed as a generic IoT activity.

In summary, the scope of the NIS Directive with respect to IoT appears to clearly exclude the edge elements that comprise IoT devices, although a naïve reading may suggest that in this case NIS does not apply to the IoT this should not be the interpretation - the NIS directive applies to the whole system and does not seek to distinguish between forms of device that make up either of the key forms of organization addressed by NIS:

- operators of essential services (OES); and
- relevant digital service providers (RDSPs).

OES include organizations that run services that are critical to the economy and wider society, such as water, transport, energy, healthcare and digital infrastructure. RDSPs include online search engines, online marketplaces and cloud computing services. IoT devices may be key elements of either of these forms of service provision.

If the OESs, or the RDSPs, make special provisions for IoT devices then the NIS Directive obligations do apply. This is difficult to fully assess as whilst IoT elements, endpoints, devices and other solutions may form a significant part of the connected ecosystem and thus be addressed by provisions of the NIS Directive they may not be legally bound by it. However, the assertions made in the present document for best practice will result in compliance to the existing scope of the NIS Directive [i.9] and any extension of it made by, for example, the Cyber Security package discussed in clause 7.4.

7.3.3 Security and incident notification requirements

Aside from improving national cybersecurity capabilities, the Directive aims to build cooperation at EU level and promote a culture of risk management and increase resilience. These two objectives are addressed by identifying various relevant stakeholders and their responsibilities, as well as notification obligations for operators of essential services and digital service providers to comply with, respectively. Figure 4 illustrates the "landscape" as set out by NIS Directive, as well as relations between individual stakeholders involved.

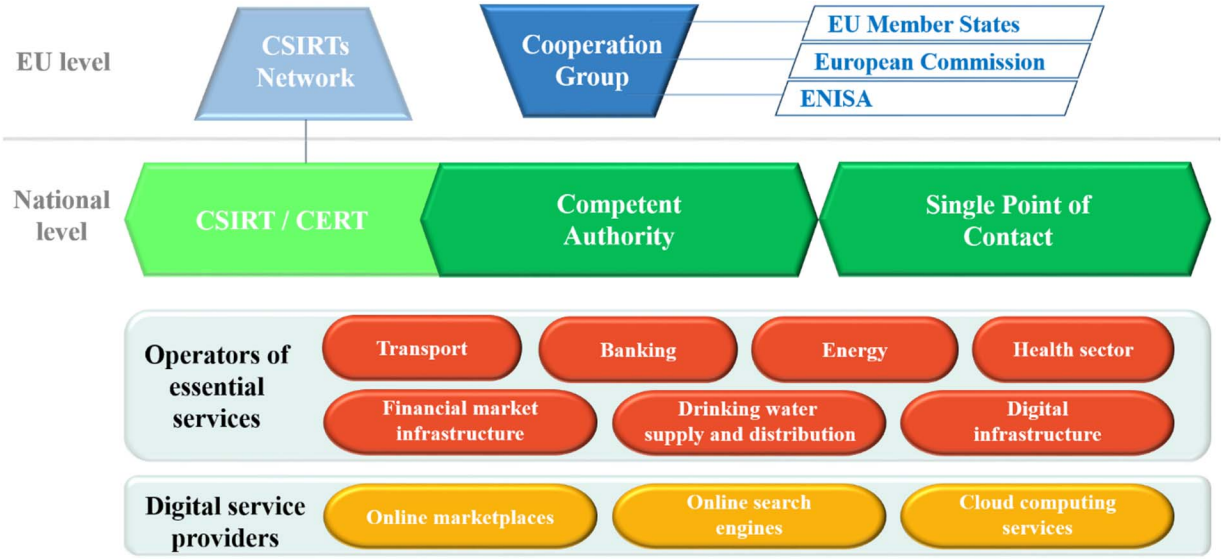

Figure 4: Overview of NIS Directive Stakeholders (from [i.14])

To support and facilitate strategic cooperation and exchange of information among Member States, the Directive establishes the *Cooperation Group*, composed of representatives of EU member states, European Commission and European Union Agency for Network and Information Security (ENISA).

NOTE: The implementation of the Directive will be facilitated on the basis of guidance provided by the Commission on how organizations are expected to implement the Directive in practice. The Commission is also expected to provide additional interpretation of specific provisions.

7.3.4 Available security analysis of NIS

The Network Information Security Directive analysis prepared by ENISA [i.9] has identified that Network Information Systems share the same set of fundamental building blocks as any other system. The bulk of IoT exists at the edge of the network that is addressed by the NISD and only makes use of services offered in the core of the network, that may include connectivity, data storage and processing.

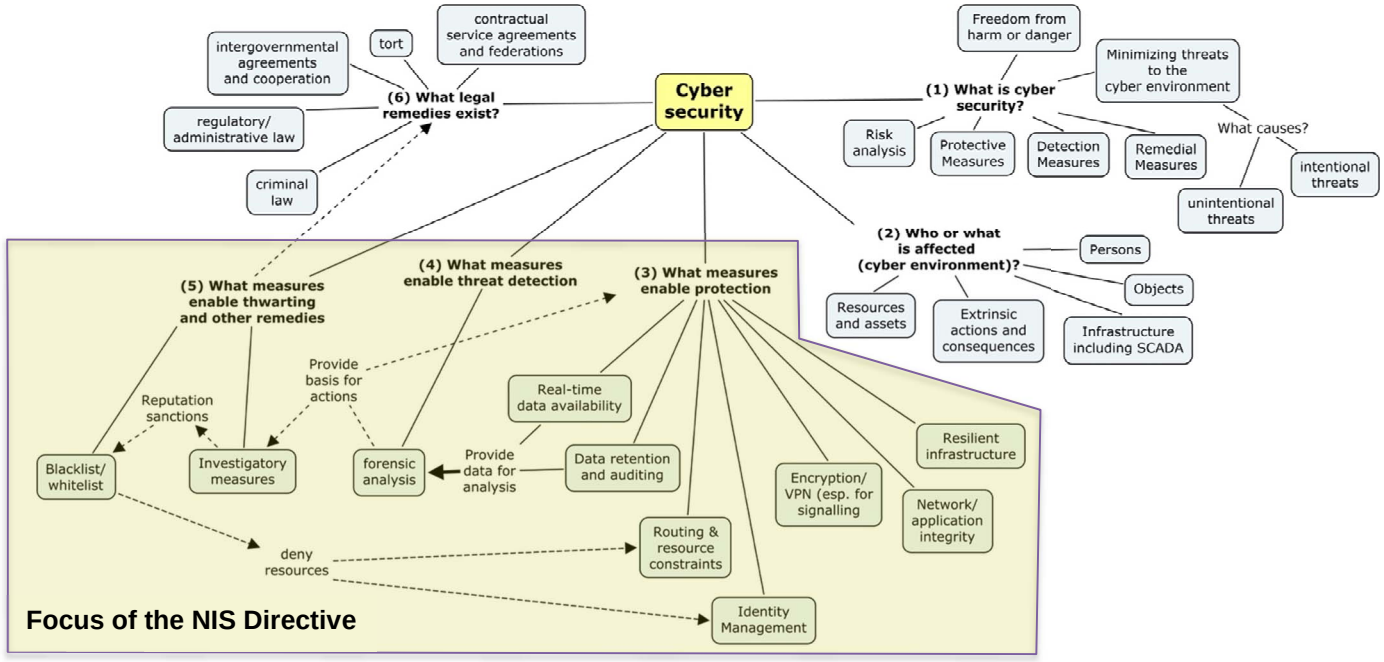

Figure 5: Visualization of the relationship of NISD to Cyber-security

In terms of NIS and IoT, the primary concerns for securing the Network against an IoT adversary and vice versa are the ability to mutually identify and authenticate the IoT device and the Network.

7.4 Cyber Security package (in development)

NOTE: The Cyber Security Package is an ongoing development of actions undertaken in the EU that aims to build EU resilience to cyber-attacks and to improve the EU's cybersecurity capacity, it also aims to create an effective criminal law response, and to strengthen global stability through international cooperation.

Implementation of the NIS Directive is an essential part of the Cybersecurity package presented on 13 September 2017. Member States are therefore encouraged to take appropriate measures to ensure that the provisions and the cooperation models of the NIS Directive can provide the best possible EU-level tools to achieve a high common level of security of network and information systems across the Union [i.27] and [i.9].

Finally, it is important to stress that the obligations set under the GDPR, also, with respect to security of personal data apply in addition to obligation set under NIS. Organizations, thus, falling under both legal acts may encounter practical implications. For example, what is deemed to be an appropriate technical measure to protect personal data in line with the GDPR may differ from the respective measures to protect service continuity in the light of the NIS. Similarly, the incident notification requirements under both acts maybe partially overlapping yet they serve a different purpose.

8 Overview of security standardization ecosystem for IoT

8.1 Introduction

The main characteristics, and players, of the global security standardization ecosystem have been published by ETSI in ETSI TR 103 306 [i.1]. In addition, detailed aspects of that ecosystem covering specific areas have been addressed in ETSI TC CYBER by the following deliverables:

- ETSI TR 103 456 [i.38]
- ETSI TR 103 369 [i.39]
- ETSI TR 103 331 [i.40]
- ETSI EG 203 310 [i.41]
- ETSI TR 103 309 [i.16]
- ETSI TR 103 304 [i.42]

Many of these documents reference or cite security provisions from other SDOs including those from ISO, ITU-T and IETF. Of the parties identified in ETSI TR 103 306 [i.1] are actively addressing aspects of IoT security with the majority of the activity at present being in the development of best practice guides. More detailed security work addressing protocols, processes and algorithms is being undertaken across all of these groups to address specific modes of operating and deploying IoT systems and services.

8.2 Obligation of trust protocols

In IoT in general where there is no predefined relationship between entities, there is a requirement for IoT devices to find and attach to each other. The role of asset discovery is addressed in clause 8.3. Once identified the foundation of security is in trust and the present clause identifies work that enables establishment of trust.

The overall concept of Obligation of Trust (OoT) is described in ETSI TS 103 485 [i.23]. To quote from ETSI TS 103 485 [i.23], the intent of the OoT exchange is that parties to data negotiate the conditions (constraints) that apply to data that they share. Obligations that are exchanged may take 2 distinct forms:

- security obligations (cryptographic mechanisms required for protection); and
- privacy obligations (usage and onward sharing requirements).

The aim of these kind of protocols is to develop support for "non-repudiation of consent" in which the system and users build a strong proof of having given consent to specific processing of precisely defined data. ETSI TS 103 485 [i.23] addresses the application of OoT in the IoT context where there is no pre-established relationship between entities and thus uses the OoT to establish a secured and privacy protecting relationship.

8.3 Identity management and asset discovery

In IoT in general where there is no predefined relationship between entities, there is a requirement for IoT devices to find and attach to each other. In ETSI TS 103 486 [i.24] this is captured in the following thought experiment:

SCENARIO: Two parties in a crowded room need to make a secure connection but they do not know each other in advance, and they also do not actually know if they are in the room together. Thus, the parties have to find each other amongst a pool of adversaries each of whom has the opportunity to intercept the signals within the discovery protocol and to attempt a masquerade.

The scenario above is particularly applicable to IoT and has led to the development, documented in ETSI TS 103 486 [i.24], of a cryptographically strong discovery protocol.

8.4 IoT and M2M specific groups

8.4.1 ETSI groups

8.4.1.1 Overview of ETSI groups active in IoT and M2M

A number of groups in ETSI are active in the IoT/M2M domain although not all of them have specifically addressed these terms in their work plans. For example, the Intelligent Transport Systems group is primarily a machine-to-machine communications group, the work in ETSI's membership of 3GPP has recently focussed on the requirements for cellular based networking for IoT and M2M. Similar examples can be found across the ETSI Technical Bodies.

8.4.1.2 SmartM2M

Activity in security across the SmartM2M is generally low with no active work items (the present document and its associated training material is not considered) and publications pre-dating the split from TC M2M to SmartM2M and the partnership project oneM2M.

ETSI TR 103 167 [i.15] does provide a base threat analysis however the resultant security requirements are not clearly identifiable in a resultant security architecture and suite of services.

8.4.1.3 eHealth

ETSI EP eHEALTH has no specific work items that address IoT or IoT security. However, the nature of eHealth in general is that many devices and functions interact with each other to monitor, diagnose and treat health conditions. Any malicious attack on such devices may lead to ill-health, or even death, of a patient. It is expected that EP eHEALTH will sponsor work in security across multiple ETSI Technical Bodies and partner SDOs as required.

8.4.1.4 SmartBAN

Nothing specific to security has been published although the developing work programme is seeking to address this topic.

8.4.1.5 ITS - Working group 5

Intelligent Transport Systems (ITS) is an example of IoT or generally of M2M and has produced a number of standards that address security of the specific Co-operative ITS for (primarily) vehicular safety using radio devices operating at 5,9 GHz.

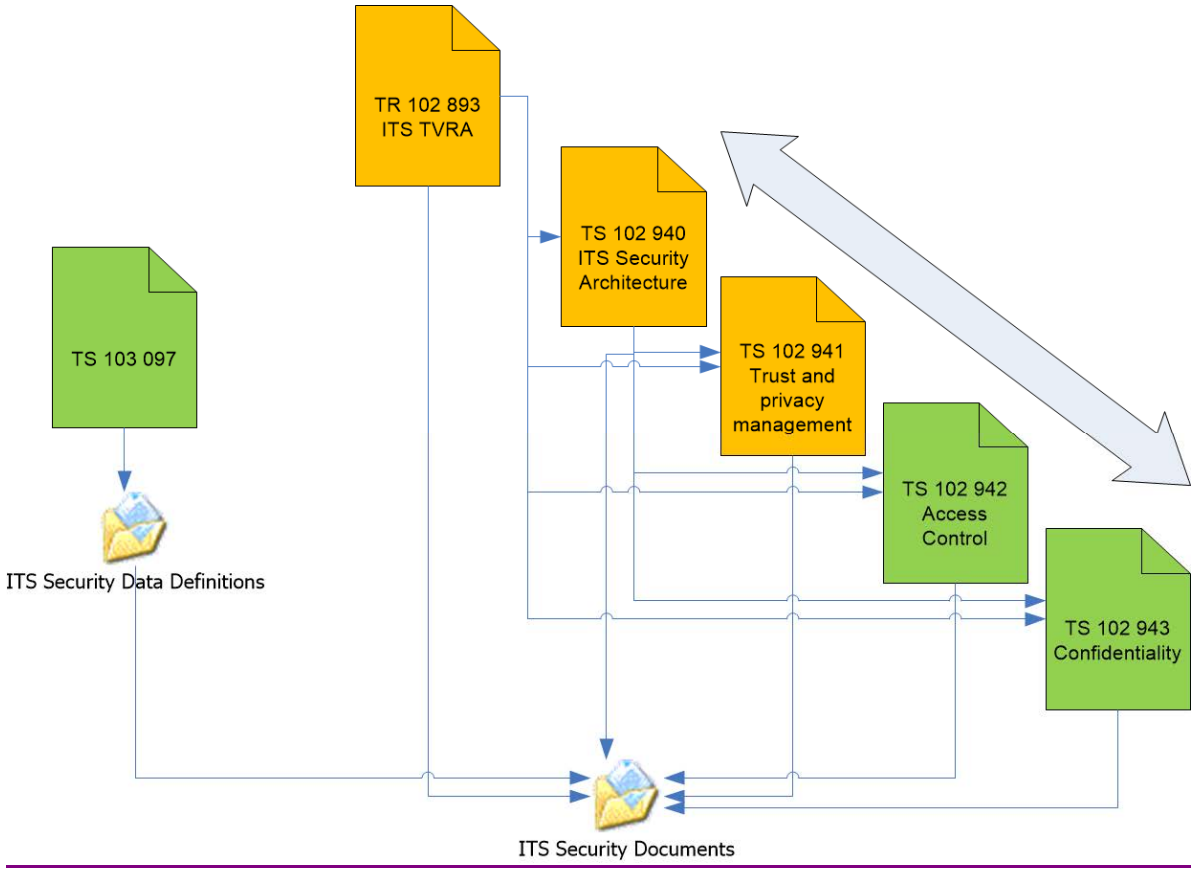

Figure 6: ETSI's ITS security documents and their relation to each other

What Figure 4 shows is that everything in the ETSI ITS suite of security documents spins out of the TVRA. Of itself the TVRA analyses the core suite of services in order to define the required security services.

8.4.1.6 ERM

The ETSI ERM group does not define IoT functionality but does define radio schemes that may be used by IoT devices.

8.4.2 Other bodies

8.4.2.1 oneM2M - Working Group 4

ETSI TS 118 103 [i.37] (derived from oneM2M TS-0003) applies.

8.4.2.2 AIOTI - The Alliance for IoT Innovation

An inclusive body of IoT industrial players - large companies, successful SMEs and dynamic start-ups - as well as well-known European research centres, universities, associations and public bodies. Its working groups (https://aioti.eu/working-groups/) cover a broad array of IoT sectors including security. The IoT Security and Privacy recommendations of AIOTI are developed in the Working Group three (WG03) "IoT Standardisation" inside two sub groups. This is done in full cooperation with AIOTI WG02 "IoT Policy". All related publicly recommendations are published at https://aioti.eu/aioti-wg03-reports-on-iot-standards/ under the section "AIOTI WG03 Sub-Groups IoT Privacy & Security".

8.4.2.3 ITU - International Telecommunication Union

The ITU is a Swiss based intergovernmental body with three sectors dealing with the development and publication of Recommendations for radio systems (ITU-R), telecommunications (ITU-T), and development assistance (ITU-D).

The relevant body addressing IoT is ITU-T SG20 "IoT and applications, smart cities". The structure of the Y-series of deliverables is given in Figure 7 below.

- Y.4000-Y.4999: Internet of things and smart cities and communities
  - Y.4000-Y.4049: General
  - Y.4050-Y.4099: Definitions and terminologies
  - Y.4100-Y.4249: Requirements and use cases
  - Y.4250-Y.4399: Infrastructure, connectivity and networks
  - Y.4400-Y.4549: Frameworks, architectures and protocols
  - Y.4550-Y.4699: Services, applications, computation and data processing
  - Y.4700-Y.4799: Management, control and performance
  - Y.4800-Y.4899: Identification and security
  - Y.4900-Y.4999: Evaluation and assessment
- Y supplements: Supplements to the Y-series Recommendations
  - Y Suppl. 45: ITU-T Y.4000-series - An overview of smart cities and communities and the role of information and communicatior
  - Y.4000-Y.5000 supplements: Supplements to the Y-series Recommendations relatedto IoT and SC&C
    - Y Suppl. 27: ITU-T Y.4400 series – Smart sustainable cities - Setting the framework for an ICT architecture
    - Y Suppl. 28: ITU-T Y.4550 series – Smart sustainable cities - Integrated management
    - Y Suppl. 29: ITU-T Y.4250 series – Smart Sustainable Cities - Multi-service infrastructure in new-development areas
    - Y Suppl. 30: ITU-T Y.4250 series – Smart sustainable cities - Overview of smart sustainable cities infrastructure
    - Y Suppl. 31: ITU-T Y.4550 series – Smart sustainable cities - Intelligent sustainable buildings
    - Y Suppl. 32: ITU-T Y.4000 series – Smart sustainable cities - A guide for city leaders
    - Y Suppl. 33: ITU-T Y.4000 series – Smart sustainable cities - Master plan
    - Y Suppl. 34: ITU-T Y.4000 series – Smart sustainable cities - Setting the stage for stakeholders' engagement
    - Y Suppl. 36: ITU-T Y.4550-Y.4699 - Smart water management in cities
    - Y Suppl. 37: ITU-T Y.4050-Y.4099 - Definition for smart sustainable city
    - Y Suppl. 38: ITU-T Y.4050-Y.4099 - Smart sustainable cities - An analysis of definitions
    - Y Suppl. 39: ITU-T Y.4900 Series - Key performance indicators definitions for smart sustainable cities
    - Y Suppl. 42: ITU-T Y.4100-series - Use cases of user-centric work space service

Figure 7: ITU-T Y-series of recommendations for IoT and Smart Cities

The suite of IoT security recommendations are outlined in Figure 8 below:

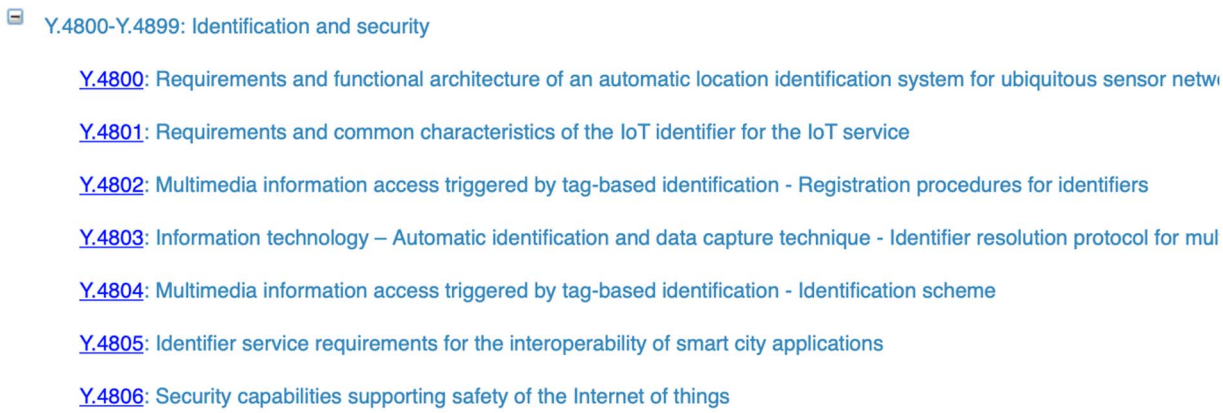

Figure 8: ITU-T Y-series recommendations for identification and security

The activity in security of IoT as published by ITU-T SG20 concerns the risk to safety of IoT devices and is not strictly in the realm of cyber-security mitigation against cyber-threats to data or operation unless they impact safety Furthermore Recommendation ITU-T Y.4806 [i.5] does not specify mechanisms in detail but only outlines requirements for security measures.

8.4.2.4 TCG - Trusted Computing Group®

TCG develops, defines and promotes open, vendor-neutral, global industry standards, supportive of a hardware-based root of trust, for interoperable trusted computing platforms. IT platforms provide for authentication, cloud security, data protection, mobile security, and network access & identity. TCG presently has twelve working groups of which IoTWG is responsible for IoT activity.

TCG has published a multiple page infographic Recommendation ITU-T X.1205 [i.33] and an architect's guide to IoT Security [i.32].

8.4.2.5 OASIS

OASIS (Organization for the Advancement of Structured Information Standards) is the home of the development of a number of security standards across their working groups. Whilst the core may be considered to be the Security Assertion Markup Language (SAML) and the eXtensible Access Control Markup Language (XACML) many other developments have been made in OASIS. The base language of much of the OASIS work is eXtensible Markup Language and it is noted that many of the provisions apply at the higher application layer of communications protocols stacks.

8.5 Other EU and non-EU bodies

8.5.1 European Union Agency for Network and Information Security (ENISA)

The European Union Agency for Network and Information Security (ENISA) is a centre of expertise for cybersecurity in Europe. It actively contributes to a high level of network and information security within the EU and to the development of a culture of network and information security in society in order to raise awareness about these topics.

NOTE: Most member states have their own Cyber Security agencies that act as national centres of expertise and often work to assure protection of Nation State assets in close co-operation with business, industry, SDOs and across government.

The Cybersecurity Act outlined in clause 7.4 of the present document proposes to further strengthen ENISA's role by granting to ENISA the permanent mandate as well as new tasks and resources to ensure that ENISA can provide support to Member States, EU institutions and businesses in key areas, including the implementation of the NIS Directive. It is proposed that ENISA has an increased role of assisting and advising on the development and review of Union policy and law in the area of cyber security which can be key to a more effective protection of the EU digital assets and the policies they support. It will also contribute to stepping up both operational cooperation and crisis management across the EU.

ENISA has published a number of guidelines for securing IoT in a number of contexts, including Smart Manufacturing [i.28], Cloud convergence [i.30], Smart Home [i.31], and also addressing a set of baseline security recommendations [i.29]. In addition, ENISA is developing an analysis of the mapping of security requirements to standards prior to recommendations for IoT device certification.

8.5.2 National Institute of Standards and Technology (NIST)

National Institute of Standards and Technology (NIST) is a physical sciences laboratory and a non-regulatory agency of the United States Department of Commerce, promoting innovation and industrial competitiveness. NIST's activities are organized into laboratory programs that include information technology, nanoscale science and technology, amongst others. The relevant laboratory programs include the following:

- Information Technology Laboratory;
- Communications Technology Laboratory;
- Center for Nanoscience and Technology; and
- Engineering Laboratory.

In the context of IoT Security there is some activity in NIST addressing the role of cryptography for low resource environments that may be cited by other SDOs. This is similar to, and coordinated with, similar activity undertaken in ISO, ETSI and ITU-T.

NOTE: NIST SP800-183 [i.35], from July 2016, states that (to paraphrase) there are very few standards in the specific domain of IoT security. The present document addresses parts of the ecosystem that the NIST report may have overlooked.

9 IoT specific security guidance and best practices

9.1 Introduction

The preceding clauses of the present document give a general outline of the security process and core procedures. The message that is delivered from the text to date in the present document is that security mechanisms, processes, procedures, are all reliant, for their success, on understanding of risk. A summary before consideration of using any security guidance or best practice is to reflect on the purpose of security technologies and processes.

- System protection role:
  - Core CIA roles - least knowledge model to assure system operation.
  - Analytic role - data required to forecast, resolve, recover, etc.
- Anti-adversary role:
  - Identify who gains from system breaches.
- Risk management role.
- Regulatory compliance role:
  - Assurance of technical provisions for GDPR, for Cyber-Security directive, for law enforcement, etc.

In looking at best practice addressed to non-security professionals, e.g. to developers to ensure that they have designed the necessary capability (the power or ability to do something) and functionality (the quality of being suited to serve a purpose well) into their products and services, to managers to ensure they have recruited the necessary expertise, to users to ensure they maximize the available features of their devices, the guidance and best practices have to address some or all of the roles in the foregoing list. Guidelines and best practices should be written in such a way that they recognize the overlap of each of the roles. For example in looking at guidance that limits the attack surface exposed to an adversary (anti-adversary role) it is necessary to consider guidance on how to achieve proof of who is acting in the system (system protection and CIA roles) but as this may have an impact on regulatory compliance the guidance in that role needs to be considered, also if data is required to protect the system by analysis of how the system is used then the guidelines for system protection by analytics needs to be taken into account.

The understanding of risk requires an understanding of the role and intent of the adversary. For example, if the adversary by attacking a small number of instances of a device can gain sufficient knowledge to attack all instances of the device then the risk of deployment is more significant that if an attack against each instance of a device only impacts that instance. This is why, in the set of published best practice and security guidelines that are considered in this clause, many strongly recommend against the use of default credentials. The rationale being that if default credentials are used then if they can be captured then the set of vulnerable devices is all devices using those defaults.

The available best practices and guidance need to be read with the understanding outlined above. Thus all guidance has to be applied with knowledge of the risk that is either inherent in the system or that the measures deployed are intended to manage.

However, once risk is understood the second key characteristic that is endemic to all security provisions is that of trust. The guidelines regarding trust are generally not explicitly stated but underpin most of the published guidance for security. The common example of discouraging default passwords is underpinned by the notion of trust - if both Alice and Bob use the same password, and that fact is known to the entity relying on distinguishing Alice and Bob, then the trust associated to the password, and the associated trust in the party using the password, effectively reduces to zero. Whilst there is often heated debate amongst security experts the generally held view is that if credentials are bound to hardware the level of trust is higher than if those credentials are held only in software. This is also bound to the understanding of authentication factors which has received a lot of examination in recent times with the increasing use of 2-factor authentication. The factors that are concerned are related to what Alice is, has or knows. The use of non-forgeable tokens in hardware are at the root of trust, this gives confidence to the relying party that the claim comes from specific hardware. The most common hardware token of this type is the UICC or SIM card used in cellular networks, where the UICC contains a non-forgeable key (the key is not directly readable from the device either). If Alice holds the UICC/SIM the relying party has a higher level of trust as the relying party "knows" that the key has been safely stored. If in addition Alice provides additional data that she knows (a password) that is distinct from the knowledge stored on the UICC/SIM the relying party can raise the level of trust (2 tests have to be passed).

9.2 Overview

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 the present document the principles of security design outlined in clause 10 are suggested as having precedence (in addition to the arguments outlined above).

9.3 GSMA guidelines

The GSMA prepares a number of guidelines and recommendations of best practice for its members. These guidelines are not binding on members. Furthermore, the guidance offered addresses a very specific set of domains: service ecosystems; endpoint ecosystems; and, the network operator's domain. The GSMA encourages members to self-assess against the guidelines and to record the results of the assessment for public view.

The GSMA IoT Security Guidelines and IoT Security Assessment promote best practices for the secure design, development and deployment of IoT services. They can be found at: https://www.gsma.com/iot/iot-security/iot-security-guidelines/

The audience of the GSMA guidelines is stated as:

- IoT Service Providers - enterprises or organizations who are looking to develop new and innovative connected products and services. Some of the many fields IoT Service Providers operate in include smart homes, smart cities, automotive, transport, heath, utilities and consumer electronics.
- IoT Device Manufacturers - providers of IoT Devices to IoT Service Providers to enable IoT Services.
- IoT Developers - build IoT Services on behalf of IoT Service Providers.
- Network Operators who are themselves IoT Service Providers or build IoT Services on behalf of IoT Service Providers.

This therefore excludes the end user of an IoT device.

9.4 DCMS guidelines and ETSI TS 103 645

The UK Government's Department of Culture, Media and Sport (DCMS) published a set of guidelines to industry in 2018, on securing consumer IoT devices which was fed into ETSI TS 103 645 [i.36]. ETSI TS 103 645 [i.36] contains normative guidance for Consumer IoT and establishes the baseline in ETSI for IoT security.

The introduction and scope of these guidelines aim to protect consumers, putting requirements on manufacturers to, bring together widely considered good practice in security for internet-connected consumer devices in a set of high-level outcome-focused provisions. Thus the objective is to support all parties involved in the development and manufacturing of consumer IoT with guidance on securing their products. The guidance can be gathered as part of the secure by default initiative, in that when followed the guidelines are intended that a consumer will not be placed at risk by the default, ex-factory, configuration of the product.

The ETSI Technical Committee on Cybersecurity (TC CYBER) released ETSI TS 103 645 [i.36], in order to establish a security baseline for internet-connected consumer products and provide a basis for future IoT certification schemes.

ETSI TS 103 645 [i.36] specifies high-level provisions for the security of internet-connected consumer devices and their associated services. IoT products in scope include connected children's toys and baby monitors, connected safety-relevant products such as smoke detectors and door locks, smart cameras, TVs and speakers, wearable health trackers, connected home automation and alarm systems, connected appliances (e.g. washing machines, fridges) or smart home assistants.

ETSI TS 103 645 [i.36] requires implementers to forgo the use of universal default passwords, which have been the source of many security issues. It also requires implementation of a vulnerability disclosure policy to allow security researchers and others to report security issues.

As is clearly noted in the ETSI publication the guidelines are informed by other activity in the field. In particular it is stated that the mappings from of the ETSI Publication have been mapped in an interactive format at the web-site https://iotsecuritymapping.uk/, which is closely aligned to the similar tool from ENISA that allows a reader to view "Security Recommendations for IoT" interactively using a web-application (https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-security-recommendations-for-iot-interactive-tool).

The interactive view of the guidance from ETSI TS 103 645 [i.36] can be seen in the snapshot for the guidance "No default passwords" which identifies a set of bodies who have provided guidance or standards in support of the guideline.

The guidance given is not prescriptive as has been stated but establishes objectives. Thus whilst a statement such as "no default passwords" is made, there is no prescription of how to enable that guidance in products or services, although for each guideline there is some additional text that clarifies why the guidance is given. In addition, the final annex of ETSI TS 103 645 [i.36] provides a pro-forma for a developer to make an assertion of how each guideline has been implemented.

9.5 ENISA and ECSO

ENISA is the formal EU body charged by mandate to act as the centre for expertise in Cyber-Security in Europe and to contribute to a high level of Network and Information Security (NIS) within the European Union, by developing and promoting a culture of NIS in society to assist in the proper functioning of the internal market, and ENISA is complemented to some extent by ECSO acting as the manager of the Public Private Partnership programme for cyber security implementation in the EU.

The work of ENISA is broad based and has collated the best practices of many other organizations in one interactive web-site (this has been cited in clause 9.4 above): "Security Recommendations for IoT" [i.6] (from https://www.enisa.europa.eu/topics/iot-and-smart-infrastructures/iot/baseline-security-recommendations-for-iot-interactive-tool).

An example of the form of result available from the ENISA tool.

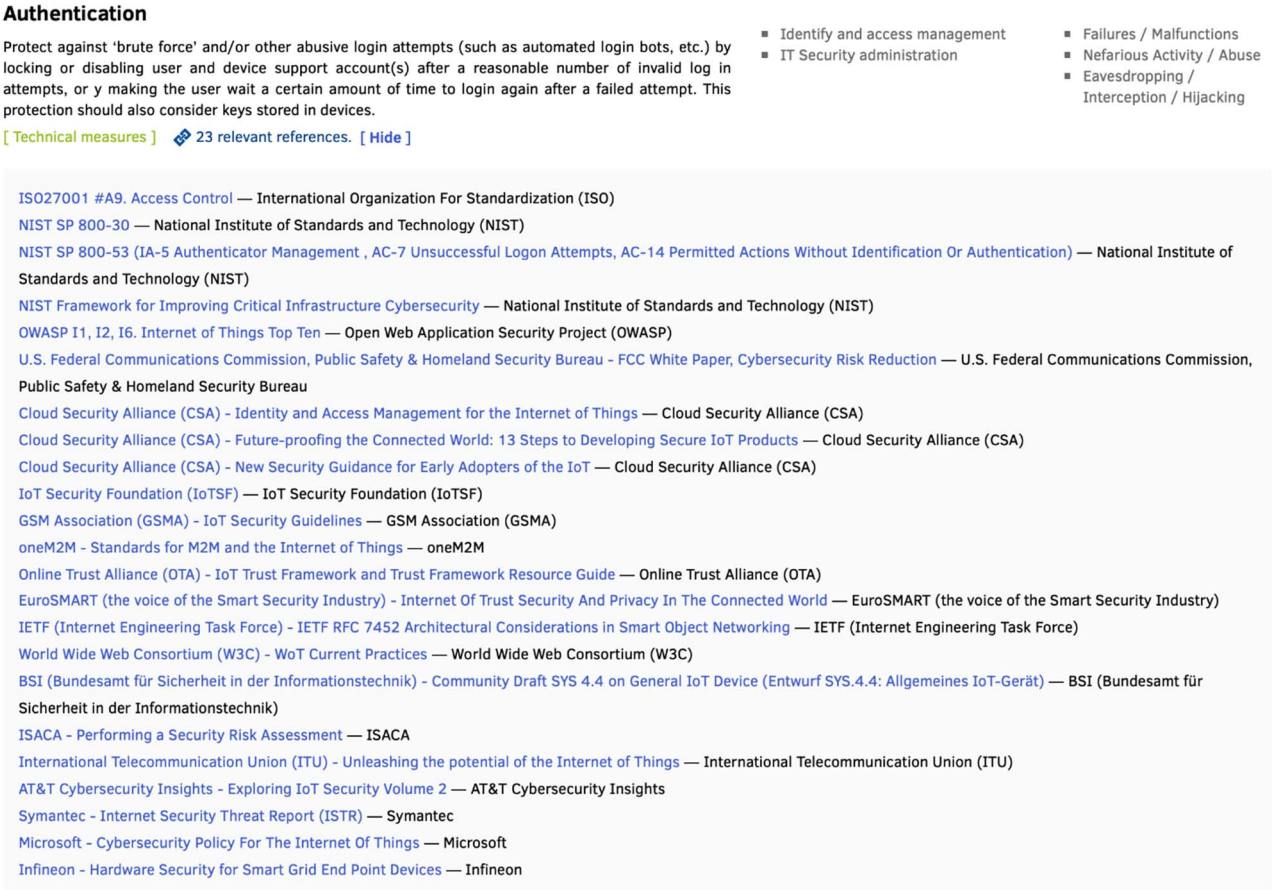

Figure 9: Screenshot from ENISA website for references against Authentication practice

It is noted that the ENISA interactive review does not of itself write new best practices.

In addition ENISA has made available a wide set of its own publications, the most recent of which, "IoT Security Standards Gap Analysis: Mapping of existing standards against requirements on security and privacy in the area of IoT" has identified no standards gap in meeting the requirements identified in the earlier publication "Baseline Security Recommendations for IoT" and which is supported by "Good Practices for Security of Internet of Things in the context of Smart Manufacturing". The broad intent of ENISA in such cases has been to inform industry that such guidance exists without making any judgement on their applicability. The exception to this is the gap analysis document which states very strongly "… *standards are essential but not sufficient to ensure open access to markets. In the particular case of security a large number of processes as well as technical standards have to be in place to ensure that any device placed on the market is assuredly secure*", this is further reinforced by the statement "*The process recommended in this document is intended in part to engender a change in attitude towards device security by making secure IoT the only form of IoT that reaches the market and to give confidence to the market through a mélange of certification, assurance testing & validation, and market surveillance*".

The role of ECSO, as representing the contractual counterpart to the European Commission for the implementation of the Cyber Security contractual Public-Private Partnership (cPPP), is to support all types of initiatives or projects that aim to develop, promote, encourage European cybersecurity. In this regard IoT is one of many domains addressed by ECSO. A primary focus of ECSO has been on labelling as a mark of security provisions. This is a work in practice and is expected to be further developed in collaboration with ENISA as identified above.

9.6 Other industry guidelines

9.6.1 Trusted Computing Group

The activity of the Trusted Computing Group (TCG) is closely aligned to that of the Global Platform group discussed below. The TCG has made a number of publications and standards available that address the requirements associated to a root of trust as a Trusted Platform Module (TPM), and the associated TSS (TCG Software Stack) that interacts with the TPM. The TPM is itself often associated to a Hardware Security Module (HSM) but declares itself through related activities of the TPM/TSS. Thus a TPM will often have capabilities such as a "Root of Trust for Storage (RTS)", or "Root of Trust for Verification (RTV)" and the associated "Root of Trust for Signature (RTSig)". The first of these establishes the capability and functionality for secure storage of data, often credentials such as public and private keys for asymmetric cryptography or the secret key for symmetric cryptography. The RTV establishes the capability and functionality for verification of a cryptographically signed object and so forth. As many of these capabilities and functions are resource intensive (requiring significant levels of storage and processing power) that may not be available to IoT devices the TCG has made steps to address the application of the TPM and TSS standards to the more constrained resource world of the IoT.

The list below highlights those publications aimed to the IoT:

- TCG Guidance for Securing Resource-Constrained Devices:
  - This reference document provides implementation guidance for trusted platforms built with resource-constrained devices.

9.6.2 Global Platform

In the previous clauses of the present document it has been suggested that understanding of risk is critical to understanding what security functions have to be implemented. Once that decision has been made a number of further considerations have to be made and a large part of this is to consider how code runs on an IoT device that enables the management of risk. The role of GlobalPlatform has been to provide technology to do this, and in particular in the form of two standardized secure component technologies: Secure Element (SE) and Trusted Execution Environment (TEE). These address various functional and security requirements of the market, while offering service providers the required levels of on-device security for their needs. Assuming these fit to the risk management model, and when further associated to a well understood and protected root of trust these technologies then fit to the defence in depth and platform segregation approaches described in more depth in clause 10 of the present document.

The list below highlights those publications aimed to the IoT:

- Made Simple: How GlobalPlatform Supports the Internet-of-Things.

9.6.3 NIST

NIST SP 800 183 [i.35] uses two acronyms, IoT and NoT (Network of Things), extensively and interchangeably-the relationship between NoT and IoT is subtle. IoT is an instantiation of a NoT, more specifically, IoT has its 'things' tethered to the Internet. A different type of NoT could be a Local Area Network (LAN), with none of its 'things' connected to the Internet. Social media networks, sensor networks, and the Industrial Internet are all variants of NoTs. This differentiation in terminology provides ease in separating out use cases from varying vertical and quality domains (e.g. transportation, medical, financial, agricultural, safety-critical, security-critical, performance-critical, high assurance, to name a few). That is useful since there is no singular IoT, and it is meaningless to speak of comparing one IoT to another.

10 General security guidance and best practices

10.1 Overview and introduction to 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.26], or from adaptations of the ISO/IEC 27000 [i.48] series of specifications. Examples include the following:

- Apple® secure development guidelines, from https://developer.apple.com/library/content/documentation/Security/Conceptual/SecureCodingGuide/Introduction.html
- Microsoft® Security Development Lifecycle (SDL) from https://www.microsoft.com/en-us/sdl
- Open Software Assurance Maturity Model (SAMM) from http://www.opensamm.org
- Building Security in Maturity Model (BSIMM), incorporating the SSDL method, from https://www.bsimm.com

In looking to hardware based security there are a number of best practice guidelines published by the Trusted Computing Group (TCG) and by Global Platform. The wider application of the SIM in 3GPP and in ETSI TC SCP for applications in IoT and in embedded devices is also relevant here but has to date concentrated on the provision of technical specifications and not on best practice, or generic guidance, to date.

10.2 Defence in depth

The overall model of defence in depth is derived from a military stance or strategy that seeks to delay rather than prevent the advance of an attacker. Rather than defeating an attacker with a single, strong defensive line, defence in depth relies on the tendency of an attack to lose momentum over time or as it covers a larger area. A defender can thus yield lightly defended territory in an effort to stress an attacker's logistics or spread out a numerically superior attacking force. Once an attacker has lost momentum or is forced to spread out to pacify a large area, defensive counter-attacks can be mounted on the attacker's weak points, with the goal being to cause attrition or drive the attacker back to its original starting position. This strategy has been deployed in many systems where there is a very thin line between interpretation of security and safety. For example, cars have passive and active safety systems that work to absorb momentum in an accident that whilst leading to damage to the vehicle tend to preserve the passenger compartment which is then further protected using air bags and seat belts to restrain the occupants. In fire control in buildings a similar approach to defence in depth is used with fire doors for isolation for a certain period, sprinkler systems and so forth. The intent in each case is not to disallow the attack but to spread its effects to the point where the primary asset (in the car and fire cases this is considered as human life) is not impacted.

In information security, or ICT in general, the principle of defence in depth simply means using more than one technique to secure the system assets. This may require parallel implementation of border security, identity verification and authentication, access control, confidentiality and integrity measures.

NOTE: The board game Chess offers an instance of defence in depth using strategies that sacrifice assets (e.g. pawns) in seeking to defend the King piece.

There are very few guides and standards to defence in depth although the practice is well known and taught in most security practitioner specialist courses. Example guides include those from the NSA (US Government body) [i.51] (https://apps.nsa.gov/iaarchive/library/ia-guidance/archive/defense-in-depth.cfm), NCSC (UK Government body) and the SANS institute (published by ETSI as ETSI TR 103 305 [i.26]).

10.3 Secure by default

It is a generally held view that one cannot make anything secure after the fact. However, it is also a generally held view that security is a cost only exercise. The latter view is held because when security works properly it has no impact on functionality, and as it thwarts attacks in such a way that attacks do not succeed it is not always clear if this is because of the money spent on the security features rather than by an attacker simply failing to attack. Thus, the cost effectiveness of working security is often considered as hard to quantify.

ETSI TR 103 309 [i.16] provides a general overview of the approach.

10.4 Design for assurance

The design for assurance paradigm was introduced in ETSI as a means to be able to design security features in such a way that the rationale for them can be proven, and that the claims made for the level of security they provide can also be proven. In each case the intent is to clearly identify what is being secured, against what form of attack, and over what period of time. Design for assurance has been developed from the foundation of the Common Criteria and its mirror in ISO/IEC 15408 [i.17] but dealt with from the perspective of developers and implementors rather than from the perspective of testers and evaluators. The approach has subsequently been applied in a number of domains in ETSI including Intelligent Transport (ITS), Network Function Virtualisation (NFV), and across the output of ETSI TC CYBER.

The core documents for the design for assurance paradigm are:

- ETSI EG 202 387 [i.18].
- ETSI ES 202 383 [i.19].
- ETSI ES 202 382 [i.20].
- ETSI TS 102 165-1 [i.10].
- ETSI TS 102 165-2 [i.25].

Whilst many of these are quite old the key concepts are still applicable and in most cases are in the process of evolution towards the ETSI CYBER work programme. In addition, a lot of the key thinking behind the Design for Assurance approach has been adopted in the development of the co-operative Protection Profile (cPP) approach in the Common Criteria Recognition Agreement (CCRA) group that may deprecate some of the deliverables in this paradigm.

10.5 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, one of the privacy by design principles is 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 web-page 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).

It should be noted that there are many laws to protect victims of public statements including those of libel and slander, of copyright, and so forth, in addition to the laws surrounding data protection captured in the GDPR [i.21]. Thus, if Alice makes a public statement regarding Bob that Bob believes reveals data that is private or wrong whilst Bob is not directly in the GDPR chain his rights are still protected.

The revealing of private data in content is difficult to protect against when the intent of the author is to publish (make public). It is essential therefore to be clear about what can be protected in the privacy domain using the toolkit of security, and what has to be protected by other measures, e.g. judicial measures, against attacks in the content of messages.

Figures 10 and 11 from the ETSI CYBER document ETSI TR 103 370 [i.22] illustrate some of the commonality between the technology for security and the application of those technologies in privacy protection.

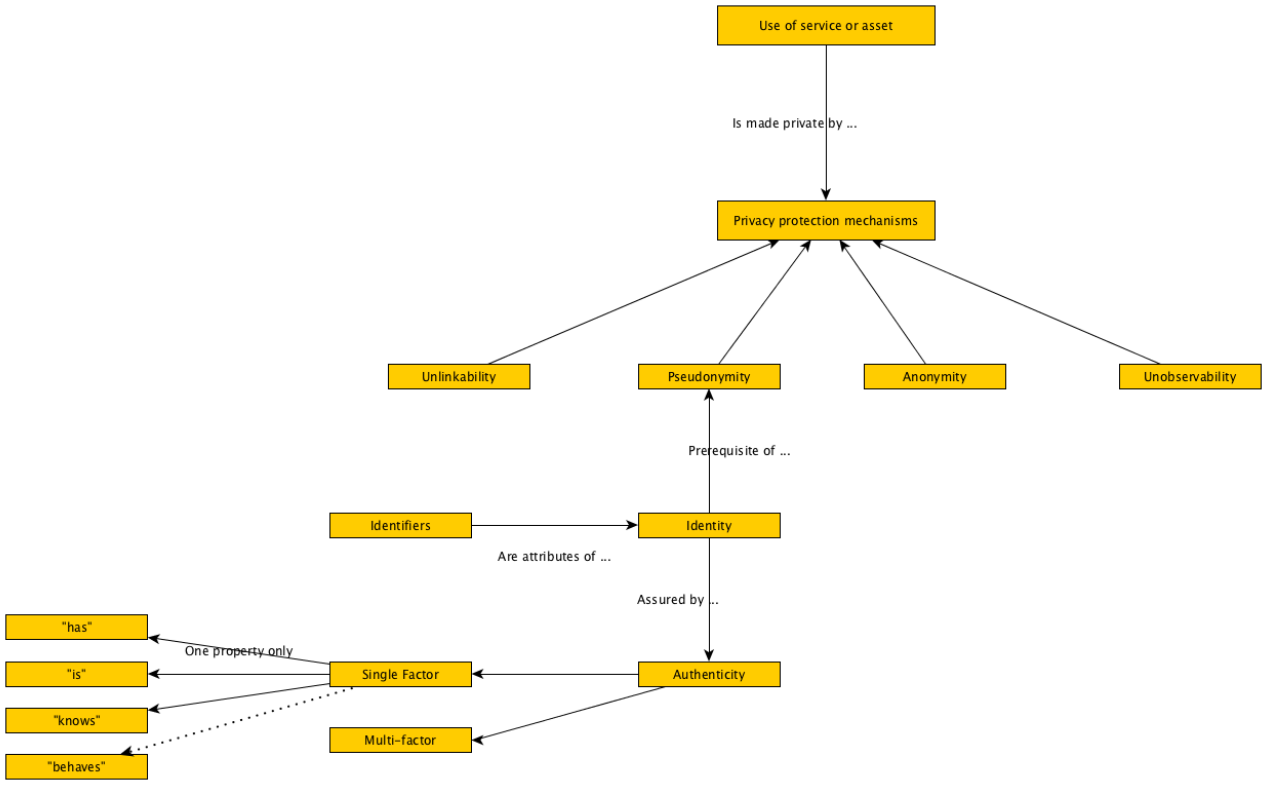

Figure 10: Role of protection technologies in privacy protection

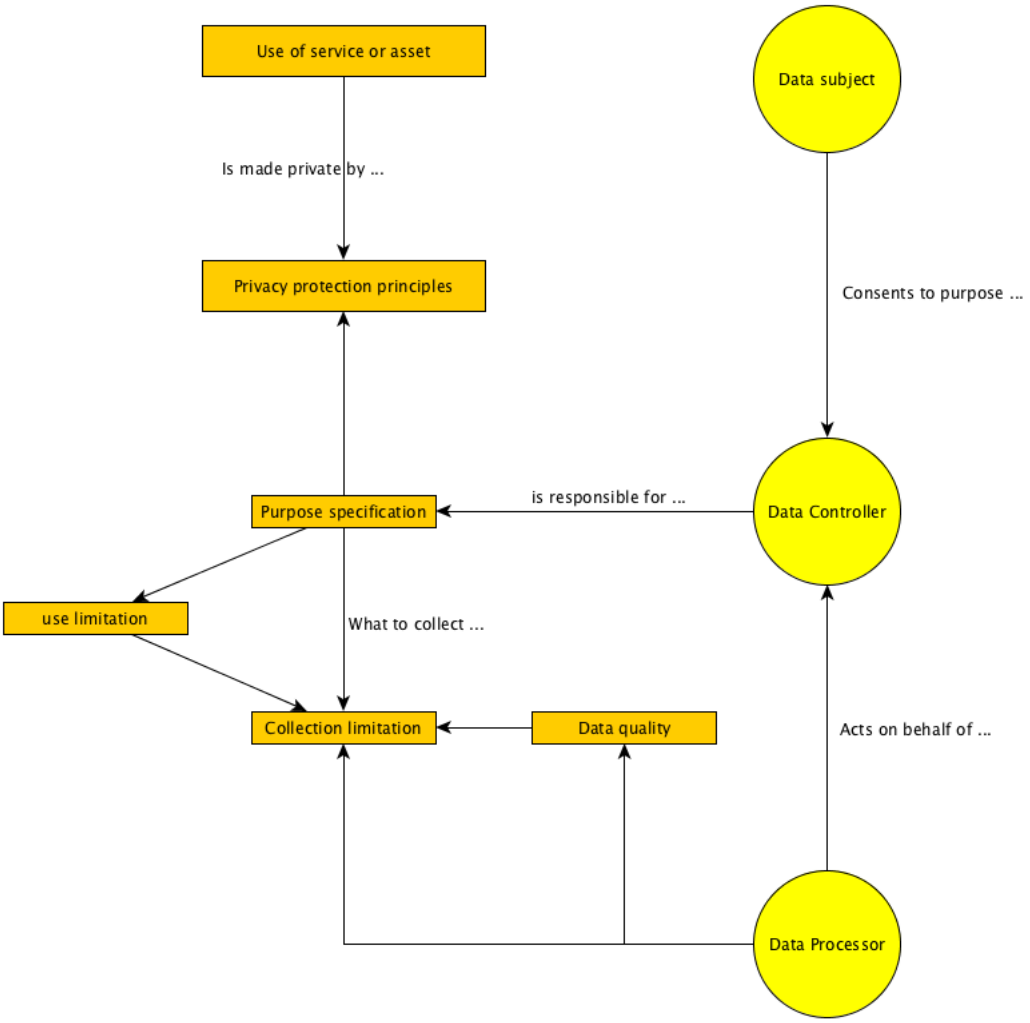

Figure 11: Extending privacy protection to address principles of privacy protection

11 Lessons learned and conclusions

As has been identified throughout the present document the task of designing security into any system is difficult.

The best practices 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. The oft-cited 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. So, 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.

As has been stated in the present document regarding security provisions it is 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. However it is also true that an insecure product or service, or a poorly implemented one, may never be subjected to attack and may never lead to a loss of any type to the user or owner.

Many of the guidelines that have been cited in the present document are old, and the principles behind them date back many decades, in some cases for centuries. Security technology is not new, the base principles that underpin the CIA paradigm, the need to understand the abilities of the adversary are not new, as is the need to always keep one step ahead of the adversary. Whilst guidelines are effective, their applicability are only as effective as the knowledge of the designer implementing them. The conclusion of the present document is therefore for all designers, developers, implementors and users, to be aware of the guidelines but to recognize that without expert knowledge and care they may act to give a false sense of security.

Annex A:
Best practice security guidelines for implementation, development and operation of IoT

A number of IoT specific best practices have been published by EU Member States and by some consumer bodies as has been intimated in the body of the present document.

In the context of IoT for consumer devices the content of ETSI TS 103 645 [i.36] apply.

In all other IoT contexts the guidelines given in ETSI TS 103 645 [i.36] apply with the following extensions given in Table A.1.

Table A.1: Best practices to be followed for non-consumer IoT sectors extending ETSI TS 103 645 [i.36]

	Development	Implementation/ installation	Operation	Decommission/ End-of-life
Ensure all security is enabled from a hardware root of trust	X	X	X	
At end of life destroy all key material associated to the hardware root of trust	X			X

Annex B:
Change History

Date	Version	Information about changes
May 2018	0.1.0	Initial draft version (Milestone A) for review at SmartM2M #46.
To August 2018	0.1.1	Updates from SmartM2M#46 meeting.
September 2018	0.1.2	Update with reference to NISD and GDPR. Addition of annex covering ENISA IoT security requirements.
September 2018	0.1.3	Update incorporating new text from Arthur's Legal (edited to conform to ETSI rules). Modification of emphasis by movement of text (IoT first, general issues second).
October 2018	0.1.4	Inclusion of common text in scope and clause 4. Re-ordering of text clauses to emphasize IoT before other parts.
October 2018	0.1.5	Deletion of clauses that are addressed in ETSI TS 103 645 [i.36].
November 2018	0.1.6	Preparation for SmartM2M review in December.
November 2018	0.1.7	Submission to SmartM2M meeting.
December 2018	0.1.8	Internal maintenance copy updated by STF547.
December 2018	0.2.0	Stable draft submission.
March 2019	0.2.1	Proposal as final draft (pending edithelp review and addition of conclusion clause).
March 2019	0.3.0	Addition of extended text in clause 9, Addition of clause 11.
March 2019	0.3.1	Refinement suggested by CYBER in clause 9 when referring to ETSI TS 103 645 [i.36].
July 2019	0.3.1	ETSI Techical Officer check for EditHelp registration for publication & processing.

History

Document history		
V1.1.1	August 2019	Publication