AIOTI

ALLIANCE FOR INTERNET OF THINGS INNOVATION

Identifiers in Internet of Things (IoT)

Version 1.0, February 2018

AIOTI WG03 – IoT Standardisation

Executive Summary

Identification is a major topic in Internet of Things (IoT). Beside identification of the things itself, many other entities have to be identified in IoT solutions. In this paper we discuss the various identification needs with related use cases and requirements. Furthermore we look at identifier standards, their applicability for the different identifier needs and discuss identifier allocation, registration, resolution, security, privacy and interoperability.

The starting point for this deliverable was a survey that was conducted in spring 2017 within the IoT standardization and research community. This survey is a significant input to this deliverable, along with several research and standardisation documents related to IoT identities. Due to the large application area for IoT and the wide landscape of standardization activities, research work, technologies and already existing IoT platforms and solutions the paper can only provide a general overview. It does not claim to cover the whole space of IoT use cases, requirements and standards for identifiers.

The document provides a high level discussion on the above topics. It provides a structured approach by classification of identifier usage and a categorization of requirements. In general no single identification scheme fits all needs. Furthermore many identification are already standardized and in use. It therefore does not define or recommend specific solutions and standards, but provides examples and summaries in order to indicate what has to be taken into account when considering identifiers in IoT. This also includes different topics related to interoperability of identifiers. Furthermore security and privacy are raised as important topics for identifiers and appropriate threat and risk analysis have to be performed and relevant regulatory and legal framework have to be taken into account.

Table of Contents

1. Introduction

Identification plays an important role for the Internet of Things (IoT). First discussions in AIOTI focused around the use of communication identifiers like IP addresses and mobile phone numbers in IoT. This was triggered by similar discussions in the Body of European Regulators for Electronic Communications (BEREC) [1]. However identification has a much wider scope and is relevant for many applications and entities in IoT. Beside identification for communication means this includes identification of the things, but also for example of services, users, data and locations. Various identification schemes already exist, have been standardized, and are deployed in the market.

To address the wider scope of identifiers in IoT, the AIOTI Working Group 03 (WG03) IoT Identifier task force was set up. The task force objectives are to provide a thorough analysis of the identification needs and related standardization for IoT, specifically:

- to evaluate identification needs for IoT and related requirements;
- and to describe existing identification standards and ongoing standardization work and elaborate their applicability for IoT.

This public deliverable is the first outcome of the work of the task force.

1.1 Identifiers in IoT

In any system of interacting components, identification of these components is needed in order to ensure the correct composition and operation of the system. This applies to all lifecycle phases of a system from development to assembly, commissioning, operations, maintenance and even end of life. Especially in case of flexible and dynamic interactions between system components identification plays an important role.

Identifiers are used to provide identification. In general an identifier is a pattern to uniquely identify a single entity (instance identifier) or a class of entities (i.e. type identifier) within a specific context.

> Definition: An identifier is a pattern to uniquely identify a single entity (instance identifier) or a class of entities (i.e. type identifier) within a specific context.

Depending on the application and user need various types of identifiers are used.

IoT is about interaction between things and users by electronic means. Both things and user have to be identified in order to establish such interaction. Various other entities are involved in the interaction and are part of an IoT system and identification is also relevant for them. Figure 1 shows the different entities with the related identifiers in the IoT Domain Model of the AIOTI WG03 High Level Architecture [2]. The different types of identifiers are described in detail in Chapter 3.

Various identification schemes already exist, are standardized and deployed. This document

- evaluates IoT identification needs;
- classifies the different identification schemes;
- evaluates and categorises related requirements;
- provides examples of identifier standards and elaborates their applicability for IoT;
- discusses allocation, registration resolution of identifiers;
- considers security and privacy issues;
- and discusses interoperability of identifiers.

This is done from a high level viewpoint. The document does not define or recommend specific solutions and standards, but provides examples and summaries in order to indicate what has to be taken into account for identifiers in IoT.

It should be noted that the document does not cover identity and identity management issues. An identifier is usually part of the identity of an entity, but many other topics are relevant for identities and are

not discussed in the document. Specific coding technologies for identifiers like printed numbers, bar codes or Radio Frequency Identification (RFID) are also not evaluated in the document.

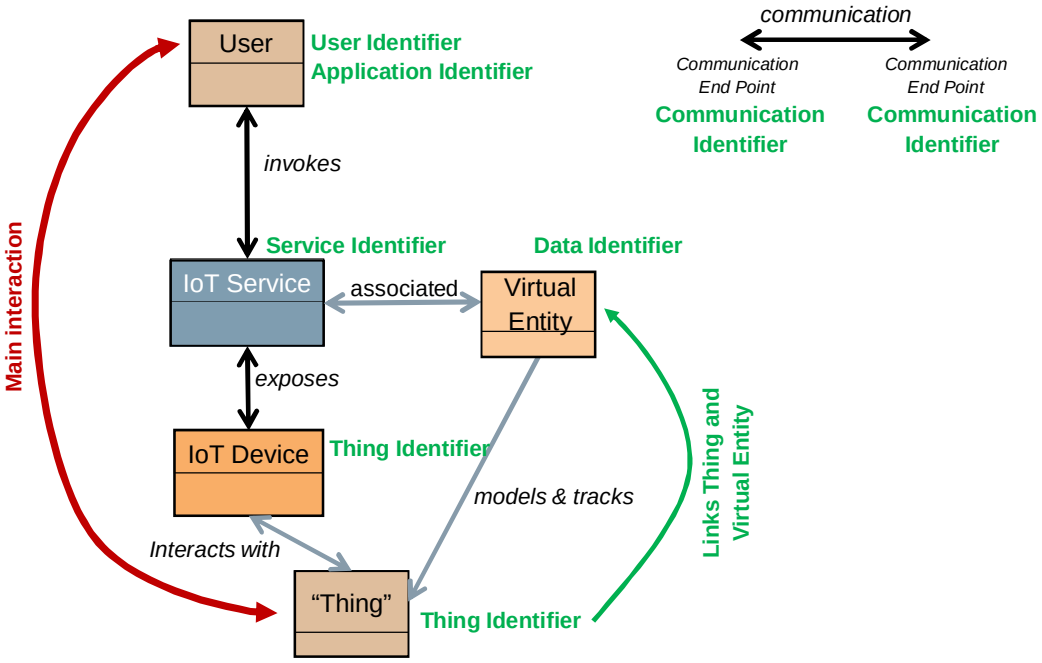

Figure 1 - IoT Identifiers in the Domain Model of the AIOTI High Level Architecture [2]

1.2 IoT Identifier Survey

In order to evaluate identification needs for IoT, related requirements and existing standards and standardization activities a survey was performed in March and April 2017.

The survey asked questions about IoT use cases that use identifiers, the specific purpose of the identifiers, related requirements, standards and standardization gaps. The detailed questions are listed in Annex I.

It was sent to over eighty standardization bodies, industry alliances, research projects and individual companies around the world. Eighty-two responses were received including AIOTI WG03 internal feedback.

The survey, together with other input like the EU-China Joint White Paper on the Internet of Things Identification [3], was used to make an initial classification of identifier usage in IoT which resulted in the classification scheme as defined in Chapter 3. Furthermore the collected requirements have been categorized in a set of generic categories as defined in Chapter 4 and the input on relevant standards contributed to the standardization examples in Chapter 5.

2. IoT Use Cases of Interest

AIOTI WG01 published a report that summarizes the IoT use cases of interest to AIOTI [4]. This report is relevant to this discussion on identifiers, because requirements for and types of identifiers are mainly derived from such use cases. The listed use cases in the report [4] are categorized and structured similarly to the vertical AIOTI WGs (WG05-13). The following list summarizes these use cases, and also contains additional use cases taken from the survey responses and not covered by the WG01 report [4].

- Smart living environment for ageing well (WG05): IoT use for smart homes and smart living environments to support for example people in need of care, elderly or disabled people, also lead-

ing to reduced costs for care systems and better quality of life. The WG05 report [5] provides more details.

- Smart Farming and Food Security (WG06): IoT use cases that allow monitoring and control of plant and animal product life cycles and management and control of the production assets for example farm equipment. See the WG06 report [6] for details.
- Wearables (WG07) and Healthcare, Wellness: IoT use cases that integrate key technologies (e.g. nano-electronics, organic electronics, sensing, actuating, communication, low power computing, visualisation and embedded software) into intelligent systems to bring new functionalities into clothes, other fabrics, patches, watches and other body-mounted devices. This includes healthcare, well-being, safety, security and infotainment applications. See the WG07 report [7] for details.
- Smart Cities (WG08): IoT use cases for municipalities to enhance city performance, safety and well being of its inhabitants, to reduce costs and resource consumption, and to engage more effectively and actively with citizens. Key smart city sectors include government, transport, energy, healthcare, lighting, water, waste and other city related sectors. See the WG08 report [8] for details.
- Smart Mobility (WG09): IoT use cases that allow for increased mobility, more efficient traffic management, a dynamic road infrastructure, automated road tolling, usage based insurance and improved policy making through the analysis of road usage data. Smart vehicles include autonomous and connected cars. See the WG09 report [9] for details.
- Environment and Smart Water Management (WG10): IoT use cases that improve water management efficiency by controlling environmental implications such as surface water retention, or flooding.
- Smart Manufacturing (WG11): IoT use cases that bring together information, technology and human knowledge to achieve a rapid revolution in the development and application of manufacturing intelligence, for Industry 4.0 and the Factory of the Future. See the WG11 report [10] for details.
- Smart Energy and Smart Grid (WG12): IoT use cases that enable the performance optimisation of energy asset portfolios (renewables plants, grid substations, control rooms, prosumer demand responsive loads and electric vehicle charging infrastructures).
- Smart Buildings and Architecture (WG13): IoT use cases deployed in public and commercial buildings to improve life by addressing, for example, comfort, light, temperature, air quality, water, nourishment, fitness, and energy usage.
- Smart Home: IoT use cases for private homes to control and automate heating, lightning, smart appliances, security devices, multimedia equipment, metres, etc., in order to improve comfort, security and living in general.
- Smart Logistics: IoT use cases for management and control of supply chains, device location tracking, store, restaurant or hospital inventory management and logistics and similar activities.

3. Classification of Identifiers

Identifiers are used for different purposes in IoT applications. Most prominent is the thing identifier which identifies the things, the entities of interest of an IoT application. Other relevant entities that are identified are applications and services, users, data, communication endpoints, protocols and locations. These classes are defined in more detailed in the following sections.

3.1 Thing Identifier

Thing identifiers identify the entity of interest of the IoT application. This can be for example any physical object (e.g. machines, properties, humans, animals, plants) or digital data (e.g. files, data sets, metadata); basically anything that one can interact with.

Examples for usage of Thing Identifiers:

Predictive Maintenance

A company provides predictive maintenance services for products (e.g. electrical drives, production machines). The products have built in sensors and communication interfaces. The predictive maintenance service is running in the cloud. At the customer premises the product is securely connected (e.g. Virtual Private Network) to the maintenance service using for example the customer's network or a mobile network connection. The product has a thing identifier that is stored in its non-volatile memory and is referenced (logged) by the maintenance service in the cloud.

Asset tracking

A company keeps track of all its assets (large and small, stationery and moveable) by checking regularly where they are. All assets have a thing identifier which is a barcode or RFID tag with a unique identifier attached. They are regularly scanned by staff using a hand scanner that communicates with a server. With each scan status information about the asset can be provided via the scanner user interface.

Provenance and quality control of track & trace information

The following example shows how important it is to clearly define the thing of interest.

A freight and logistics company tags the goods it transports with RFID tags. These tags store the thing identifier of the good together with potentially other attributes of the good (e.g. manufacturer, date of manufacture, etc). The location of the good is recorded whenever the tag crosses a reading point. The tags might be reused at a later time for other goods with a different thing identifier. The tag also stores an identifier of the tag itself, which is used by the company to check provenance of the information, control quality of the tags, etc. For this application the tag itself is the thing of interest.

An example of such identifiers that are contained on the same tag but related to different entities are the Electronic Product Code (EPC) and the Tag Identifier (TID) both defined by GS1 [11]. The EPC identifies the product to which the tag is attached and the TID identifies the tag itself. The EPC changes which each new product the tag is attached to while the TID stays with the tag during its lifetime.

3.2 Application & Service Identifier

Application and Service identifiers identify software applications and services. This also includes identifiers for methods on how to interact with the application or service (i.e. Application Programming Interfaces, Remote Procedure Calls)

Examples for usage of Application & Service Identifiers:

IoT Platform Services

An IoT platform provides various services like communication, application store, device management, and device registration. Each service has a unique identifier. Services can be registered in a registry so that applications can search for services. Services can also be announced to the applications. In a federated platform, where the same service (e.g. registration) might be provided by different (e.g. regional) software platforms, there might be several unique identifiers for the same type of service.

3.3 Communication Identifier

Communication identifiers identify communication (end) points (e.g. source, destination) and sessions.

Examples for usage of Communication Identifiers:

Low Power Wide Area Networks

Low Power Wide Area Networks (LPWANs), as for example defined by ETSI GS LTN 002 [12], use uniquely assigned communication identifiers to identify end devices in the scope of each network's communication. Central service centres and end devices communicate data to each other via access points, in uplink and downlink. End devices are registered and authorized based on their unique communication

identifiers. When communicating data in uplink, end devices use their unique communication identifier as source addresses: Each transmitted packet contains the communication identifier as source address so that processing and forwarding the packet to a central service centre can be validated. For downlink communication, end devices query the network for existing data, using their communication identifier as destination address.

Ethernet MAC address

In Ethernet Networks (see IEEE 802.3 [13]) the Media Access Control (MAC) address is an identifier for communication endpoints at the data link (media access) layer. MAC addresses are usually assigned by the manufacturer of the Ethernet network interface. The MAC address consists of 48 bits (6 bytes) with a 3 byte Organizationally Unique Identifier (OUI) which is assigned by the IEEE Registration Authority and a 3 byte number assigned by the manufacturer.

IP Address

IPv4 (see IETF RFC 791 [14]) and IPv6 addresses (see IETF RFC 4291 [15]) are used in IP networks to identify communication endpoints at the network layer. IPv4 uses 32 bit and IPv6 128 bit addresses. IP addresses can be global/public, local or even link local (for IPv6) unique depending on the specific use case and network. Furthermore unicast, multicast and broadcast (IPv4 only) addresses are supported. IP addresses are structure based on the IP routing hierarchy and consist of a network prefix and host/interface identifier which can be of variable length. Globally unique IP address ranges are distributed and registered via the five Regional Internet Registries (RIRs) and subsequently can be further distributed via the Internet Service Provider (ISP) to end user networks. Management of the global pool of addresses is performed by the Internet Assigned Numbers Authority (IANA under memorandums of understanding with the RIRs who coordinate IP address policy. IANA assigns larger blocks of IP addresses to the RIRs.

Phone Number

Phone numbers are assigned to a specific subscriber station in a phone network. Both global and local unique numbers are used based on the specific application. Local numbers are usually extended with an extension that provides global uniqueness when calling outside the local area. A global phone number starts with a country code that is defined by ITU-T (see ITU-T E.164 [16]). Regional or provider codes assigned by the telecommunication regulation body of the country can follow.

HTTP Session Token

A communication session is a series of related message exchanges. An example is a web store where a user puts several articles into its shopping basket and then checks out. The web server has to keep track of the user thru all these activities. As the HTTP protocol is stateless a dedicated session identifier is needed in order to do so. The identifier is generated by the server, usually stored as cookie on the client and a parameter in the HTTP GET and POST request.

3.4 User Identifier

User identifiers identify users of IoT applications and services. Users can be humans, parties (e.g. legal entities) or software applications that access and interact with the IoT application or service.

Examples for usage of User Identifiers:

Human user

A human logs into an IoT system in order to get some data from or to control the thing of interest. The human has to identify itself (e.g. username, chip card, fingerprint) to the system. Depending on the security needs an additional authentication is performed. The system checks that the user has the proper rights to access the thing or services and performs the intended actions. The user's rights depend on its (assigned) specific role in the given scenario. Within the IoT system, the user is assigned a specific identifier which is used for all trust/security associations and which might be different from the identifier used by the human for identification.

Application access to things

A software application wants to interact with a thing via an IoT system. The application identifies itself to the system with a unique key. The system checks that the application has the proper rights to access the thing and performs the intended actions.

3.5 Data Identifier

This class covers both identification of specific data instances and data types (e.g. meta data, properties, classes).

Examples for usage of Data Identifiers:

Digital Twin

A digital twin is a data set containing the virtual representation of the thing. It is related to the thing based on the thing identifier. Also the digital twin itself needs an identifier in order to be referable and accessible from applications and services. Note that a thing may have more than one digital twin and that they may contain different sets of information.

Time series data set

Sensor data from a thing is provided automatically in (constant) intervals. The data is stored as time series in the IoT platform for further use. Various applications may access these data for example for predictive maintenance, process optimization or forecasts. The data set needs an identifier that allows accessing it from the applications.

Property types

Properties are characteristics of objects like for example weight, dimensions and temperature. Such properties are standardized for specific application areas. The definition of property data elements includes for example the meaning, value range and format of specific properties. The data elements need to be uniquely identified in order to provide a reference to them.

3.6 Location Identifier

This class is about Identification of locations within a geographic area (e.g. geospatial coordinates, postal addresses, room numbers).

Examples for usage of Location Identifiers:

Goods tracking

A company wants to track the delivery of high value goods. A GPS receiver with a cellular network modem is part of the packet in which the goods are transported. The GPS coordinates of the packet are transmitted in regular intervals to a cloud application which keeps track of the packet.

Real estate maintenance

A facility manager takes care of the maintenance of the Heating, Ventilation, and Air Conditioning (HVAC) equipment of a large campus. The HVAC equipment reports alarms and a predictive maintenance services is used. In order to guide the maintenance personal to the right location for each device an identifier for its location in the facility (i.e. building, floor and room number) has to be provided.

3.7 Protocol Identifier

Protocol identifiers inform for example communication protocols about the upper layer protocol they are transporting or applications about the protocol they have to use in order to establish a specific communication exchange.

Examples for usage of Protocol Identifiers:

Ethertype

Various high level protocols can be encapsulated into an Ethernet frame. The Ethertype field in the Ethernet MAC frame indicates which higher level protocol is transported (see IEEE 802.3 [13]).

IPv6 Next Header

The IPv6 next header field specifies the transport layer protocol that is transported via IP. In case extension headers are used it indicates which extension header follows (see IETF RFC 8200 [17]).

URI Scheme

The scheme field of a Unified Resource Identifier (URI) indicates how the URI should be interpreted (see IETF RFC 3968 [18]). It often indicates which protocol is used to access the resource identified by the URI (e.g. http, ftp, nntp).

4. Requirement Categories for Identifiers

The responses to the survey provide a long list of requirements with various levels of details. They show that most requirements are not limited to a specific identifier class or set of classes.

Due to the diverse nature and various levels of details of the contributed requirements, categories of requirements are defined and detailed in the following sections. For each requirements category, the survey feedback is summarized and the view of AIOTI WG03 is provided.

4.1 Uniqueness

From Survey:

Uniqueness of the identifier is mentioned by most responders; however the scope of uniqueness strongly varies. Many ask for global uniqueness while some limit it to local uniqueness or uniqueness within the customer or vendor domain. One response also asks to disable uniqueness for privacy reasons (see section 4.2 for privacy requirements).

A specific topic is to ensure uniqueness even if the identifiers are managed by different organizations.

AIOTI WG03 View:

Within the context of the specific application, a unique identifier is needed in order to identify an entity. We recognize that in case new scenarios go beyond the original context and the existing scheme is not unique within this wider context, either (1) an identification scheme that supports this larger context can be used, or (2) the existing identification scheme can be extended with an additional pattern that ensures uniqueness within the wide scope, or (3) the identification scheme can be mapped to the scheme of the wider context in a collision free manner (e.g. IPv4 Network Address Translation (NAT)). See also Chapter 8 on interoperability of identifiers for further information.

4.2 Privacy & Personal Data Protection

From Survey:

Privacy is a topic for use cases that involve humans and personal data. It is related to user identifiers that directly identify humans, but also to identifiers for entities that can be closely related to humans and their activities like cars, personal equipment, goods, locations and communication addresses belonging or assigned to a specific human user or equipment in its possession.

In the survey, it is asked for anonymization of identifiers, use of non-unique identifiers, identifiers that do not have personal data included in the identifier itself, disabling of tracking, access control to identifier information, data aggregation and reduction.

AIOTI WG03 View:

We recognize that privacy and personal data protection are important topics that have to be taken into account when using and processing identifiers (privacy by design and privacy by default). Personal data protection is not only relevant to human identifiers but many other identifiers that are capable of generating personally identifiable information. Hence, all identifiers classified under Chapter 3 of the present document are relevant and fall within the scope of this category. In this respect, it should also be noted that the European General Data Protection Regulation (GDPR) [19] puts strong restrictions on the processing and storage of such personal data.

4.3 Security

From Survey:

Security requirements are mainly related to the identifier itself, but it is also asked that the data associated with the identifier (i.e. associated with the entity identified by the identifier) is secured. The latter is not in the scope of the document.

It has to be ensured that the identifier identifies the correct entity and that it is not tampered during its allocation, transfer and usage. Signing of the identifier is mentioned as one method to achieve that. Duplication and use of the identifier for other entities should be prevented. Verification of the correctness of the identifier should be possible in online and offline situations.

Authentication of the identifier is requested in order to proof that it belongs to the correct entity. This is part of identity management and will not be covered in this document.

AIOTI WG03 View:

Although security requirements strongly depend on the specific use cases, we note that security is highly relevant and in scope with respect to all identifiers classified under Chapter 3 of the present document. We recognize that the GDPR [19] requires manufacturers and organisations to ensure "state of the art" security. Hence, as security has become dynamic, a threat and risks analysis should be performed for the systems and its components to justify the security requirements. This also relates to the security requirements for the identifier. However, the capabilities of the involved entities have to be taken into account (e.g. constraint devices, entities without processing capabilities).

4.4 Identified Entities

From Survey:

In the survey responses, a very diverse set of entities is mentioned from small items like medical pills to larger items like machines, vehicles and whole factories and also living things (people, animals, plants). Identification of sub parts of a larger entity has to be supported. Also non-physical things are mentioned like data sets, organizations and traffic flows. In general there is no limit on what can be identified.

As different stakeholders or applications may use different identifier schemes, the support of several identifiers for the same entity might be required (e.g. manufacturer identifier and asset management identifier of the owner/user).

Identifier schemes should be clearly fit to the specific use case and identified entity (e.g. thing, user, application). For example a network address (communication identifier) should not be used as thing identifier as the network address of a thing may change during its lifetime.

AIOTI WG03 View:

In general, Chapter 3 defines classes of identifiers for the entities that need to be identified in IoT. Some of these classes have a diverse set of entities (e.g. thing identifiers). We do not expect that one identification scheme will cover them all. Ideally one IoT identification scheme should be used in a specific context. IoT solutions may have to take into account that multiple identifiers, even from different identifier schemes, could identify the same entity, independently (see Annex II for examples).

4.5 Identifier Pattern

In general we can differentiate between identification based on (1) inherent patterns of the entity itself like fingerprints and face recognition and (2) dedicated patterns that are attached to the entity by technical means like printed serial numbers, bar codes, Quick Response (QR) codes, RFID tags and electronic codes in general. The requirements provided by the survey are related to the latter case.

From Survey:

It is often mentioned that the pattern should be short enough to be used in a constrained environments (i.e. network capacity, processing power, energy consumption) or with a specific coding technology like QR codes and RFID. It should be human and machine readable and easy to enter by a human user. Also a specific pattern format (IEEE 64-bit Extended Unique Identifier (EUI64)) is often requested.

While some ask that the identifier should not carry information about the identified entity, others ask for a structure or hierarchy that allows categorizing entities, indicating specific types of entities, producer and other information about the entity.

AIOTI WG03 View:

We note that due to practical and technical reasons (e.g. allocation process, resolution and routing approach) identifiers often have a certain hierarchical structure (e.g. MAC address, IP address). Ideally an identifier should have no significant information about the identified entity. Putting information about the entity into an identifier makes it inflexible and limits its application to specific scenarios. It should therefore be avoided in case the identifier will be used in a wider context.

We recognize that the diverse list of requirements show that a one size fits all approach for identifier pattern will not work. Many identifier schemes, often domain specific, exist and are or will be standardized.

4.6 Traceability, Authenticity & Origin

From Survey:

Traceability is mentioned in relation to the identifier and the identified entity. The latter (i.e. tracing an entity along its life cycle to provide for example food security and sustainable production) is an identifier use case and not a specific requirement on the identifier. Especially for privacy reasons traceability should not be supported if it provides personal information (see privacy category, Section 4.2).

Specifically for the identifier it is requested that it is traceable to the issuer, the correct entity and an authenticator.

AIOTI WG03 View:

We recognise that tracing the identifier itself to its origin (issuer, identified entity) and proofing its authenticity is relevant for many applications and are important security topics (see section 4.3).

4.7 Scalability

From Survey:

Scalability of identifiers is a general concern. However no specific numbers are provided. In general, problems like we have with the limited IPv4 address space should be avoided.

Not only the identifier pattern should be scalable but also the identifier lifecycle management and processing has to be future proof.

AIOTI WG03 View:

We are not in the position to provide specific estimates for the numbers of identifiers that are needed in the future as it strongly depends on the context (use case, identified entity). Beside the context of the application, the structure of the identifier and topics like re-use contribute to the required pattern space. Especially for the context of usage it should be taken into account that it might strongly increase

for future applications. On the other hand the pattern size might be limited due to resource constraints of devices and networks.

4.8 Interoperability & Standards

From Survey:

Interoperability of identifiers within and across application domains, industries and geographical regions is of high importance. The various established and emerging identification schemes of the different domains have to be taken into account and supported.

In case multiple identifiers are used for the same entity mapping between these identifiers has to be supported. Also the mapping between different identifiers of related entities (e.g. thing identifier and communication identifier of the network interface of that thing) has to be supported (see Annex II for examples).

Also the use of a common identifier scheme across different domains is asked for. Worldwide standards are seen as one of the ways to achieve that. One survey responder asks that standards should be preferably royalty free and open. Also open source solutions and community standards (not controlled by a single governing body) are seen as an approach.

AIOTI WG03 View:

We recognise that IoT solutions have to deal with various identifier schemes for different or even the same entities. Many standards already exist and have to be considered. We do not assume that one standard and one scheme will prevail in the future. Handling relations between different identifier schemes (e.g. mapping, resolution) is expected to be a basic functionality of IoT systems. Methods to ensure uniqueness and interoperability of identifiers across domains, schemes and name spaces exist. See Chapter 5 and 8 for more details.

4.9 Persistency & Re-use

From Survey:

A persistent identifier during the lifetime of the entity is asked by many responders. Some ask that the identifier may change, for example if the owner of the entity changes and that identifiers are revocable and replaceable.

While many ask that the identifier is not re-used even beyond the lifetime of the entity, others allow the re-use.

AIOTI WG03 View:

We recognise that persistency and re-use of identifiers are strongly application dependent. We note also that they impact scalability (see section 4.7). Furthermore some identifier types introduce constrains on the level of persistency due to their specific usage (e.g. IP addresses).

4.10 Allocation, Registration & Resolution

From Survey:

Allocation of identifiers should be organized in such a way that individual organizations can allocate their own set of identifiers without conflicting with other organizations (federate approach). The issuing body shall keep track of identifiers (individual or ranges) allocated to an organization.

It shall be possible to register identifiers in a global database which may store information about the identified entity and how to access it. Various identifier schemes should be supported.

Information related to the identified entity should be available by using the identifier. This can be directly provided by the entity or via a link to another location. Depending on the application the information should be available not only online, but also in offline situations.

AIOTI WG03 View:

We note that various allocation methods from allocation at a central authority to independent local allocation have to be supported depending on the use case. Central, federated or local registration and resolution is relevant for many use cases and appropriate solutions have to be provided. We note that usually allocation, registration and resolution are defined as part of the overall identifier scheme and cannot be selected independently. See also Chapter 6 for more details.

5. Identifier Standards

Identifiers for the different classes and entities listed in Chapter 3 are already in use for a long time. A lot of identifier related standards therefore already exist and standardization activities are ongoing. Many of them are applicable for specific domains, set of domains and usage scenarios. Identifier standards are often applicable to more than one of the identifier classes listed.

In this paper we cannot list all of the standards provided by the survey or collected otherwise. A listing would only be useful if we could provide the technical impact and the relevance and applicability for IoT solutions for each standard. This is not possible due to the large number of relevant standards, limited access to some of them and the amount of work that would be required for a detailed analysis. Instead of a complete listing we therefore provide for each identifier category some standards as examples. This does not mean the standards selected as examples are preferred and specifically promoted by AIOTI WG03. They are just examples that were selected due to the expertise of the contributors.

It should be noted that beside identifier standards from standards development organizations and industry associations, governmental bodies have defined identifiers for their applications like social security numbers and number plates for cars. Also companies may have their own definitions for identifiers like serial numbers for products. They are not covered in this chapter.

5.1 Thing Identifier Standards

Numerous standards are available for identifying things. They are often defined for specific domains or specific types of entities, but some are used in several domains and for different types and classes of entities. Some standards provide mechanisms to enable multiple identification schemes to interwork in the same IoT application. They are indicated as meta-identification schemes in the examples below.

Examples:

Vehicle Identification Number (VIN), ISO 3779 [20], specifies a uniform identification numbering system for road vehicles.

Freight containers coding, identification and marking is specified in ISO 6346 [21]. It provides an identification system with mandatory marks for visual interpretation and optional features for automatic identification and electronic data interchange and a coding system for data on container size and type.

Animal identification with radio frequency tags is specified in ISO 11784 [22], independently of the transmission protocol used between the tag and the reader.

The identification of RFID tags through a numbering system is defined in ISO/IEC 15963 [23]. The Tag ID (TID) can be used for traceability and quality control of the tag's integrated circuit. It can also be used for traceability of the item to which the tag is attached. It is however generally considered a good practice to identify objects independently from the technology.

Legal entities can be identified uniquely at global level with the legal entity identifier (LEI) specified in ISO 17442 [24]. The standard was developed in the context of the financial services sector. It can however potentially be used for any application needing to refer to legal entities.

Unique identification of product logistic items, products, returnable transport items and groupings can be achieved with the ISO/IEC 15459 [25] series of standards. The standard makes provision for issuing agencies recognised by a registration authority. These agencies manage the actual identification schemes that can coexist without conflict in IoT applications. GS1 is an example of an ISO/IEC 15459 [25]

compliant issuing agency that manages global identification schemes for products (Global Trade Item Number GTIN), logistic units (Serial Shipping Container Code SSCC), locations and parties (Global Location Number GLN), assets (Global Returnable Asset Identifier GRAI, Global Individual Asset Identifier GIAI), etc. [meta-identification scheme]

The Digital Object Identifier DOI specified in ISO 26324 [26] is a means of identifying an entity over the Internet and used primarily for sharing with an interested user community or managing as intellectual property. The DOI system is designed for interoperability: that is to use, or work with, existing identifier and metadata schemes. [meta-identification scheme]

5.2 Application & Service Identifier Standards

Application and service identifiers are usually defined in the context of the specific platforms (e.g. service platform, operating system) on which they are provided. This can be based on standards or proprietary. In case the platform is standardized also the application and service identifiers are standardized.

Examples:

OneM2M Application & Service Identifiers: OneM2M TS-0001 [27] defines various identifiers that are used by OneM2M based IoT solutions. This includes identifiers for applications, application entities and common service entities.

REST Resource Identifier: Representational State Transfer (REST) is a programming paradigm for distributed systems. It offers services by an electronic device to another electronic device using a uniform and predefined set of stateless operations. The resources of these services are identified by URIs. The URI format is defined in IETF RFC 3968 [18].

5.3 Communication Identifier Standards

Communication identifiers are essential for a communication protocol and impact its functionality (e.g. routing, switching). Usually the identifier scheme cannot be changed without major changes to the protocol itself. Identifiers are therefore defined as part of the specific communication protocol standards.

Examples:

IPv6 Address: IETF RFC 4291 [15] defines the addressing architecture for IPv6. IPv6 addresses are 128-bit identifiers for interfaces (unicast) and sets of interfaces (anycast and multicast).

MAC Address: IEEE 802 [28] defines the MAC Addresses, a network address for most IEEE 802 network technologies, like Ethernet and Wireless LAN. They can be 48-bit or 64-bit numbers, but many IEEE 802 standards refer only to a 48-bit MAC address. MAC addresses can be globally or locally administered addresses. A universal MAC address is globally administered and unique. It is a 48-bit or 64-bit Extended Unique Identifier (EUI-48/64). EUIs have the first 24/28/36 bits assigned by the IEEE Registration Authority as OUI. The assignment of the number for the remaining bits is within the responsibility of the specific organization that allocated the first 24/28/36 bits. EUIs are also used by other communication protocols like Bluetooth.

Telephone Numbers: ITU-T E.164 [16] defines a numbering plan for the worldwide public telephone network (i.e. landlines, mobile networks). E.164 numbers can be a maximum of 15 digits. The first 1 to 3 digits are the country code which is assigned by ITU-T.

5.4 User Identifier Standards

User identifier formats are usually defined by the specific system for which user access is needed. They could be provided by the user (human user) and checked by the system for uniqueness or assigned by the system. Email addresses are often used as identifiers for human users. Governmental organizations often have their own specifications for identifiers for humans and organizations.

Note that the document does not discuss identities and identity management.

Examples:

Email Address: IETF RFC 5322 [29] defines the format of an Internet Email address. It consists of a string followed by the at-sign character ("@") followed by an Internet domain.

Organization Identifier: ISO/IEC 6523-1 [30] defines a structure for uniquely identifying organizations and parts thereof. It uses a hierarchical approach starting with an identifier for the registration authority (max. 4 digits), a organization identifier (max. 35 characters) allocated by the registration authority, an optional organization part identifier (max. 35 characters) allocated by the organization or a 3rd party and an optional organization part identifier source indicator (1 digit/capital letter.)

5.5 Data Identifier Standards

Various standards for the identification of data sets, files, streams, metadata, data types and other data elements exist. Some standardized solutions provide support for multiple identification schemes (see examples below) in order to cover already existing schemes and enable the definition of domain and context specific schemes.

Examples:

Metadata Identifier: ISO/IEC 11179-6 [31] describes the procedure by which metadata could be assigned an internationally unique identifier and registered in a metadata registry maintained by one or more Registration Authorities. It supports multiple identification schemes and ensures the uniqueness of the identification by defining a namespace for each scheme. It does not mandate specific schemes, but provides an annex that describes the structure for the identifier if the identification scheme specified by ISO/IEC 6523-1 [30] is used. Such an identifier is hierarchical structured consisting of a registration authority identifier, a data identifier which is unique within the registration authority and a version identifier for the data item.

Data (Type) Identifier: ISO/IEC 15418 [32] specifies the use of GS1 Application Identifiers and ASC MH10 Data Identifiers for the purpose of identifying encoded data. They are alpha-numeric prefixes used in data carriers like barcodes and RFID-tags that define the meaning and format of encoded data elements (e.g. trade item number, serial number, weight, production date).

Uniform Resource Identifier URI: IETF RFC 3968 [18] defines the syntax for URIs. URIs are used to identify resources which are accessible over a network, typically the World Wide Web. Such resources are often data elements (e.g. documents, programs, data sets) in various formats. URIs support various identifier schemes by having a scheme identifier at the start of each URI. Examples are the “epc” scheme for Electronic Product Codes identified by “urn:epc”.

Properties of electric items: ISO 61360-1 [33] is the basis specification for clear and unambiguous definition of characteristic properties of all elements of electrotechnical systems from basic components to sub-assemblies and full systems. It is the base for the IEC Common Data Dictionary (IEC CDD) [34], a common repository of concepts for all electrotechnical domains. The identifier of a data element type shall consist of the combination of the six-character data element type code, followed by a hyphen followed by the three-digit version number of the data element type. In order to make the code globally unique it is extended with a registration authority identifier ("0112/2///61360_4") according to ISO/IEC 6523-1 [30] and ISO 13584-26 [35].

Database keys: Universally Unique Identifiers (UUIDs) as defined by IETF RFC 4122 [36] are often used as unique keys in databases. UUIDs are 128 bits long and can be locally generated without the need for a central authority for administration. Generation can be based on various methods, including (pseudo-) random generation and algorithmic generation using current time, other local unique identifiers or names.

5.6 Location Identifier Standards

Location identification is important in many IoT applications. Location identification standards exist for the objective naming of a geographical location. This information is often carried in IoT application to keep track of where an event happened or where things are supposed to be or should go to.

Examples:

The standard representation of geographic point location by coordinates, including latitude and longitude, to be used in data interchange is specified in ISO 6709 [37]. It additionally specifies representation of horizontal point location using coordinate types other than latitude and longitude. It also specifies the representation of height and depth that can be associated with horizontal coordinates. Representation includes units of measure and coordinate order.

The International Air Transport Association's (IATA) Location Identifier, a unique 3-letter code, is used in aviation to identify locations of airports throughout the world. IATA also provides codes for railway stations and for airport handling entities. The code is administered by IATA and governed by IATA Resolution 763 [38].

The United Nations Code for Trade and Transport Locations UN/LOCODE [39] is used by most major shipping companies, by freight forwarders and in the manufacturing industry around the world. It is also applied by national governments and in trade related activities, such as statistics where it is used by the European Union, by the Universal Postal Union for certain postal services, etc. Each code element consists of a five characters, where the two first indicate the country (according to ISO 3166-1[40]) and the three following represent the place name.

5.7 Protocol Identifier Standards

Similar to communication identifiers, protocol identifiers are usually defined as part of the protocol that uses them.

Examples:

Ethertype: IEEE 802.3 [13] defines the Ethertype as a 2 octet value that indicates the MAC client protocol. Ethertypes are assigned by the IEEE Registration Authority. The Ethertype is transported in the dual purpose length/type field of the Ethernet Frame. If the value of this field is greater than or equal to 1536 decimal (0600 hexadecimal), then the length/type field indicates the Ethertype.

IPv6 Next Header: IETF RFC 8200 [17] defines the IPv6 packet format. The Next Header field is part of the packet header and defines the type of header immediately following the IPv6 header. That can be an extension header or the header of an upper layer protocol like TCP, UDP or ICMP.

CoAP Content Format Identifier: IETF RFC 7252 [41] defines the CoAP protocol. The content format identifier is an optional part of the protocol that indicates the representation format of the message payload. It is a numeric identifier in the range 0-65535. It is a short form to indicate internet media types like “text/plain”, “application/XML” or “charset=utf-8”.

6. Allocation, Registration and Resolution of Identifiers

Allocation, registration and resolution of identifiers are three distinct processes. Allocation is the process that issues identifiers and ensures that they are unique within their scope. Registration is a means to provide access to public or private information related to the identifier and the related entity. Resolution is a mechanism that provides the means on how to interact with entities or access entity specific services and information.

6.1 Allocation

By definition and purpose, Identifiers are unique in the domain (local or wider area) where they are first assigned to entities and used. Uniqueness can be achieved using the following mechanisms:

1) Extraction: random or next-in-queue extraction of the identifier from a single Registry instance (global repository) of a pre-defined pool of unique identifiers (can be sequential numbers). Every assignment of an identifier requires look-up to the central Registry.
2) Federated extraction: regional, local, domain or organizational specific registries or individual companies have pre-defined subsets of the pool of unique identifiers, whereby the subset is usually identified by a hierarchical structure of the identifier pattern, such as "first 3 digits indicate Registry". Communication between federated registries is not required. The administration of the subsets is done by a central authority. Examples are IP addresses, URNs and MAC addresses.
3) Random and algorithm based generation: random or algorithm based selection from a sufficiently large pool of identifiers (e.g. 100 digits) may provide acceptable risk of duplication of an identifier. If duplication is detected, reconciliation may be applied. Such identifiers can be generated locally without the need for a central authority to administer them. An example is the UUID.
4) Natural: Biometrics (e.g. fingerprint, retina pattern, DNA trace) and other physical characteristics, when reduced to a concise digital form, can be used as "naturally unique" identifiers.

During the lifetime of identifiers duplication conflicts with identifiers from other domains may occur. The following methods can be used in order to resolve the conflicts:

1) Reconciliation: Identifiers are assigned uniquely within a given domain of usage, until duplication with an identifier from another domain is encountered, whereupon one or both identifiers are re-issued to ensure uniqueness.
2) Aliasing: Identifiers are assigned uniquely within a given domain of usage, and ALL usage outside of that domain is mapped to another externally unique identifier (alias).
3) Wrapping: The identifiers are extended with a pattern that is unique for each domain (see chapter 8 on interoperability for more details). This approach can be used just outside the original domain of usage (with a mapping at the domain border -> similar to aliasing) or across all domains (similar to reconciliation).

6.2 Registration

Registration is the process of achieving a mechanism to store and retrieve information related to an identifier and the entity with which an identifier is associated. The process varies depending on the nature of the identifier and of the allocation process. Registration of information about the entity is almost always required, at the minimum to know which entity is associated to the Identifier.

Registration may be done upon allocation of the identifier by the responsible body, but also registration with other bodies during various stages of the life cycle of an entity is possible. For example regulated bodies assign car license plates or telephone numbers and register the data associated with the identifier. In case of federated allocation processes, the final user who has a block of identifiers at his disposal may register them when he associates identifiers with specific entities. This is for example the case for MAC addresses where a chip manufacturer keeps track of the MAC addresses all produced Ethernet and Wireless LAN interface chips. In the case of internet domain names as another example, the final user can assign individual server names within his domain. For these server names to be resolved by DNS, they need to be registered with the responsible registry.

Registration of information about the entity, in association with its identifier, when taken to the extreme case provides a "digital twin" of the entity (as discussed in previous sections). Further discussion is out of scope of this document.

6.3 Resolution

Resolution is the mechanism by which a user/application, based on the entity identifier, gets the information on how to interact with the entity or how to access entity specific services and information. The specific actions depend on the entity, identifier and use case.

A first example is the well-known URL; typing a URL in a web browser will automatically direct the user to the web page identified by the URL thanks to the Domain Name System that resolves the domain name into an IP address.

A second example is the Object Name Service (ONS) standardised by GS1, which is built on DNS (see GS1 Object Name Service specification [42]). It provides a way to resolve identifiers by directing the application to an Internet based resource.

A third example is the Handle System (see IETF RFC 3650 [43]); it is a distributed computer system for assigning persistent identifiers, or handles, to information resources, and for resolving "those handles into the information necessary to locate, access, and otherwise make use of the resources."

7. Security, Privacy and Personal Data Protection

Trust remains one of the main challenges of any technology, and given (a) the data-centric nature of IoT products, systems and services, (b) the fact that such data is to a large extent highly sensitive, personal or otherwise valuable to individuals, companies and organisations, and (c) the fact that digital technologies are nowadays a need to have, and individuals, companies and organisations fully rely – and need to be able to fully rely – on these, security as well as privacy and data protection are key components to trustworthiness. They therefore also have to be considered for identifiers. Related requirements are discussed in Sections 4.2 and 4.3.

Security for identifiers is mainly concerned with the authenticity of the identifier, ensuring that they identify the correct entity in order to prevent that malicious, untrusted and faked entities get access to the IoT system. This requires additional measures like authentication which are outside the scope of this document. Tampering an identifier during its storage, transfer and processing can also strongly impact the behaviour of a system and result for examples in wrong system behaviour which could lead to health, environmental or financial impacts. Appropriate measures to prevent such tampering have to be implemented in such cases. In general, a security threat and risk analyses of the system has to be performed in order to define the technical and organizational measures.

Privacy and Personal Data Protection mainly concerns human related information. Besides human identifiers, this includes identifiers for all entities that can be related to a human like cars, personal devices, goods and health information. Appropriate measures like encryption and access control have to ensure that information related to the identifiers and identified entities are only accessible to permitted and trusted users (humans, applications). Identifiers might be detached from the information or anonymized for certain processing in order to prevent their relation to a specific entity. Also obfuscation of identifiers like continuously changing the identifier of an entity could be appropriate. The principles of data parsimony and data avoidance should also apply to the use and processing of identifiers. In addition, to ensure accountability and thus legal compliance, organisations should be concerned with privacy-related issues throughout their entire life-cycle, ensuring support during designing, manufacturing, sales (incl. subsequent resale), use, as well as at the end of the product life-cycle. A privacy threat and impact analysis of the system along its life-cycle has to be performed in order to define the specific technical and organizational measures.

There is no data protection without security. This goes for both personal data as well as any non-personal data. For instance, personal data protection and privacy is as much about security as it is about data management. Through IoT products, systems and services, organizations create, collect, process, derive, archive and (ideally and to the extent permitted) delete large amounts of data. As part of this data lifecycle, digital data is also transmitted, exchanged and otherwise processed around the world, any time, (almost) any place. In short: data likes to travel. Therefore, information security nowadays is not about data ownership but about data control, access, use and digital rights management. With appropriate and dynamic technical and organisational security measures in place it is possible to achieve a dynamic yet appropriate level of personal data protection. In other words, security is a necessary prerequisite for privacy and (personal) data protection. As a consequence, both security and privacy provide essential building blocks for trustworthiness in digital technologies which includes the identifiers. It

should be noted that security, privacy and personal data protection have to be considered within the context and the system an identifier is used. The type of identified entity, its integration and role in the system, the collected data and their processing contribute to the related requirements.

As technology has accounted for the dynamic developments of markets and society, the rule of law has had to respond accordingly. This has resulted in a set of dynamic principle-based frameworks like the GDPR [19] and Directive on Security of Network and Information Systems (NIS Directive) [44] which take into account the ever-changing nature of the. The European Commission, together with relevant stakeholders including AIOTI and key IoT industrial, demand side and policy players has organised two workshops in 2016 and 2017 (AIOTI Workshop on Security & Privacy in IoT in June 2016 & European Commission's Workshop on Security in January 2017). They resulted in recommendations, principles and requirements as set forth in the respective reports [45][46] in order to enable and facilitate the increase of security and privacy, identify minimum baseline principles and requirements for any IoT product, service or system, and therewith foster trust in human-centric IoT. It should be noted that the workshops and related reports cover security and privacy for IoT solutions in general. They do not discuss security and privacy for identifiers specifically. However the general principles also apply to the use of identifiers in IoT.

8. Interoperability of Identifiers

Interoperability issues for identifiers occur when different identifier schemes have to be supported by IoT solutions. Basically we can differentiate between 3 cases which can happen also in combination:

(1) Different identifier schemes are used for the same entity (e.g. a device manufacturer and the device owner use different identifiers for the same device).
(2) Identifiers from different, but related entities have to be related to each other (e.g. in order to get data from a device the IP address of the sensor attached to the device has to be known).
(3) Applications that go across domains with different identifier schemes for the same entity classes.

For (1) the different identifiers might be (a) actually attached to the identified entity or (b) some of them might only be part of the virtual representation (e.g. digital twin). In case functions and applications deal only with one specific identifier we do not have an interoperability problem (e.g. predictive maintenance application uses only the identifier of the manufacturer). However even in that case the different identifier schemes may come together at some point (e.g. the results of predictive maintenance are used to update the device status in the asset management). At least a mapping between the different identifiers has to be performed in that case. The case that functions and applications have to deal with multiple identifier schemes in general is identical to case (3) and discussed below.

Case (2) requires a resolution mechanism between the different identifiers. The relation between the identifiers may change dynamically over time. Examples are The Domain Name System (DNS) (see IETF RFC 1035 [47]) that resolves domain names into IP addresses and the Neighbor Discovery Protocol NDP (see IETF RFC 4861 [48]) that discovers the link layer address (e.g. Ethernet MAC address) for an IPv6 address. For things the related identifiers like communication addresses and locations could be part of its virtual representation.

In case (3) a differentiation between the different identifier schemes is needed in order to ensure uniqueness and correct interpretation and processing of the identifiers. This might be the unique context in which the identifier is used and processed or a dedicated identification of the identifier scheme is needed. ISO/IEC 29161 [49] for example introduces an unambiguous wrapper based on URNs for the differentiation. The wrapper allows to identify identifier schemes based on various standards for which URN namespaces are defined (e.g. urn:epc, urn:oid, urn:isbn, urn:uuid). Also proprietary identifier scheme could be covered by registering an urn namespace with IANA (see IETF RFC 8141 [50]) or a sub namespace with a registration entity that offers such a service.

9. Conclusion

Identifiers play an important role in IoT. They are used to identify various types of entities for many purposes and within different context. This leads to a wide variety of, sometimes even contradicting, requirements. Special operating constraints for many IoT applications (e.g. constrained devices and networks, entities without processing capabilities) further contribute to that. With the classification of identifiers and the categorization of requirements we provide a structure that may help system architects and developers to identify the type of identifiers and related requirements that they need for their solution and guide them in selecting the specific identifier schemes.

In general, no single identification scheme fits all needs. Furthermore, various identifiers schemes are already in use and standardized for years. They are often application or domain specific, but also generic identifier schemes that cover a wide application area exist. These existing schemes will be used in IoT, and new schemes might be added. We therefore cannot recommend specific schemes and only provided some examples except for the case that the identifier scheme is directly bound to a specific technology like IP and MAC addresses. IoT applications have to deal with the variety of identification schemes and as long as they are used in their defined context this should not be a problem. Mapping and resolution between different schemes is already a standard feature of today's solutions. Still, system architects should have in mind that IoT systems might be used in a wider context and have to interact with other IoT systems in the future. For identifiers that will be impacted by that, an identification scheme that can already handle such situations or can be easily extended should be considered.

Security and privacy are important for identifiers. The specific requirements strongly depend on the use case and identified entity. As part of a security and privacy threat and risk analysis, also the specific requirements related to the identifiers have to be identified and relevant legal and regulatory frameworks have to be taken into account in order to ensure state of the art security and privacy.

Annex I IoT Identifiers Survey

The Survey was launched between 14 March and 19 April 2017. The structure and questions asked are given in the following.

1. Source
   - Organisation / Company name (optional)
   - Organisation / Company web site(s) (optional)
   - I want my organization/company listed as contributor to the survey
   - Email address (optional)
   - First name / last name (optional)
   - I want my name listed as contributor to the survey in the AIOTI IoT Identifier report
   - Country (optional)

2. Application context
   - Provide a brief description of the context. Examples: 1) identify live animals in a farming IoT application; 2) identify equipment on a production line; 3) identify web service in healthcare (required)

3. Identifier
   - What is the purpose of the identifier? (required)
   - How would you classify this identifier? (required)
     - Thing ID (identification of the thing that is in the interest of the specific use case/application)
     - Communication ID (identification of communication source/destination addresses in a communication network, e.g. IP address, MAC address)
     - Application ID (identification of application, e.g. software program)
     - Protocol ID (identification of protocols at the various levels of the OSI stack e.g. IP, http, CoAP)
     - Other

4. Requirements
   - List at least 1 and up to 5 requirements that the identifier needs to fulfil like uniqueness, scalability, privacy, size, accessibility. Please provide background information on the requirements like use cases, specific scenarios, usage in more than one application domain (cross-domain use).
   - Example 1: Uniqueness: the identifier should be unique globally. It will be used in the IoT application and beyond to uniquely refer to the item
   - Example 2: Persistence: the identifier must never be reused. It is the main access key to data related to the item
     - Requirement 1
     - Requirement 2
     - Requirement 3
     - Additional requirements

5. Relevant standards
   - List at least 1 and up to 5 standards that might fulfil the identification needs and requirements with a description, standardization body, technical committee, working group, contact point. Indicate status of the standard (published, under development, in

revision, work item proposal). Please also indicate a web page to access the standard or information about the standard.

Example: ISO/IEC 15459-4:2014 - Unique identification of products and products packages, developed by JTC 1/SC 31. Web page: http://www.iso.org/15459-4

- Standard 1
- Standard 2
- Standard 3
- Additional reference standards

6. Standardisation gaps

   Are you aware of gaps related to standards for IoT identifiers? Please describe up to 5 gaps below.

   - Gap 1
   - Gap 2
   - Gap 3
   - Additional gaps

7. Additional comments

Annex II Multiple Identifiers Examples

In IoT systems multiple identifiers are used. They identify different or the same entity and belong to multiple classes. Two examples are provided below, one in the context of a specific device (smart phone) and the other for a specific application (fitness tracking).

Annex II.1 Smart phone

In the context of a smart phone multiple identifiers are used which are directly or indirectly related to the smart phone, user, subscriber and other purposes. Below is a list of these identifiers. Note that the list is not necessarily complete and that not all listed identifiers are relevant for a specific IoT application.

- Device Identifier (Device ID) or serial number is a unique identifier for the smart phone and assigned by the vendor of the system software. It is for example used for the device identification in USB communication.
  - Ø The Device ID is a thing identifier.
- International Mobile Equipment Identity (IMEI) is a unique identifier for mobile phones (3GPP based networks). It is used by the mobile network to identify the specific smart phone and can for example be used to identify stolen devices. It has no relation to the subscriber. It consists of 15 digits starting with an 8 digit Type Allocation Code (TAC) which identifies the mobile phone type followed by the 6 digit serial number and an optional 1 digit checksum. The TAC is assigned by organizations that are approved by the GSM Association and the first 2 digits of the TAC indicate the organization.
  - Ø The IMEI is a thing identifier.
- International Mobile Subscriber Identity (IMSI) identifies the subscriber on the mobile network. The IMSI is stored on the SIM card. It is usually a 15 digit number with 3 digits for the Mobile Country Code (MCC) and 2 or 3 digits for the Mobile Network Code (MNC). The reminder is the Mobile Subscription Identification Number (MSIN). The MCC is assigned by ITU and the MNC by country specific authorities (e.g. regulator).
  - Ø The IMSI is a user identifier.
- Mobile Station ISDN Number (MSISDN) is the phone number of the subscriber which has to be dialled in order to call it. A subscriber can have multiple MSISDN but only on IMSI.
  - Ø The MSISDN is a communication identifier.
- Integrated Circuit Card Identifier (ICCID) is the identifier of the SIM card itself.
  - Ø The ICCID is a thing identifier.
- Hostname of the smart phone for the internet connection via the wireless LAN interface.
  - Ø Hostname is a communication identifier.
- IP addresses for network connections when the smart phone is connected to the internet.
  - Ø The IP address is a communication identifier.
- MAC address of the wireless LAN interface.
  - Ø The MAC address is a communication identifier.
- Bluetooth device address of the Bluetooth interface.
  - Ø The Bluetooth device address is a communication identifier.
- Near Field Communication (NFC) identifier of the NFC interface.
  - Ø The NFC identifier is a communication identifier.

- Android ID (aka SSAID for Settings.Secure#ANDROID_ID) is generated on first setup of a smart phone (also after factory reset) and identifies the user account. In case of multiple user accounts on a device each account has its unique Android ID.
  - Ø The Android ID is a user identifier.
- Google Services Framework (GSF) Android ID is generated during the initialization of the GSF and is used as identifier for all Google services.
  - Ø The GSF Android ID is a service identifier.
- Usernames for specific applications (e.g. Google applications, email, messenger)
  - Ø User names are user identifiers.
- iOS Application ID and Android Application Package ID are identifiers for smart phone applications.
  - Ø iOS Application ID and the Android Application Package ID are application identifiers
- Vendor specific identifier for advertising purposes like Android Advertising ID, Apple Identifier for Advertising, Windows Advertising ID.
  - Ø Advertising identifiers are application specific identifiers.

Annex II.2 Fitness tracking

In this example the person Paul uses a smart watch for fitness tracking as shown in Figure 2. It is a simplified representation with only the major interactions and related identifiers. Some of the specific identifier schemes shown in the figure are only examples.

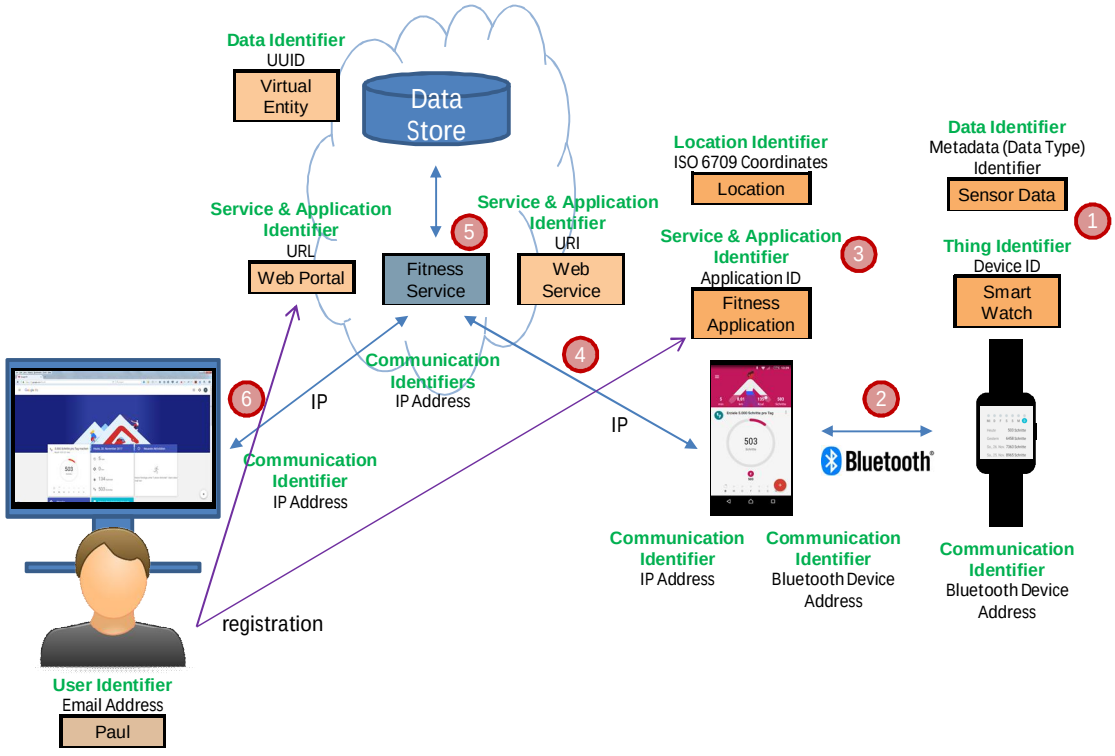

Figure 2 – Identifiers in a fitness tracking use case

(1) The smart watch collects fitness related sensor data (e.g. heart rate, steps).
  - Ø Thing Identifier of smart watch
  - Ø Data Identifier for sensor data

(2) The smart watch sends the data to Paul's smart phone via Bluetooth.

- Ø Communication identifiers of smart watch and smart phone Bluetooth interfaces

(3) A fitness app is running on the smart phone which collects the data from the smart watch and adds location and user information.
- Ø Service & Application identifier of fitness application
- Ø Location identifier from GPS data
- Ø User identifier of Paul

(4) The fitness application sends the data to the fitness service in the cloud.
- Ø Service & Application identifier of fitness service
- Ø Communication identifiers of smart phone and fitness service IP interfaces (web address, IP address)

(5) The fitness application stores and analyzes the data and generates the visualization for the web portal.
- Ø Data identifier of user specific data set

(6) Paul accesses the visualization of his data via the web portal of the fitness service from any internet connect device.
- Ø Service & Application identifier of fitness service web portal
- Ø Communication identifier of internet device and fitness service web portal IP interfaces (web address, IP address)
- Ø User identifier of Paul

The common user identifier, used in step (3) and (6), establishes the relation between the data collection on the smart watch and smart phone and the data visualization on the web portal.

Annex III Bibliography

[1] BEREC, Report Enabling the Internet of Things, 12.02.2016, [Online] Available: http://berec.europa.eu/eng/document_register/subject_matter/berec/download/0/5755-berec-report-on-enabling-the-internet-of_0.pdf [Accessed 15.12.2017]

[2] AIOTI WG03, „High Level Architecture (HLA)“, June 2017, [Online] Available: https://aioti.eu/wp-content/uploads/2017/06/AIOTI-HLA-R3-June-2017.pdf [Accessed 15.12.2017]

[3] China Academy of Telecommunication Research (CATR) & Research Cluster on the Internet-of-Things (IERC), „EU-China Joint White Paper on Internet-of-Things Identification“, 31.10.2014, [Online] Available: http://www.miit.gov.cn/newweb/n1146312/n1146909/n1146991/n1648536/c3489529/part/3489530.pdf [Accessed 15.12.2017]

[4] AIOTI WG01, „Report on Internet of Things Applications“, 15.10.2015, [Online] Available: https://aioti.eu/aioti-wg01-report-on-internet-of-things-applications [Accessed 15.12.2017]

[5] AIOTI WG05, „Report on Smart Living Environment for Ageing Well“, 15.10.2015, [Online] Available: https://aioti.eu/aioti-wg05-report-on-smart-living-environment-for-ageing-well [Accessed 15.12.2017]

[6] AIOTI WG06, „Report on Smart Farming and Food Safety Internet of Things Applications“, 2015, [Online] Available: https://aioti.eu/aioti-wg06-report-on-smart-farming-and-food-safety-internet-of-things-applications [Accessed 15.12.2017]

[7] AIOTI WG07, „Report on Wearables“, 2015, [Online]. Available: https://aioti.eu/aioti-wg07-report-on-wearables [Accessed 15.12.2017]

[8] AIOTI WG08, „Report on Smart Cities“, 2015, [Online], Available: https://aioti.eu/aioti-wg08-report-on-smart-cities [Accessed 15.12.2017]

[9] AIOTI WG09, „Report on Smart Mobility“, 16.10.2015, [Online] Available: https://aioti.eu/aioti-wg09-report-on-smart-mobility [Accessed 15.12.2017]

[10] AIOTI WG11, „Report on Smart Manufacturing“, 2015, [Online], Available: https://aioti.eu/aioti-w11-report-on-smart-manufacturing [Accessed 15.12.2017]

[11] GS1, „EPC Tag Data Standard“, Release 1.11, September 2017, [Online], Available: https://www.gs1.org/epcrfid-epcis-id-keys/epc-rfid-tds/1-11 [Accessed 02.01.2018]

[12] ETSI, GS LTN 002 V1.1.1. „ Low Throughput Networks (LTN); Functional Architecture“, September 2014, [Online], Available: http://www.etsi.org/deliver/etsi_gs/LTN/001_099/002/01.01.01_60/gs_LTN002v010101p.pdf [Accessed 15.12.2017]

[13] IEEE, IEEE 802.3 „Standard for Ethernet“, 2015, [Online]. Available: http://ieeexplore.ieee.org/document/7428776/ [Accessed 15.12.2017]

[14] IETF, RFC 791 „Internet Protocol - DARPA Internet Program Protocol Specification“, 1981, [Online] Available: https://tools.ietf.org/html/rfc791 [Accessed 15.12.2017]

[15] IETF, RFC 4291 „IP Version 6 Addressing Architecture”, [Online]. Available: https://tools.ietf.org/html/rfc4291 [Accessed 15.12.2017]

[16] ITU-T, E.164 „The international public telecommunication numbering plan“, November 2010, [Online] Available: https://www.itu.int/rec/T-REC-E.164-201011-I/ [Accessed 15.12.2017]

[17] IETF, RFC 8200 „Internet Protocol, Version 6 (IPv6) Specification“, 2017, [Online] Available: https://tools.ietf.org/html/rfc8200 [Accessed 15.12.2017]

[18] IETF, RFC 3968 „Uniform Resource Identifier (URI): Generic Syntax“, 2005, [Online] Available: https://tools.ietf.org/html/rfc3968 [Accessed 15.12.2017]

[19] European Commission, General Data Protection Regulation (GDPR), [Online] Available: https://www.eugdpr.org/ [Accessed 15.12.2017]

[20] ISO, ISO 3779 „Road vehicles -- Vehicle identification number (VIN) -- Content and structure”, 2009

[21] ISO, ISO 6346 „Freight containers -- Coding, identification and marking”, 1995

[22] ISO, ISO 11784 „Radio frequency identification of animals -- Code structure”, 1996

[23] ISO/IEC JTC1, ISO/IEC „15963 Information technology -- Radio frequency identification for item management -- Unique identification for RF tags”, 2009

[24] ISO, ISO 17442 „Financial services -- Legal Entity Identifier (LEI)”, 2012

[25] ISO/IEC JTC1, ISO/IEC 15459 „Series Information technology -- Automatic identification and data capture techniques -- Unique identification“, 2014

[26] ISO, „ISO 26324„ Information and documentation -- Digital object identifier system“, 2012

[27] OneM2M, TS-0001 „Functional Architecture“,V2.10.0, 30.8.2016, [Online] Available: http://www.onem2m.org/images/files/deliverables/Release2/TS-0001-%20Functional_Architecture-V2_10_0.pdf [Accessed 15.12.2017]

[28] IEEE, IEEE 802 „Standard for Local and Metropolitan Area Networks: Overview and Architecture“, 2014, [Online] Available: http://ieeexplore.ieee.org/document/6847097/ [Accessed 15.12.2017]

[29] IETF, RFC 5322 „Internet Message Format“, 2008, [Online] Available: https://tools.ietf.org/html/rfc5322 [Accessed 15.12.2017]

[30] ISO/IEC JTC1, ISO/IEC 6523-1 „Information technology – Structure for the identification of organizations and organization parts - Part 1: Identification of organization identification schemes“, 1998

[31] ISO/IEC JTC1, ISO/IEC 11179-6 „Information technology — Metadata registries (MDR) — Part 6: Registration“, 2015

[32] ISO/IEC JTC1, ISO/IEC 15418 „Information technology -- Automatic identification and data capture techniques -- GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance“, 2016

[33] IEC, IEC 61360-1 „Standard data element types with associated classification scheme - Part 1: Definitions - Principles and methods“, 2017

[34] IEC, IEC 61360 - Common Data Dictionary, IEC, [Online]. Available: https://cdd.iec.ch/ [Accessed 15.12.2017]

[35] ISO, ISO 13584-26 „Industrial automation systems and integration -- Parts library -- Part 26: Logical resource: Information supplier identification“, 2000

[36] IETF, RFC 4122 „A Universally Unique IDentifier (UUID) URN Namespace“, 2005, [Online] Available: https://tools.ietf.org/html/rfc4122 [Accessed 15.12.2017]

[37] ISO, ISO 6709 „Standard representation of geographic point location by coordinates“, 2008

[38] IATA, Resolution 763 „Location Identifiers“

[39] UN Centre for Trade Facilitation and E-business, „UN/LOCODE United Nations Code for Trade and Transport Locations“, [Online]. Available: http://www.unece.org/cefact/locode/welcome.html [Accessed 15.12.2017]

[40] ISO, ISO 3166-1 „Codes for the representation of names of countries and their subdivisions -- Part 1: Country codes“, 2013

[41] IETF, RFC 7252 „The Constrained Application Protocol (CoAP) “, 2014, [Online] Available: https://tools.ietf.org/html/rfc7252 [Accessed 15.12.2017]

[42] GS1, „Object Name Service“, 2013, [Online] Available: https://www.gs1.org/sites/default/files/docs/epc/ons_2_0_1-standard-20130131.pdf [Accessed 15.12.2017]

[43] IETF, RFC 3650 „Handle System Overview“, 2003, [Online] Available: https://www.ietf.org/rfc/rfc3650 [Accessed 15.12.2017]

[44] European Parliament and Council, Directive (EU) 2016/ „Measures for a high common level of security of network and information systems across the Union“, 06.07.2016, [Online] Available: http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC [Accessed 15.12.2017]

[45] AIOTI, Report on Workshop on Security and Privacy in the Hyper-Connected World, 16.06.2016 [Online] Available: https://aioti-space.org/wp-content/uploads/2017/03/AIOTI-Workshop-on-Security-and-Privacy-in-the-Hyper-connected-World-Report-20160616_vFinal.pdf [Accessed 15.12.2017]

[46] European Commission & AIOTI, Report on Workshop on Security & Privacy in IoT, 13.01.2017, [Online] Available: http://ec.europa.eu/information_society/newsroom/image/document/2017-15/final_report_20170113_v0_1_clean_778231E0-BC8E-B21F-18089F746A650D4D_44113.pdf [Accessed 15.12.2017]

[47] IETF, RFC 1035 „Domain Name – Implementations and Specification“, 1987, [Online] Available: https://tools.ietf.org/html/rfc1035 [Accessed 15.12.2017]

[48] IETF, RFC 4861 „ Neighbor Discovery for IP version 6 (IPv6) “, 2007, [Online] Available: https://tools.ietf.org/html/rfc4861 [Accessed 15.12.2017]

[49] ISO/IEC JTC1, ISO/IEC 29161 „Information technology -- Data structure -- Unique identification for the Internet of Things“, 2016

[50] IETF, RFC 8141 „Uniform Resource Names (URNs) “, 2017, [Online] Available: https://tools.ietf.org/html/rfc8141 [Accessed 15.12.2017]

Annex IV List of Abbreviations

AIOTI	Alliance for Internet of Things Innovation
BEREC	Body of European Regulators for Electronic Communications
CDD	Common Data Dictionary
CoAP	Constrained Application Protocol
DNS	Domain Name System
DOI	Digital Object Identifier
EPC	Electronic Product Code
EUI	Extended Unique Identifier
EUI48	48-bit Extended Unique Identifier
EUI64	64-bit Extended Unique Identifier
ftp	File Transfer Protocol
GDPR	General Data Protection Regulation
GIAI	Global Individual Asset Identifier
GLN	Global Location Number
GPS	Global Positioning Service
GRAI	Global Returnable Asset Identifier
GTIN	Global Trade Item Number
HTTP	Hypertext Transfer Protocol
HVAC	Heating, Ventilation, and Air Conditioning
IANA	Internet Assigned Numbers Authority
IATA	International Air Transport Association
ICCID	Integrated Circuit Card Identifier
ICMP	Internet Control Message Protocol
ID	Identifier
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
IoT	Internet of Things
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
isbn	International Standards Book Number
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITU	International Telecommunication Union
ITU-T	International Telecommunication Union Telecommunication Standardization Sector
LAN	Local Area Network
LPWAN	Low Power Wide Area Network
MAC	Media Access Control
MCC	Mobile Country Code
MNC	Mobile Network Code
MSIN	Mobile Subscription Identification Number
MSISDN	Mobile Station ISDN Number
NAT	Network Address Translation
NDP	Neighbour Discovery Protocol
NFC	Near Field Communication
NIS	Network and Information Security
nntp	Network News Transfer Protocol
OUI	Organizationally Unique Identifier
QR	Quick Response
REST	Representational State Transfer
RFC	Request for comments
RFID	Radio Frequency Identification
RIR	Regional Internet Registries
SIM	Subscriber Identity Module
SSCC	Serial Shipping Container Code
TAC	Type Allocation Code
TCP	Transport Control Protocol
TID	Tag Identifier
TS	Technical Specification
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URN	Uniform Resource Name
utf	Unicode Transformation Format
UUID	Universal Unique IDentifier

WG	Working Group	XML	eXtensible Markup Language

Annex V Contributors to the Survey

The following people, companies or organizations have contributed to the survey and agreed that they are listed here:

Aitor Cochero, Eurecat
Albertus Pretorius, LicenSys
Antonio Grosso, Digital Business Innovation Srl
Arthur van der Wees, Arthur's Legal
Azael Fernandez, UNAM
Benoît Ponsard, Sigfox
Bruce Nordman, Lawrennce Berkeley National Laboratory
Cedric Crettaz, Mandat International
Cees J.M. Lanting, DATSA Belgium & eHealth experts & WssTP
Christian Schenk, SILVERLINE CONSULTING
Dalibor Pokrajac, GuardRFID
Dan Kimball, ISO/IEC JTC1 SC31
Dave Raggett, W3C
Friedbert Berens, FBConsulting Sarl
Harris Moysiadis, Future Intelligence
Henri Barthel, GS1
Herve Collignon, e-TIC Consulting
Jason Xabier Mansell, Tecnalia
Joaquin Prado, Open Mobile Alliance
John Howie, Huawei Technologies
John Petze
Josef Preishuber-Pflügel, CISC Semicondutor GmbH
Jürgen Heiles, Siemens AG
Ken Sinclair
Konstantinos Michalakis, Intelligent Interaction
Lars Thuring, Logopak Systeme GmbH & Co. KG
Lluis Bueno, NextPointsRFID
Luis Miguel Gracia, INDRA
Maria Eugenia Garcia de Garayo, Empresa de Transformación Agraria S.A.
Mariusz Postol, CAS
Matthew Young
Michael Richardson, Sandelman Software Works
Michele Nati, Digital Catapult
Mika Karttunen, NoridcID
Nicola Fabiano, Studio Legale
Omar Elloumi, Nokia
Pablo Chacin, Sensefields
Paul Murdock, Landis+Gyr
Peter Parslow
Rainer Schrundner, ident.one
Richard Aufreiter, HDI Global
Richard Hill, Hill & Associates
Romain Picard, SoftAtHome
Ruud van Bokhorst, Fairhair Alliance
Sandoche Balakrichenan, AFNIC
Sharon Allen, SGIP
Shunji Mandai, Murat Manufacturing
Srdjan Krco, TagItSmart Project
Sylvie Wuidart, STMicroelectronics
Telit
Tim Bartram, GS1 Germany GmbH
Toon Norp, TNO
Topi Mikkola, BaseN oy
Victor Hailey, VHG
Wanda Jackson, PWD Groups Inc.
Wenyan Bai, Proudsmart
Yves Leboucher, Standardization Council Industrie 4.0

Annex VI Editors and Contributors to this Deliverable

The document was written by the AIOTI WG03 IoT Identifier Task Force

Chairs:

Henri Barthel, GS1, Co-Chair
Jürgen Heiles, Siemens AG, Co-Chair

Editor:

Jürgen Heiles, Siemens AG

Main Contributors:

Arthur van der Wees, Arthur's Legal
Harm Jan Arendshorst, Verizon
Henri Barthel, GS1
Lindsay Frost, NEC Laboratories Europe
Marco Hogewoning, RIPE NCC
Stefan Mangold, Lovefield Wireless GmbH (consultant to Benoît Ponsard, Sigfox)
Thomas Klein, IBM