INTERNATIONAL STANDARD

ISO/IEC 29161

First edition
2016-08-01

Information technology — Data structure — Unique identification for the Internet of Things

Technologies de l'information — Structure de données — Identification unique pour l'Internet des Objets

Reference number
ISO/IEC 29161:2016(E)

ISO copyright office
Ch. de Blandonnet 8 • CP 401
CH-1214 Vernier, Geneva, Switzerland
Tel. +41 22 749 01 11
Fax +41 22 749 09 47
copyright@iso.org
www.iso.org

Contents

Page

Foreword ... **iv**
Introduction ... **v**
1 Scope ... **1**
2 Normative references ... **1**
3 Terms and definitions ... **1**
4 Abbreviated terms ... **1**
5 Identification of an "entity" ... **2**
5.1 General ... 2
5.2 Overview of the "IoT Network" ... 3
6 Unambiguous wrapper for unique identifiers in IoT applications ... **4**
6.1 Overview ... 4
6.2 URN schemes suitable for identification in IoT systems ... 5
6.2.1 Instances of URN schemes ... 5
6.2.2 Listing of existing URN schemes referenced by this International Standard ... 6
6.3 URI usage in IoT systems ... 6
7 Use of unique identification ... **7**
7.1 UI concept ... 7
7.2 UI encoding ... 7
Annex A (informative) **URI usage with ISO/IEC JTC 1/SC 31 standards** ... **8**
Annex B (informative) **OID wrappers and sensor networks** ... **10**
Annex C (informative) **Identification Schemes possible to use in Networks** ... **12**
Annex D (informative) **Ontology of Identification** ... **13**
Bibliography ... **15**

Foreword

ISO (the International Organization for Standardization) and IEC (the International Electrotechnical Commission) form the specialized system for worldwide standardization. National bodies that are members of ISO or IEC participate in the development of International Standards through technical committees established by the respective organization to deal with particular fields of technical activity. ISO and IEC technical committees collaborate in fields of mutual interest. Other international organizations, governmental and non-governmental, in liaison with ISO and IEC, also take part in the work. In the field of information technology, ISO and IEC have established a joint technical committee, ISO/IEC JTC 1.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of document should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO and IEC shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the World Trade Organization (WTO) principles in the Technical Barriers to Trade (TBT) see the following URL: www.iso.org/iso/foreword.html.

The committee responsible for this document is ISO/IEC JTC 1, *Information technology*, Subcommittee SC 31, *Automatic identification and data capture techniques*.

Introduction

In applications of the Internet of Things (IoT), one “thing” can communicate with other “things” via the Internet. For that “thing” to communicate, it should possess an identifier of “which” it is.

The ISO/IEC 15459- series does a good job identifying how groups that have been assigned an issuing agency code can create a character-based system of unique identification.

There is no shortage of claimants to provide that identifier. Each is understandable due to its origins and the perspective from which it comes. The Internet is a network and groups such as the International Telecommunications Union (ITU) and the Internet Engineering Task Force (IETF) view this identifier as a mechanism to facilitate network routing. ITU-T X.668 | ISO/IEC 9834-9 and ITU-T X.660 | ISO/IEC 9834-1 attempt to fill this need from a network perspective. From a network perspective, it is accepted that the identification of an entity must resolve to an IP address for contacting it, whether its domain name “hangs” from an OID root using an OID resolver, or from a more general DNS node (which may end up as the same thing).

However, not everything is viewed from the perspective of the network, nor necessarily should it so be viewed. The network is a transport mechanism and the entities themselves have historic identifiers, which have their genesis from supply chain applications and identification.

Ultimately, the various forms of unique identification identified within this International Standard need to be combined in a single message in an unambiguous form. This International Standard provides a method enabling this combination in an unambiguous form.

Information technology — Data structure — Unique identification for the Internet of Things

1 Scope

This International Standard establishes a unique identification scheme for the Internet of Things (IoT), based on existing and evolving data structures. This International Standard specifies the common rules applicable for unique identification that are required to ensure full compatibility across different identities. The unique identification is a universal construct for any physical object, virtual object, or person. It is used in IoT information systems that need to track or otherwise refer to entities. It is intended for use with any IoT media.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

There are no normative references in this document.

3 Terms and definitions

For the purposes of this document, the terms and definitions given in ISO/IEC 19762 and the following apply.

3.1
coap
constrained application protocol

[SOURCE: RFC 7252]

3.2
entity
any concrete or abstract thing of interest, including associations among things

[SOURCE: ISO/PAS 16917]

Note 1 to entry: Information also provided in Annex D.

3.3
rest
representational state transfer

4 Abbreviated terms

2D	2 Dimensional
AIDC	Automatic Identification and Data Capture
IC	Integrated Circuit
IoT	Internet of Things

IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
MAC	Media Access Control
RF	Radio Frequency
RFID	Radio Frequency Identification
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
URN	Uniform Resource Name
XMPP	Extensible Messaging and Presence Protocol

5 Identification of an "entity"

5.1 General

For the purpose of this International Standard, the term "thing" considers the following as synonyms; "item", "object" and "entity". A thing may be a person, object, or location; see also Annex D.

When one considers the Internet of Things (IoT), the definition of the "thing" is most often coloured by the perspective of the person undertaking the consideration. If one is coming from the world of sensors, the IoT is simply an expansion of a sensor network. If one is coming from the world of RFID, the IoT is simply an expansion of an RFID infrastructure. If one is coming from the world of geospatial data, the IoT is simply an expansion of a location-based network. If one is coming from the world of telecommunications, the IoT is simply an expansion of a telecommunications network. In truth, all are correct. Figure 2 shows some of the possible iterations of "things" that would be possible to connect through the IoT, using various existing communication interfaces. Of course, there are other possibilities and these iterations of IoT might actually be combined, e.g. a mobile phone reading a 2D symbol, an RF tag, or a wireless IC device.

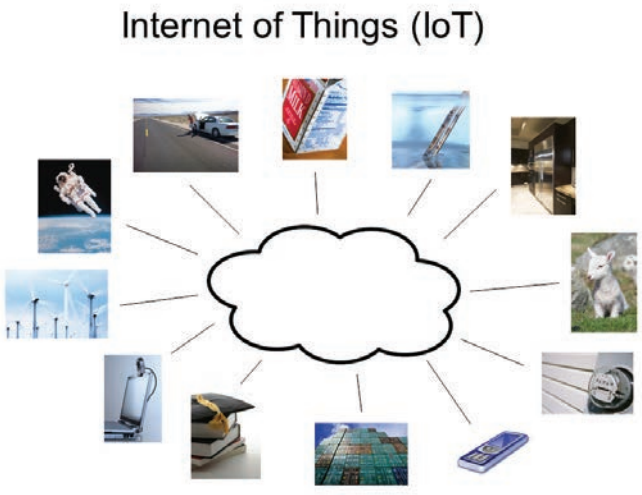

Figure 1 — IoT — everything possible being connected

A single transaction may need to capture several identities as it progresses from origin to destination (and return). For example, there may exist a need to capture, each time a transaction is recorded, the following:

— item identification;

— sensor identification;

— node identification;

— gateway identification;

— target resource identification;

— location of data capture, if mobile;

— time of data capture;

— identification of the individual;

As a virtual thing, software, or software content, ISO/IEC 8824-1:2015, 3.8.52 defines an "object" as *A well-defined piece of information, definition, or specification which requires a name in order to identify its use in an instance of communication. An object is an abstraction or simulation of physical things such as people* ("people" are included in this definition of object only to be true to the quote, whereas this International Standard discriminates between people, objects, and locations) *and machines or intangible things such as events and processes that captures their characteristics and behaviour. Something you can do things to. An object has* ***state***, ***behaviour***, *and* ***identity****; the structure and behaviour of similar objects are defined in their common class*.[64]

The following are properties that may characterize a thing:

a) Identity: the property of an entity that distinguishes it from other entities;

b) Type: describes the type of entity;

c) Data: describes if and how persons, locations and/or other entities can be tied to the entity;

d) Behaviour: describes the methods in the location's interface by which the location can be used.

5.2 Overview of the "IoT Network"

The Internet of Things (IoT) network aims to enable almost everything to communicate with each other, being connected using various communication interfaces and protocols like IPv4, IPv6, MAC addresses, CoAP/REST, XMPP, etc.

Prerequisite for the IoT network is the possibility to tie various information to the right thing for a given purpose using unambiguous identities to which specified information is tied which is then exchanged using application defined protocols.

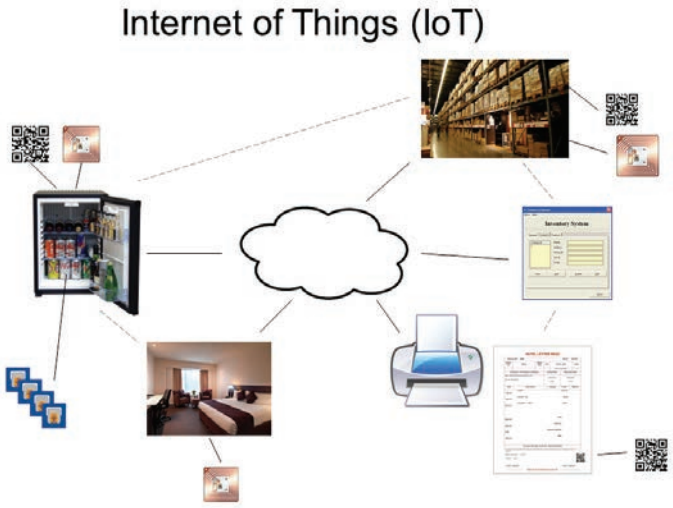

Figure 2 — Possible information exchange using IoT

Figure 2 shows an example where the items positions in a minibar in a hotel room are defined and monitored using sensing techniques. When an item is removed, it is automatically sensed and information is sent so it is registered as being removed. The item will then be added as purchased and the price added to the room bill, to be paid at check out. Received information will also trigger refilling of minibar with the removed item.

The scenario above requires that everything is possible to be uniquely identified, for which this International Standard is to provide a method for adding a wrapper to already existing identification schemes.

6 Unambiguous wrapper for unique identifiers in IoT applications

6.1 Overview

Each form of unique identification stands on its own within the context of applications within that specific identification's domain. When one travels outside of that closed system, an open system form of the identification is required. The nature of the Internet of Things (IoT) is for people and objects to communicate with one and the other. This means that the unique identification scheme will need to accommodate established forms of identification.

For the purposes of this International Standard, the "unambiguous wrapper" for identifiers used in IoT communications shall be a Uniform Resource Identifier (URI) defined by IETF, in RFC 3986. URIs are traditionally classified as either a Uniform Resource Locator (URL, using a string starting with "http://") denoting a web resource, or a Uniform Resource Name (URN, using a string starting with "urn:") as defined in RFC 2141. In both cases, the URI is a text string from a limited subset of US ASCII (for maximum portability across systems). The URI syntax is organized hierarchically, with components listed in order of decreasing significance from left to right. Other structures were considered, but the URI structure is widely accepted and extensively used with today's AIDC data carriers, while providing the flexibility of a broader implementation.

This International Standard is primarily concerned with supporting the interoperable use of Identification schemes from different domains, using existing URNs as needed to provide this interoperability in an efficient manner. Although URLs will also be used extensively in IoT applications, no special treatment of them is required for interoperability, and so this International Standard does not also define headers for URLs.

Various current AIDC data carriers and published ISO/IEC standards already make extensive use of URIs, including the following:

— the encoding of web addresses such as "http://www.iso.org/iso/home.html" in QR Code symbols;

— EPCglobal identifiers such as "urn:epc:id:sgtin:0614141.033254.1" encoded in RFID tags;

— the encoding and transmission protocols for RFID data objects using object identifiers (such as "urn:oid:1.0.15961.9.1" for GS1 Application Identifier "01") in accordance with ISO/IEC 15961-2 and ISO/IEC 15962.

Messages may freely and unambiguously mix identifiers from various AIDC media if published standards already specify a URI format for the identifier. However, no standard URI format is specified for many other identifier schemes that will likely see widespread usage in IoT systems. If an unambiguous wrapper for those identification schemes is needed, it is recommended to use ITU-T X.668 | ISO/IEC 9834-9.

6.2 URN schemes suitable for identification in IoT systems

6.2.1 Instances of URN schemes

Several instances of unique identifiers have already been assigned URN schemes and one of these shall be used if there does not exist an URN representation for an identification scheme to be used. In general, pre-existing URN formats for Identifiers that are recognized by this International Standard include all of those listed in the IANA Registry of URN Namespaces (see http://www.iana.org/assignments/urn-namespaces). Two forms of registered URNs are already in widespread use in AIDC applications and are of particular interest for IoT identification; these URNs are those with a prefix of:

— urn:epc [RFC 5134] in a format defined in the GS1/EPCglobal Tag Data Standards

— urn:oid:1.0.sssss [RFC 3061] where:

  — Per RFC 3061, the first numeric arc of "1" denotes an ISO-assigned OID, then

  — Per ITU-T X.660, the second numeric arc of "0" denotes an International Standard issued by ISO or IEC, and sssss is a specific standard number. Arcs below this are determined as necessary by the corresponding International Standard.

  — Pre-existing urn schemes of this form, of particular relevance to IoT identification, include those with a prefix of:

    — urn:oid:1.0.15961.df, as defined in ISO/IEC 15962 and the ISO/IEC 15961 multi-part series of standards;

  NOTE These OID formats may be utilized both to encode individual data items on RFID tags using a registered Data Format 'df' and to convey the resulting identifier "names" in RFID middleware protocols.

    — urn:oid:1.0.15434.fh, which assigns an OID when the data structure represents an entire ISO/IEC 15434 Format Envelope that utilizes Format Header "fh", as might be encoded in a two-dimensional bar code or RFID tag;

    — urn:oid:1.0.15459.gh, which assigns an OID for the unique identification of products, packages, transport units and groupings. Where "gh" indicates which part of ISO 15459 that is used.

— Other registered urns of interest for identification purposes in IoT applications include (but are not limited to) urn:clei (RFC 4152), urn:isbn (RFC 3187), urn:issn (RFC 3044), urn:iso (RFC 5141), and urn:uuid (RFC 4122).

6.2.2 Listing of existing URN schemes referenced by this International Standard

The following listing shows some of those URN schemes already defined.

— Unique identifiers called out in ISO standards using the Object Identifiers as listed in the ISO/IEC 15961-2 Data Constructs Register. For example, Table 3 of the ISO/IEC 15961-2 Data Construct Register, includes the unique identifier starting with the character string "25S" that is part of the Data Identifier system (see ISO/IEC 15418). The Data Constructs Register shows that this corresponds to the URN "urn:oid:1.0.15961.13.1" because 15961 assigns a Data Format number "13" for Data Identifiers, and the associated Relative OID Table assigns '1' for "25S."

— Unique identifiers called out in ISO standards using the Object Identifiers as listed in the ISO/IEC 15459-1, ISO/IEC 15459-4, ISO/IEC 15459-5 and ISO/IEC 15459-6, URN for ISO/IEC 15459-1 is "urn:1.0.15459.1"

— IPV4: see RFC 3291. The inetAddressMIB is 1.3.6.1.2.1.76 and the type ipv4 (1).

— IPV6: see RFC 3291. The inetAddressMIB is 1.3.6.1.2.1.76 and the type ipv6 (2).

— Jabber ID: RFC 3920, 5.1.1 defines this OID: urn:oid:1.3.6.1.5.5.7.8.5.

— MII: urn:oid:2.27.1, per ISO/IEC 29174 and the Data Constructs Register.

6.3 URI usage in IoT systems

In some existing applications, a specific data carrier only encodes one type of identifier, and the choice of a specific URI as an unambiguous wrapper is predetermined. In other cases, however, a data carrier may encode a wide variety of different unique identifiers, and the appropriate "wrapper" cannot be unambiguously distinguished from context. Therefore, it will often be the case that the appropriate URI wrapper must be determined (from some sort of encoded signal in the data carrier) in order to include that encoded identifier in a mixed-format IoT message.

It is important to note that the URI always provides an unambiguous name for the identifier and in some cases provides the value of that identifier as well. For example, URLs always provide a value (the destination web address) along with the name of the identifier ("http"). The same is true for some forms of URN, such as the "urn:epc" form. For example, "urn:epc:id:sgtin:0614141.033254.1" not only names the identifier (as a pure SGLN) but also provides the specific unique value of that instance.

In other cases, such as the "urn:oid:1.0.15961.n.n" form used to encode item-attendant data in ISO/IEC 18000-63 tags, the URI supplies only the name of the identifier. In this case, the name is efficiently encoded on the tag as a "relative oid," and the complete identifier is both encoded and transmitted as a <name, value> pair. This <name, value> format can be easily represented in many relevant protocols, such as those based on XML.

For example, in a hypothetical XML-based protocol, a <name,value> identifier could be represented as follows:

<widgetID IDname="urn:oid:1.0.15961.13.1">25S123456789ABC123</widgetID>

Continuing the same hypothetical example, an identifier whose urn conveys both name and value could be represented as an empty-element tag, such as:

<widgetID IDname=" urn:epc:id:sgtin:0614141.33254.1"></widgetID>

or

<widgetID>urn:epc:id:sgtin:0614141.33254.1"> </widgetID>

Annex A details how "unambiguous wrapper" URIs could be encoded or otherwise signalled in relevant SC 31 data carriers, and how they could be conveyed in relevant data protocols. Therefore, Annex A

provides multiple use cases for handling a specific scenario. Annex C provides an example of URI usage in a protocol suitable for data carriers including sensor networks.

In many of the protocols that are likely to convey IoT identifiers, such as those based on XML, pure binary data cannot be directly supported. That is to say that although the data carrier may encode such identifiers as a series of 8-bit binary values, when transmitted each such byte value shall be represented as two ASCII characters, each in the range '0'..'9' or 'a'..'f'.

7 Use of unique identification

7.1 UI concept

The Unique Identification (UI) concept employs a qualifier and string component which shall be unambiguous within its qualifier, in the sense that no issuer re-issues the string within the qualifier over the entire life cycle for the identified entity or until a sufficient period of time has passed so that the identity has ceased to be of significance to any user.

7.2 UI encoding

Depending upon existing schemes Unique Identification (UI) can be either numeric, binary or alphanumeric.

When the URN is encoded in a data carrier, it should comply with the encoding rules of that carrier technology.

Annex A
(informative)

URI usage with ISO/IEC JTC 1/SC 31 standards

A.1 Signalling URIs in SC 31 Data Carriers

In some existing AIDC applications, a specific data carrier only encodes one type of identifier, either by design or due to the specific context in which it is used. In such cases, there is no need to modify the encoding or usage of the data carrier in order to add an unambiguous wrapper, because the choice of wrapper is predetermined. Examples include EAN/UPC bar codes (which by design only encode GTINs, as described below), or a bar code on a cell phone card that encodes the phone's IMEI. In the majority of cases, however, a data carrier (bar code, RFID tag, etc.) may encode a wide variety of different identifiers, and the appropriate "wrapper" cannot be unambiguously distinguished from context. Therefore, it will usually be the case that the appropriate URI wrapper should be determined (from some sort of encoded signal in the data carrier) in order to include that encoded identifier in a mixed-format IoT message. The following subclauses detail how URIs can be encoded or otherwise signalled in relevant SC 31 data carriers.

A.2 EAN/UPC and GS1 DataBar symbols

A.2.1 General

With the exception of GS1 DataBar Expanded, these data carriers can only encode a GS1-defined GTIN, and therefore the existence of the appropriate GS1 Application Identifier (01) is implied rather than explicitly encoded. For conveying the GTIN into an IoT message, therefore, it is only necessary to zero-preface the encoded number (as needed, to pad it to a 14-digit length) to create the appropriate value, and the appropriate URI is represented (in a protocol-specific manner as described below) as "urn:oid:1.0.15961.9.1" (per the GS1 table registration to the Data Constructs Register). For the case of GS1 DataBar Expanded, the URI for the Unique Identifier shall be derived from the first encoded AI string, and represented as "urn:oid:1.0.15961.9.n" where n is the first encoded AI.

A.2.2 Code 39, Code 128, and GS1 128 symbols

With the exception of GS1 128 (with FNC1 encoded in the first character position), Code 128 symbols may signal the chosen URN by literally encoding it as a prefix to the data (terminated by two periods, to separate the URN from the remaining data). However, the resulting symbol may be unacceptably long, and so the second method may be preferred.

For the case of GS1 128, the URI is not explicitly encoded, but instead is derived, in exactly the same manner as for GS1 DataBar Expanded.

A.2.3 Two-dimensional symbols

Several options are available for signalling a URI from a two-dimensional symbol.

— URIs that represent web addresses (URLs) are increasingly common, especially in QR Code symbols. These may be unambiguously encoded as verbatim strings (e.g., starting with "http://", or starting with a symbology codeword that expands to such a string). However, because it may not be possible to determine the boundary between the end of a URL and the start of a next data item, this International Standard recommends that if a URL is encoded in a two dimensional symbol, that it be the *only* data item encoded in that symbol. An exception can be made, however, if the URL is prefaced by a data qualifier denoting the encoding of a URL.

— Many two-dimensional symbologies support an encoded indicator for GS1 applications. When these are employed, then the URN is not explicitly encoded, but instead a urn of the form "urn:oid:1.0.15961.9.n" is derived, in exactly the same manner as for GS1 DataBar Expanded.

— Some two-dimensional symbologies support AIM Application Indicators, in which case a URN can be unambiguously signalled.

A.2.4 RFID tags, per ISO/IEC 18000-63

One of two different URN formats is implied, depending on the setting of Bit 0x17 of the tag's UII memory bank.

— If Bit 0x17 is '0', then the UII memory encodes a unique identifier complying with GS1 standards. The implied URN is of the form "urn:epc:(…)" and the details of the URN format are as defined in the GS1/EPCglobal Tag Data Standards.

— If Bit 0x17 is '1' then the UII memory encodes a unique identifier encoded in accordance with ISO/IEC 15962. In this case, an encoded 8-bit Application Family Identifier (AFI) determines the implied URN and this URN is as specified in the ISO/IEC 15961-2 Data Constructs Register.

A.2.5 RFID tags, per ISO/IEC 18000-3 Mode 3

One of two different URN formats is implied, in the same manner as described above for ISO/IEC 18000-63.

A.2.6 RFID tags, per ISO/IEC 18000-3 Mode 1

This RFID air interface does not support signalling a urn of the form "urn:epc:". However, OIDs can be signalled using the same AFI mechanism as is described above for ISO/IEC 18000-63 tags.

A.3 How URIs are conveyed in relevant data protocols

A URI text string (whether it represents a URN or a URL) is inherently unambiguous and can be easily distinguished from other text elements. However, there are a few points to consider in terms of how relevant IoT communications protocols will convey the unambiguous wrapper of each unique identifier presented for transmission.

— Does the URI provide an unambiguous name for the identifier and in some cases provide the value of that identifier as well?

— Is the name efficiently encoded on the tag as a "relative OID" and is the complete identifier both encoded and transmitted as a <name, value> pair?

A.4 Examples

(Volkswagen AG)

Format template <widgetID IDname=" urn:oid:ISO.standard.header">AFI:DI IAC CIN SN</widgetID>

Format example <widgetID IDname="urn:oid:1.0.15459.4">A1:37SUN123456789
5Q1721095BK+123456789</widgetID>

Annex B
(informative)

OID wrappers and sensor networks

B.1 Overview

This Annex provides an example of using OID wrappers recommended by this International Standard in a sensor network environment.

B.2 Use case

A possible use case could be where information from a sensor connected to an RFID tag is to be provided to a user or another system when a given threshold for the actual sensor is being exceeded.

Table B.1 shows the type of information and it sources for the exchange of the following:

— identify destination resource address;

— identify media (RFID);

— identify sensor;

— identify exceeded threshold

— identify item (UII) to which RF tag is attached;

— identify RF reader (identify MAC address);

— identify read location;

— identify time of read.

Table B.1 — Use case flow

Field	Header name	URN	Data
Identify destination resource address	IPv6	No one defined yet.	2001:0db8:85a3:0042:1000:8a2e:0370:7334
Identify media (RFID)	]Z2	Not Used in XMPP src	]Z2
Identify sensor	EUI-64 (MAC, DI:23S)	urn:oid:1.0.15961.13.375	ACDE48FFFE232567
Sensor value	—	—	From ISO/IEC/IEEE 21451-7 (or other)
Identify item (UII)	Transport Unit (J)	urn:oid:1.0.15459.1.2	UN433257110123456789
Identify reader	EUI-64 (MAC, DI:23S)	urn:oid:1.0.15961.13.375	00127FFFFEEB6B40
Identify read location	GPS Location (DI:11L)	urn:oid:1.0.15961.13.469	41.99869/-91.608037/237
Identify time of read	UTC (DI:22D)	urn:oid:1.0.15961.13.92	20130322193351

Example of output based on information in Table B.1 using example XMPP output could appear as follows.

```
<?xml version="1.0" encoding="utf-8"?>
<fields seqnr="1" xmlns="urn:xmpp:iot:sensordata">
<node nodeIdName="urn:oid:1.0.15961.13.375" nodeId="ACDE48FFFE232567">
<timestamp timeStampName="urn:oid: 1.0.15961.13.92" value="20130322193351">
<string name="IPv6" value="2001:0db8:85a3:0042:1000:8a2e:0370:7334"
automaticReadout="true" identity="true"/>
<!------ Example sensor value, in this case from XMPP.IoT.Sensor.Weight ------>
<numeric name="Weight" value="23578" unit="kg" automaticReadout="true" momentary="true"/>
<string name="urn:oid:1.0.15459.1.2" value="UN433257110123456789" automaticReadout="true"
identity="true"/>
<!------ XMPP.IoT.Identity.Ethernet ------>
<string name=" urn:oid: 1.0.15961.13.375" value="00127FFFFEEB6B40" automaticReadout="true"
identity="true"/>
<!------ XMPP.IoT.Identity.Location ------>
<numeric name="urn:oid: 1.0.15961.13.469" value="41.99869/-91.608037/237"
automaticReadout="true" identity="true"/>
</timestamp>
</node>
</fields>
```

Annex C
(informative)

Identification Schemes possible to use in Networks

Table C.1 provides a list of identification schemes that could be used for unique identification in networks, which not claims to be comprehensive. Other schemes may be used and may be created after publication of this International Standard.

Table C.1 — Network Identity Schemes

Identity Scheme	Usage
Extended Unique Identifier (EUI), as per RFC 2373	Allows a host to assign itself a unique 64-Bit IP Version 6 interface identifier (EUI-64). IEEE 802.11 (WLAN), IEEE 802.15.4 (WPAN), and IEEE 802.3 (Ethernet)
Transducer Electronic Data Sheet (TEDS), as per IEEE 1451 set of interface standards	Standardized method of storing transducer (sensors or actuators) identification, calibration, correction data, and manufacturer-related information.
The international public telecommunication numbering plan, as per ITU-T recommendation E.164	Defines the general format for international telephone numbers.
The international identification plan for public networks and subscriptions, as per ITU-T recommendation E.212	Defines the structure of the International Mobile Subscriber Identity (IMSI), which is primarily used by Mobile Network Operators (MNOs) to identify individual subscriptions on mobile networks. Every SIM card in every mobile device in the world is programmed with a unique IMSI number.
International Mobile Equipment Identities (IMEI), as per 3GPP/TS 22.016	The IMEI number is used by a GSM network to identify valid devices and can therefore be used for stopping a stolen phone from accessing that network.
Integrated circuit card identifier (ICCID), as per ITU-T recommendation E.118	Defines the international integrated circuit card identifier used and marked on each SIM.
Unambiguous Individual Identification Number (IIN)	Primary Account number (PAN) based on ISO/IEC 7812-1
	Individual identification using ISO/IEC 15459
	Individual identification using ISO/IEC 15961-2
World Geodetic System (WGS), as per EPSG:4326 (aka WGS 84)	It comprises a standard coordinate system for the Earth, a standard spheroidal reference surface (the datum or reference ellipsoid) for raw altitude data, and a gravitational equipotential surface (the geoid) that defines the nominal sea level , used as the reference coordinate system by the Global Positioning System.
Multimedia information access triggered by tag-based identification - Identification scheme, as per ITU-T recommendation H.642.1	Provides a novel method for to access multimedia content without typing its address on a keyboard or inputting the name of objects and/or places of relevant information.
Representation of dates and times, as per ISO 8601	In representations for interchange, dates and times are arranged so the largest temporal term (the year) is placed to the left and each successively smaller term is placed to the right of the previous term. UTC uses no time zone offset.
Unique identification for RF tags, as per ISO/IEC 15963	Describes numbering systems that are available for the identification of RF tags.

Annex D
(informative)

Ontology of Identification

The “entity” (person, object or location) as shown in Figure D.1 is represented by an identity to be able to connect and provide various associated information for that “entity”. For that “entity” to communicate, it should possess an identifier of “which” it is, that further can be used to answer other questions as for example given in Table D.1.

The seven “questions” in the left column in Table D.1 underpin the very heart of traceability, tracking, and chain of custody, and if using a supply chain system, the columns to the right in Table D.1, provides examples of different types of transactional identification to answer on these seven questions.

Table D.1 — Transactional identification

WHO	Individual	Identification of the individual
WHAT	Product code	Identification of the product (SKU)
WHICH (Item)	Unique item	Globally unique item serial number
WHICH (Group)	Specific group	Identification of the lot or batch
WHICH (Container)	Package ID	Globally unique transport unit identifier
WHERE	Location (Storage/Postal/ Lat Long Alt)	Unambiguous identification of the location
WHEN	At what time	Unambiguous time stamp
HOW	Method	Unambiguous identification of the process
WHY	Authority	Purchase Order/Work Order

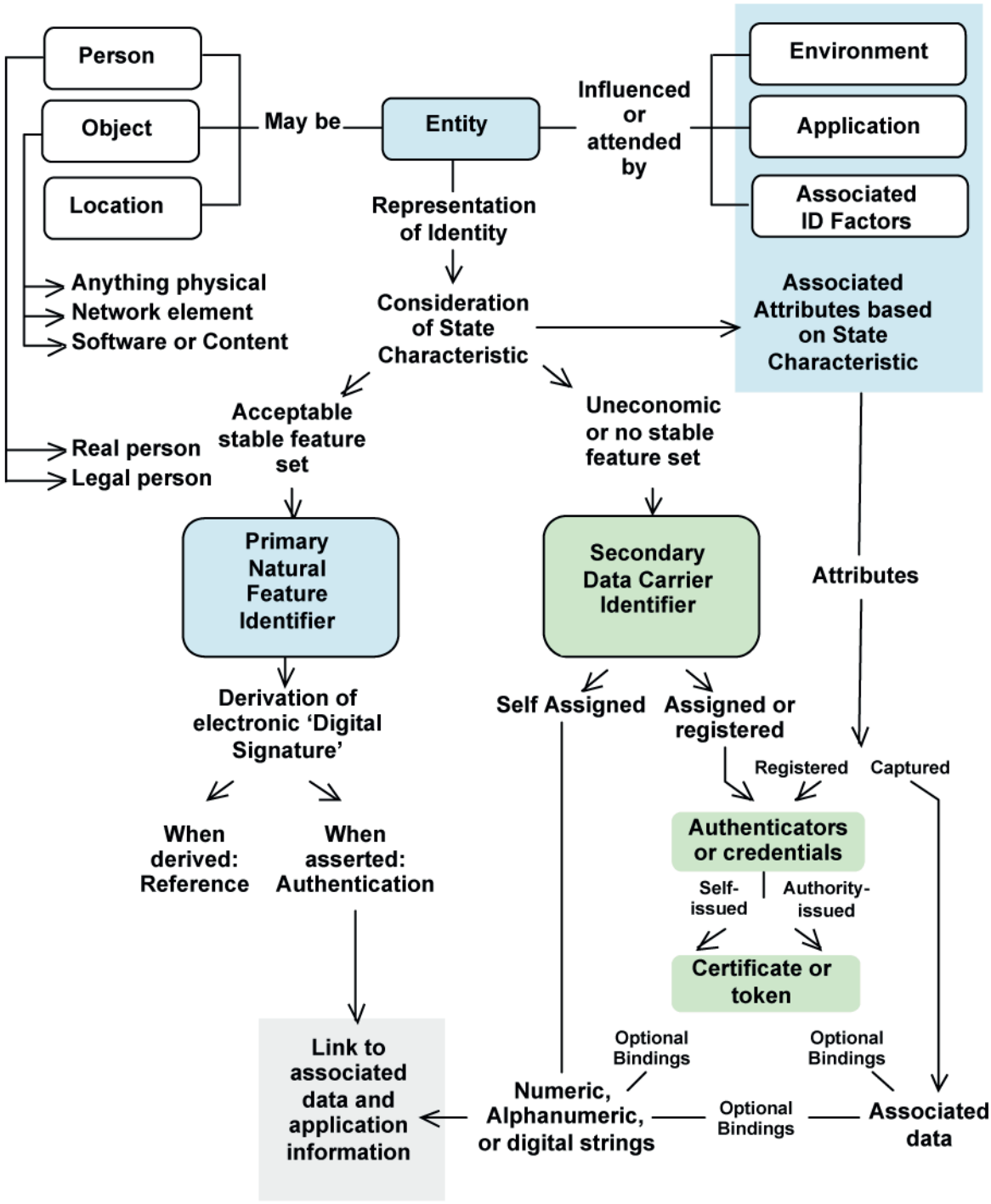

Figure D.1 — Ontology of identity

Bibliography

[1] ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

[2] ISO/IEC 7812-1, *Identification cards — Identification of issuers — Part 1: Numbering system*

[3] ISO/IEC 7812-2, *Identification cards — Identification of issuers — Part 2: Application and registration procedures*

[4] ISO/IEC 7816-5, *Identification cards — Integrated circuit cards — Part 5: Registration of application providers*

[5] ISO/IEC 7816-6, *Identification cards — Integrated circuit cards — Part 6: Interindustry data elements for interchange*

[6] ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

[7] ISO/IEC 15417, *Information technology — Automatic identification and data capture techniques — Code 128 bar code symbology specification*

[8] ISO/IEC 15418, *Information technology — Automatic identification and data capture techniques — GS1 Application Identifiers and ASC MH10 Data Identifiers and maintenance*

[9] ISO/IEC 15420, *Information technology — Automatic identification and data capture techniques — EAN/UPC bar code symbology specification*

[10] ISO/IEC 15434, *Information technology — Automatic identification and data capture techniques — Syntax for high-capacity ADC media*

[11] ISO/IEC 15963, *Information technology — Radio frequency identification for item management — Unique identification for RF tags*

[12] ISO/IEC 16388, *Information technology — Automatic identification and data capture techniques — Code 39 bar code symbology specification*

[13] ISO 17363, *Supply chain applications of RFID — Freight containers*

[14] ISO 17364, *Supply chain applications of RFID — Returnable transport items (RTIs) and returnable packaging items (RPIs)*

[15] ISO 17365, *Supply chain applications of RFID — Transport units*

[16] ISO 17366, *Supply chain applications of RFID — Product packaging*

[17] ISO 17367, *Supply chain applications of RFID — Product tagging*

[18] ISO/TR 17370, *Application Guideline on Data Carriers for Supply Chain Management*

[19] ISO/IEC 18004, *Information technology — Automatic identification and data capture techniques — QR Code bar code symbology specification*

[20] ISO/IEC 24724, *Information technology — Automatic identification and data capture techniques — GS1 DataBar bar code symbology specification*

[21] ISO/IEC/TR 29162, *Information technology — Guidelines for using data structures in AIDC media*

[22] ISO 6346, *Freight containers — Coding, identification and marking*

[23] 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*

[24] IEEE 802.15.4, *IEEE Standard for Local and metropolitan area networks--Part 15.4: Low-Rate Wireless Personal Area Networks (LR-WPANs)*

[25] IEEE 802.3, *IEEE Standard for Ethernet*

[26] ISO/IEC/IEEE 21451-4, *Information technology — Smart transducer interface for sensors and actuators — Part 4: Mixed-mode communication protocols and Transducer Electronic Data Sheet (TEDS) formats*

[27] ISO 8583-1, *Financial transaction card originated messages — Interchange message specifications — Part 1: Messages, data elements and code values*

[28] ISO/IEC 18000-3, *Information technology — Radio frequency identification for item management — Part 3: Parameters for air interface communications at 13,56 MHz*

[29] ISO/IEC 18000-63, *Information technology — Radio frequency identification for item management — Part 63: Parameters for air interface communications at 860 MHz to 960 MHz Type C*

[30] ISO/PAS 16917, *Ships and marine technology — Data transfer standard for maritime, intermodal transportation and security*

[31] ITU-T E.118, *Telecommunication standardization sector of ITU, Series E: Overall network operation, Telephone service, Service operation and human factors, International operation — General provisions concerning administrations the international telecommunication charge card*

[32] ITU-T E.164, *International operation – Numbering plan of the international telephone service — The international public telecommunication numbering plan*

[33] ITU-T E.212, *The International Identification Plan For Mobile Terminals and Mobile users*

[34] ITU-T H.642.1 (ex H.IDscheme), *Multimedia information access triggered by tag-based identification: Identification scheme*

[35] IETF RFC 791, *Internet Protocol, DARPA Internet Program Protocol Specification*

[36] IETF RFC 2460, *Internet Protocol, Version 6 (IPv6) Specification*

[37] IETF RFC 4291, IP Version 6 Addressing Architecture

[38] IEEE 1451.4, *IEEE Standard for A Smart Transducer Interface for Sensors and Actuators — Mixed-Mode Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats*

[39] *International Mobile Subscriber Identity (IMSI) Assignment and Management Guidelines and Procedures*

[40] GSMA TS.06 (DG06), *IMEI Allocation and Approval Guidelines, Version 6*

[41] IEEE EUI-64, *Guidelines for 64-bit Global Identifier (EUI-64™) Registration Authority*

[42] IETF RFC 7230, *Hypertext Transfer Protocol (HTTP/1.1): Message Syntax and Routing*

[43] IETF RFC 7231, *Hypertext Transfer Protocol (HTTP/1.1): Semantics and Content*

[44] IETF RFC 7232, *Hypertext Transfer Protocol (HTTP/1.1): Conditional Requests*

[45] IETF RFC 7233, *Hypertext Transfer Protocol (HTTP/1.1): Range Requests*

[46] IETF RFC 7234, *Hypertext Transfer Protocol (HTTP/1.1): Caching*

[47] IETF RFC 7235, *Hypertext Transfer Protocol (HTTP/1.1): Authentication*

[48] IETF RFC 7236, *Initial Hypertext Transfer Protocol (HTTP) Authentication Scheme Registrations*

[49] IETF RFC 7237, *Initial Hypertext Transfer Protocol (HTTP) Method Registrations*

[50] IETF RFC 7252, *Constrained Application Protocol (CoAP)*

[51] IETF RFC 2141, *URN Syntax*

[52] IETF RFC 3986, *Uniform Resource Identifier (URI): Generic Syntax*

[53] IETF RFC 5134, *A Uniform Resource Name Namespace for the EPCglobal Electronic Product Code (EPC) and Related Standards*

[54] IETF RFC 4152, *URN Namespace for the CLEI Code*

[55] IETF RFC 3187, *Using International Standard Book Numbers as Uniform Resource Names*

[56] IETF RFC 3044, *Using The ISSN (International Serial Standard Number) as URN (Uniform Resource Names) within an ISSN-URN Namespace*

[57] IETF RFC 5141, *A Uniform Resource Name (URN) Namespace for the International Organization for Standardization (ISO)*

[58] IETF RFC 3061, *A URN Namespace of Object Identifiers*

[59] IETF RFC 2373, *IP Version 6 Addressing Architecture*

[60] 3GPP/TS 22.016, *International Mobile station Equipment Identities (IMEI)*

[61] ANSI MH10.8.2, *Data Identifier and Application Identifier Standard*

[62] GS1, *GS1 General Specifications*

[63] Booch G. Objected-Oriented Analysis And Design With Applications. Addison-Wesley, Menlo Park, CA, Second Edition, 1994

[64] IETF RFC 3291, *Textual Conventions for Internet Network Addresses*

[65] IETF RFC 3920, *Extensible Messaging and Presence Protocol (XMPP): Core*

[66] IETF RFC 4122, *A Universally Unique IDentifier (UUID) URN Namespace*

[67] GS1/EPC, *GS1/EPCTag Data Standard*

[68] ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

[69] ISO/IEC 9834-1, *Information technology — Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree — Part 1*

[70] ISO/IEC 9834-9, *Information technology — Open Systems Interconnection — Procedures for the operation of OSI Registration Authorities: Registration of object identifier arcs for applications and services using tag-based identification*

[71] ISO/IEC 15459-1, *Information technology — Automatic identification and data capture techniques — Unique identifiers — Part 1: Individual transport units*

[72] ISO/IEC 15459-4, *Information technology — Automatic identification and data capture techniques — Unique identifiers — Part 4: Individual products and product packages*

[73] ISO/IEC 15459-5, *Information technology — Automatic identification and data capture techniques — Unique identifiers — Part 5: Individual returnable transport items (RTIs)*

[74] ISO/IEC 15459-6, *Information technology — Automatic identification and data capture techniques — Unique identifiers — Part 6: Groupings*

[75] ISO/IEC 15961-2, *Information technology — Radio frequency identification (RFID) for item management: Data protocol — Part 2: Registration of RFID data constructs*

[76] ISO/IEC 15962, *Information technology — Radio frequency identification (RFID) for item management — Data protocol: data encoding rules and logical memory functions*

[77] ISO/IEC 19762, *Information technology — Automatic identification and data capture (AIDC) techniques — Harmonized vocabulary*

[78] ISO/IEC 29174-1, *Information technology — UII scheme and encoding format for Mobile AIDC services — Part 1: Identifier scheme for multimedia information access triggered by tag-based identification*

ICS 35.040

Price based on 18 pages