International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Y.4808

(08/2020)

SERIES Y: GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

Internet of things and smart cities and communities – Identification and security

Digital entity architecture framework to combat counterfeiting in Internet of things

Recommendation ITU-T Y.4808

ITU-T Y-SERIES RECOMMENDATIONS

GLOBAL INFORMATION INFRASTRUCTURE, INTERNET PROTOCOL ASPECTS, NEXT-GENERATION NETWORKS, INTERNET OF THINGS AND SMART CITIES

GLOBAL INFORMATION INFRASTRUCTURE	
General	Y.100–Y.199
Services, applications and middleware	Y.200–Y.299
Network aspects	Y.300–Y.399
Interfaces and protocols	Y.400–Y.499
Numbering, addressing and naming	Y.500–Y.599
Operation, administration and maintenance	Y.600–Y.699
Security	Y.700–Y.799
Performances	Y.800–Y.899
INTERNET PROTOCOL ASPECTS	
General	Y.1000–Y.1099
Services and applications	Y.1100–Y.1199
Architecture, access, network capabilities and resource management	Y.1200–Y.1299
Transport	Y.1300–Y.1399
Interworking	Y.1400–Y.1499
Quality of service and network performance	Y.1500–Y.1599
Signalling	Y.1600–Y.1699
Operation, administration and maintenance	Y.1700–Y.1799
Charging	Y.1800–Y.1899
IPTV over NGN	Y.1900–Y.1999
NEXT GENERATION NETWORKS	
Frameworks and functional architecture models	Y.2000–Y.2099
Quality of Service and performance	Y.2100–Y.2199
Service aspects: Service capabilities and service architecture	Y.2200–Y.2249
Service aspects: Interoperability of services and networks in NGN	Y.2250–Y.2299
Enhancements to NGN	Y.2300–Y.2399
Network management	Y.2400–Y.2499
Network control architectures and protocols	Y.2500–Y.2599
Packet-based Networks	Y.2600–Y.2699
Security	Y.2700–Y.2799
Generalized mobility	Y.2800–Y.2899
Carrier grade open environment	Y.2900–Y.2999
FUTURE NETWORKS	Y.3000–Y.3499
CLOUD COMPUTING	Y.3500–Y.3599
BIG DATA	Y.3600–Y.3799
QUANTUM KEY DISTRIBUTION NETWORKS	Y.3800–Y.3999
INTERNET OF THINGS AND SMART CITIES AND COMMUNITIES	
General	Y.4000–Y.4049
Definitions and terminologies	Y.4050–Y.4099
Requirements and use cases	Y.4100–Y.4249
Infrastructure, connectivity and networks	Y.4250–Y.4399
Frameworks, architectures and protocols	Y.4400–Y.4549
Services, applications, computation and data processing	Y.4550–Y.4699
Management, control and performance	Y.4700–Y.4799
Identification and security	**Y.4800–Y.4899**
Evaluation and assessment	Y.4900–Y.4999

For further details, please refer to the list of ITU-T Recommendations.

Recommendation ITU-T Y.4808

Digital entity architecture framework to combat counterfeiting in Internet of things

Summary

Recommendation ITU-T Y.4808 is intended to provide a solution framework employing digital entity architecture to combat the use of counterfeit Internet of things (IoT) devices worldwide.

There are challenges related to the use and circulation of counterfeit devices in the market, including adverse consequences for users, governments and the private sector.

As documented in the ITU-T Technical Report on Counterfeit ICT equipment [b-Counterfeit ICT Equipment], there are a lot of technical solutions which are widely used for combating counterfeit products the world over. The report indicates that radio frequency identification (RFID) tags are among technologies which are used for combating counterfeiting. While this may be true, there are some difficulties associated with securing these systems with regard to the access control exercised to write on the tags.

There are solutions established for combating counterfeit devices for specific technologies and/or industries which may not be applicable to all use cases. On the other hand, there are solutions which may be applicable to all use cases, these solutions are based on the ITU-T Recommendations such as ITU-T Y.4459 *Digital entity architecture framework for Internet of things interoperability* and ITU-T X.1255 *Framework for discovery of identity management information*.

Resolution 188 (Busan, 2014) on combating counterfeit telecommunication/information and communication technology devices recognized that Recommendation ITU-T X.1255, which is based on the digital entity architecture, provides a framework for discovery of identity management information.

A digital entity architecture, as described in Recommendation ITU-T Y.4459, defines a minimum set of needed architectural components and services to provide a generic information and service interoperability. It will facilitate the interoperability of identification, description, representation, access, storage and security of Internet of things (IoT) devices. This architecture framework encourages a common security and management interface across different IoT applications.

Digital entity architecture provides additional means of security (e.g., public key infrastructure) features to authenticate the parties involved in the identifiers registration process. Other industry approaches to combat counterfeiting are available. They rely on commonly acknowledged identifiers including, but not limited to media access control (MAC), international mobile equipment identity (IMEI), radio frequency identification (RFID), etc.

Systems based on digital entity architecture may be considered as one category of candidate tools which allow vendors/industries (not only ICT industry) to store their products' profile in digital form. Therefore, Recommendation ITU-T Y.4808 can be used in different industries such as the information communication technology (ICT), pharmaceutical, automotive and aviation industries.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Y.4808	2020-08-29	20	11.1002/1000/14381

Keywords

Counterfeit, digital entity architecture, Internet of things.

---

* To access the Recommendation, type the URL http://handle.itu.int/ in the address field of your web browser, followed by the Recommendation's unique ID. For example, http://handle.itu.int/11.1002/1000/11830-en.

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The World Telecommunication Standardization Assembly (WTSA), which meets every four years, establishes the topics for study by the ITU-T study groups which, in turn, produce Recommendations on these topics.

The approval of ITU-T Recommendations is covered by the procedure laid down in WTSA Resolution 1.

In some areas of information technology which fall within ITU-T's purview, the necessary standards are prepared on a collaborative basis with ISO and IEC.

NOTE

In this Recommendation, the expression "Administration" is used for conciseness to indicate both a telecommunication administration and a recognized operating agency.

Compliance with this Recommendation is voluntary. However, the Recommendation may contain certain mandatory provisions (to ensure, e.g., interoperability or applicability) and compliance with the Recommendation is achieved when all of these mandatory provisions are met. The words "shall" or some other obligatory language such as "must" and the negative equivalents are used to express requirements. The use of such words does not suggest that compliance with the Recommendation is required of any party.

INTELLECTUAL PROPERTY RIGHTS

ITU draws attention to the possibility that the practice or implementation of this Recommendation may involve the use of a claimed Intellectual Property Right. ITU takes no position concerning the evidence, validity or applicability of claimed Intellectual Property Rights, whether asserted by ITU members or others outside of the Recommendation development process.

As of the date of approval of this Recommendation, ITU had not received notice of intellectual property, protected by patents, which may be required to implement this Recommendation. However, implementers are cautioned that this may not represent the latest information and are therefore strongly urged to consult the TSB patent database at http://www.itu.int/ITU-T/ipr/.

Table of Contents

		Page
1	Scope	1
2	References	1
3	Definitions	1
	3.1 Terms defined elsewhere	1
	3.2 Terms defined in this Recommendation	2
4	Abbreviations and acronyms	2
5	Conventions	3
6	Principles of identification of products for combating counterfeiting	3
	6.1 Hardware identifiers of IoT things	3
	6.2 Universal product identifier	4
	6.3 Universal identification system using IoT digital entity architecture-based solution	4
7	Verification procedures of product identifiers	5
8	General framework of the IoT digital entity architecture-based identification system for combating counterfeiting	5
	8.1 Digital entity architecture-based IoT system	7
	8.2 UPI interface reader	7
	8.3 Digital entity representation	8
	8.4 How it works	9
Bibliography		10

Recommendation ITU-T Y.4808

Digital entity architecture framework to combat counterfeiting in Internet of things

1 Scope

The intent of this Recommendation is to provide a solution framework employing digital entity architecture to combat the use of counterfeit Internet of things (IoT) devices worldwide.

This Recommendation covers digital entity architecture based systems, including:

– General description of the IoT digital entity architecture-based systems for combating counterfeiting

– Compatibility with other anti-counterfeit systems

– Principles of products identification.

– Universal identification system, which is the same as the global identification system in [ITU-T Y.4459]

– Verification procedures of product's identifiers

2 References

The following ITU-T Recommendations and other references contain provisions which, through reference in this text, constitute provisions of this Recommendation. At the time of publication, the editions indicated were valid. All Recommendations and other references are subject to revision; users of this Recommendation are therefore encouraged to investigate the possibility of applying the most recent edition of the Recommendations and other references listed below. A list of the currently valid ITU-T Recommendations is regularly published. The reference to a document within this Recommendation does not give it, as a stand-alone document, the status of a Recommendation.

[ITU-T X.1255] Recommendation ITU-T X.1255 (2013), *Framework for discovery of identity management information*.

[ITU-T Y.4050] Recommendation ITU-T Y.4050/Y.2069 (2012), *Terms and definitions for the Internet of things*.

[ITU-T Y.4459] Recommendation ITU-T Y.4459 (2020), *Digital entity architecture framework for Internet of things interoperability*.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following terms defined elsewhere:

3.1.1 Internet of things (IoT) [b-ITU-T Y.4000]: A global infrastructure for the information society, enabling advanced services by interconnecting (physical and virtual) things based on, existing and evolving, interoperable information and communication technologies.

NOTE 1 – Through the exploitation of identification, data capture, processing and communication capabilities, the IoT makes full use of things to offer services to all kinds of applications, whilst ensuring that security and privacy requirements are fulfilled.

NOTE 2 – In a broad perspective, the IoT can be perceived as a vision with technological and societal implications.

3.1.2 thing [b-ITU-T Y.4000]: In the Internet of things, object of the physical world (physical things) or of the information world (virtual things), which is capable of being identified and integrated into the communication networks.

3.1.3 device [b-ITU-T Y.4000]: With regard to the Internet of things, this is a piece of equipment with the mandatory capabilities of communication and the optional capabilities of sensing, actuation, data capture, data storage and data processing.

3.1.4 address [b-ITU-T Y.2091]: An address is the identifier for a specific termination point and is used for routing to this termination point.

3.1.5 entity [b-ITU-T Y.2720]: Anything that has separate and distinct existence that can be uniquely identified. In the context of IdM, examples of entities include subscribers, users, network elements, networks, software applications, services and devices. An entity may have multiple identifiers.

3.1.6 digital entity [ITU-T X.1255]: An entity represented as, or converted to, a machine-independent data structure consisting of one or more elements in digital form that can be parsed by different information systems; the structure helps to enable interoperability among diverse information systems in the Internet.

3.1.7 identifier [ITU-T X.1255]: A sequence of bits used to obtain state information about the digital entity being identified; typically, this is done via an appropriate resolution system.

3.1.8 metadata [ITU-T X.1255]: Structured information that pertains to the identity of users, systems, services, processes, resources, information or other entities.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

EPC Electronic Product Code

eSIM embedded SIM

GRI Global Registry of Identifiers

IMEI International Mobile Equipment Identity

IoT Internet of Things

IoTIS Internet of Things based Identification System

LRI Local Registry of Identifiers

MAC Media Access Control

MCU Microcontroller Unit

MPU Microprocessor Unit

NFC Near Field Communication

PID Product Identifier Database

RFID Radio Frequency Identification

UIS Universal Identification System

UPI Universal Product Identifier

TE Terminal Equipment

5 Conventions

None.

6 Principles of identification of products for combating counterfeiting

The principle of product identification is based on allocation and attachment of the particular Internet of things (IoT) unit/tag to the particular product. There are various types of IoT units/tags which can be used for combating counterfeiting, including passive tags such as radio frequency identification (RFID) and near field communication (NFC) and active tags such as microcontroller unit (MCU) and microprocessor unit (MPU).

In general, every product needs to be associated with an IoT tag/unit which becomes a gate to the product's profile that contains detailed information about the product itself. In this regard, a universal product identifier (UPI) needs to be assigned to every IoT tag/unit.

In general, the universal identification system (UIS) should meet the following requirements:

– to be independent from the identified product/technology and should allow identification of services, processes and entities;

– to provide access to the product's profile which contains different types of information about the product (e.g., shape/dimensions, picture, logo, serial number, software version, etc.).

– to have a secure mechanism for preventing cloning and duplication of the used universal product identifier (UPI).

– to be globally unique in global identifier namespace.

6.1 Hardware identifiers of IoT things

According to [ITU-T Y.4050], a "thing" can be physical and virtual.

In accordance with the above requirements, the IoT module which is used for this particular case needs to provide a suitable secure mechanism which guarantees the high level of security.

In general, the IoT module could be based on one of the following interfaces:

– Wired
  - IEEE 802.3

– Wireless
  - GPRS/EDG/3G
  - LTE (IMT-Advanced) / 5G (IMT2020)
  - RFID
  - NFC (QR code)
  - IEEE 802.11
  - IEEE 802.15.1
  - IEEE 802.15.4
  - IEEE 802.15.6
  - IEEE 802.16

Each technology indicated above has particular technical features (e.g., current deviation, power of transmitter, etc.) which can be unique. These features may be used for creating an identification mechanism for a particular technology. Different technologies have different features which may be utilized, where hardware identifiers represent the relevant parameters of IoT entities.

6.2 Universal product identifier

The universal product identifier (UPI) which is used for combating counterfeit goods may be used for getting access to the product's profile. The product's metadata may contain the following information about the product:

– IoT module ID (unique hardware identifier);
– entity (product) type;
– date of registration in the database;
– general information about the product:
  - vendor name;
  - producing date;
  - expiry date;
  - characteristics of the product (e.g., shape, picture, serial number, etc.)
– compliance/certification;
  - the set of standards which product complies with;
  - certificate's date of issue;
  - testing laboratory/certification body;
  - expiry date;

The identifier of a digital entity is used to determine information about the state of the entity itself, which can include, inter-alia, the location of the object, authentication methods, public keys and other relevant data. Because a digital entity is essentially a string of bits that can be uniquely identified, then part of the entity can also be identifiable. Thus, when an IoT device is used as a digital entity, it is possible to identify it. The universal product identifier is not mutable by itself, the identifier is used to refer to the digital entity. When digital entity changes its meta information, this identifier stays persistent.

An example for the structure of data is represented in Figure 1.

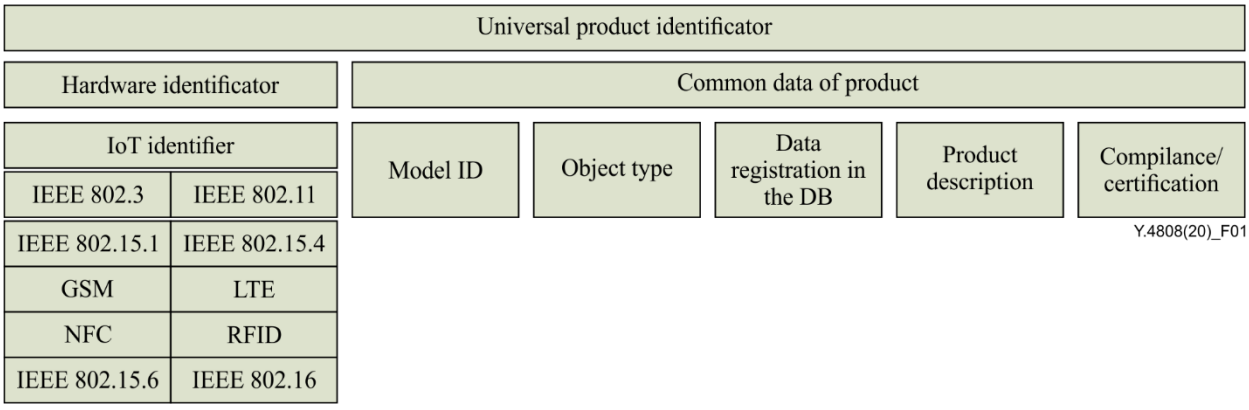

Figure 1 – An example structure of the universal product identifier which is based on IoT tags

6.3 Universal identification system using IoT digital entity architecture-based solution

Under a digital entity architecture, information represented in digital form is structured as digital entities, each of which has an associated unique persistent identifier. This persistent identifier can be represented in the format of a prefix/suffix.

where;

"prefix" determines the location of the registered domain (country/region),

"suffix" determines the relevant information about the product.

7 Verification procedures of product identifiers

There are two types of procedures for verification of universal product identifiers:

Option 1 Purchaser can check the identity of the product using an independent technical solution (e.g., scanning the bar code by mobile phone, getting a code through RFID, etc.);

Option 2 Purchaser can check the identity of the product using the facilities of this product (e.g., mobile phone, tablet, PC, car's media system, etc.).

The details of these options are shown on Figure 2 and Figure 3, respectively.

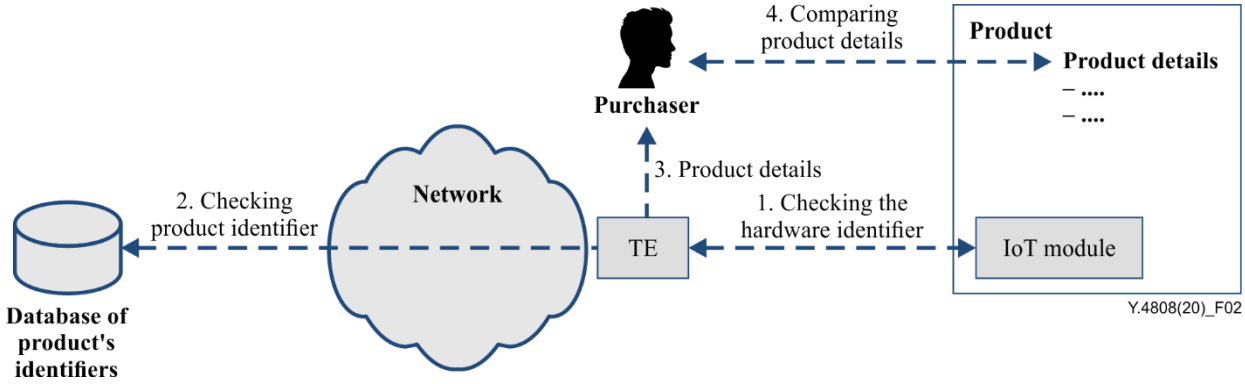

Figure 2 – Verification of product identifiers using an independent technical solution (Option 1)

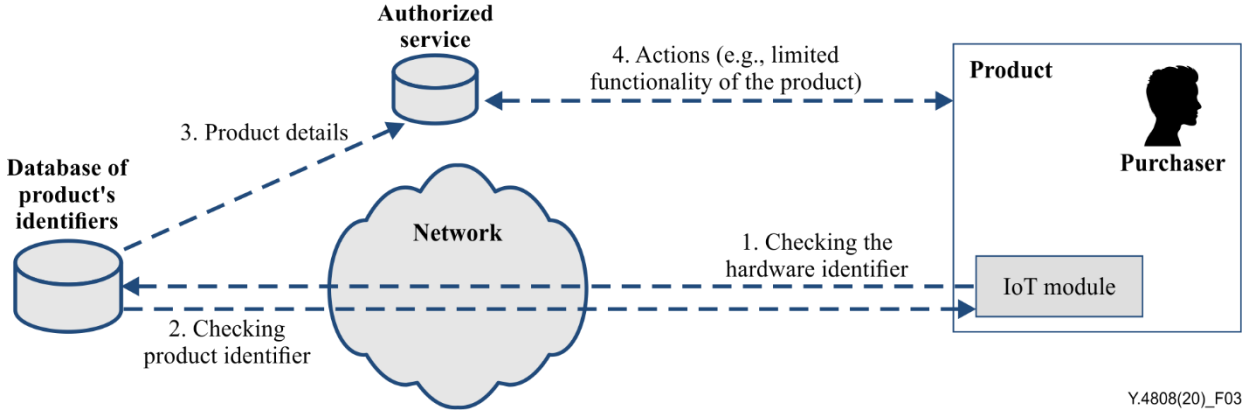

Figure 3 – Verification of product identifiers using the facilities of the product (Option 2)

8 General framework of the IoT digital entity architecture-based identification system for combating counterfeiting

As described in [ITU-T Y.4459], the digital entity architecture framework consists of three basic and fundamental components that when implemented, yield the following services: a global identifier service, a repository service and a registry service. The global identifier service allows a globally unique identifier to be assigned to any digital entity. The identifier service provides a resolution and administration protocol that is used to resolve an identifier into the state information associated with the digital entity, such as storage location and provenance information, may be

retrieved and managed in a secure fashion. The identifier service shall be a distributed service with built-in security such as service integrity, service non-repudiation, data integrity, data authentication, data confidentiality and discretionary access control on any identifier's associated state information.

The set of distributed repository services facilitates the secure storage, access and dissemination of digital entities based on the use of their identifiers. A repository is a digital entity which may or may not contain other digital entities.

The identification system, which is aimed at combating counterfeit goods, is the distributed client-server oriented architecture with a product identifier database (PID). The PID is based on the digital entity architecture concept, and can be divided in two layers; a global registry of identifiers (GRI) and a local registry of identifiers (LRI).

The GRI layer is used for managing the identifier's domain entities whereas the LRI is used for identification of the product represented by the digital entity. Figure 4 shows the relationships of identifiers of the global identification system which is used for combating counterfeit goods.

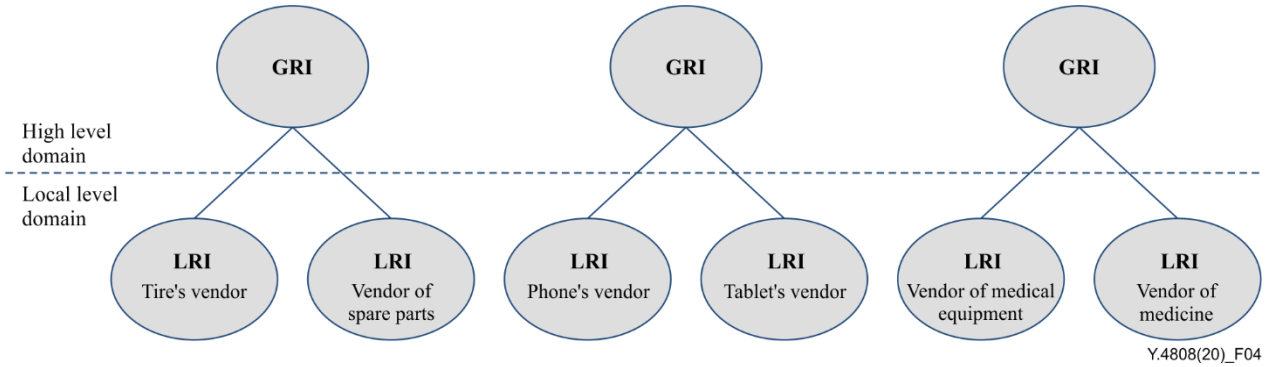

Figure 4 – The relationship of identifiers of the global identification system which is used for combating counterfeit goods

GRI can serve countries or regions whereas LRI is located at the site of the particular vendor. The GRI should provide pointer to corresponding LRI, in accordance with the relevant request received at the point of sale which is represented as terminal equipment (TE) in Figure 5.

In general, the global PID can be accessed by the set of GRI containing the pointers to LRI's which contain necessary information (e.g., owner, location, etc.) that are used for combating counterfeit goods.

The PID can be checked by purchasers at the point of sale using one of the technical tools (e.g., mobile phone, PC, tablet, etc.). The architecture of the identification system is shown in Figure 5.

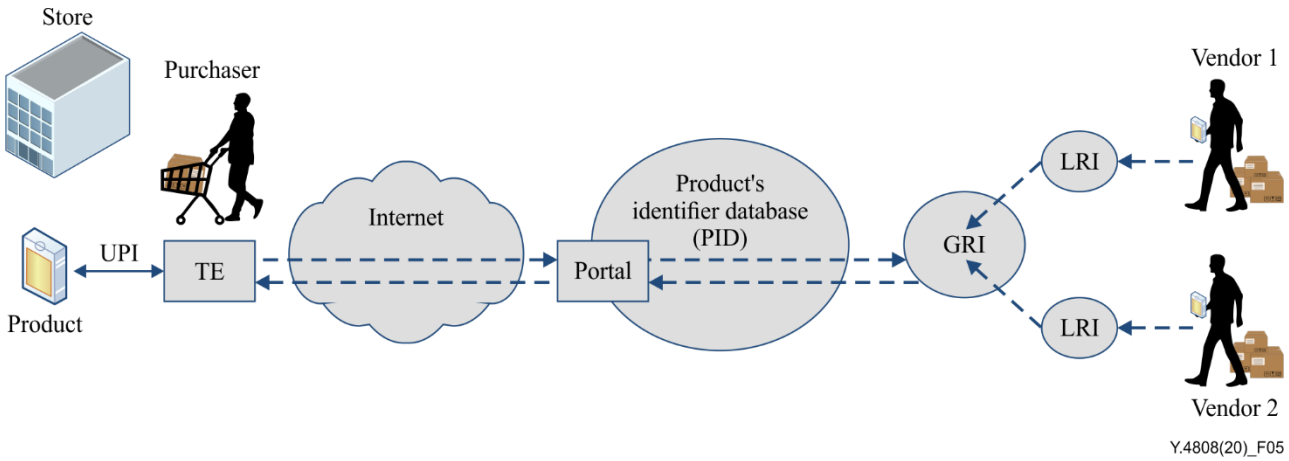

Figure 5 – The architecture of the ICT identification system, aiming to combat counterfeit goods

8.1 Digital entity architecture-based IoT system

Employing digital entity architecture for IoT devices allows an IoT device to be represented as a digital entity and assigned a unique persistent identifier. A digital entity for an IoT device manages metadata about the device, provides state information and interfaces to the device, and defines access control to these interfaces. A unique persistent identifier of a digital entity can be represented in the form: prefix/suffix in accordance with two-layer representation of digital entities registry. In such a representation the identifier's prefix should refer to the global entities registry in the specific country or region, while the suffix will point to a concrete local entity registry under this region that managed the digital entity. Local entities registry may be dedicated with a vendor and located within its vicinity, or may serve for multi-vendors.

The IoT device metadata that is stored in the form of a digital entity can be accessed through a resolution system of the digital entity architecture. By passing a unique identifier that is assigned to the digital entity that represents the IoT device, the metadata about the device can be retrieved.

Figure 6 shows the structure and procedures for the IoT device checking for counterfeiting using the digital entity architecture resolution sub-system.

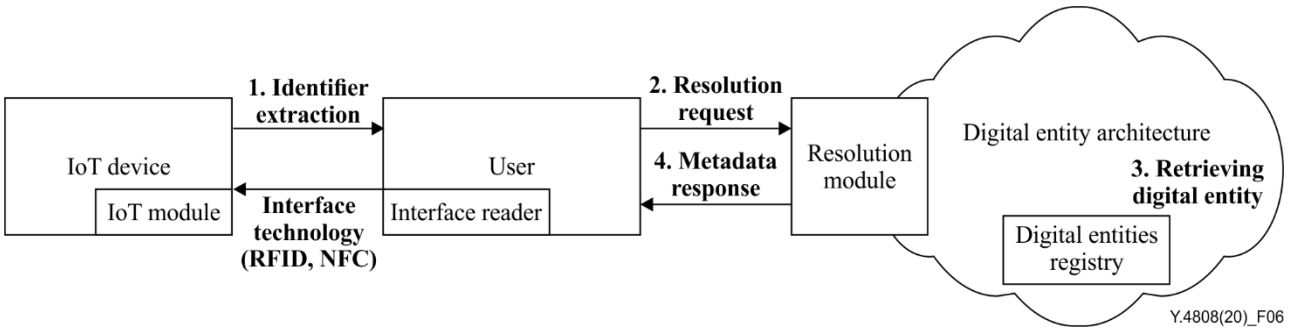

Figure 6 – Digital entity architecture-IoT system

8.2 UPI interface reader

The unique identifier should be integrated in the device hardware for resolution purposes. One way to achieve this is to integrate a separate module into an IoT device that is responsible for the emitting of identification information. The identifier may be stored in a non-volatile read-only-memory (ROM) in the IoT module and can be read and extracted by the user through an interface technology circuit. The user can check the counterfeiting of an IoT device by using a prober interface supported by the IoT module in the device to get the identifier.

There are many technologies that can be deployed as a user interface such as:

1 Near field communication (NFC) technology interface:

The IoT device can support NFC tag, which can be read by any other devices that support the read/write mode of NFC technology. An example of such devices is a mobile device that supports NFC technology.

2 Radio frequency identification (RFID) technology interface:

A passive RFID tag can be implemented in the IoT device which maps to the unique identifier. The RFID tag can be read using any RFID reader device. A mobile device with an operating system that supports a built in RFID reader can be used.

8.3 Digital entity representation

The IoT unique persistent identifier is used to retrieve device metadata and specifications that are represented in the form of a digital entity. Once the user gets the device identifier, the user can extract the device information via the previously illustrated procedures. The device metadata in the digital entity can be divided in a three main parts; the general information, the technical information and the software and application information as illustrated in Figure 7. The general information part contains information associated with the device manufacturer and a general description of the device. The fields of the general information may include the following:

1 Product name,

2 Product type,

3 Manufacturer name,

4 Data assembled,

5 Dimensions and packaging,

6 Associated certificates,

7 Guarantee and maintenance validity.

The second part is the technical information, which contains all information associated with the hardware specifications. This part may include the following fields:

1 Storage specifications,

2 Power specifications,

3 Processing specifications,

4 Communication standard supported.

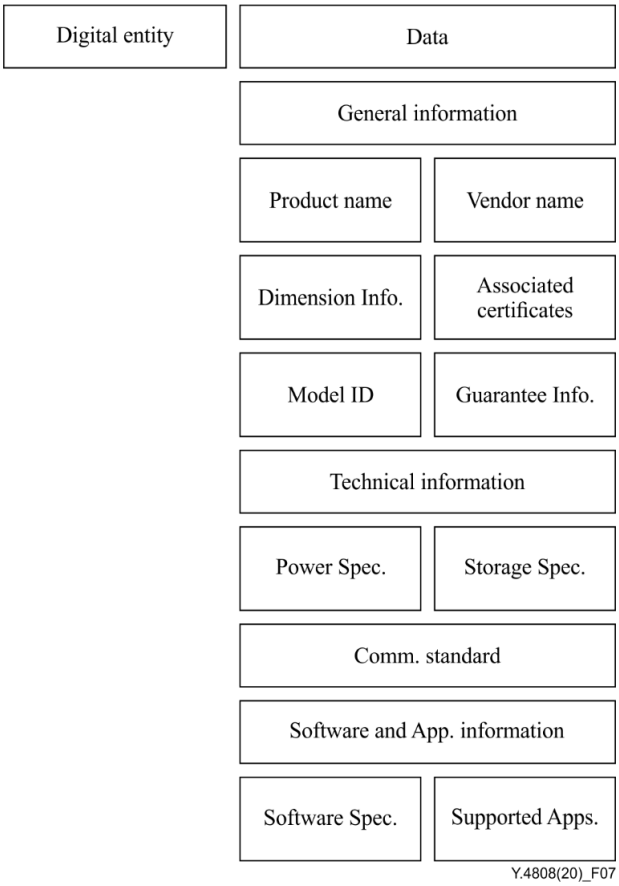

Figure 7 – Device information and digital entity structure

The last part contains information about the software supported by the IoT device. This includes operating system and interface specifications used to interact with other IoT devices and systems. For example, such an interface specification provides the underlying physical interface used for communication (i.e., vendor's API to extract extended information). Also, a list of applications and use cases of the IoT device including the deployment scenarios may be included.

8.4 How it works

The vendor's administrator or another authorised person sends a request to register the new digital entity to the registration system of the digital entity architecture. After receiving a unique persistent identifier for the digital entity, the authorised user can integrate this identifier in a concrete IoT device and using it in various applications to manage the digital entity or concrete device metadata by using a digital entity architecture infrastructure.

Using the digital entity and unique persistent identifiers as the IoT device identifier achieves various benefits. The digital entity architecture-based system can be used to combat counterfeiting in IoT devices. Moreover, the IoT device can use the persistent identifier for the digital entity as the device identification when registered in a network. IoT networks and associated devices may deploy a register for the identifiers of the authorized IoT devices.

Provisioning of data in a digital entity architecture by manufacturers and vendors is voluntary and subject to commercial arrangements. This ensures stakeholders will be able to select the most appropriate solution which meets their needs.

Other methods of identification are reflected in the ITU technical report on counterfeiting [b-Counterfeit ICT Equipment].

Bibliography

[b-ITU-T Y.2091]	Recommendation ITU-T Y.2091 (2011), *Terms and definitions for next generation networks*.
[b-ITU-T Y.2720]	Recommendation ITU-T Y.2720 (2009), *NGN identity management framework.*
[b-ITU-T Y.4000]	Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things*.
[b-Counterfeit ICT Equipment]	ITU-T Technical Report on *Counterfeit ICT Equipment*, version 2, 2015.
[ISO 12931]	ISO 12931:2012, *Performance criteria for authentication solutions used to combat counterfeiting of material goods*.
[ISO 16678]	ISO 16678:2014, *Guidelines for interoperable object identification and related authentication systems to deter counterfeiting and illicit trade*.

SERIES OF ITU-T RECOMMENDATIONS

Series A	Organization of the work of ITU-T
Series D	Tariff and accounting principles and international telecommunication/ICT economic and policy issues
Series E	Overall network operation, telephone service, service operation and human factors
Series F	Non-telephone telecommunication services
Series G	Transmission systems and media, digital systems and networks
Series H	Audiovisual and multimedia systems
Series I	Integrated services digital network
Series J	Cable networks and transmission of television, sound programme and other multimedia signals
Series K	Protection against interference
Series L	Environment and ICTs, climate change, e-waste, energy efficiency; construction, installation and protection of cables and other elements of outside plant
Series M	Telecommunication management, including TMN and network maintenance
Series N	Maintenance: international sound programme and television transmission circuits
Series O	Specifications of measuring equipment
Series P	Telephone transmission quality, telephone installations, local line networks
Series Q	Switching and signalling, and associated measurements and tests
Series R	Telegraph transmission
Series S	Telegraph services terminal equipment
Series T	Terminals for telematic services
Series U	Telegraph switching
Series V	Data communication over the telephone network
Series X	Data networks, open system communications and security
Series Y	**Global information infrastructure, Internet protocol aspects, next-generation networks, Internet of Things and smart cities**
Series Z	Languages and general software aspects for telecommunication systems

Printed in Switzerland
Geneva, 2020