INTERNATIONAL TELECOMMUNICATION UNION

TELECOMMUNICATION STANDARDIZATION SECTOR

STUDY PERIOD 2022-2024

SG20-TD203-R4

STUDY GROUP 20

Original: English

Question(s): 6/20 Geneva, 18-28 July 2022

TD

Source: Rapporteur Q6/20

Title: A.13 justification for proposed draft new Technical Report ITU-T YSTR.IoT-IMS "Requirements and capability framework for identification management service of IoT device"

Contact: Dr. Abdulhadi AbouAlmal E-mail: aalmal@etisalat.ae
Etisalat by e&
ITU-T Q6/20 Rapporteur

Abstract: This TD contains the A.13 justification for proposed draft new Technical Report ITU-T YSTR.IoT-IMS "Requirements and capability framework for identification management service of IoT device".

Please see below.

ITU-T A.13 justification for proposed draft new ITU-T YSTR.IoT-IMS "Requirements and capability framework for identification management service of IoT device"

Question:	Q6/20	**Proposed new ITU-T Technical report**	Geneva, 18-28 July 2022	
Reference and title:	YSTR.IoT-IMS "Requirements and capability framework for identification management service of IoT device"			
Base text:			**Target date:**	2024-08
Editor(s):	Xueqin Jia, China Unicom, jiaxq11@chinaunicom.cn Chao Ma, CAICT, machao@caict.ac.cn Xiaobo Yu, Alibaba China Co, Ltd, shibo.yxb@alibaba-inc.comXiangyu Qu, Zhejiang Dahua Technology Co. Ltd., qu_xiangyu@dahuatech.com Ziqin Sang, China Information Communication Technologies Group, zqsang@ycig.com		**Approval process:**	Agreement

Purpose and scope (defines what issue this non-normative document will address, thus permitting readers to judge its usefulness for their work; also defines the intent or objective of the non-normative document and the aspects covered, thereby indicating the limits of its applicability):

The proposed identification management service is independent from specific existing identification schemes and specific IoT devices. The scope of the Technical report includes:

- Introduction on identification management service of IoT device
- Service requirements of identification management service of IoT device
- Capabilities framework of identification management service of IoT device
- Appendix: use cases for identification management service of IoT device

The interoperation interfaces and procedures between the identification management service proposed and the existing identification scheme are out of the scope. Regulatory policies relate to the proposed ID management service is out of the scope. The security mechanism is not within the scope neither.

Summary (provides a brief overview of the proposal):

To support complex IoT scenarios, identification management service of the IoT device is needed. The proposed identification management service of the IoT device can help IoT platform service providers to manage the access control of the IoT device for platform services. The main purpose of this proposed draft Technic report is to help IoT platform service providers write identification data to IoT devices of different venders, and to help IoT platforms identify identification data from a variety of IoT devices. The requirements related to the modification and deletion of identification data in IoT devices are also included in the proposed draft Technical report. The significance of this proposed draft Technical report is to improve the operation efficiency of the IoT platform on the identification data of IoT devices, so as to reduce the time and money spent on the integration of IoT devices and platforms.

The proposed identification management service is independent from specific existing identification schemes and specific IoT devices. The scope of this technical report includes:

- Introduction on identification management service of the IoT device
- Service requirements of identification management service of the IoT deviceT
- Capabilities framework of identification management service of the IoT device
- Appendix: use cases for identification management service of the IoT device

The interoperation interfaces and procedures between the identification management service proposed and the existing identification scheme are out of the scope. Regulatory policies relate to the proposed ID management service is out of the scope. The security mechanism is not within the scope neither.
Relations to ITU-T Recommendations or other documents (approved or under development): ITU-T Y.4459 (12/2020), ITU-T Y.4808 (8/2020), ITU-T Y.4810 (11/2021), ITU-T Y.4811 (11/2021), ITU-T Y.4805 (08/2017)
Liaisons with other study groups or with other standards bodies: ITU-T SG17, ITU-T SG2, oneM2M, IETF, GSMA, CSA-IoT, AIOTI, ISO/IEC JTC1, ETSI, IEEE
Supporting members that are committing to contributing actively to the work item: China Unicom, CAICT, MPT of Algeria, Zhejiang Dahua Technology Co. Ltd., Alibaba China Co, Ltd, China Information Communication Technologies Group

Appendix

1. Problems to be solved

1.1 One existing scheme for IoT platform service providers to manage their identification data of the IoT devices

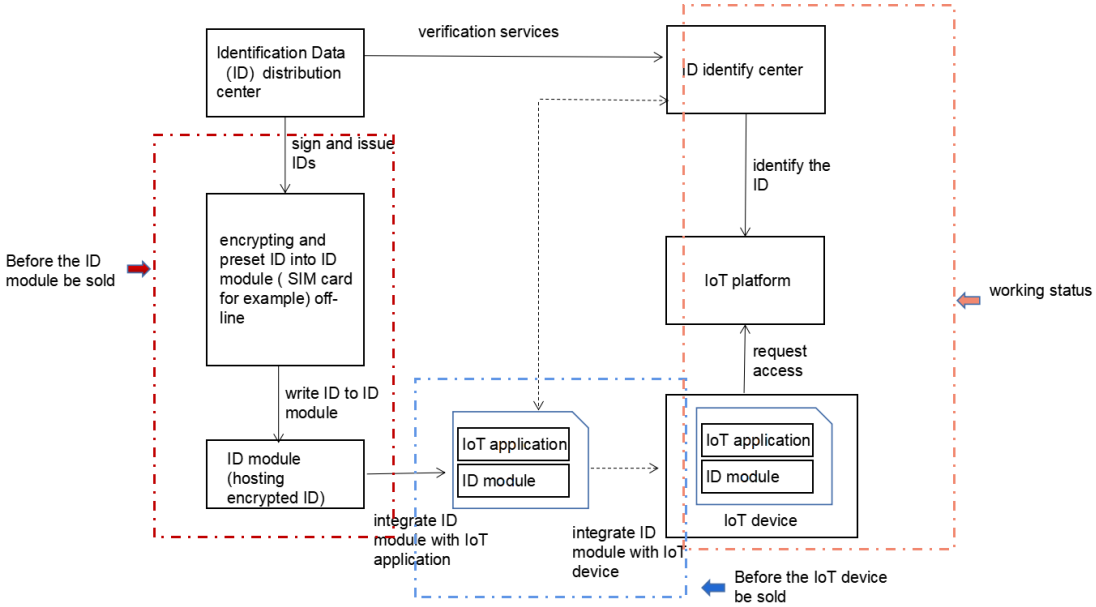

Figure 1 One existing scheme

The problems need to be solved:

- The ID is preset to the ID module before the ID module be sold out. Due to ID module providers usually don't know where their ID modules will be sold or who will buy them, the IoT platform service providers need to customize the ID modules. Customization has high cost, including time and money.
- ID module needs to be integrated with the IoT application of the IoT device, the IoT application may need to be customized (because the ID module is customized).
- The IoT device may need to be customized. Due to the ID module is customized, the IoT device may need to adopt to the customized ID module. The cost of IoT device may be high.

1.2 A potential ID management scheme for IoT platform service providers to manage their identification data of the IoT devices

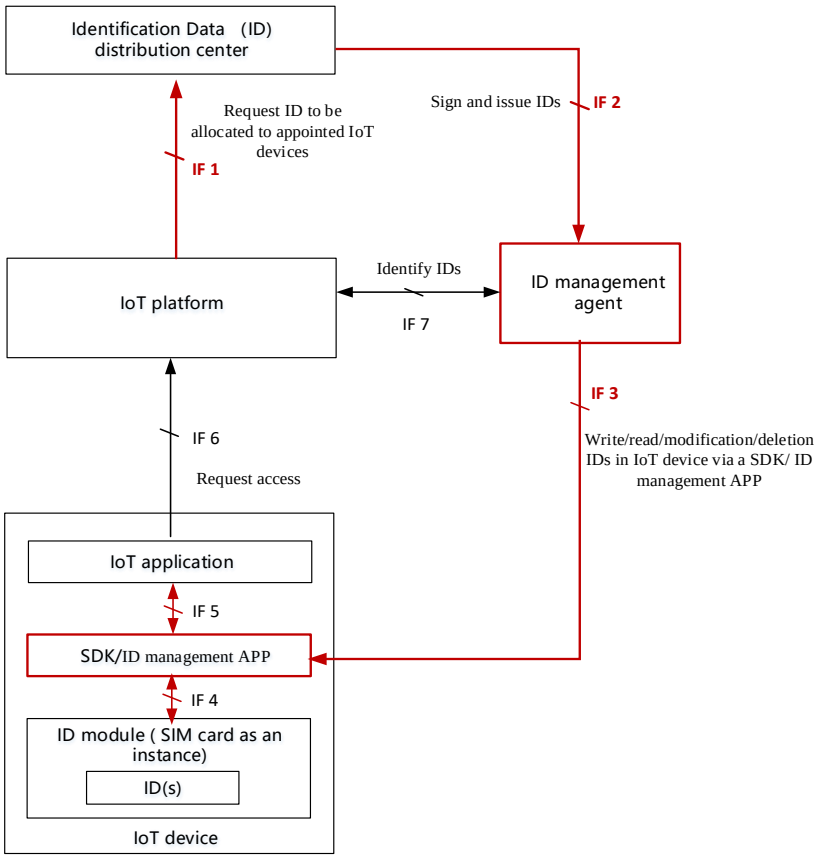

Figure 2 A potential ID management scheme

The owner of the ID distribution center can be many cases. For example, the owner of the ID distribution center can be an independent institution, or the ID distribution center can integrate with the IoT platform owned by the IoT platform provider, or maybe the ID distribution center can be owned by a IoT device vendor or ID module vendor. Every IoT stakeholder may own its ID distribution center under the regulatory policies of their countries. But this proposed NWI only focuses on requirements and capabilities of ID management service of the IoT device, the related regulatory policies is out of the scope of this proposed NWI. And the security mechanism is not within the scope neither.

The potential ID management scheme, which can be the start point of this proposed new work item, has the following advantages:

- No need to preset the ID in the ID module. ID distributor center, ID management agent and SDK/ID management APP can works on-line.
- No customization for ID module because no need to preset IDs in the ID module.
- No customization for IoT device. Because SDK/ID management APP can support the IoT device to interwork with the ID management agent.
- In case the IoT device supports the evolving scheme, the IoT platform service provider can allocate the IoT device desired IDs on-line whatever the vendor of the IoT device is.

2. What we proposed to do?

Requirements and capability framework for ID management service of the IoT devices is an important topic that will help to benefit multiple vertical use cases with lower cost and more efficiency.

3. Use cases

The potential ID management scheme can be used in many use cases. There are a good number of smart city use cases as examples.

3.1.Domestic gas meters

Domestic gas meters have multiple vendors. Gas meters vendors sell their meters to multiple gas service providers.

Each gas service providers may have their own gas management platform (from some point of view, they can be regarded as a IoT platform providers) to manage gas meters for household users.

To avoid fake gas meter accessing the gas management platform, the gas service provider need to assign each gas meter identification data (i.e., ID) for accessing control.

If the gas meter support the potential ID management scheme indicated in 1.2, the gas service provider can assign each gas meter an ID on-line, no need to request the vendor to preset the IDs for the gas meters in customized way.

Highlight: not all identification data need to be managed by the potential ID management scheme indicated in figure 2. This scheme is just candidate or optional.

3.2.Environmental monitoring of construction site

The site environment monitor needs to be connected to the platform of the site management organization. When the construction team changes the construction site, it often needs to change the site management organization and the related platform. Each site management organization needs to write identification data to the site environment monitor. In this scenario, the ID of the site environment monitor needs to be written by different site management organization platforms.

If the site environment monitor supports the potential ID management scheme indicated in 1.2, the site management organization can assign each site environment monitor an ID on-line, no need to request the vendor of the site environment monitor to preset the IDs for the site environment monitor in customized way.

4. Additional material for gap analysis

SG17: X.ztd-iot: Security Methodology for Zero-Touch Deployment in Massive IoT based on Blockchain

X.ztd-iot focuses on the security methodology and related security designs for realizing zero-touch deployment of future massive IoT (mIoT). To be specific, this Technical report covers the security architecture, the security considerations and personally identifiable information protection, and the related security procedures (such as device attestations, authentication, and credential provisioning) which are needed for building such a zero-touch mIoT deployment platform.

The proposed new work item focuses on how IoT platform provider/service provider to manage identification data for IoT devices. No overlap.

5. What identification data the proposed NWI will manage?

For various reasons (such as network access, data collection, device management, etc.) in the IoT scenarios, IoT devices may be given multiple IDs. This project does not distinguish between these reasons, but refers to the subject that gives the ID of the IoT device as the ID distribution center. This distribution center may be centralized or distributed. Many technologies can help realize distributed distribution centers, such as distributed ledgers. This can be one of the study points of this project.

6. **What relationship with existing identification schemes?**

The proposed NWI can interoperate with the exiting identification schemes, please refer to clause 8.

7. How does the system handle the new devices added or removed to the network?

It is the platform service provider who can handle the new devices added or removed to the service, but not the network. In the case of domestic gas meters, clause 3.1, it is the gas service providers handle the gas meters added or removed to their gas management platform. In the case of environmental monitoring of construction site, clause 3.2, it is the site management organization. The site management organization handles the site environment monitors added or removed to the platform of the site management organization based on the request from the construction team.

8. Further clarification to how the new identification schemes will interoperate with existing schemes?

The proposed NWI interoperates with existing identification schemes, as shown below in figure 3. It is necessary that the ID distribution center can obtain identifiers from existing identification systems. Considering the existing identification systems are diversity, the interfaces between the existing identification systems and the ID distribution center are diversity too. Since the proposed NWI is independent from the specific existing identification schemes, these interfaces and the associated processes for these interfaces are out of the scope of the proposed NWI.

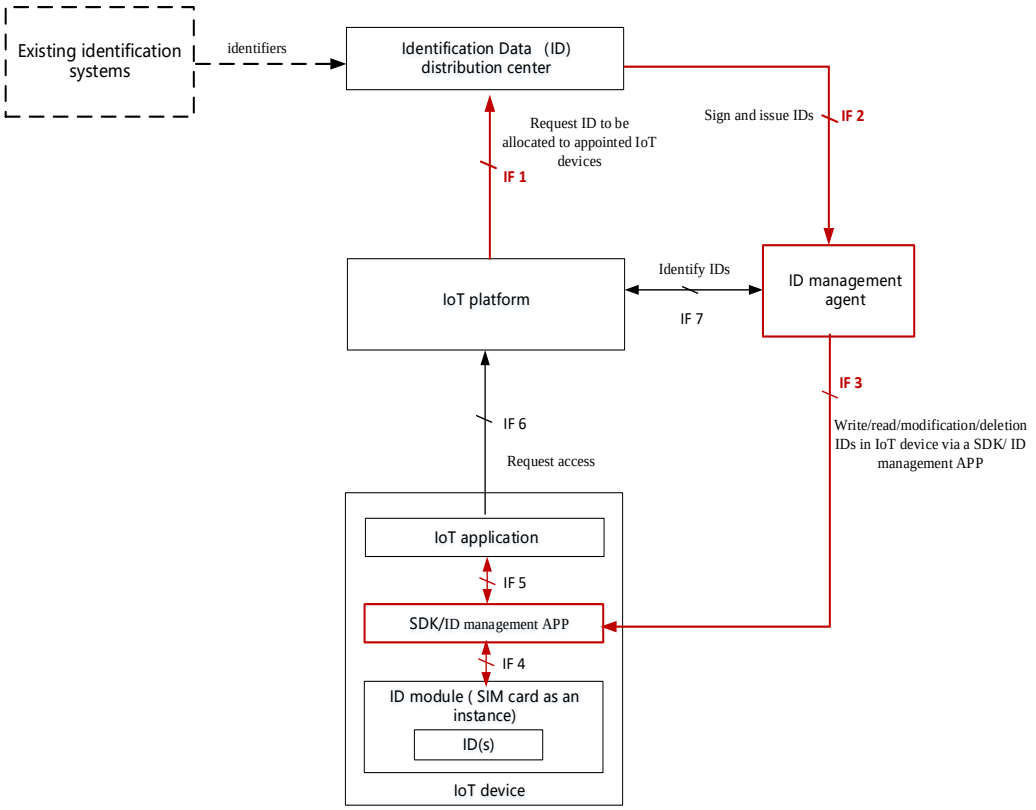

Figure 3 A potential ID management scheme with existing identification systems

9. Further use-cases to clarify the scale in magnitude for the new identification system?

For a city, there may be more than 7000 street lamps in the main roads. Street lamps are likely to become smart street lamps. Smart street lamps may provide multiple services, including but not limited to electronic billboard services, charging services, environmental monitoring services.

Use case: smart street lamp

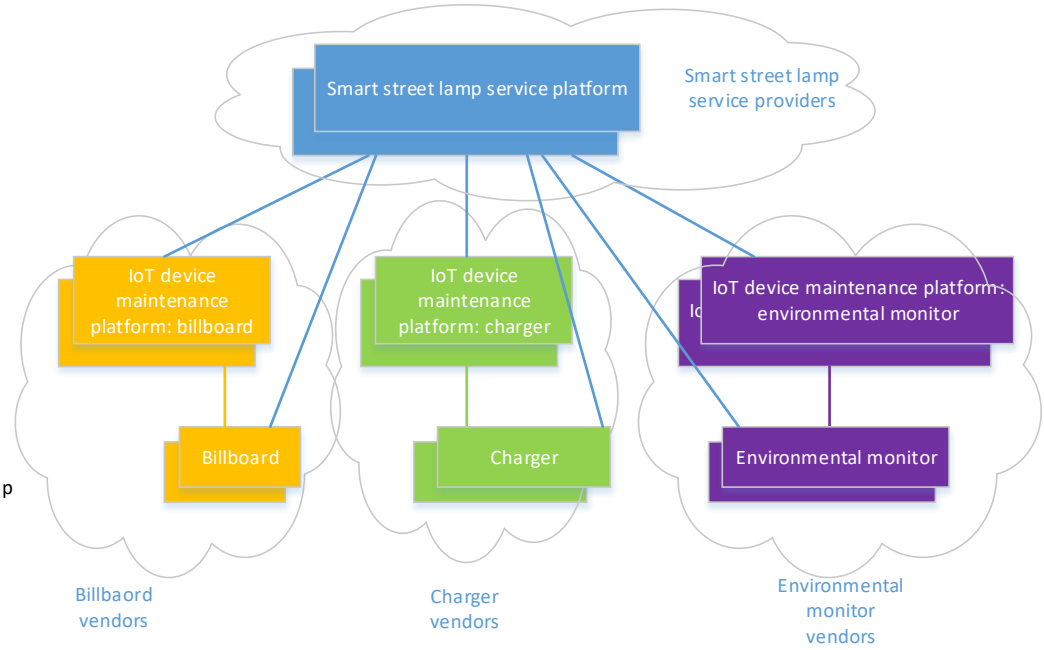

Figure 4 Use case of smart street lamp

As shown in figure 4, diversity IoT devices, including but not limited to electronic billboard, charger, environmental monitor, may be integrated with the smart street lamp.

For the smart street lamp, IoT devices need to be interoperated with the smart street lamp service platform and at the same time to be connected with a corresponding maintenance platforms of corresponding vendors.

There are many cases which need identification data interoperation to enable related services.

For example, when an electronic billboard of the smart street lamp broken, the corresponding maintenance platform of the electronic billboard may find and then will inform the smart street lamp service platform. Next, the smart street lamp service platform can trigger repairing request to the maintenance platform and may order a new electronic billboard to the vendor. In these process, the identification data interoperation between the smart street lamp service platform and the maintenance platform of the electronic billboard is necessary.

Using the scheme proposed by the proposed NWI, the new electronic billboard can be debugged with the maintenance platform first, and then the smart street lamp service platform can remotely allocate identification data to the new electronic billboard in order to support services of the electronic billboard.

10. What are the issues related to implementation and deployment?

In practice, it is necessary to have a mechanism to allocate identification data to the IoT devices and to bind the IoT devices with the allocated identification data after the IoT devices deployed and in use.

The scheme proposed by the proposed NWI will benefit IoT devices to migrate from one IoT platform to another IoT platform, clause 3.2 the site environment monitor is an example.

The scheme proposed by the proposed NWI will also benefit massive IoT device management. Clause 9 the smart street lamp is an example. Without the scheme of the propose NWI, the smart street lamp service platform providers need to preset identification data to the IoT devices with the help of the IoT device vendors. If the IoT device vendors and the IoT platform providers are both support the proposed NWI, the identification data of IoT devices can easily to be migrated from the smart street lamp service platform to the maintenance platforms of the venders.

11. Comments:

- **The current mechanisms are operational, still not clear why the new mechanism is needed?**
- Please refer to clause 1, 9 and 10.**It is useful to have standard which flexible enough to address the need of different identification schemes across different verticals and industries**The proposed NWI is flexible because it is independent from the specific existing identification scheme and study object is the general IoT device which intends to be generic.

_____