International standardization of ICT/IoT solutions to be used for combating counterfeiting

Alexey Borodin

Representative of Rostelecom in Geneva

Network Changes in IoT Era

1. Enormous number of Internet of Things
   (up to trillion, maximum value is 50 trillions, according to J.-B. Waldner "Nano-computers and swarm intelligence")

2. Self-organized architecture
   (instead of «heavy» existing networks)

3. Super-dense heterogeneous network
   (5G includes mobile and sensor networks, VANET, medicine networks, etc.)

4. Ultra-low latency networks
   (Tactile Internet, some applications of medicine networks)

Security of IoT

1. Substitution of MAC and IP of IoT-based device – less than 1 min → high probability of cloning of IoT devices

2. Wide usage of wireless technologies (e.g. WiFi, BLE, ZigBee, LoRa) for connecting IoT devices → high probability of the data intercept in "air"

3. ITU-T X.1255 "Framework for discovery of identity management information" – as an approach to combat counterfeiting

Combating counterfeiting using IoT

Key issues for standardization:

1. Secure and trustable identification procedure for IoT which is based on identifiers to be used in different industries (ICT, health, transport, etc.)
2. Checking the authenticity of IoT's ID (testing)
3. Handle System (getting access to the IoT tag's profile)

Secure and trustable identification procedure for IoT

ITU-T SG20 started a new work item Y.IoT-IoD-PT *"Identity of IoT devices based on secure procedures and ensures privacy and trust of IoT systems"* *(Jan.2016)*

Scope: the methods and scenarios of IoT identification procedure to be used with simple IoT devices such as RFID, NFC, SAW and complex IoT devices which are based on the microcontroller or microprocessor

Work item

Checking the authenticity of IoT’s ID (testing)

ITU-T SG11 started a new work item Q.39_FW_Test_ID_IoT *“The framework of testing of identification systems used in IoT” (Dec.2015, June 2016)*

Scope: description and test suites of identification procedures used in Internet of Things according to IoT identification procedures specified in Y.IoT-IoD-PT

Work item

Handle System
(getting access to the IoT tag's profile)

ITU-T SG20 started a new work item Y.IoT-DA-Counterfeit *"Information Management Digital Architecture to combat counterfeiting in IoT" (August 2016)*

Scope: ICT solutions to contain the spread of counterfeit IoT devices over the globe. Recommendation contains description of the systems which are based on digital object architecture (DOA)

Combating counterfeiting using IoT and DOA

IoT+DoA chain is a good tool to combat counterfeiting:

- IoT interfaces have specific features which are complicated to duplicate – it allows customer to be sure that the purchased product which equipped with IoT module is a genuine (not counterfeit)
- Using Digital Object Architecture (DoA) concept, each product which equipped with IoT module/interface may have a unique identity which purchaser of ICT product will be familiar with

Y.IoT-DA-Counterfeit

“Information Management Digital Architecture to combat counterfeiting in IoT” (August 2016)

Content:

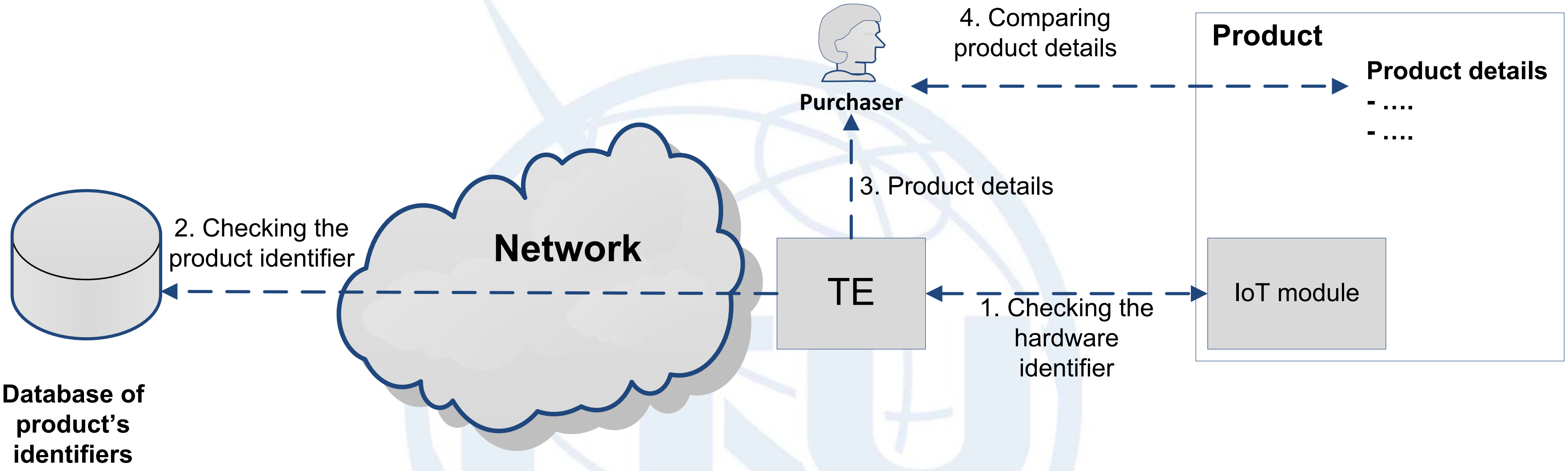
- General description of the IoT-DOA-based systems for combating counterfeiting
- Compatibility with other anti-counterfeit systems
- Principles of products identification
- Universal identification system
- Verification procedures of product’s identifiers

References to the current ITU-T work items:

Y.IoT-IoD-PT (identification, SG20)

Q.39_FW_Test_ID_IoT (testing, SG11)

Procedures of verification of product’s identifiers using IoT and DoA concept (1/2)

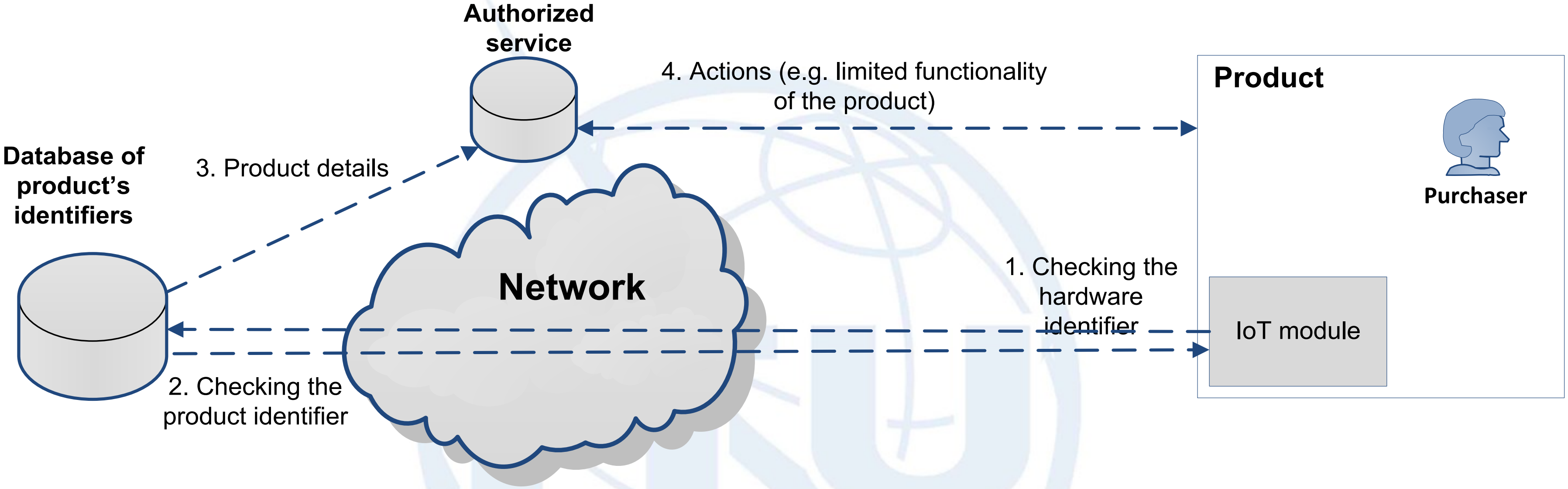

Purchaser
4. Comparing product details
Product
Product details
- ….
- ….
3. Product details
2. Checking the product identifier
Network
TE
IoT module
1. Checking the hardware identifier
Database of product’s identifiers

Purchaser can check the identity of the product using an independent technical solution, for example, scanning BAR code, RFID

Note: detailed info is available in C297R1 (SG 20)

(Source: Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE)

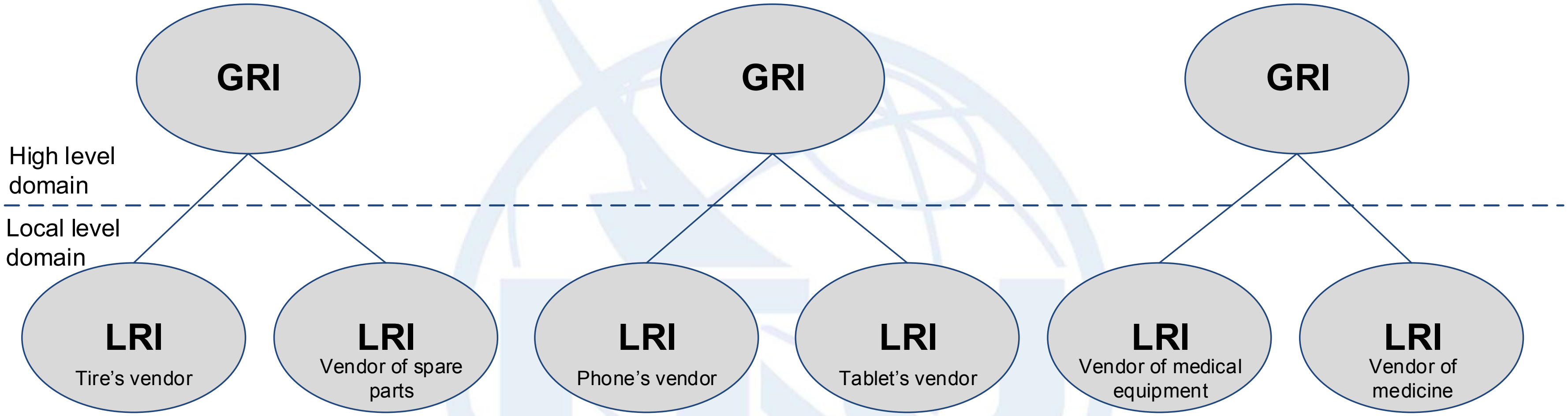
Procedures of verification of product’s identifiers using IoT and DoA concept (2/2)


Authorized service
4. Actions (e.g. limited functionality of the product)
Product
Purchaser
Database of product’s identifiers
3. Product details
Network
1. Checking the hardware identifier
IoT module
2. Checking the product identifier

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.)

Note: detailed info is available in C297R1 (SG 20)
(Source: Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE)

Global identification system based on DOA/IoT

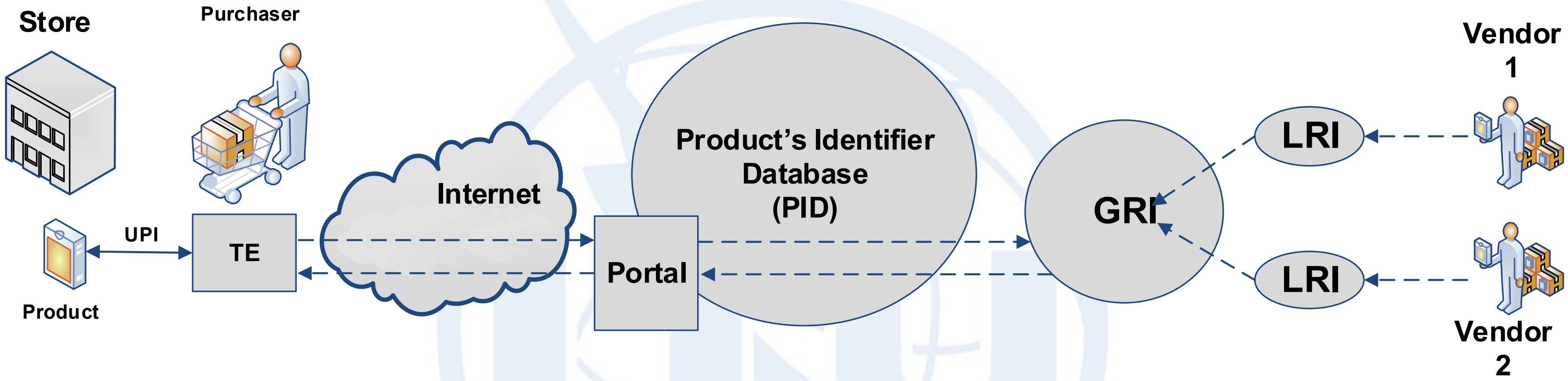


Global Registry of Identifiers (GRI) is located in countries and regions

Local Registry of Identifiers (LRI) is located in vendor's premises

Note: detailed info is available in C297R1 (SG 20)
(Source: Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE)

The architecture of the ICT identification system, aiming to combat counterfeit goods based on DoA/IoT



The detailed architecture was proposed by Russian Federation , Jordan , Rostelecom , Saudi Arabia , SPbSUT , Sudan , Tunisia , UAE at the SG20 meeting in August 2016 (Q.IoT-DOA_counterfeit "IoT-DOA-based systems to be used for combating counterfeiting", *C297R1*)

Conclusions

1. The era of IoT poses new challenges in terms of the fight against counterfeiting
2. IoT/DoA is secure and universal solution to be used for combating counterfeiting which may be used in different industries (not limited to ICT)
3. The identification procedure is very important from user’s perspective. There is a need to develop ITU-T Recommendations to be used for checking the authenticity of IoT’s ID

Alexey Borodin

Representative of Rostelecom in Geneva

E-mail: alexey.borodin@rt.ru