SPbSUT

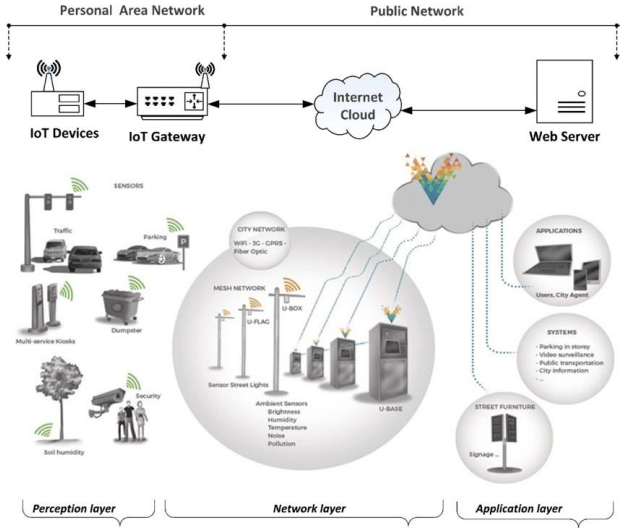
# Seamless connectivity for the IoT devices in Smart Cities

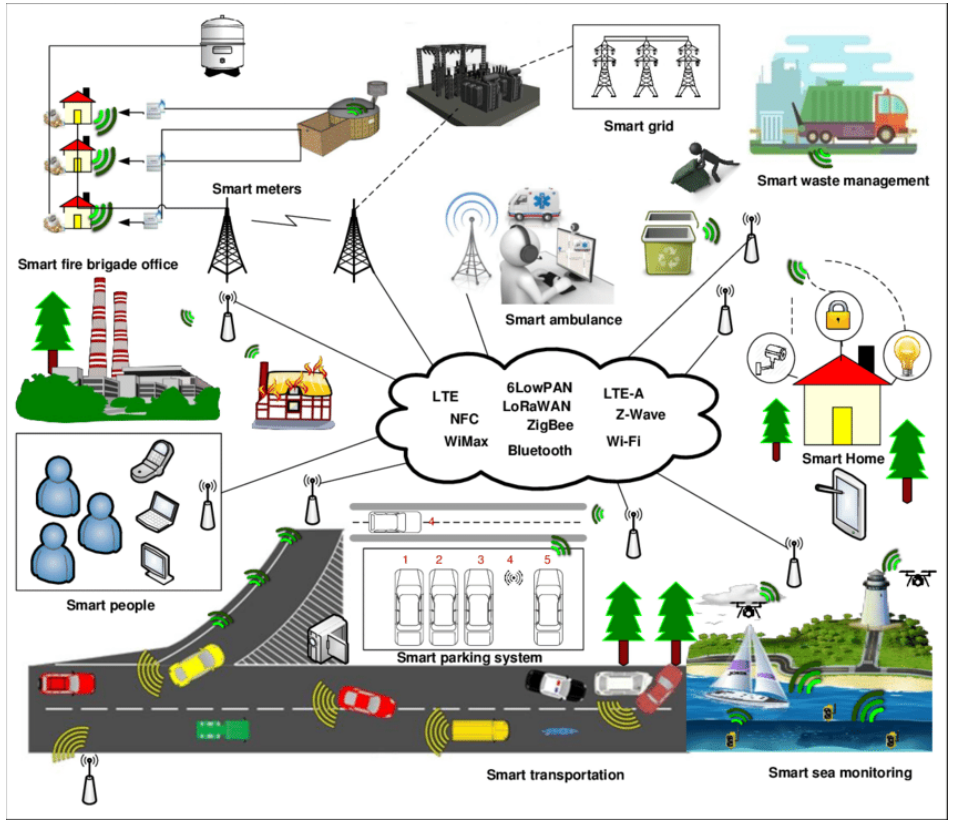
Ruslan Kirichek,
State University of Telecommunication (St.Petersburg, Russia)

# SMART CITY INFRASTRUCTURE FOR IOT DEVICES

SPbSUT

## ITU-T SG20: Internet of Things, smart cities and communities



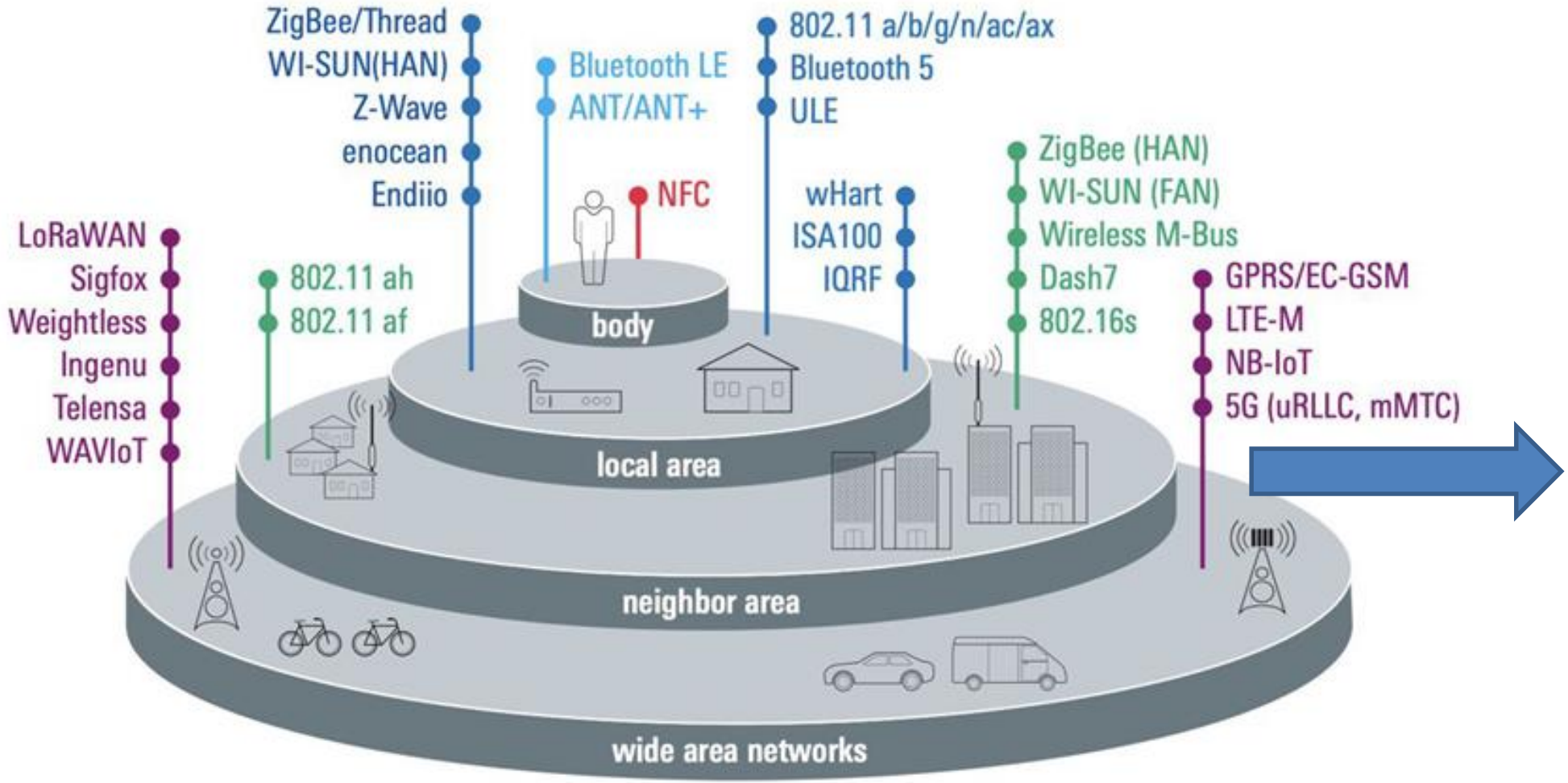




Key features:

- Easy connection of any IoT devices and applications to the Internet (any connection TIME, any connection PLACE, any connection THING)
- Support connecting of any data technology wired and wireless (heterogeneous communication)

# TECHNOLOGIES VERSUS DEPLOYMENT AREAS

SPbSUT





The initial stage of creating Smart Cities - providing full WiFi coverage for connecting IoT devices

# AUTHENTICATION METHODS FOR PUBLIC WIFI

SPbSUT

**OSI Model**

*Layer*

- **Application** — Network Process to Application
- **Presentation** — Data Representation and Encryption
- **Session** — Interhost Communication
- **Transport** — End-to-End Connections and Reliability
- **Network** — Path Determination and IP (Logical Addressing)
- **Data Link** — MAC and LLC (Physical Addressing)
- **Physical** — Media, Signal, and Binary Transmission

WEB – authentication

- SMS authorization
- Login and password
- Call request
- QR-code


How to do it in the scale of Smart Cities

| Authentication method | Encryption method |
|---|---|
| WPA-Personal | TKIP |
| | AES |
| WPA2-Personal | AES |
| OPEN | WEP |
| | NONE (without encryption) |
| Shared key | WEP |

ПРАВИТЕЛЬСТВО РОССИЙСКОЙ ФЕДЕРАЦИИ

ПОСТАНОВЛЕНИЕ

от 31 июля 2014 г. № 758

МОСКВА

О внесении изменений в некоторые акты Правительства Российской Федерации в связи с принятием Федерального закона "О внесении изменений в Федеральный закон "Об информации, информационных технологиях и о защите информации" и отдельные законодательные акты Российской Федерации по вопросам упорядочения обмена информацией с использованием информационно-телекоммуникационных сетей"

A user who connects to a Wi-Fi access point of an network operator cannot do it anonymously and is obliged to give his personal data as first name, last name, number of certifying document, for example, passport, or other identifier. In return, the telecom operator is obliged to identify the terminal equipment providing access to the Internet, for example, by the unique access point number.

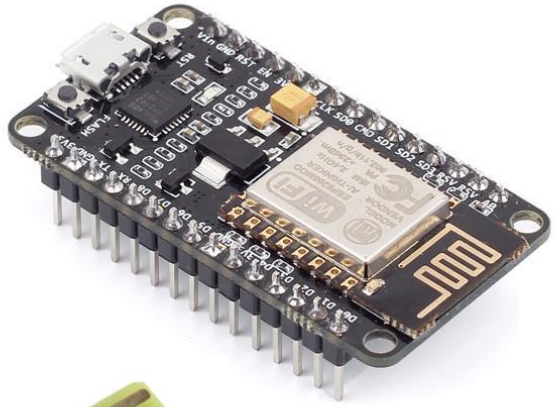
# ELECTRONIC PRODUCT MARKET TREND (CAGR*)


| End Product | CAGR% | Major *Product* Category | PKG Requirement Feature |
|---|---|---|---|
| IoT/Wearable Device | 50.0%/ 51.8% | Connectivity (WiFi, BT, NFC,.. ) MCU/ Memory/ Sensor/ PMIC | • Small Form & Ultra Thin PKG |
| SMART Phone/ Tablet | 12.0%/ 1.3% | AP & BB / LP Memory Connectivity/ PMIC/ Finger Print | • High Bandwidth I/O • Small Form & Thin PKG |
| Networking | 2.7% | ASIC Controller / OI | • High Bandwidth I/O (Large PKG Size) & High Thermal |
| Automotive | 6.8% | Infotainment / Entertainment | • High Reliability & Maturity PKG |

*CAGR - Compound Annual Growth Rate; Source: Gartner, IDC, IEK

# WEARABLE DEVICE CONNECTION PROBLEM IN SMART CITY

SPbSUT



ONLY SUPPORT DATA LAYER AUTHENTICATION FOR WIFI (WPA2, WEP….)

# DIGITAL OBJECT ARCHITECTURE AS BASE FOR IDENTIFICATION IOT DEVICES IN SMART CITY

SPbSUT

- ✓ Digital Object Architecture - an advanced architecture for information management. Can be used for presentation of data on the Internet, identify IoT devices and applications, to detect and deliver information in the form of digital objects using method of two-level resolving.
- ✓ Equal distribution of Global Handle Register.
- ✓ The use of an identifier based on DOA will allow you to take into account all existing unique identifiers (MAC, IMEI, ID, IPv4 / IPv6, etc.), providing end-to-end identification of IoT devices and applications without being tied to a specific identifier.
- ✓ The use of DOA identifiers will enable the implementation of a global and truly international identification system, since it is implemented with the support and participation of ITU.

# MOBILE PHONE IDENTIFICATION FOR EASY CONNECTION TO WIFI ACCESS POINT

SPbSUT

1 Pre-installation of the Application from:
- Google Play
- Apple Store

2


Telecom Operator

INTERNET

Local Handle Registry (LHR)

3

4

Global Handle Registry (GHR)


| Parameter | Value |
|---|---|
| DOA | 10.1525/59.5.9 |
| IMEI | 35-209900-176148-1 |
| MAC | 67-78-89-AB-CD-EF |

1 **Pre-installation of the Application from: Google Play or Apple Store**

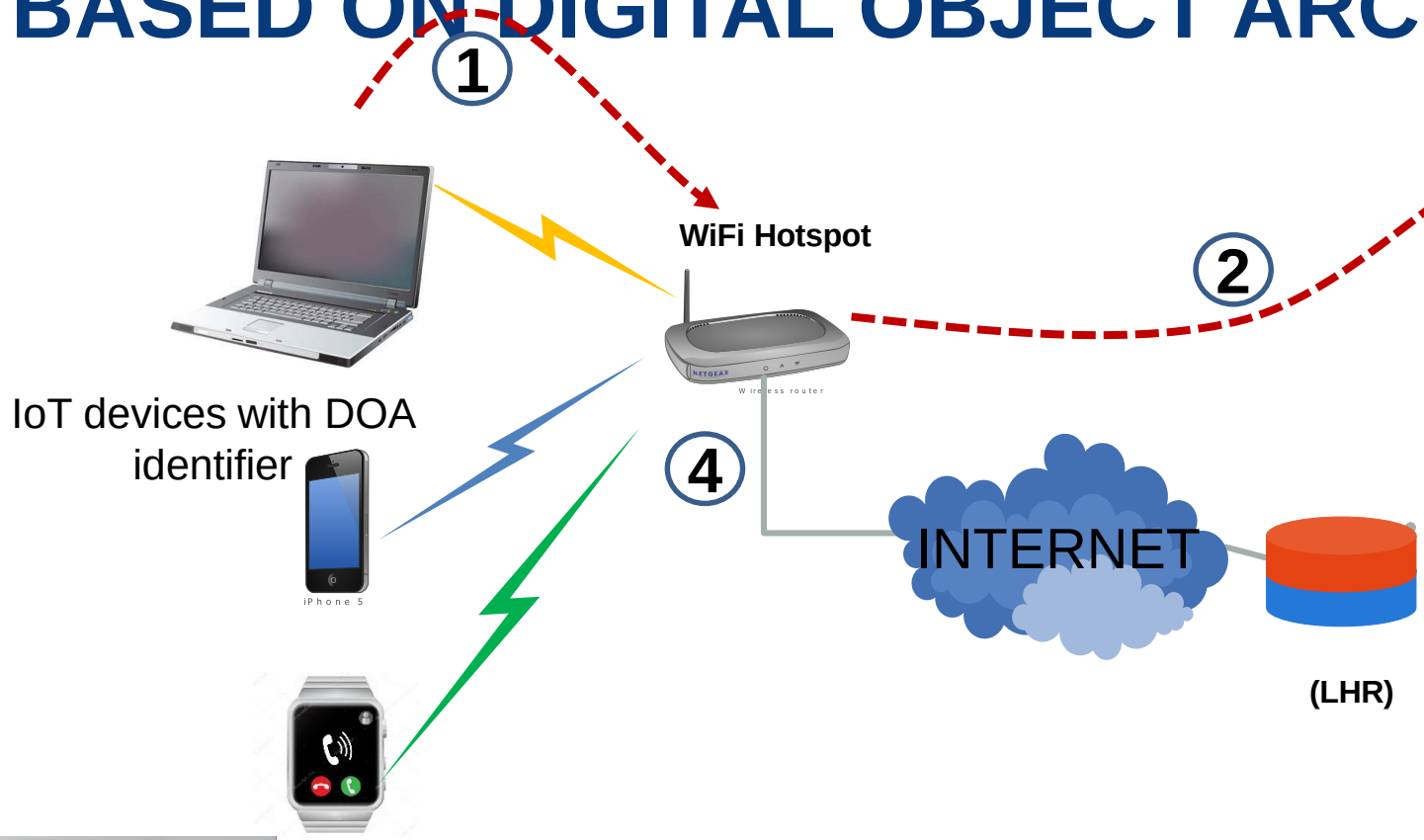
2 **Recording of the DOA identifier in the Application using secure QR code**

3 **Passing values to Handle + unique information to the LHR server (GHR base)**

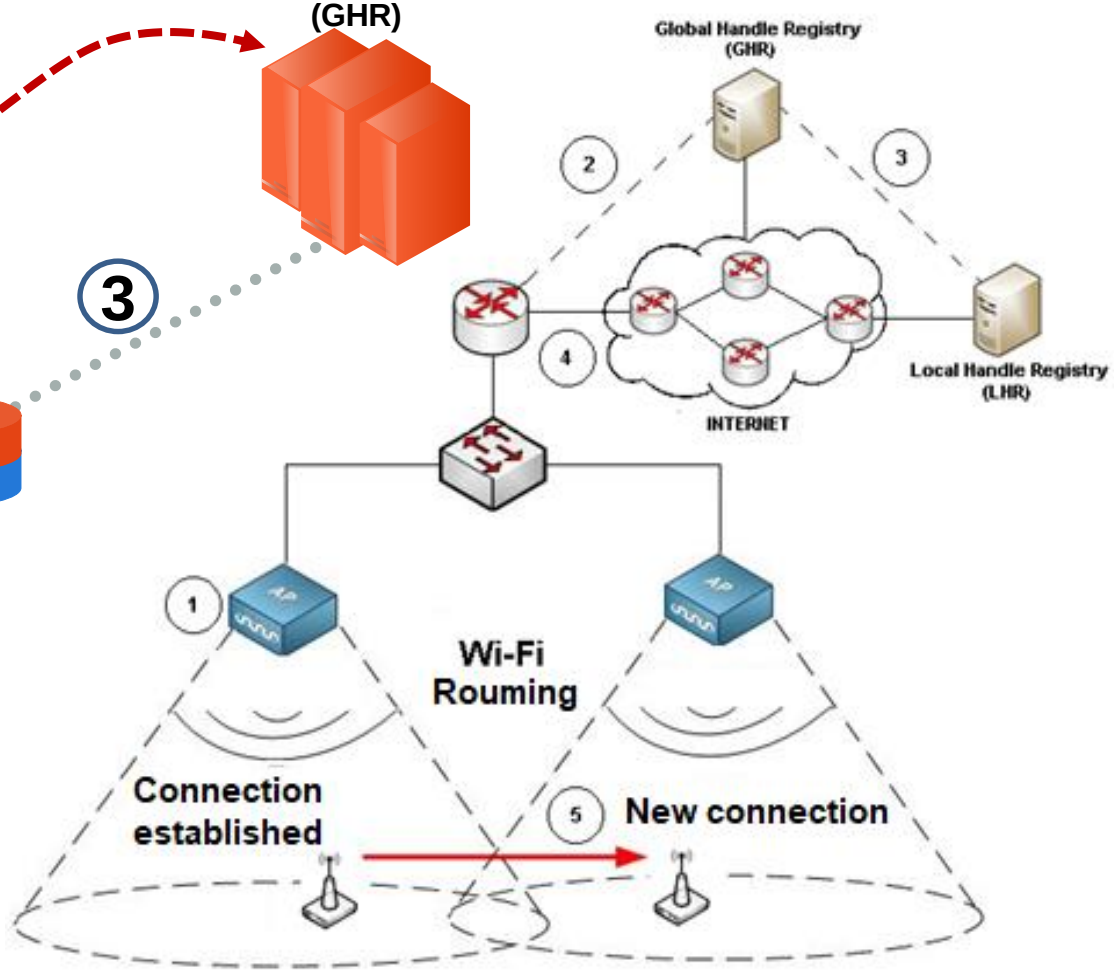
4 **To verify the originality of the mobile phone request is sent to the LHR. After checking the entry in the LHR the response is sent to the mobile phone with verification status**

# SEAMLESS CONNECTIVITY FOR IOT DEVICE BASED ON DIGITAL OBJECT ARCHIECTURE

SPbSUT




- Prototype was present on ITU Workshop "Global approaches on combating counterfeiting and stolen ICT devices" 23 june 2018.
- ITU Regional Forum “Internet of Things, Telecommunication Networks and Big Data as Basic Infrastructure for Digital Economy” 4-6 june 2018.



# CONCLUSION

- The infrastructure of Smart Cities is not ready to connect devices of the Internet of things.
- Simple and cheap IoT devices do not have an interface for web authentication on Application Layer.
- DOA-identification technology can be a universal solution for the unification of services  across the world.
- Identification of IoT devices and applications with DOA based identification will allow to create a seamless connection in Smart Cities.

SPbSUT

# Thank You for your attention !

Ruslan Kirichek
kirichek@sut.ru
+7 921 970 0160
sut.ru, seti.sut.ru, iotlab.ru