International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

Q.4063

(09/2020)

SERIES Q: SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

Testing specifications – Testing specifications for IMT-2020 and IoT

Framework for testing identification systems used in Internet of things

Recommendation ITU-T Q.4063

International Telecommunication Union

ITU-T Q-SERIES RECOMMENDATIONS

SWITCHING AND SIGNALLING, AND ASSOCIATED MEASUREMENTS AND TESTS

SIGNALLING IN THE INTERNATIONAL MANUAL SERVICE	Q.1–Q.3
INTERNATIONAL AUTOMATIC AND SEMI-AUTOMATIC WORKING	Q.4–Q.59
FUNCTIONS AND INFORMATION FLOWS FOR SERVICES IN THE ISDN	Q.60–Q.99
CLAUSES APPLICABLE TO ITU-T STANDARD SYSTEMS	Q.100–Q.119
SPECIFICATIONS OF SIGNALLING SYSTEMS No. 4, 5, 6, R1 AND R2	Q.120–Q.499
DIGITAL EXCHANGES	Q.500–Q.599
INTERWORKING OF SIGNALLING SYSTEMS	Q.600–Q.699
SPECIFICATIONS OF SIGNALLING SYSTEM No. 7	Q.700–Q.799
Q3 INTERFACE	Q.800–Q.849
DIGITAL SUBSCRIBER SIGNALLING SYSTEM No. 1	Q.850–Q.999
PUBLIC LAND MOBILE NETWORK	Q.1000–Q.1099
INTERWORKING WITH SATELLITE MOBILE SYSTEMS	Q.1100–Q.1199
INTELLIGENT NETWORK	Q.1200–Q.1699
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2000	Q.1700–Q.1799
SPECIFICATIONS OF SIGNALLING RELATED TO BEARER INDEPENDENT CALL CONTROL (BICC)	Q.1900–Q.1999
BROADBAND ISDN	Q.2000–Q.2999
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR THE NGN	Q.3000–Q.3709
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR SDN	Q.3710–Q.3899
TESTING SPECIFICATIONS	Q.3900–Q.4099
Testing specifications for next generation networks	Q.3900–Q.3999
Testing specifications for SIP-IMS	Q.4000–Q.4039
Testing specifications for Cloud computing	Q.4040–Q.4059
Testing specifications for IMT-2020 and IoT	**Q.4060–Q.4099**
PROTOCOLS AND SIGNALLING FOR P2P COMMUNICATIONS	Q.4100–Q.4139
SIGNALLING REQUIREMENTS AND PROTOCOLS FOR IMT-2020	Q.5000–Q.5049
COMBATING COUNTERFEITING AND STOLEN ICT DEVICES	Q.5050–Q.5069

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

Recommendation ITU-T Q.4063

Framework for testing identification systems used in Internet of things

Summary

The concept of the Internet of things (IoT), defined in Recommendation ITU-T Y.4000/Y.2060, plays an important role for telecommunication and information technologies. It has been forecasted that the number of devices in the Internet of things will be in the order of hundreds of billions pieces in the foreseeable future, and that the number will later will grow to trillions of devices. It is essential that most customers of telecommunication networks are IoT-based devices in the near future. In other words, all objects that surround us might become IoT objects. In accordance with Recommendation ITU-T Y.4050/Y.2069, the IoT are things with a network address and with the ability to integrate it. The penetration of IoT devices is going very fast, and therefore it requires the standardization of identification procedures and relevant testing methods.

Also, bearing in mind that there are many applications of Internet of things, testing their identity might be considered as a very important issue as it allows customers to ensure the authenticity of the IoT.

Recommendation ITU-T Q.4063 also addresses the classification of IoT, in terms of testing the identification systems and the relevant testing approaches.

History

Edition	Recommendation	Approval	Study Group	Unique ID*
1.0	ITU-T Q.4063	2020-09-29	11	11.1002/1000/14391

Keywords

Identification procedures, IoT, testing.

* 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/.

© ITU 2020

All rights reserved. No part of this publication may be reproduced, by any means whatsoever, without the prior written permission of ITU.

Table of Contents

Recommendation ITU-T Q.4063

Framework for testing identification systems used in Internet of things

1 Scope

The Recommendation provides approaches for the identification of devices used in Internet of Things (IoT). There are many applications of IoT, and the testing of their identity might be considered as it allows customers to ensure the authenticity of the IoT. The classification of IoT, in terms of testing of their identification procedures and the relevant testing procedures are also subjects of this Recommendation.

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.

None.

3 Definitions

3.1 Terms defined elsewhere

This Recommendation uses the following term 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.

3.2 Terms defined in this Recommendation

None.

4 Abbreviations and acronyms

This Recommendation uses the following abbreviations and acronyms:

6LoWPAN	IPv6 Over Low power Wireless Personal Area Networks
ADC	Analogue-to-Digital Converter
ANT+	Adaptive Network Topology Plus
BLE	Bluetooth Low Energy
DOI	Digital Object Identifier
GeoIP	Geolocation by Internet protocol
GPIO	General-Purpose Input/Output
GPS	Global Positioning System
ICT	Information and Communication Technology

ID	Identification
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IrDA	The Infrared Data Association
LoRa	Long Range
LPWAN	Low-Power Wide-Area Network
MAC	Medium Access Control
MCU	Microcontroller
MPU	Microprocessor
NB-IoT	Narrow Band Internet of Things
NFC	Near-Field Communications
PC	Personal Computer
PDU	Protocol Data Unit
PKI	Public Key Infrastructure
RFID	Radio Frequency Identification
RSSI	Received Signal Strength Indicator
SAW	Surface Acoustic Wave
SPI	Serial Peripheral Interface
TAP	Terminal Access Point
TCP	Transmission Control Protocol
TID	Terminal Identification Number
Tx power	Transmit Power
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
UUID	Universally Unique Identifier
UWB	Ultra-Wide Band
Wi-Fi	Wireless Fidelity
WLAN	Wireless Local Area Network

5 Conventions

None.

6 Approaches for testing of IoT identification

Various IoT identification elements can be used for IoT authentication. These can include: various network interface identifiers (MAC); device identifiers (international mobile equipment identity (IMEI), terminal identification number (TID) for radio frequency identification (RFID), etc.);

network identifiers ((Internet protocol version 4 (IPv4), Internet protocol version 6 (IPv6), etc.); IoT network port number (User Datagram protocol (UDP) and Transmission Control protocol (TCP) ports); high-level device identifiers (uniform resource identifier (URI), OpenID, digital object identifier (DOI), OAuth, etc.); manufacturer device identifiers; manufacturer; place of production; date and time of manufacture; list of suppliers; transport company identifier; global positioning system (GPS) coordinates; geolocation by Internet protocol (GeoIP) devices; information on the manufacturing enterprise, etc.

Information on an object's current geographical location (GeoIP, GPS coordinates, etc.) enables one to define the object's current location and compare it with its previous location, and this in turn enables one, with the aid of available identification data and machine learning algorithms in current use, to determine if the IoT device has been compromised.

7 Structure of testing identification systems used in IoT

A structural diagram of the organization of testing, which can be applied to various identification technologies, taking into account their specifics is shown on Figure 7-1.

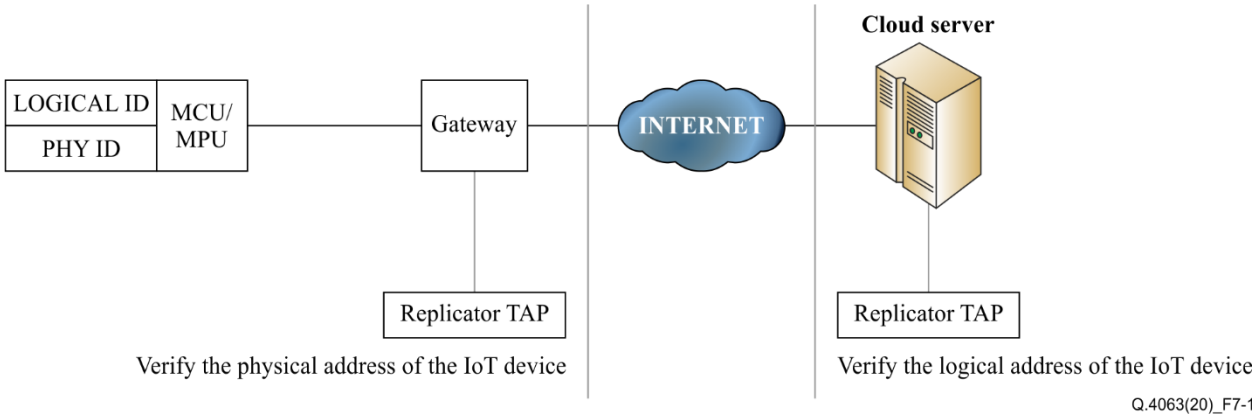

Figure 7-1 – An identification system testing used in IoT

All IoT devices consist of a physical and logical identifier that allows to identify the device on the network.

For testing of physical and logical IoT devices identifiers, the following sequence can be followed:

1) Connect a monitoring terminal access point (TAP)/replicator to the gateway;
2) Send a request to the gateway port to which the IoT device is connected;
3) Reduce the received parameters of the physical identifier and the parameters of the identifier on the IoT device (example: from the box, OS, etc.);

A similar procedure can be used to verify the logical identifier.

An IoT server might be under test as well as an IoT device. The aim of such testing is to assess the reaction of the server to the changes of the identifier of the IoT device. The server has to determine the change, and initiate the procedure of authentication for such device.

8 Classification of the IoT devices for the purpose of testing their identification procedures

Classification of the IoT devices in terms of identification procedures may be carried out according to the computing power of the IoT device(s).

According to the computing power IoT devices can divided:

− on basis of microprocessor (MPU);
− on the basis of microcontroller (MCU);
− on the basis of microchip (RFID, NFC tag);
− other without the use of the analogue-to-digital converter, ADC (surface acoustic wave, SAW).

Classification of the IoT devices in terms of identification procedures may be carried out according to the wireless technology interfaces of the IoT devices that are embedded in the host system.

According to the wireless technology interfaces, IoT devices can divided into:

– RFID
– Near field communication
– Bluetooth/ Bluetooth low energy (BLE)
– IEEE 802.15.4 (ZigBee/6LoWPAN/Therad)
– Low-power wide-area network (LPWAN) (long range (LoRa), Sigfox)
– Wireless local area network (WLAN)/ wireless fidelity (Wi-Fi)
– Cellular
– Infrared (IrDA)
– ultra-wide band (UWB)
– Z-wave
– Enocean
– DASH7
– NB-IoT
– Ultrasound
– wirelessHART
– Other

9 Testing procedures

9.1 Testing procedures for the identification of IoT devices based on microcontroller

The model of IoT devices based on microcontroller is usually used in information and communication technology (ICT) equipment (e.g., smart phones, tablets, PCs, etc.), consumer electronics, etc.

IoTs devices are based on a microcontroller. Such IoT devices are present in the network most of the life cycle and do not depend on the presence or absence of the IoT's reader. Therefore, testing and identification of the IoT devices based on microcontroller may be performed remotely on an occasional basis.

In general, the identification procedure of such IoT devices is complex and, as a rule, based on sophisticated methods that require a significant size of memory and a microcontroller's computation power. However, the digital signature and digital watermark are innovative and effective methods for ensuring the authenticity of such IoT devices. Also, a unique traffic profile of an IoT device might be used as an additional option for IoT device identification procedures.

9.2 Testing procedures for identification of IoT devices based on microprocessor

As already mentioned, it is possible to use a digital signature algorithm to verify identifiers from IoT devices. Not only an identifier can be authenticated with a digital signature, as well as complex meta-

information on the device, which contains the identifier and other data for identifying the device. This testing procedure requires additional computing resources. It is advisable to apply this method for IoT devices based on a microprocessor. The basic scheme of working with a digital signature is shown in Figure 9-1.

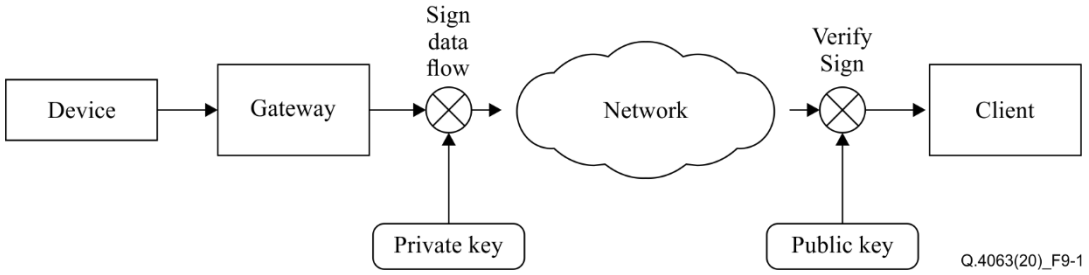

Figure 9-1 – Using digital signature

For digital signing it is possible to use different approaches such as asymmetric algorithms (based on public/private keys) and symmetric algorithms. It is also possible to use the public key infrastructure (PKI) infrastructure.

9.3 Testing procedure for the identification of IoT devices based on BLE

In the case of BLE beacon based IoT devices, devices are connectionless and broadcast their signals periodically. In this mechanism, no device pairing is required to receive the signals advertised by the beacon. The advertising signals generally contain a small data payload (generally known as an advertising protocol data unit (PDU)) which may include the packet header, MAC address, universally unique identifier (UUID), Tx power and a small headroom for manufacturer-specific data. The identification can be done using UUID that acts as the ID/passport of these devices. Authentication is done by the cloud IoT server to which these BLE devices are sending the data.

Received signal strength indicator (RSSI) received by the beacon reader/smart device from these BLE devices can be used for determining geo-location of the IoT device.

The testing of the IoT based on BLE beacon devices can be performed both locally and remotely. Figure 9-2 shows a block diagram for the testing of the BLE beacon based IoT.

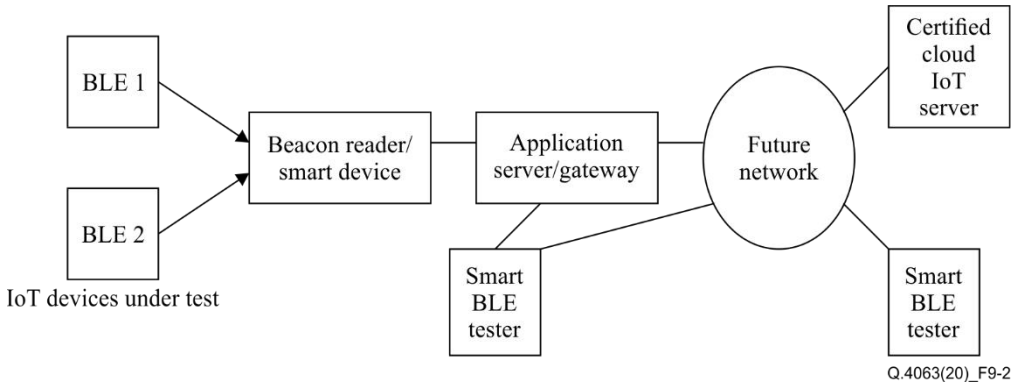

Figure 9-2 – Block diagram of Identification of testing of the BLE beacon based IoT device

The smart BLE tester receives the PDU and extracts the MAC address and UUID of the BLE beacon device. The BLE tester requests the UUID by sending a MAC address to a certified cloud IoT server. The cloud IoT server extracts UUID mapped to that MAC address and sends this information to the testing device.

The testing device compares the received UUID from the BLE device under test with the UUID held on the authentication server.

The current geographical position of the BLE beacon device can be authenticated using RSSI received by server and location of the beacon reader/gateway.

Appendix I

Main characteristics of the various communication and identification technologies used in IoT devices

(This appendix does not form an integral part of this Recommendation.)

Table I.1 – Main characteristics of the various communication and identification technologies used in IoT devices

Technology	Frequency band	Maximum range	Data rate	Power/Main features
ANT+	2.4 GHz	30 m	20 kbit/s	Ultra-low power, up to 65,533 nodes
Bluetooth 5 LE	2.4 GHz	< 400m	1360 kbit/s	Low power and rechargeable (days to weeks)
DASH7/ISO 18000	315-915 MHz	< 10km	27.8 kbit/s	Very low power, alkaline batteries last months to years
HF RFID	3-30 MHz (13.56 MHz)	a few meters	< 640 kbit/s	NLOS, low cost
Infrared (IrDA)	300 GHz to 430 THz	a few meters	2.4 kbit/s-1 Gbit/s	Security, high-speed
LF RFID	30-300 kHz (125 kHz)	< 10 cm	< 640 kbit/s	NLOS, durability, low cost
NB-IoT,	LTE in-band guard-band	< 35km	< 250 kbit/s	Low power and wide area
NFC	13.56MHz	< 20 cm	424 kbit/s	Low cost, no power
LoRa	433 MHz 868 MHz 915 MHz	kilometres	0.25-50 kbit/s	Long battery life and range
SigFox	868-902 MHz	50 km	100 kbit/s	Global cellular network
UHF NLOS,	30 MHz-3GHz	RFID tens of meters	< 640 kbit/s	durability, low cost
Ultrasound	> 20 kHz (2-10 MHz)	< 10 m	250 kbit/s	Based on sound wave propagation
UWB/IEEE 802.15.3a	3.1 to 10.6 GHz	< 10m	> 110 Mbit/s	Low power, rechargeable (hours to days)
Weightless-P	License-exempt sub-GHz	15 km	100 kbit/s	Low power
Wi-Fi (IEEE 802.11b/g/n/ac	2.4-5 GHz	< 150 m	up to 433 Mbit/s (one stream)	High power, rechargeable (hours)
Wi-Fi HaLow/IEEE 802.11ah	868-915 MHz	< 1 km	100 kbit/s	per channel Low power
WirelessHART	2.4 GHz	< 10 m	250 kbit/s	HART protocol

Table I.1 – Main characteristics of the various communication and identification technologies used in IoT devices

Technology	Frequency band	Maximum range	Data rate	Power/Main features
Wi-Sun/IEEE 802.15.4g	< 2.4 GHz	1000 m	50 kbit/s-1 Mbit/s	Field area networking, Home area networking
EnOcean	868-915 MHz	300 m	120 kbit/s	Up to 2^32 nodes
RuBee	131 kHz	30 m	8 kbit/s	Magnetic propagation
Zigbee	868-915 MHz 2.4 GHz	< 100 m	20-250 kbit/s	Very low power
Z-wave	868-915 MHz	100 m	40 kbit/s	Very low power, up to 232 nodes

Appendix II

Testing of the identification method based on the degraded flash memory on IoT device

(This appendix does not form an integral part of this Recommendation.)

To test the identification method based on the degraded flash memory, it is convenient to use NOR flash memory chips with a serial peripheral interface (SPI) interface in a SO-8 or DIP-8 package. Such chips are used in most network devices. NOR-flash chips use a unified system of control commands (instructions) with minimal differences depending on the chip manufacturer. The commands for controlling a particular memory chip are listed in the datasheet.

For testing, it is convenient to use a testbed based on the Raspberry Pi microcomputer (or similar), which contains an embedded SPI interface. A standard scheme of SPI programmer should be connected to the microcomputer's general-purpose input/output (GPIO) connectors (Figure II.1).

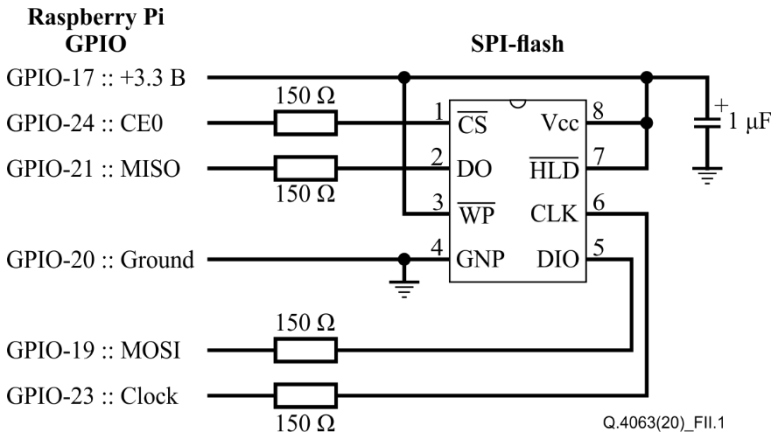

Figure II.1 – Scheme of the RaspberryPi based testbed

To work with the memory chip on PaspberryPi and compatible devices, open-source software pi-spiflash[1] is written in Python using the py-spidev module, which defines functions for working with the Linux kernel spidev driver, which provides low-level mechanisms for working with the SPI interface.

The second version of the testbed bases on a CH341a programmer, connected to a personal computer running GNU/Linux. To test the NOR flash, the open source software ch341prog-extended[2] is written. This software provides the possibility of parallel operation with a large number of CH341a programmers on one computer.

1 https://github.com/vlad-ss/pi-spiflash

2 https://github.com/YAost/ch341prog-extended

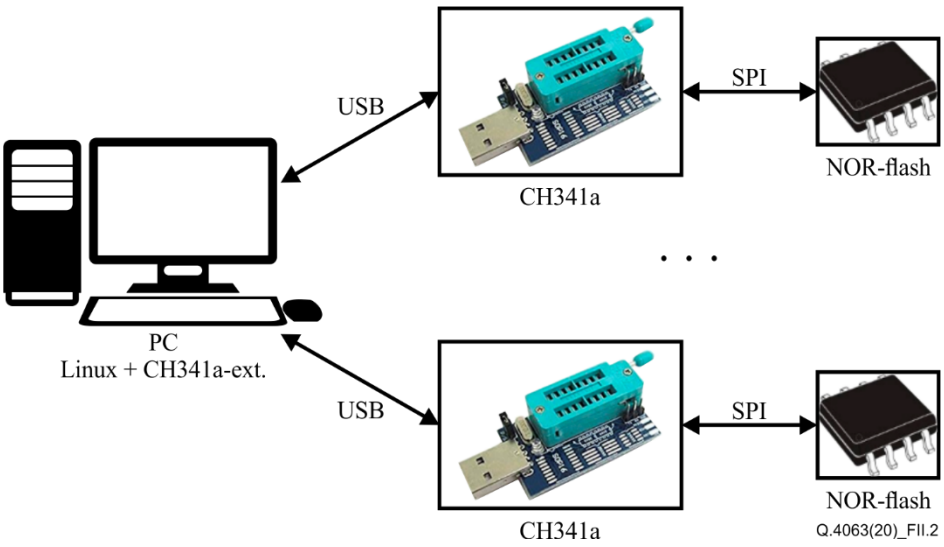

Figure II.2 – Scheme of the CH341a based testbed

Both versions of testbed perform the following algorithm:

1) Cyclic rewriting of one sector of a flash memory chip until stable appearance of bad-cells (before sector degradation).
2) Preservation of the image (pattern of bad-cells) of the degraded sector of the flash memory chip.
3) Comparison of the sector of the flash memory chip connected to the experimental setup with saved images and identification of the chip using the maximum likelihood method.

Cyclic rewriting is performed by erasing the flash memory sector with the command and then writing the sector page-by-page with an array of zeros, which ensures the equiprobability of potential degradation of the sector memory cells.

As soon as bad-cells (non-erasable memory cells that always contain a zero value) appear in the rewritten memory sector, such a sector can be considered degraded. To use such a sector as an identifier, it is desirable to get several dozen bad-cells.

The image (bad-cell's pattern) of the degraded sector, which serves as an identifier, must be saved in the database of identifiers.

In order to verify the correctness of the memory chip identification, it must be connected to a testbed and the sector used for identification must be erased. After that, the contents of the sector are read and compared bit by bit with each identifier in the database of identifiers. According to the results of the comparison by the maximum likelihood method, the identifier corresponds to the checked memory chip. It should be noted that if there are several dozens of bad-cells in the sector, there may be intersections with other identifiers in the database, but the number of such intersections will be much less than when compared with the identifier corresponding to the chip. In the experiments, the correspondence of the contents of the erased sector of the chip coincided with its identifier stored in the database by more than 98% of the total number of bad-cells contained in it, while the coincidence with other identifiers (sector images) was less than 1-2%.

Bibliography

[b-ITU-T Y.4000] Recommendation ITU-T Y.4000/Y.2060 (2012), *Overview of the Internet of things.*

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

[b-IETF RFC 2460] Internet Protocol, Version 6 (IPv6), Specification. https://www.rfc-editor.org/rfc/pdfrfc/rfc2460.txt.pdf

[b-BLE LS] Ke, Chih-Kun & Wu, MeiYu & Chan, YuWei & Lu, KeCheng. (2018), *Developing a BLE Beacon-Based Location System Using Location Fingerprint Positioning for Smart Home Power Management*. Energies. 11.3464.10.3390/en11123464.

[b-IoT Testing] Internet Of Things (IoT) Testing, Challenges, Tools and Testing Approach. https://www.softwaretestinghelp.com/internet-of-things-iot-testing/

[b-Notif] Ministry of Communications and Information Technology (Department of Telecommunications), Notification. https://dot.gov.in/sites/default/files/2016_04_11%20GAZ-AS-III.pdf?download=1 (Referenced 22.04.2016)

[b-TR CT] Technical Report, Communication Technologies in M2M/IoT Domain. http://tec.gov.in/pdf/M2M/Communication%20Technologies%20in%20IoT%20domain.pdf (Referenced 07.2017)

[b-TR Sec] Technical Report, Recommendations for IoT/M2M Security. https://www.tec.gov.in/pdf/M2M/TECHNICAL%20REPORT%20Recommendations%20for%20Iot%20M2M%20Security.pdf (Referenced 01.2019)

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