TEST REPORT
PPP 17003A:2020
TÜV SÜD Test Report for IoT Consumer products – Cybersecurity – US market

Report No.: Date of issue: Project handler:	6818922001601 2022-03-14 Tommy Zheng
Testing laboratory: Address: Testing location:	TÜV SÜD Certification and Testing (China) Co., Ltd. Shenzhen Branch Building 12 & 13, Zhiheng Wisdomland Business Park, Guankou Erlu, Nantou, Nanshan District Shenzhen 518052, P.R. China. as above
Client: Client number: Address: Contact person:	Hangzhou Tuya Information Technology Co., Ltd 104731 Room701, Building3, More Center, No.87 GuDun Road 310000 Hangzhou, People's Republic of China Eaton Wang
Standard:	This TÜV SÜD test report form is based on the following requirements: PPP 17003A: 2020 rev. 0: 2020 *Evaluation method:* *TÜV SÜD Testing Guidelines for NISTIR 8259 V2:2021-03* *Based on:* *NISTIR 8259:2020-05 (Manufacturer Activities)* *NISTIR 8259A:2020-05 (Technical Core Baseline of Cybersecurity Capability)*
TRF number and revision:	TRF PPP 17003A:2020 rev. 0:2020
eDoc_ID:	—
TRF originated by:	TÜV SÜD Product Service, Mr. Roland Fiat
Copyright blank test report:	This test report is based on the content of the standard (see above). The test report considered selected clauses of the a.m. standard(s) and experience gained with product testing. It was prepared by TÜV SÜD Product Service. TÜV SÜD Group takes no responsibility for and will not assume liability for damages resulting from the reader's interpretation of the reproduced material due to its placement and context.
General disclaimer:	This test report may only be quoted in full. Any use for advertising purposes must be granted in writing. This report is the result of a single examination of the object in question and is not generally applicable evaluation of the quality of other products in regular production.
Scheme:	☐ TÜV Mark ☒ without certification ☐ other:
Non-standard test method: National deviations:	☒ No ☐ Yes, see details under Summary of testing N/A
Number of pages *(Report)*: Number of pages *(Attachments)*:	11 1 pages for Attachment No.1

Compiled by: (+ signature)	Tommy Zheng Tommy Zheng	Approved by: (+ signature)	Stone Zhong Stone Zhong

Test sample: Type of test object: Trademark: Model and/ or type reference:	Mass Production Sample **Wi-Fi Module** CBU, CBU-IPEX
Rating(s):	3.0V to 3.6V
Manufacturer: Manufacturer number: Address:	Hangzhou Tuya Information Technology Co., Ltd 104731 Room701, Building3, More Center, No.87 GuDun Road,310000 Hangzhou, People's Republic of China
Name and address of factory(ies) N/A	
Sub-contractors / tests (clause):	N/A
Name:	N/A
Order description:	☐ Complete test according to TRF ☒ Partial test according to manufacturer's specifications ☐ Preliminary test ☐ Spot check ☐ Others:
Date of order: Date of receipt of test item: Date(s) of performance of test:	2022-01-25 2022-01-27 2022-02-10 ~ 2022-03-03
Test item particulars:	
Firmware version: PCB Version: Device Operating System: Hardware Interfaces: Network Protocols: External Sensors: Other Features:	Firmware version: V1.3.20 App version (Android): TuyaSmart 3.33.1 App version (iOS): TuyaSmart 3.33.1 PCB version: V1.0.1 FreeRTOS V7.5.2 Wi-Fi (802.11 b/g/n), Bluetooth 5.2 (Low Energy) MQTT over HTTPS (MQTT version: 3.1 TLS version: 1.2) / Tuya proprietary protocol on BLE None None

Purpose of the product (description of intended use):

A general wireless communication module that could be integrated to traditional electrical products making it connectable.
CBU, CBU-IPEX are identical in electrical circuit design, layout and components, except the antenna connector.

Characteristic data (not shown on the marking plate):

N/A

Attachments:

Attachment No.1:

Photo document of the Item Tested.

If additional information is necessary, please provide

N/A

Copy of marking plate:

Marking plate on the left: CBU
Marking plate on the right: CBU-IPEX

Pictures of the product:

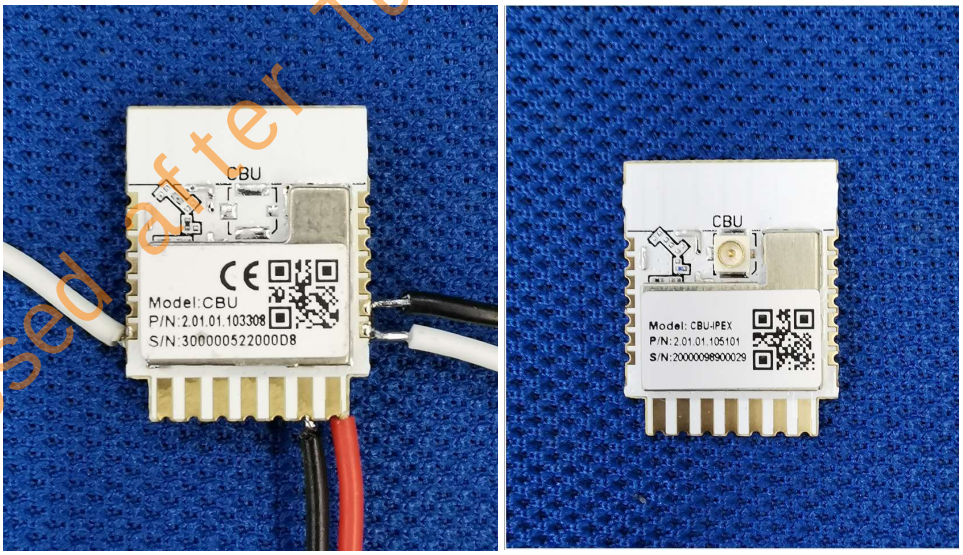


Photo on the left: CBU
Photo on the right: CBU-IPEX

Summary of testing:

Test was performed according to TÜV SÜD_PPP 17003A:2020.

Testing was conducted only on Activity 3 of PPP17003A, which is a customized testing.

The submitted samples were found to comply with the above specification.

☐ deviation(s) found

☒ no deviations found

Additional information on non-standard test method(s)

Sub clause:	N/A
Page:	N/A
Rational:	N/A

Possible test case verdicts:

test case does not apply to the test object:	N/A (not applicable)
test object does meet the criteria at testing guideline:	P (Pass)
test object does not meet the criteria at testing guideline:	F (Fail)
test cases are not tested according to customer customization requirements	/

General remarks:

"(see remark #)" refers to a remark appended to the report.
"(see appended table)" refers to a table appended to the report.
Throughout this report ***a comma*** *is used as the decimal separator.*
The test results presented in this report relate only to the object tested.
This report shall not be reproduced except in full without the written approval of the testing laboratory.

Clause	Requirement + Test	Result – Remark	Verdict
TÜV SÜD Testing Guidelines for NISTIR 8259: 2021-05-18			
3	**This Testing Guidelines evaluate on the tests with reference to NISTIR 8259 Foundational Cybersecurity Activities for IoT Device Manufacturers published in May 2020. It also uses NISTIR 8259A referenced in NISTIR 8259's activity 3 of Manufacturer Activities Impacting the IoT Device Pre-Market Phase**		/
3.1	**Activity 1: Identify Expected Customers and Define Expected Use Cases**		/
3.1.1	Types of people who are expected customers for this device		/
3.1.2	Types of organizations which are expected customers for this device		/
3.1.3	Usage of the device		/
3.1.4	Geographical locations for device use		/
3.1.5	Physical environments for device use		/
3.1.6	Expected time for device use		/
3.1.7	Dependencies on other systems the device will likely have		/
3.1.8	Potential threats and vulnerabilities how attackers might misuse and compromise the device		/
3.1.9	Other aspects of device use that might be relevant to the device's cybersecurity risks		/
3.2	**Activity 2: Research Customer Cybersecurity Needs and Goals**		/
3.2.1	The potential impact of the IoT device's interaction with the physical world		/
3.2.2	The methods likely to be used by IoT device that need to be accessed, managed, and monitored by authorized people, processes, and other devices:		/
3.2.3	Known cybersecurity requirements for the IoT device		/
3.2.4	Potential interference of the device's operational or environmental characteristics with the device's cybersecurity capabilities		/
3.2.5	Nature of the IoT device's data		/
3.2.6	Degree of trust in the IoT device that customers may need		/

Clause	Requirement + Test	Result – Remark	Verdict
3.2.7	Complexities that will be introduced by the IoT device interacting with other devices, systems, and environments		/
3.3	**Activity 3: Determine How to Address Customer Needs and Goals**		**P**
3.3.1	**Device Identification**		**P**
3.3.1.1	A unique logical identifier	The DUT's logical identifier fits the description provided by vendor.	P
3.3.1.2	A unique physical identifier at an external or internal location on the device authorized entities can access	Information about the physical identifier generation method is provided and is valid.	P
3.3.2	**Device Configuration**		**P**
3.3.2.1	The ability to change the device's software configuration settings	The provided listed configuration settings matches the configuration settings of the DUT.	P
3.3.2.2	The ability to restrict configuration changes to authorized entities only	The DUT only accepts configuration changes by authorized entities.Other changes are not permitted.	P
3.3.3	**Data Protection**		**P**
3.3.3.1	The ability to use demonstrably secure cryptographic modules for standardized cryptographic algorithms (e.g., encryption with authentication, cryptographic hashes, digital signature validation) to prevent the confidentiality and integrity of the device's stored and transmitted data from being compromised	Confidential data and information is protected using strong implementations. Integrity of other data is protected using public known methods.	P
3.3.4	**Logical Access to Interfaces**		**P**
3.3.4.1	The ability to logically restrict access to each network interface to only authorized entities (e.g., device authentication, user authentication) .	Access restriction is in place to protect network interface and it cannot be bypassed.	P
3.3.5	**Software Update**		**P**
3.3.5.1	The ability to update the device's software through remote (e.g., network download) and/or local means (e.g., removable media)	Frimware in device are updatable(OTA)	P
3.3.5.2	The ability to verify and authenticate any update before installing it	Device will verify the integrity and authenticity of the firmware and it will rejects the unauthorizated update.	P
3.3.5.3	The ability to restrict updating actions to authorized entities only	Device only accepts the update with the authorized user.	P
3.3.5.4	Test of configurability of update mechanism, but without any	TL has confirmed the availability of automatic/manual configuration setting.	P

Clause	Requirement + Test	Result – Remark	Verdict
	mandatory requirements about what shall be configurable		
3.3.6	**Cybersecurity State Awareness**		**P**
3.3.6.1	The ability to report the device's cybersecurity state	Vendor lists the various statuses and provides a report of the triggered statuses.	P
3.3.6.2	The ability to restrict access to the state indicator so only authorized entities can access it	State change only can be accessed by authorized user.	P
3.4	**Activity 4: Plan for Adequate Support of Customer Needs and Goals**		**/**
3.4.1	Considering expected terms of support and lifespan, what potential future use needs to be taken into account?		/
3.4.2	An established IoT platform is supposed to be used instead of acquiring and integrating individual hardware and software components.		/
3.4.3	Info about device cybersecurity capabilities being hardware-based		/
3.4.4	Hardware or software (including the operating system) includes unneeded device capabilities with cybersecurity implications. If so, the ability to be disabled to prevent misuse and exploitation.		/
3.4.5	Mechanism that IoT device code protects from unauthorized access and tampering.		/
3.4.6	The mechanism that customers verify hardware or software integrity for the IoT device.		/
3.4.7	Verification mechanism that is done to confirm that the security of third-party software used within the IoT device meets the customers' needs.		/
3.4.8	Mechanisms taken to minimize the vulnerabilities in released IoT device software.		/
3.4.9	Measures taken to accept reports of possible IoT device software vulnerabilities and respond to them.		/
3.4.10	Processes that are in place to assess and prioritize the remediation of all vulnerabilities in IoT device software		/

Clause	Requirement + Test	Result – Remark	Verdict
4	**Manufacturer Activities Impacting the IoT Device Post-Market Phase**		**/**
4.1	**Activity 5: Define Approaches for Communicating to Customers**		**/**
4.1.1	Terminology the customer will understand		/
4.1.2	Information quantity based on customers' need		/
4.1.3	Locations where the information is readily provided		/
4.1.4	Verification on the integrity of the information		/
4.1.5	Functionality, usability and efficacy of the communication channels that customers have to communicate with the manufacturer		/
4.2	**Activity 6: Decide What to Communicate to Customers and How to Communicate It**		**/**
4.2.1	**Cybersecurity Risk-Related Assumptions**		
4.2.1.1	Information on expected customers		/
4.2.1.2	Information on intended usage		/
4.2.1.3	Information on types of environment for device use		/
4.2.1.4	Information on sharing of responsibilities among the manufacturer, the customer, and others		/
4.2.2	**Support and Lifespan Expectations**		/
4.2.2.1	Information on intended support lifespan of the device		/
4.2.2.2	Information on intended schedule plan for device end-of-life notice		/
	Information on the process for end-of-life		/
4.2.2.3	Information on functionality, if any, the device will have after support ends and at end-of-life		/
4.2.2.4	Information on how customers can report suspected problems with cybersecurity implications, such as software vulnerabilities, to the manufacturer		/

Clause	Requirement + Test	Result – Remark	Verdict
	Acceptance of reports after support ends		/
	Acceptance of reports after end-of-life		/
4.2.2.5	Information on process or method provided for customers to maintain securability even after official support for the device has ended		/
	Availability of essential files or data made in a public forum to allow others, even the customers themselves, to continue to support the IoT device		/
4.2.3	**Device Composition and Capabilities**		**/**
4.2.3.1	Information customers need on general cybersecurity-related aspects of the device, including device installation, configuration (including hardening), usage, management, maintenance, and disposal		/
4.2.3.2	Information on potential effect on the device if the cybersecurity configuration is made more restrictive than the default		/
4.2.3.3	Inventory-related information customers need related to the device's internal software, such as versions, patch status, and known vulnerabilities		/
	Policy that customers are able to access the current inventory on demand, if needed		/
4.2.3.4	Information customers need about the sources of the device's software, hardware, and services		/
4.2.3.5	Information customers need on the device's operational characteristics so they can adequately secure the device. How this information is made available.		/
4.2.3.6	Information on functions the device can perform		/
4.2.3.7	Information on data types the device can collect		/
4.2.3.8	Information on the identities of all parties (including the manufacturer) that can access that data		/

Clause	Requirement + Test	Result – Remark	Verdict
4.2.4	**Software Updates**		**/**
4.2.4.1	Availability of updates		/
	If so, details of release schedule		/
4.2.4.2	Circumstances under which updates will be issued		/
4.2.4.3	Information on how updates are made available or delivered		/
	Notifications when updates are available or applied		/
4.2.4.4	Information on entity (e.g. customer, manufacturer, third party) responsible for performing updates		/
	Information on measures for the customer to designate which entity will be responsible		/
4.2.4.5	Information on measures for customers to verify and authenticate updates		/
4.2.4.6	Information that should be communicated with each individual update		/
4.2.5	**Device Retirement Options**		**/**
4.2.5.1	If customers are expected to transfer ownership of their devices to another party, information on what customers need to do so their user and configuration data on the device and associated systems is not accessible by the party who assumes ownership		/
4.2.5.2	If customers are expected to render their devices inoperable, information on how customers can do that		/
4.2.6	**Technical and Non-Technical Means**		**/**
4.2.6.1	Technical means provided a. by the device itself (device cybersecurity capabilities). b. by a related device. c. by a manufacturer service or system.		/
4.2.6.2	Description of non-technical means provided by the manufacturer or other organizations and services acting on behalf of the manufacturer		/

Clause	Requirement + Test	Result – Remark	Verdict
4.2.6.3	Description of technical or non-technical means the customer should provide themselves or consider providing themselves		/
4.2.6.4	Information on technical and non-technical means expected to affect cybersecurity risks		/

END OF TEST REPORT

Attachment No.1

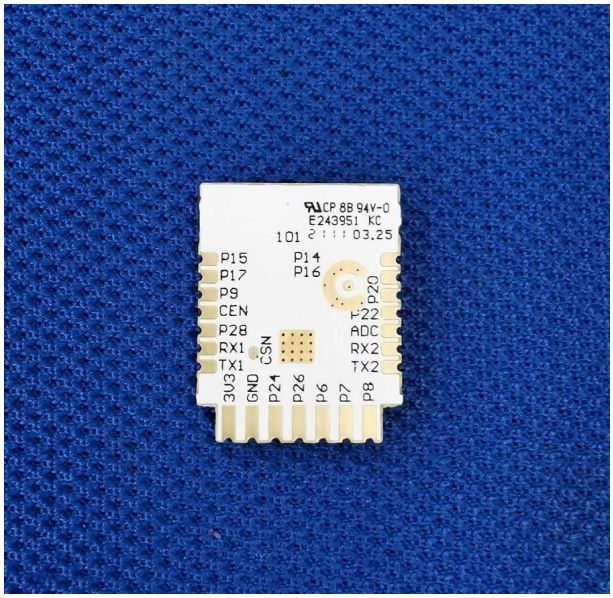
Photo documentation Page 1 of 1 Report No.: 6818922001601

Details of: Wi-Fi and Bluetooth Module

Remark: Model: CBU

Details of: Wi-Fi and Bluetooth Module

Remark: Model: CBU-IPEX



***** END OF REPORT *****