TEST REPORT

PPP 17004A: 2020

TÜV SÜD Test Report for IoT Consumer products – Cybersecurity – European market

Report No.:	874012210514
Date of issue:	2023-03-24
Project handler:	Eason Kin
Testing laboratory:	TÜV SÜD Certification and Testing (China) Co., Ltd. Ningbo Branch
Address:	Building 2, No. 350, Jinghua Road, Essence Adream of Space II, National Hi-Tech Industrial Development Zone, Ningbo, Zhejiang Ningbo 315040 P.R. China
Testing location:	as above
Client:	AISWEI Technology Co.,Ltd.
Client number:	0099567
Address:	Room 905B,757 Mengzi Road, Huangpu District, 200023 Shanghai, P.R, China
Contact person:	Sandy Gong
Standard:	This TÜV SÜD test report form is based on the following requirements: ETSI EN 303 645 V2.1.1:2020-06
TRF number and revision*:*	TRF_ PPP 17004A:2020 rev. 1.1:2021
TRF originated by:	TÜV SÜD Product Service, Mr. Roland Fiat *(senior product specialist)*
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
Non-standard test method:	☒ No ☐ Yes, see details under Summary of testing
National deviations:	N/A
Number of pages *(Report)*:	10
Number of pages *(Attachments)*:	6 pages for Attachment No.1

Compiled by: Eason Kin (+ signature) Eason Kin

Approved by: Johson Li (+ signature) Johson Li

Attachments: Attachment No.1: Photo document of the Item Tested. Considering security of report, we do not attach self-declaration document.	
Test sample: Type of test object: Trademark: Model and/or type reference:	**Pre-production Sample** Information Technology Equipment Communication module  WiFi Stick
Parameters:	Device firmware version: 20A12-012R SoC Chip: ESP32-WROOM-32UE PCB model and version: AISWEI 270-92001-00 Communication interface: Wi-Fi 802.11 App (Android): Solplanet 3.1.0(33) App (iOS): Aiswei&Solplanet 3.1.1(3)
Manufacturer: Manufacturer number: Address:	AISWEI New Energy Technology (Yangzhong) Co.,Ltd. 099678 No.588 Gangxing Road, Economic Development Zone, 212200 Yangzhong City, Jiangsu Province, P.R. CHINA
Sub-contractors/ tests (clause): Name:	N/A 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:	2022-09-01 2022-11-28 2022-11-28~2023-03-14
Test item particulars: **Device features:** - Sensors - Actuators - Human user interfaces - Communication interfaces	 N/A Motor N/A Wi-Fi 802.11

- Local interfaces	USB serial port interface
Software versions:	
- Android IoT app versions	Solplanet 3.1.0(33)
- iOS IoT app versions	Aiswei&Solplanet 3.1.1(3)
- Firmware/software versions	20A12-012R

Purpose of the product (Description of intended use):

This product is used for playing real-time video, and capturing video/screenshots.

Characteristic data *(not shown on the marking plate)*:

This is optional. Only add relevant information here if not in the section "Parameters" above.

None

Copy of the marking plate

Figure 01. Rating label

Picture of the product:

One overview picture of the product. (Detailed pictures in the annexes)

Figure 02. WiFi Stick

Summary of testing:

Tests performed (name of test and test clause):
ETSI EN 303 645 V2.1.1:2020 – all provisions listed in Annex B
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:	None
Page:	N/A
Rationale:	N/A
If additional information is necessary, please provide.	N/A

Possible test case verdicts:	
- test object does meet the requirement:	P (Pass)
- test object does not meet the requirement:	F (Fail)
- test case does not apply to the test object:	N/A (Not applicable)
Possible suffixes to the verdicts:	
- suffix for detailed information for the client:	C (Comment)
- suffix for important information for factory inspection:	M (Manufacturing)

Test Environment

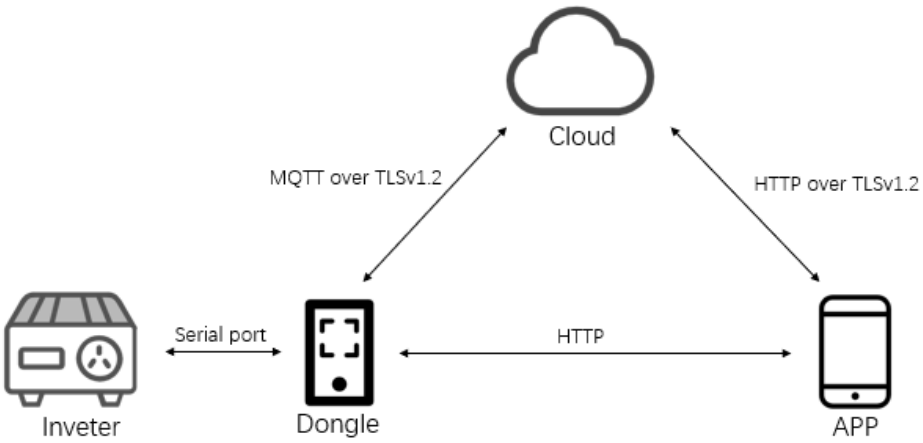


Figure 03. Test environment

Clause	Requirement + Test	Remark	Verdict
4	**Reporting implementation**		/
4-1	(M) A justification shall be recorded for each recommendation in the present document that is considered to be not applicable for or not fulfilled by the consumer IoT device.		P
5	**Cyber security provisions for consumer IoT**		/
5.1	**No universal default passwords**		/
5.1-1	(MC) Where passwords are used and, in any state, other than the factory default, all consumer IoT device passwords shall be unique per device or defined by the user.	We don't have any password authentication on the device.	N/A
5.1-2	(MC) Where pre-installed unique per device passwords are used, these shall be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.	We don't have any password authentication on the device.	N/A
5.1-3	(MC) Authentication mechanisms used to authenticate users against a device shall use best practice cryptography, appropriate to the properties of the technology, risk and usage.	We don't have user authentication on the device.	N/A
5.1-4	(MC) Where a user can authenticate against a device, the device shall provide to the user or an administrator a simple mechanism to change the authentication value used.	We don't have user authentication on the device.	N/A
5.1-5	(MC) When the device is not a constrained device, it shall have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.		P
5.2	**Implement a means to manage reports of vulnerabilities**		/
5.2-1	(M) The manufacturer shall make a vulnerability disclosure policy publicly available.		P
5.2-2	(R) Disclosed vulnerabilities should be acted on in a timely manner.		P
5.2-3	(R) Manufacturers should continually monitor for, identify and rectify security vulnerabilities within products and services they sell, produce, have produced and services they operate during the defined support period.		P
5.3	**Keep software updated**		/
5.3-1	(R) All software components in consumer IoT devices should be securely updateable.		P
5.3-2	(MC) When the device is not a constrained device, it shall have an update mechanism for the secure installation of updates.		P
5.3-3	(MC) An update shall be simple for the user to apply.		P
5.3-4	(RC) Automatic mechanisms should be used for software updates.	The device does not support automatic updates.	N/A
5.3-5	(RC) The device should check after initialization, and then periodically, whether security updates are available.	The device does not support automatic updates.	N/A

Clause	Requirement + Test	Remark	Verdict
5.3-6	(RC) If the device supports automatic updates and/or update notifications, these should be enabled in the initialized state and configurable so that the user can enable, disable, or postpone installation of security updates and/or update notifications.	The device does not support automatic updates.	N/A
5.3-7	(MC) The device shall use best practice cryptography to facilitate secure update mechanisms.		P
5.3-8	(MC) Security updates shall be timely.		P
5.3-9	(RC) The device should verify the authenticity and integrity of software updates.		P
5.3-10	(MC) Where updates are delivered over a network interface, the device shall verify the authenticity and integrity of each update via a trust relationship.		P
5.3-11	(RC) The manufacturer should inform the user in a recognisable and apparent manner that a security update is required together with information on the risks mitigated by that update.	Users can not update the firmware from the cloud, We will push the latest firmware to the device and let the device update when we found critical/high vulnerabilities on the device.	N/A
5.3-12	(RC) The device should notify the user when the application of a software update will disrupt the basic functioning of the device.		P
5.3-13	(M) The manufacturer shall publish, in an accessible way that is clear and transparent to the user, the defined support period.		P
5.3-14	(RC) For constrained devices that cannot have their software updated, the rationale for the absence of software updates, the period and method of hardware replacement support and a defined support period should be published by the manufacturer in an accessible way that is clear and transparent to the user.	The device is not constrained.	N/A
5.3-15	(RC) For constrained devices that cannot have their software updated, the product should be isolable and the hardware replaceable.	The device is not constrained.	N/A
5.3-16	(M) The model designation of the consumer IoT device shall be clearly recognizable, either by labelling on the device or via a physical interface.		P
5.4	**Securely store sensitive security parameters**		/
5.4-1	(MC) Sensitive security parameters in persistent storage shall be stored securely by the device.		P
5.4-2	(MC) Where a hard-coded unique per device identity is used in a device for security purposes, it shall be implemented in such a way that it resists tampering by means such as physical, electrical or software.		P
5.4-3	(M) Hard-coded critical security parameters in device software source code shall not be used.		P

Clause	Requirement + Test	Remark	Verdict
5.4-4	(MC) Any critical security parameters used for integrity and authenticity checks of software updates and for protection of communication with associated services in device software shall be unique per device and shall be produced with a mechanism that reduces the risk of automated attacks against classes of devices.		P
5.5	**Communicate securely**		/
5.5-1	(M) The consumer IoT device shall use best practice cryptography to communicate securely.		P
5.5-2	(R) The consumer IoT device should use reviewed or evaluated implementations to deliver network and security functionalities, particularly in the field of cryptography.		P
5.5-3	(R) Cryptographic algorithms and primitives should be updateable.		P
5.5-4	(RC) Access to device functionality via a network interface in the initialized state should only be possible after authentication on that interface.		P
5.5-5	(MC) Device functionality that allows security-relevant changes in configuration via a network interface shall only be accessible after authentication. The exception is for network service protocols that are relied upon by the device and where the manufacturer cannot guarantee what configuration will be required for the device to operate.	The user cannot access the device functionality via a network without authentication and the device does not have security-relevant configurations that can be changed via a network interface.	N/A
5.5-6	(RC) Critical security parameters should be encrypted in transit, with such encryption appropriate to the properties of the technology, risk and usage.		P
5.5-7	(MC) The consumer IoT device shall protect the confidentiality of critical security parameters that are communicated via remotely accessible network interfaces.		P
5.5-8	(MC) The manufacturer shall follow secure management processes for critical security parameters that relate to the device.		P
5.6	**Minimize exposed attack surfaces**		/
5.6-1	(M) All unused network and logical interfaces shall be disabled.		P
5.6-2	(M) In the initialized state, the network interfaces of the device shall minimize the unauthenticated disclosure of security-relevant information.		P
5.6-3	(R) Device hardware should not unnecessarily expose physical interfaces to attack.	.	P
5.6-4	(MC) Where a debug interface is physically accessible, it shall be disabled in software.	There's no debug interface on the device.	N/A
5.6-5	(R) The manufacturer should only enable software services that are used or required for the intended use or operation of the device.		P

Clause	Requirement + Test	Remark	Verdict
5.6-6	(R) Code should be minimized to the functionality necessary for the service/device to operate.		P
5.6-7	(R) Software should run with least necessary privileges, taking account of both security and functionality.	The DUT only has the only user(root) who has the highest permission. All software is running by the root. We considered it secure because we closed unnecessary physical and logical interfaces, and all opened interfaces have authentication. We don't have to debug the interface too.	N/A
5.6-8	(R) The device should include a hardware-level access control mechanism for memory.	The device only runs a single thread FreeRTOS which does not have multiple processes and multiple access roles. The entire program space belongs to the main thread of this FreeRTOS. Therefore, it doesn't have to apply access control.	N/A
5.6-9	(R) The manufacturer should follow secure development processes for software deployed on the device.		P
5.7	**Ensure software integrity**		/
5.7-1	(R) The consumer IoT device should verify its software using secure boot mechanisms.		P
5.7-2	(R) If an unauthorized change is detected to the software, the device should alert the user and/or administrator to the issue and should not connect to wider networks than those necessary to perform the alerting function.		P
5.8	**Ensure that personal data is secure**		/
5.8-1	(RC) The confidentiality of personal data transiting between a device and a service, especially associated services, should be protected, with best practice cryptography.		P

Clause	Requirement + Test	Remark	Verdict
5.8-2	(MC) The confidentiality of sensitive personal data communicated between the device and associated services shall be protected, with cryptography appropriate to the properties of the technology and usage.		P
5.8-3	(MC) All external sensing capabilities of the device shall be documented in an accessible way that is clear and transparent for the user.	There are no sensors on the DUT.	N/A
5.9	**Make systems resilient to outages**		/
5.9-1	(R) Resilience should be built into consumer IoT devices and services, considering the possibility of outages of data networks and power.		P
5.9-2	(R) Consumer IoT devices should remain operating and locally functional in the case of a loss of network access and should recover cleanly in the case of restoration of a loss of power.		P
5.9-3	(R) The consumer IoT device should connect to networks in an expected, operational and stable state and in an orderly fashion, taking the capability of the infrastructure into consideration.	The compensation mechanism is implemented on the cloud.	N/A
5.10	**Examine system telemetry data**		/
5.10-1	(RC) If telemetry data is collected from consumer IoT devices and services, such as usage and measurement data, it should be examined for security anomalies.		P
5.11	**Make it easy for users to delete user data**		/
5.11-1	(MC) The user shall be provided with functionality such that user data can be erased from the device in a simple manner.		P
5.11-2	(RC) The consumer should be provided with functionality on the device such that personal data can be removed from associated services in a simple manner.	The compensation mechanism is implemented in the APP.	N/A
5.11-3	(RC) Users should be given clear instructions on how to delete their personal data.		P
5.11-4	(RC) Users should be provided with clear confirmation that personal data has been deleted from services, devices and applications.		P
5.12	**Make installation and maintenance of devices easy**		/
5.12-1	(R) Installation and maintenance of consumer IoT should involve minimal decisions by the user and should follow security best practice on usability.		P
5.12-2	(R) The manufacturer should provide users with guidance on how to securely set up their device.		P
5.12-3	(R) The manufacturer should provide users with guidance on how to check whether their device is securely set up.	The DUT does not need to check the secure setup because the capability of securely set up is implemented by the device itself.	N/A

Clause	Requirement + Test	Remark	Verdict
5.13	**Validate input data**		/
5.13-1	(MC) The consumer IoT device software shall validate data input via user interfaces or transferred via application programming interfaces (APIs) or between networks in services and devices.		P
6	**Data protection provisions for consumer IoT**		/
6-1	(MC) The manufacturer shall provide consumers with clear and transparent information about what personal data is processed, how it is being used, by whom, and for what purposes, for each device and service. This also applies to third parties that can be involved, including advertisers.		P
6-2	(MC) Where personal data is processed on the basis of consumers' consent, this consent shall be obtained in a valid way.		P
6-3	(MC) Consumers who gave consent for the processing of their personal data shall have the capability to withdraw it at any time.		P
6-4	(RC) If telemetry data is collected from consumer IoT devices and services, the processing of personal data should be kept to the minimum necessary for the intended functionality		P
6-5	(MC) If telemetry data is collected from consumer IoT devices and services, consumers shall be provided with information on what telemetry data is collected, how it is being used, by whom, and for what purposes.		P

- - End of report - -

Attachment No.1

Details of: Outlook – Front view

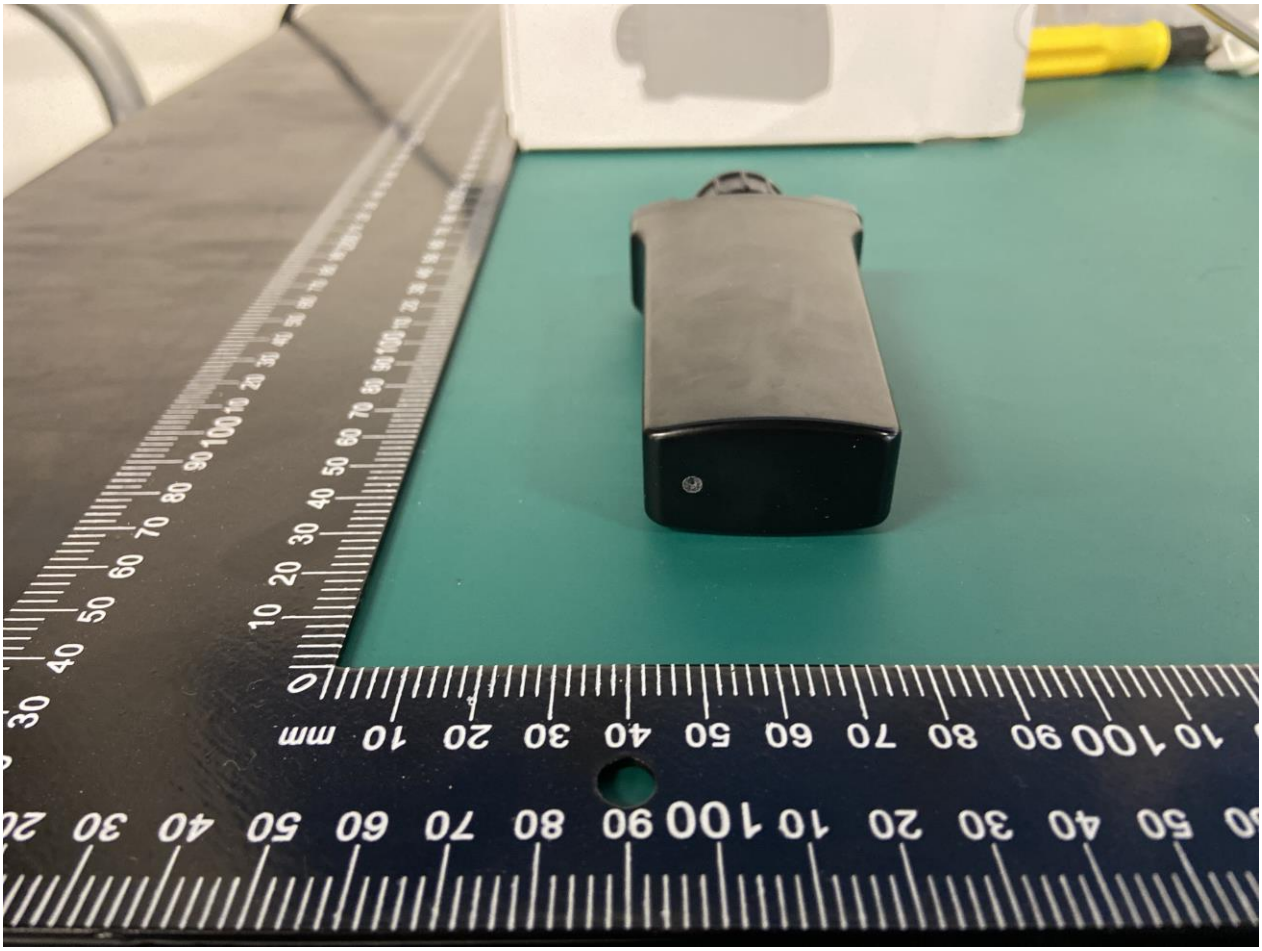
Remark: Model: Wi-Fi stick

Details of: Outlook – Back view

Remark: Model: Wi-Fi stick

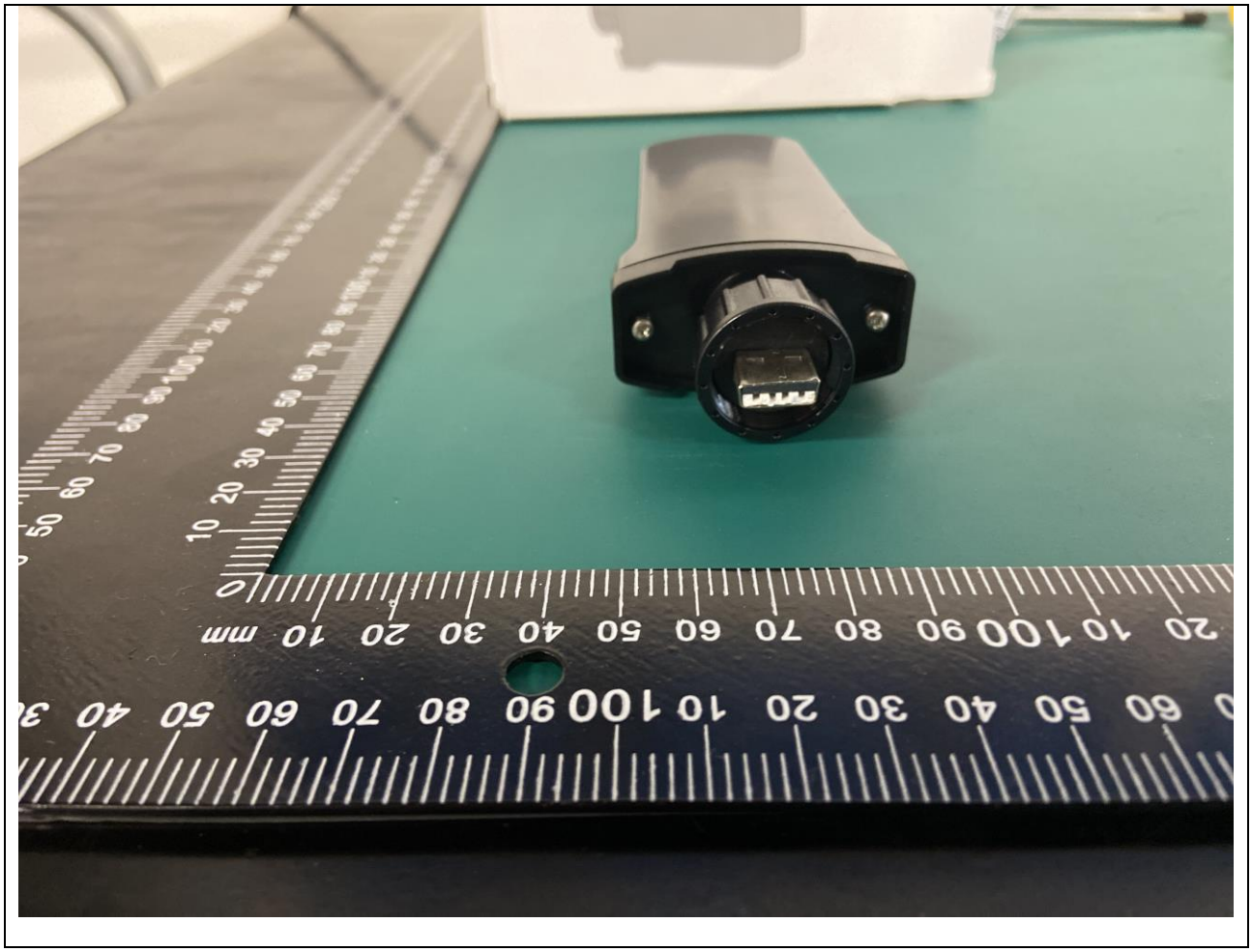
Details of: Outlook – Bottom view

Remark: Model: Wi-Fi stick



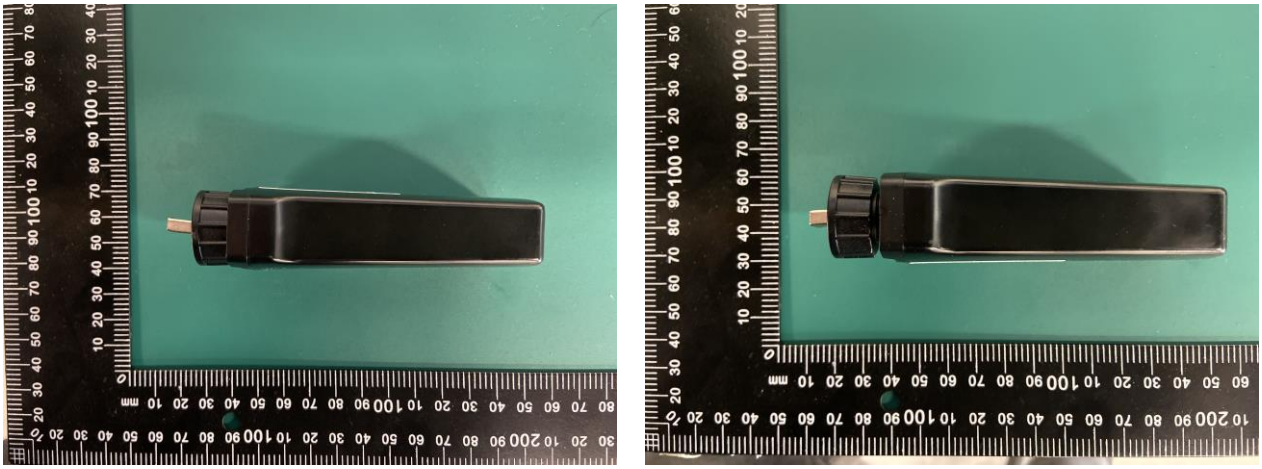
Details of: Outlook – Above view

Remark: Model: Wi-Fi stick



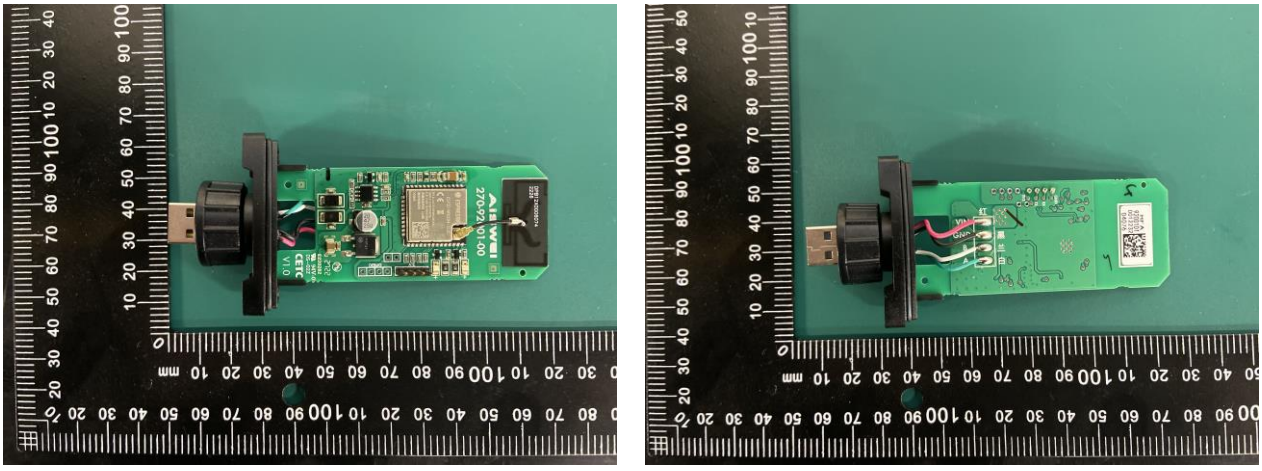
Details of: Outlook – Side view

Remark: Model: Wi-Fi stick



Details of: Insidelook – PCB layout

Remark: Version：AISWEI 270-92001-00



Details of: Insidelook – SoC

Remark: Model: ESP32-WROOM-32UE

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