ilac-MRA

ACCREDITED
CERT#4344.01

TEST REPORT

Applicant:	DrayTek
Address:	No. 26, Fu Shing Road, Hukou County,Hsin-Chu Industrial Park, Hsinchu, Taiwan
EUT Name:	Gigabit Broadband Router
Model Name:	Vigor2136ax-4G
Brand Name:	DrayTek
Test Standard:	EN 18031-1:2024
Sample Arrival Date:	Jul. 30, 2025
Test Date:	Aug. 8, 2025 - Sep. 26, 2025
Date of Issue:	Oct. 10, 2025

CERTIFICATION • CONSULTING • SOLUTION • SERVICE
BALUN

ISSUED BY:

Shenzhen BALUN Technology Co., Ltd.

Tested by: Yang Shengzhao	**Checked by:** Sunny Zou	**Approved by:** Jason Yang (Supervisor)
Yang Shengzhao	Sunny Zou	Jason Yang

Revision History

Version	Issue Date	Revisions Content
Rev. 01	Oct. 10, 2025	Initial Issue

TABLE OF CONTENTS

1 GENERAL INFORMATION

1.1 Identification of the Testing Laboratory

Company Name	Shenzhen BALUN Technology Co., Ltd.
Address	Block B, 1/F, Baisha Science and Technology Park, Shahe Xi Road, Nanshan District, Shenzhen City, Guangdong Province, P. R. China
Phone Number	+86 755 6685 0100

1.2 Identification of the Responsible Testing Location

Test Location	Shenzhen BALUN Technology Co., Ltd.
Location	□Block B, 1/F, Baisha Science and Technology Park, Shahe Xi Road, Nanshan District, Shenzhen City, Guangdong Province, P. R. China
	☑1/F, Building B, Ganghongji High-tech Intelligent Industrial Park, No. 1008, Songbai Road, Yangguang Community, Xili Sub-district, Nanshan District, Shenzhen, Guangdong Province, P. R. China

2 PRODUCT INFORMATION

2.1 Applicant Information

Applicant	DrayTek
Address	No. 26, Fu Shing Road, Hukou County,Hsin-Chu Industrial Park, Hsinchu, Taiwan

2.2 Manufacturer Information

Manufacturer	DrayTek
Address	No. 26, Fu Shing Road, Hukou County,Hsin-Chu Industrial Park, Hsinchu, Taiwan

2.3 General Description for Equipment under Test (EUT)

EUT Name	Gigabit Broadband Router
Model Name Under Test	Vigor2136ax-4G
Hardware Version	V6B
Software Version	5.3.3
EUT SN/IMEI	EUT1 IMEI: 867151070024156

2.4 Technical Information

Network and Wireless Connectivity	3G: WCDMA/HSDPA/HSUPA/DC-HSDPA 4G: LTE FDD/TDD Wi-Fi: 802.11a/b/g/n/ac/ax
Applicable Scope	☑RED 3.3.d □RED 3.3.e □RED 3.3.f

3 SUMMARY OF TEST RESULTS

3.1 Test Standards

No.	Identity	Document Title
1	EN 18031-1:2024	Common security requirements for radio equipment - Part 1: Internet connected radio equipment

3.2 Verdict

EN 18031-1:2024		
Clause	Test Items	Verdict
6.1.1	[ACM-1] Applicability of access control mechanisms	PASS
6.1.2	[ACM-2] Appropriate access control mechanisms	PASS
6.2.1	[AUM-1] Applicability of authentication mechanisms	PASS
6.2.2	[AUM-2] Appropriate authentication mechanisms	PASS
6.2.3	[AUM-3] Authenticator validation	PASS
6.2.4	[AUM-4] Changing authenticators	PASS
6.2.5	[AUM-5] Password strength	PASS
6.2.6	[AUM-6] Brute force protection	PASS
6.3.1	[SUM-1] Applicability of update mechanisms	PASS
6.3.2	[SUM-2] Secure updates	PASS
6.3.3	[SUM-3] Automated updates	PASS
6.4.1	[SSM-1] Applicability of secure storage mechanisms	PASS
6.4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	PASS
6.4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	PASS
6.5.1	[SCM-1] Applicability of secure communication mechanisms	PASS
6.5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication mechanisms	PASS
6.5.3	[SCM-3] Appropriate confidentiality protection for secure communication mechanisms	PASS

EN 18031-1:2024		
Clause	Test Items	Verdict
6.5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms	PASS
6.6.1	[RLM-1] Applicability and appropriateness of resilience mechanisms	PASS
6.7.1	[NMM-1] Applicability and appropriateness of network monitoring mechanisms	PASS
6.8.1	[TCM-1] Applicability of and appropriate traffic control mechanisms	PASS
6.9.1	[CCK-1] Appropriate CCKs	PASS
6.9.2	[CCK-2] CCK generation mechanisms	PASS
6.9.3	[CCK-3] Preventing static default values for preinstalled CCKs	N/A
6.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	N/A
6.10.2	[GEC-2] Limit exposure of services via related network interfaces	PASS
6.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces	PASS
6.10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network interfaces	PASS
6.10.5	[GEC-5] No unnecessary external interfaces	PASS
6.10.6	[GEC-6] Input validation	PASS
6.11.1	[CRY-1] Best practice cryptography	PASS

Possible test case verdicts:

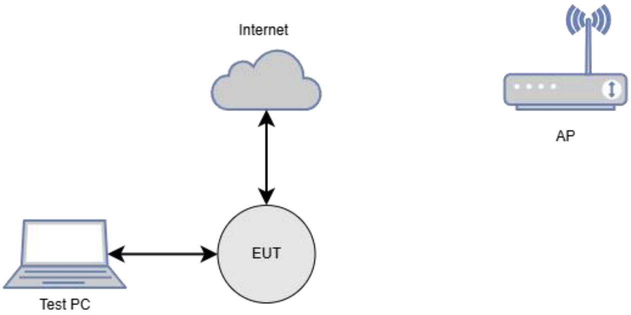
- test case does not apply to the test object	: N/A
- test case has not been tested	: --
- test object does meet the requirement	: PASS
- test object does not meet the requirement	: FAIL

4 GENERAL TEST CONFIGURATIONS

4.1 Test Environment

Temperature (℃)	15-35 ℃
Relative Humidity (%)	25 -70 %
Atmospheric Pressure (kPa)	86-106 kPa

4.1.1 Test Environment Setup



4.2 Hardware Resource

Equipment No.	Description	Model	Operating System
BZ-SIS-L008	Computer	ThinkBook 14 G5+IRH	Microsoft Windows 11
BZ-SIS-L041	Facedancer21	/	/

4.3 Test Tool

Equipment No.	Description	Version
BZ-SIS-L028	Wireshark	V4.4.1
BZ-SIS-L038	Nmap	V7.9.4SVN
BZ-SIS-L035	cve-bin-tool	V 3.4
BZ-SIS-L024	Burp Suite	V2024.4.5
BZ-SIS-L042	umap2	V2.0.1
BZ-SIS-L047	Binwalk	V2.4.3
BZ-SIS-L039	keytool	Jdk-8u131
BZ-SIS-L053	Zed Attack Prox	V2.16.1

ANNEX A TEST RESULT

EN 18031-1:2024			
Clause	Mechanism	Requirement	Verdict
6.1	[ACM] Access control mechanism		
6.1.1	[ACM-1] Applicability of access control mechanisms	The equipment shall use access control mechanisms to manage entities' access to security assets and network assets.	PASS
	Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-IAM Asset-PSK Asset-Log Center Asset-IMEI Asset-IMSI Asset-Network Tools Asset-Firewall Asset-Monitoring Asset-Network Settings Asset-CellularData Asset-Bandwidth Management Asset-TrafficData Asset-TACACS+ Asset-SMS Asset-VPN Asset-RADIUS Asset-Hotspot Web Portal Asset-AP Controller Asset-Switch Controller Asset-TR069 AccMech-1: Intf-Ethernet, Intf-LTE, Intf-WLAN, Intf-UI: The access control mechanism based on [IC.ACM-2.RBAC] ensures that only authorized entities can access the corresponding permission assets. AccMech-2: Intf-Ethernet, Intf-LTE, Intf-WLAN, Intf-UI:		

EN 18031-1:2024			
	The access control mechanism based on [IC.ACM-2.RBAC] ensures that only SSH authorized entities can access the corresponding permission assets.		
6.1.2	[ACM-2] Appropriate access control mechanisms	Access control mechanisms that are required per ACM-1 shall ensure that only authorized entities have access to the protected security assets and network assets.	PASS
	AccMech-1:Gateway BASE RBAC: Only authenticated entities can access assets corresponding to their authorized permissions. AccMech-1:SSH BASE RBAC: Only authenticated entities can access assets corresponding to their authorized permissions.		
6.2	[AUM] Authentication mechanism		
6.2.1	[AUM-1] Applicability of authentication mechanisms		
6.2.1.1	[AUM-1-1] Requirement network interface	Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via network interfaces that allow to: read confidential network function configuration or confidential security parameters or modify sensitive network function configuration or sensitive security parameters or use network functions or security functions.	PASS
	Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-IAM Asset-PSK Asset-Log Center Asset-IMEI Asset-IMSI Asset-Network Tools Asset-Firewall Asset-Monitoring Asset-Network Settings Asset-CellularData Asset-Bandwidth Management Asset-TrafficData		

EN 18031-1:2024			
	Asset-TACACS+ Asset-SMS Asset-VPN Asset-RADIUS Asset-Hotspot Web Portal Asset-AP Controller Asset-Switch Controller Asset-TR069 AUM-1: ACM-1 Intf-Ethernet, Intf-LTE, Intf-WLAN Only GateWay authenticated entities can access assets via network interface corresponding to their authorized permissions. AUM-2: ACM-2 Intf-Ethernet, Intf-LTE, Intf-WLAN Only SSH authenticated entities can access assets via network interface corresponding to their authorized permissions.		
6.2.1.2	[AUM-1-2] Requirement user interface	Access control mechanisms required per ACM-1 shall use authentication mechanisms for managing entities' access via user interfaces that allow to: read confidential network function configuration or confidential security parameters or modify sensitive network function configuration or sensitive security parameters or use network functions or security functions.	PASS
	Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-IAM Asset-PSK Asset-Log Center Asset-IMEI Asset-IMSI Asset-Network Tools Asset-Firewall		

<table>
<tr><th colspan="4">EN 18031-1:2024</th></tr>
<tr><td></td><td colspan="3">Asset-Monitoring
Asset-Network Settings
Asset-CellularData
Asset-Bandwidth Management
Asset-TrafficData
Asset-TACACS+
Asset-SMS
Asset-VPN
Asset-RADIUS
Asset-Hotspot Web Portal
Asset-AP Controller
Asset-Switch Controller
Asset-TR069

AUM-1:
ACM-1
Intf-Ethernet, Intf-LTE, Intf-WLAN
Only GateWay authenticated users can access assets via user interface corresponding to their authorized permissions.

AUM-2:
ACM-2
Intf-Ethernet, Intf-LTE, Intf-WLAN
Only SSH authenticated users can access assets via user interface corresponding to their authorized permissions.</td></tr>
<tr><td>6.2.2</td><td>[AUM-2] Appropriate authentication mechanisms</td><td>Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall verify an entity’s claim based on examining evidence from at least one element of the categories knowledge, possession and inherence (one factor authentication).</td><td>PASS</td></tr>
<tr><td></td><td colspan="3">AUM-1:
The gateway authentication mechanism used password for identity authentication, which is a knowledge-based authentication factor. Users need to enter the correc password to pass the authentication.

AUM-2:
The SSH authentication mechanism used password for identity authentication, which is a knowledge-based authentication factor. Users need to enter the correc password to pass the authentication.</td></tr>
</table>

EN 18031-1:2024			
6.2.3	[AUM-3] Authenticator validation	Authentication mechanisms that are required per AUM-1-1 (network interface) or AUM-1-2 (user interface) shall validate all relevant properties of the used authenticators, dependent on the available information in the operational environment of use.	PASS
	AUM-1: The gateway authentication mechanism verifies the account and password provided by the user to ensure that only authorized users can access the gateway functions in the current operating environment. AUM-2: The SSH authentication mechanism verifies the account and password provided by the user to ensure that only authorized users can access the gateway functions in the current operating environment.		
6.2.4	[AUM-4] Changing authenticators	Authentication mechanisms that are required per AUM-1-1 or AUM-1-2 shall allow for changing the authenticator except for authenticators where conflicting security goals do not allow for a change.	PASS
	AUM-1: The password for the authenticator can be changed in the settings page and prior to modification, the old authenticator must be verified. Once modified, the new authenticator enables access to the assets, while the old authenticator is permanently invalidated for assets access. AUM-2: The password for the authenticator can be changed in the settings page and prior to modification, the old authenticator must be verified. Once modified, the new authenticator enables access to the assets, while the old authenticator is permanently invalidated for assets access.		
6.2.5	[AUM-5] Password strength		
6.2.5.1	[AUM-5-1] Requirement for factory default passwords	If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall: -- be enforced to be set by the user before or on first use and before the equipment is logically connected to a network; or -- be defined by an authorized entity within a network where access is limited to authorised entities; or	PASS

<table>
<tr><th colspan="4">EN 18031-1:2024</th></tr>
<tr><td rowspan="2"></td><td></td><td>-- be generated by the equipment using best practice concerning strength and only communicated to an authorized entity within a network where access is limited to authorised entities.</td><td></td></tr>
<tr><td colspan="3">AUM-1:
The EUT used factory default password but the user must be changed when users use the device for the first time

AUM-2:
The EUT used factory default password but the user must be changed when users use the device for the first time</td></tr>
<tr><td rowspan="2">6.2.5.2</td><td>[AUM-5-2] Requirement for non-factory default passwords</td><td>If passwords other than factory default passwords are used by an authentication mechanism required per AUM-1-1 or AUM-1-2, they shall:
-- be unique per equipment; and
-- follow best practice concerning strength; or
-- be enforced to be changed by the user before or on first use.</td><td>N/A</td></tr>
<tr><td colspan="3">The device has no non-factory default password.</td></tr>
<tr><td rowspan="2">6.2.6</td><td>[AUM-6] Brute force protection</td><td>Authentication mechanisms required per AUM-1-1 or AUM-1-2 shall be resilient against brute force attacks.</td><td>PASS</td></tr>
<tr><td colspan="3">AUM-1:
Based on [IC. AUM - 6. TimeDelay],The device will be locked for five minutes after entering the wrong account and password five times.

AUM-2:
Based on [IC. AUM - 6. TimeDelay],The device will be locked for five minutes after entering the wrong account and password five times.</td></tr>
<tr><td>6.3</td><td colspan="3">[SUM] Secure update mechanism</td></tr>
<tr><td>6.3.1</td><td>[SUM-1] Applicability of update mechanisms</td><td>The equipment shall provide at least one update mechanism for updating software, including firmware,affecting security assets and/or network assets.</td><td>PASS</td></tr>
</table>

EN 18031-1:2024			
	UpdMech-1:The device has an update mechanism to update, the update mechanism is OTA UpdMech-2:The device has an update mechanism to update, the update mechanism is Manual update		
6.3.2	[SUM-2] Secure updates	Each update mechanism as required per SUM-1 shall only install software whose integrity and authenticity are valid at the time of the installation.	PASS
	UpdMech-1,UpdMech-2: AuthIntVal Type base on [IC.SUM-2.AuthIntVal. Sign] and Use ECDSAwithSHA512 signature algorithm to ensure authenticity and integrity.		
6.3.3	[SUM-3] Automated updates	Each update mechanism that is required per SUM-1 shall be capable of updating the software: —without human intervention at the equipment; or —via scheduling the installation of an update under human approval; or —via triggering the installation of an update under human approval or supervision where there is the need to prevent any unexpected damage in the operational environment.	PASS
	UpdMech-1: EUT will automatically check for updates. If a new update package is available, it can be updated with the user's approval. UpdMech-2: EUT will automatically check for updates. If a new update package is available, it can be updated with the user's approval.		
6.4	[SSM] Secure storage mechanism		
6.4.1	[SSM-1] Applicability of secure storage mechanisms	The equipment shall always use secure storage mechanisms for protecting the security assets and network assets persistently stored on the equipment, except for persistently stored security assets or network assets where: -- the physical or logical measures in the target environment ensures the security asset or network asset stored on the equipment accessibility is limited to authorized entities.	PASS
	Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate		

EN 18031-1:2024			
	Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-PSK Asset-Log Center Asset-IMEI Asset-Network Settings Asset-CellularData Asset-Bandwidth Management EUT implements the secure storage mechanism.		
6.4.2	[SSM-2] Appropriate integrity protection for secure storage mechanisms	Each secure storage mechanism that is required per SSM-1 shall protect the integrity of security assets and network assets it stores persistently.	PASS
	Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-PSK Asset-Log Center Asset-IMEI Asset-Network Settings Asset-CellularData Asset-Bandwidth Management The access control mechanism can reject unauthorized modifications.		
6.4.3	[SSM-3] Appropriate confidentiality protection for secure storage mechanisms	Each secure storage mechanism that is required per SSM-1 shall protect the secrecy of confidential security parameter and confidential network function configuration it stores persistently.	PASS
	Asset-GatewayPwd Asset-AESKEY Asset-WPAPSK Asset-Private key of https certificate		

EN 18031-1:2024			
	The access control mechanism can deny unauthorized reading.		
6.5	[SCM] Secure communication mechanism		
6.5.1	[SCM-1] Applicability of secure communication mechanisms	The equipment shall always use secure communication mechanisms for communicating security assets and network assets with other entities via network interfaces.	PASS
	Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-IAM Asset-PSK Asset-Log Center Asset-IMEI Asset-IMSI Asset-Network Settings Asset-CellularData Asset-Bandwidth Management Asset-TrafficData ComMech-HTTPS: Intf-Ethernet, Intf-LTE, Intf-WLAN: The secure communication mechanism based on TLS provides security for asset transmission, guaranteeing confidentiality, integrity, authenticity, and replay attack protection Asset-GatewayPwd Asset-Publickey of https certificate Asset-PrivacyKey of https certificate Asset-ECDSAkey Asset-AESKEY Asset-VPNcertificate Asset-RouterSettings Asset-IAM Asset-PSK Asset-Log Center Asset-IMEI Asset-IMSI		

EN 18031-1:2024			
	Asset-Network Settings Asset-CellularData Asset-Bandwidth Management Asset-TrafficData ComMech-WPA: Intf-WLAN: Secure Wi‐Fi communication using WPA2‐PSK with AES‐CCMP; provides authentication via PSK + 4‐way handshake, frame integrity (CCMP-MAC), confidentiality (AES‐CCMP), and anti‐replay using per‐packet Packet Numbers (PN). Asset-IMEI Asset-CellularData Asset-IMSI Asset-TrafficData ComMech-LTE: Intf-LTE: The secure communication mechanism based on EPS-AKA and AS/NAS security in LTE provides security for signaling and user data, guaranteeing confidentiality, integrity, authenticity, and replay attack protection.		
6.5.2	[SCM-2] Appropriate integrity and authenticity protection for secure communication Mechanisms	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the integrity and authenticity of the security assets and network assets communicated.	PASS
	ComMech-HTTPS: Authenticity:Server authentication is performed by the client using the server's public key certificate, which the server presents during the handshake. The exact nature of the cryptographic operation for server authentication is dependent on the negotiated cipher suite and extensions. In most cases (e.g., RSA for key transport, DH and ECDH), authentication is performed explicitly through verification of digital signatures present in certificates, and implicitly by the use of the server public key by the client during the establishment of the master secret. A successful Finished message implies that both parties calculated the same master secret and thus, the server must have known the private key corresponding to the public key used for key establishment. Client authentication is optional, and only occurs at the server's request. Client authentication is based on the client's public key certificate. The exact nature of the cryptographic operation for client authentication depends on the negotiated cipher suite's key exchange algorithm and the negotiated extensions. For example, when the client's public key certificate contains an RSA public key, the client signs a portion of the handshake message using the private key corresponding to that public key, and the server verifies the signature using the public key to authenticate the client. Integrity:The keyed MAC algorithm, specified by the negotiated cipher suite, provides message		

<table>
<tr><th colspan="4">EN 18031-1:2024</th></tr>
<tr><td></td><td colspan="3">integrity. Two MAC keys are derived: 1) a MAC key to be used when the client is the message sender and the server is the message receiver (the client write MAC key), and 2) a second MAC key to be used when the server is the message sender and the client is the message receiver (the server write MAC key). The sender of a message (client or server) calculates the MAC for the message using the appropriate MAC key, and encrypts both the message and the MAC using the appropriate encryption key. The sender then transmits the encrypted message and MAC to the receiver. The receiver decrypts the received message and MAC, and calculates its own version of the MAC using the MAC algorithm and sender’s MAC key. The receiver verifies that the MAC that it calculates matches the MAC sent by the sender. Two types of constructions are used for MAC algorithms in TLS. All versions of TLS support the use of the Keyed-Hash Message Authentication Code (HMAC) using the hash algorithm specified by the negotiated cipher suite. With HMAC, MACs for server to-client messages are keyed by the server write MAC key, while MACs client-to-server messages are keyed by the client write MAC key. These MAC keys are derived from the shared master secret. TLS 1.2 added support for AEAD cipher modes, such as Counter with CBC-MAC (CCM) and Galois Counter Mode (GCM), as an alternative way of providing integrity and confidentiality. In AEAD modes, the sender uses its write key for both encryption and integrity protection. The client and server write MAC keys are not used. The recipient decrypts the message and verifies the integrity information. Both the sender and the receiver use the sender’s write key to perform these operations.

ComMech-WPA:
Stations and AP run the 4- way handshake to prove possession of the PSK and derive the PTK. Data frame integrity is provided by CCMP-MAC (AES-128).

ComMech-LTE:
Mutual authentication via EPS-AKA. Integrity protection for NAS signaling (K_NASint) and RRC signaling (K_RRCint). Ensures messages cannot be modified and entities are authentic.</td></tr>
<tr><td>6.5.3</td><td>[SCM-3] Appropriate confidentiality protection for secure communication mechanisms</td><td>Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the confidentiality of communicated network assets and security assets where confidentiality protection of those is needed.</td><td>PASS</td></tr>
<tr><td></td><td colspan="3">ComMech-HTTPS:
Confidentiality is provided for a communication session by the negotiated encryption algorithm for the cipher suite and the encryption keys derived from the master secret and random values, one for encryption by the client (the client write key), and another for encryption by the server (the server write key). The sender of a message (client or server) encrypts the message using a derived encryption key; the receiver uses the same key to decrypt the message. Both the client and server know these keys, and decrypt the messages using the same key that was used for encryption. The encryption keys are
derived from the shared master secret</td></tr>
</table>

EN 18031-1:2024			
	ComMech-WPA: Data confidentiality is provided by AES-128-CCMP only; per-packet Packet Number (PN) serves as the CCM nonce. Keys are derived from the PTK; group traffic uses GTK. ComMech-LTE: Confidentiality through encryption using derived keys: K_NASenc for NAS messages, K_RRCenc for RRC signaling, and K_UPenc for user-plane data at PDCP. Algorithms: EEA2(AES-CTR)/EEA3(ZUC)		
6.5.4	[SCM-4] Appropriate replay protection for secure communication mechanisms	Each secure communication mechanism that is required per SCM-1 shall apply best practices to protect the security assets and the network assets communicated against replay attacks.	PASS
	ComMech-HTTPS: The integrity-protected envelope of the message contains a monotonically increasing sequence number. Once the message integrity is verified, the sequence number of the current message is compared with the sequence number of the previous message. The sequence number of the current message must be greater than the sequence number of the previous message in order to further process the message. ComMech-WPA: Anti-replay is enforced using per-packet Packet Numbers (PN) for CCMP with a sliding-window check; duplicates or out-of-order packets are dropped. The 4-way handshake uses nonces (ANonce/SNonce) to prevent key-establishment replay. ComMech-LTE: Replay protection with sequence numbers (COUNT values) in NAS, RRC, and PDCP. Each message carries an incrementing counter; old/replayed messages are rejected.		
6.6	[RLM] Resilience mechanism		
6.6.1	[RLM-1] Applicability and appropriateness of resilience mechanisms	The equipment shall use resilience mechanisms to mitigate the effects of Denial of Service (DoS) Attacks on the network interfaces and return to a defined state after the attack	PASS
	RLM flexible mechanism: The RLM mechanism can defend against common DOS attacks such as SYN flood attacks, UDP flood attacks,ICMP flood		

EN 18031-1:2024			
6.7	[NMM] Network monitoring mechanism		
6.7.1	[NMM-1] Applicability and appropriateness of network monitoring mechanisms	If the equipment is a network equipment, the equipment shall provide network monitoring mechanism(s) to detect for indicators of DoS attacks in the network traffic between networks which it processes.	PASS
	NMM-1: The NMM of EUT [IC.NMM-1. Generic] can not only reflect the overall load and health status of the network by collecting basic indicators such as interface traffic (TX/RX) and can conduct security analysis and monitor network attacks by collecting source/destination IP packet.		
6.8	[TCM] Traffic control mechanism		
6.8.1	[TCM-1] Applicability of and appropriate traffic control mechanisms	If the equipment is a network equipment, the equipment shall provide network traffic control mechanism(s).	PASS
	TCM-1: EUT adopts the TCM mechanism. By setting IP/Port Filtering rules, it controls the transmission of traffic data to handle abnormal patterns, malicious traffic, or data packets with specific source/destination addresses. These rules can specify the discarding, blocking or other operations on the identified data packets.		
6.9	[CCK] Confidential cryptographic keys		
6.9.1	[CCK-1] Appropriate CCKs	Confidential cryptographic keys that are preinstalled or generated by the equipment during its use, shall support a minimum security strength of 112-bits.	PASS
	CCK-1-Asset-ECDSAkey supports a security strength of over 112 bits. CCK-2-ECDSAprivatekey supports a security strength of over 112 bits CCK-3-Asset-AESKEY supports a security strength of over 112 bits CCK-4-WPA-PMK key supports a security strength of over 112 bits CCK-5-HTTPS-Session key supports a security strength of over 112 bits CCK-6-KNASint supports a security strength of over 112 bits CCK-7-KNASenc supports a security strength of over 112 bits CCK-8-RRCint supports a security strength of over 112 bits CCK-9-RRCenc supports a security strength of over 112 bits CCK-10-UPenc supports a security strength of over 112 bits		
6.9.2	[CCK-2] CCK generation mechanisms	The generation of confidential cryptographic keys shall adhere to best practice cryptography.	PASS

EN 18031-1:2024			
	CCK-1-Asset-ECDSAkey OpenSSL has been validated as a Level 1, FIPS 140 software cryptographic module. CCK-2-ECDSAprivatekey OpenSSL has been validated as a Level 1, FIPS 140 software cryptographic module. CCK-3-WPA-PMK This key is generated by the PBKDF2 algorithm, which is a recommended practice for rfc2898. CCK-4-HTTPS-Session key This key is generated by the ECDHE algorithm and complies with NIST's HTTPS best practices. CCK-5-KNASint CCK-6-KNASenc CCK-7-RRCint CCK-8-RRCenc CCK-9-UPenc These keys are derived from KDF as defined in TS 33.220.		
6.9.3	[CCK-3] Preventing static default values for preinstalled CCKs	Preinstalled confidential cryptographic keys shall be practically unique per equipment.	N/A
	CCK3-Asset-AESKEY: This key is the symmetric key for decrypting the update packet and needs to be the same as the server. Therefore. This is an intended function		
6.10	[GEC] General equipment capabilities		
6.10.1	[GEC-1] Up-to-date software and hardware with no publicly known exploitable vulnerabilities	The equipment shall not include publicly known exploitable vulnerabilities that, if exploited, affect security assets and network assets	N/A
	Although EUT has publicly known vulnerabilities, the risks have been mitigated to an acceptable risk		
6.10.2	[GEC-2] Limit exposure of services via related network interfaces	In factory default state the equipment shall only expose -- network interfaces; and -- services via network interfaces affecting security assets or network assets which are necessary for equipment setup or for basic operation of the equipment.	PASS
	Intf-Ethernet, Intf-WLAN： The EUT is a network device, and these interfaces are necessary for the basic network functions and operations of the EUT: Wi-Fi and LTE provide wireless connectivity, the WAN interface provides		

EN 18031-1:2024			
	Internet gateway functionality, and the LAN interface provides local network connectivity, which are all necessary components of the EUT's core functionality.		
6.10.3	[GEC-3] Configuration of optional services and the related exposed network interfaces	Optional network interfaces or optional services exposed via network interfaces affecting security assets or network assets, which are part of the factory default state shall have the option for an authorized user to enable and disable the network interface or service.	PASS
	Authorized users are permitted to enable/disable the following interfaces: Intf-Wi-Fi, Intf-LTE, Intf-WAN, Intf-LAN		
6.10.4	[GEC-4] Documentation of exposed network interfaces and exposed services via network Interfaces	The equipment's user documentation shall contain a description of -- all exposed network interfaces; and -- all services exposed via network interfaces, which are delivered as part of the factory default state.	PASS
	Intf-Ethernet, Intf-WLAN All exposed network interfaces are described in the user documentation DrayTek_UG_Vigor2136_V1.0.		
6.10.5	[GEC-5] No unnecessary external interfaces	The equipment shall only expose physical external interfaces if they are necessary for its intended functionality.	PASS
	Physical external interfaces on the device must exist for the intended functionality		
6.10.6	[GEC-6] Input validation	The equipment shall validate input received via external interfaces if the input has potential impact on security assets and/or network assets.	PASS
	The EUT performed input validation on all services and interfaces that could impact security. Services on ports 53, 80, and 443 underwent a comprehensive assessment. For the DNS service on port 53, extensive fuzz testing was conducted, covering labels exceeding 63 bytes, QNAMEs near and beyond the 255-byte boundary, invalid and unknown QTYPE values (0/99/65535), random payload injection, and truncated-header scenarios. The EUT strictly accepts data that conforms to protocol specifications; malformed or overly long queries are systematically dropped, and invalid or unrecognized types consistently return a NOERROR/NODATA response or are silently rejected. For the web services on ports 80 and 443, OWASP ZAP was used to fuzz APIs that accept input, focusing on authentication and configuration endpoints (including SQL injection, OS command injection, path traversal, and boundary-value attacks) and all malicious inputs were systematically rejected via 4xx responses or 302 redirects to a designated fault page. Key security checks		

EN 18031-1:2024			
	confirmed that no unauthorized commands were executed, no configuration changes occurred, and no diagnostic or database error information was disclosed. The test results verify that the EUT has implemented input validation mechanisms and that multi-layer syntactic and semantic input validation can effectively defend against common attack vectors. For USB interface security, the test lab conducted protocol-aware fuzzing tests on the USB ports using umap2. The results demonstrated the interface's robust input sanitization capabilitie.		
6.11	[CRY] Cryptography		
6.11.1	[CRY-1] Best practice cryptography	The equipment shall use best practice for cryptography that is used for the protection of the security assets or network assets.	PASS
	CRY-1-ECDSA with SHA： The use of ECDSA256&384 with SHA256&516 algorithm is in line with current cryptographic best practices. CRY-2-AES-CCMP： The use of AES 256-bit CCMP algorithm is in line with current cryptographic best practices. CRY-3-AES-GCM： The use of AES 256-bit GCM algorithm is in line with current cryptographic best practices. CRY-4-AES-CBC+IV： The use of AES 128-bit CBC with IV algorithm (The randomness and security of this IV are guaranteed by a hardware-based random byte generator (Ring Oscillator), which produces random bytes with unpredictability) is in line with current cryptographic best practices. CRY-5-EEA2： The use of EEA2(AES based algorithm) is in line with current cryptographic best practices. CRY-6-EIA2： The use of EIA2(AES based algorithm) is in line with current cryptographic best practices. CRY-7-EEA3： The use of EEA3(ZUC based algorithm) is in line with current cryptographic best practices. CRY-8-EIA3： The use of EIA3(ZUC based algorithm) is in line with current cryptographic best practices.		

ANNEX B EUT EXTERNAL PHOTOS

Please refer the document “BL-SZ2571075-AW.PDF”.

ANNEX C EUT INTERNAL PHOTOS

Please refer the document “BL-SZ2571075-AI.PDF”.

Statement

1. The laboratory guarantees the scientificity, accuracy and impartiality of the test, and is responsible for all the information in the report, except the information provided by the customer. The customer is responsible for the impact of the information provided on the validity of the results.
2. The report without China inspection body and laboratory Mandatory Approval (CMA) mark has no effect of proving to the society.
3. For the report with CNAS mark or A2LA mark, the items marked with "☆" are not within the accredited scope.
4. This report is invalid if it is altered, without the signature of the testing and approval personnel, or without the “inspection and testing dedicated stamp” or test report stamp.
5. The test data and results are only valid for the tested samples provided by the customer.
6. This report shall not be partially reproduced without the written permission of the laboratory.
7. Any objection shall be raised to the laboratory within 30 days after receiving the report.

-- End of Report --