

# TECHNICAL CODE

## SECURE AND AUTHORISED TV BOXES FOR STREAMING AND CONTENT DELIVERY

Developed by



Registered by



Registered date:

© Copyright 2026

## **Development of technical codes**

The Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) ('the Act') provides for a Technical Standards Forum designated under Section 184 of the Act or the Malaysian Communications and Multimedia Commission ('the Commission') to prepare a technical code. The technical code prepared pursuant to Section 185 of the Act shall consist of, at least, the requirements for network interoperability and the promotion of safety of network facilities.

Section 96 of the Act also provides for the Commission to determine a technical code in accordance with Section 55 of the Act if the technical code is not developed under an applicable provision of the Act and it is unlikely to be developed by the Technical Standards Forum within a reasonable time.

In exercise of the power conferred by Section 184 of the Act, the Commission has designated the Malaysian Technical Standards Forum Bhd ('MTSFB') as a Technical Standards Forum which is obligated, among others, to prepare the technical code under Section 185 of the Act.

A technical code prepared in accordance with Section 185 shall not be effective until it is registered by the Commission pursuant to Section 95 of the Act.

For further information on the technical code, please contact:

### **Malaysian Communications and Multimedia Commission (MCMC)**

MCMC Tower 1  
Jalan Impact  
Cyber 6  
63000 Cyberjaya  
Selangor Darul Ehsan  
MALAYSIA

Tel : +60 3 8688 8000  
Fax : +60 3 8688 1000  
Email : [stpd@mcmc.gov.my](mailto:stpd@mcmc.gov.my)  
Website: [www.mcmc.gov.my](http://www.mcmc.gov.my)

OR

### **Malaysian Technical Standards Forum Bhd (MTSFB)**

Level 3A, MCMC Tower 2  
Jalan Impact  
Cyber 6  
63000 Cyberjaya  
Selangor Darul Ehsan  
MALAYSIA

Tel : +60 3 8680 9950  
Fax : +60 3 8680 9940  
Email : [support@mtsfb.org.my](mailto:support@mtsfb.org.my)  
Website: [www.mtsfb.org.my](http://www.mtsfb.org.my)

## Contents

	Page
Committee representation.....	iii
Foreword .....	iv
0. Introduction.....	1
1. Scope .....	1
2. Normative references .....	1
3. Abbreviations.....	1
4. Terms and definitions .....	2
4.1 Television (TV) Box .....	2
4.2 Digital Rights Management (DRM).....	2
4.3 Firmware .....	2
4.4 Illicit streaming activities .....	2
4.5 Cryptographic key .....	2
4.6 Unauthorised access .....	2
4.7 Transport Layer Security (TLS) .....	2
4.8 Trusted Execution Environment (TEE).....	3
5. Firmware control and update management .....	3
5.1 Firmware authenticity and integrity protection .....	3
5.2 Firmware access control.....	3
5.2.1 Firmware downgrade protection.....	3
5.2.2 Firmware recovery protection.....	3
5.3 Secure firmware update delivery .....	4
5.4 Firmware update authorisation .....	4
5.5 Firmware version control management .....	5
5.6 Mandatory security updates.....	5
5.7 Update failure protection.....	5
6. Secure boot and trusted execution .....	5
6.1 Hardware root of trust .....	5
6.1.1 Secure boot verification.....	5
6.1.2 Secure boot validation.....	5
6.2 Boot failure protection.....	6
6.3 Trusted Execution Environment (TEE).....	6
6.4 Secure cryptographic key storage .....	6
6.5 Secure media pipeline .....	6
7. Application access control.....	6
7.1 Pre-loaded applications .....	6
7.2 Trusted application sources.....	7

7.3	Application signature verification .....	7
7.4	Application installation control and permission management.....	7
7.5	Developer mode .....	7
8.	System integrity and tamper protection.....	8
8.1	Root or jailbreak detection .....	8
8.2	Bootloader protection.....	8
8.3	Debugging and instrumentation detection .....	8
9.	Digital Rights Management (DRM).....	9
Annex A	Normative References .....	10
Annex B	Abbreviations .....	11
Annex C	Requirements for test suite for firmware control and update management.....	12
Annex D	Requirements for test suite for secure boot and trusted execution .....	16
Annex E	Requirements for test suite for application access control .....	20
Annex F	Requirements for test suite for system integrity and tamper protection .....	23
Bibliography	.....	24
Acknowledgements	.....	25

## **Committee representation**

This technical code was developed by Broadcast Technology Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CyberSecurity Malaysia

Measat Broadcast Network Systems Sdn Bhd

Medialab Alliance Sdn Bhd

MYTV Broadcasting Sdn Bhd

SIRIM Berhad

Sony EMCS Malaysia Sdn Bhd

TM Technology Services Sdn Bhd

Universiti Malaysia Perlis

Universiti Teknologi Mara

PUBLIC COMMENT

**Foreword**

This technical code for the Secure and Authorised TV Boxes for Streaming and Content Delivery ('Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Broadcast Technology Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

PUBLIC COMMENT

## SECURE AND AUTHORISED TV BOXES FOR STREAMING AND CONTENT DELIVERY

### 0. Introduction

The illegal streaming Television (TV) box ecosystem has evolved into a highly accessible and scalable market supported by low-cost hardware, preloaded applications, and organised distribution channels, creating an illicit parallel economy that competes with licensed services. These devices are commonly associated with cybersecurity risks arising from unverified applications and firmware, including potential exposure to malware and unauthorised data activities. At the same time, limitations in existing certification frameworks, which primarily address hardware compliance, have led to market misinterpretation whereby certified devices are perceived as fully compliant, despite the absence of software and firmware-level verification.

In view of these challenges, recognising that total prevention of such activities may not be fully attainable, it is essential to establish practical and enforceable mechanisms to support relevant authorities in carrying out compliance verification, enforcement actions, and subsequent legal proceedings, with the objective of deterring the use of non-compliant devices.

The Technical Code applies specifically to TV boxes that enable streaming functionalities and may facilitate unauthorised access to content services. The compliance assessment includes the evaluation and verification of both hardware and firmware components to ensure that such devices do not support or enable non-compliant streaming activities.

Through the implementation of this Technical Code, it is intended to strengthen national enforcement capabilities and support a coordinated regulatory approach in addressing the proliferation of illegal streaming TV boxes in Malaysia.

### 1. Scope

This Technical Code specifies the minimum requirements for the technical specifications, security, and compliance of TV boxes to ensure secure and authorised streaming and content delivery. It also aims to prevent such devices from supporting, enabling, or facilitating illicit access to content services.

### 2. Normative references

The following normative references are indispensable for the application of this Technical Code. For dated references, only the edition cited applies. For undated references, the latest edition of the normative references (including any amendments) applies.

See Annex A.

### 3. Abbreviations

For the purposes of this Technical Code, the following abbreviations apply.

See Annex B.

## 4. Terms and definitions

For the purposes of this Technical Code, the following definitions apply.

### 4.1 Television (TV) Box

A device capable of streaming audio and video content from the Internet and providing audio and video output for connection to third-party devices such as televisions, sound bars, audio video distribution systems, or any equipment capable of receiving such content.

The TV box may transmit audio and video signals to external devices through interfaces including High-Definition Multimedia Interface (HDMI) port and cable, composite port and cable, component port and cable, or other applicable transmission methods.

The device may support the installation of third-party applications to enable Internet-based streaming services. It may be available in various form factors, including box, dongle, stick, pendant, or other compact designs.

### 4.2 Digital Rights Management (DRM)

A trusted entity in the digital media content playback device responsible for execution of Digital Rights Management (DRM) content-related permissions and restrictions.

Systematic approach to protecting copyrights works from unauthorised access, use, reproduction, or distribution, and to enforce usage rights defined by content owners or right holders.

### 4.3 Firmware

Software that is installed inside the TV box that provides interface for user to interact with.

### 4.4 Illicit streaming activities

Unauthorised transmission, access, or distribution of audio-visual content over the internet without permission from the content owner or intellectual property rights holder.

### 4.5 Cryptographic key

A parameter used in conjunction with a cryptographic algorithm that determines its operation in such a way that an entity with knowledge of the key can reproduce, reverse or verify the operation while an entity without knowledge of the key cannot.

Parameter used with a cryptographic algorithm that determines its operation, such that knowledge of the key enables reproduction, reversal, or verification of the operation, while those without knowledge of the key cannot perform these operations.

### 4.6 Unauthorised access

Any attempt by users, software processes, or external interfaces that are not explicitly trusted or permitted by the device security architecture to read, write, or modify firmware memory or firmware components.

### 4.7 Transport Layer Security (TLS)

Cryptographic protocol that secures communications over unprotected computer networks, including the Internet.

#### 4.8 Trusted Execution Environment (TEE)

A secure area on the main processor of a device that ensures sensitive data is stored, processed, and protected in an isolated and trusted environment.

### 5. Firmware control and update management

This clause specifies the requirements for firmware control and update management to ensure the integrity and authenticity of firmware, preventing unauthorised modifications. Detailed test suite specifications are provided in Annex C

#### 5.1 Firmware authenticity and integrity protection

The TV box shall ensure that only authentic and unmodified firmware is installed and executed. The requirements for firmware authenticity and integrity include the following:

- a) The firmware shall be cryptographically signed by an authorised entity.
- b) The TV box shall verify the firmware signature prior to execution to ensure authenticity.
- c) All cryptographic mechanisms used shall comply with approved algorithms as specified in *MySEAL AKBA & AKSA*.
- d) The TV box shall verify the integrity of firmware images, such as using cryptographic hash, to detect unauthorised modification or corruption.
- e) The manufacturer shall declare the method used for firmware integrity verification.

#### 5.2 Firmware access control

The TV box shall implement access control mechanisms to prevent unauthorised access or modification of firmware, memory, and Random-Access Memory (RAM).

##### 5.2.1 Firmware downgrade protection

The TV box manufacturer shall control the firmware version that can be installed on the device and ensure that compromised firmware is not used for downgrade, unless necessary to address critical user experience issues.

##### 5.2.2 Firmware recovery protection

Firmware recovery protection shall ensure that system security is maintained during recovery operations, with the following controls.

- a) The TV box shall provide a secure firmware recovery mechanism that maintains all security protections and prevents bypass of firmware authentication, version control, or other system security controls.
- b) Recovery operations shall maintain all security controls and restore the device only to a secure and trusted firmware state.

- c) Firmware recovery mechanisms may include factory reset or system recovery modes. Such mechanisms should not allow installation of unsigned firmware or firmware versions that undermine security protections.
- d) The factory reset mechanism shall remove all user data and other data not that is not present in the factory default state.
- e) Where TV box recovery requires installation of a different firmware, only firmware provided by the original manufacturer shall be used.

### **5.3 Secure firmware update delivery**

Firmware updates shall be delivered securely to protect against unauthorised access and tampering, as outlined below.

- a) Firmware updates shall be delivered only through authenticated and encrypted communication channels using secure transport protocols that provide confidentiality, integrity, and server authentication.
- b) Transport Layer Security (TLS) version 1.2 or later shall be used.
- c) Secure messaging protocols shall be implemented for firmware update delivery.
- d) Firmware updates shall be performed through one or more of the following secure mechanisms:
  - i) Network (IP)
  - ii) Other mechanisms or procedures recommended by the manufacturer, provided they meet equivalent security standards

### **5.4 Firmware update authorisation**

Firmware updates shall be authorised to ensure that only trusted and approved firmware is installed. The following controls apply:

- a) Firmware updates shall be accepted and installed only through authorised update mechanisms.
- b) Firmware updates shall be cryptographically authenticated to verify that they originate from the manufacturer or other explicitly authorised entities.
- c) Authorised update mechanisms may include:
  - i) User-initiated updates
  - ii) Managed or remote updates.
  - iii) Rollback procedures
  - iv) Recovery mechanisms
- d) All update mechanisms shall enforce firmware authentication and authorisation controls.

### **5.5 Firmware version control management**

The TV box shall maintain identifiable firmware version information and provide traceability for installed firmware versions for security management, update control, and support purposes.

### **5.6 Mandatory security updates**

The TV box shall support the secure deployment and installation of mandatory security updates to address identified security vulnerabilities throughout the supported lifecycle of the device.

Mandatory security updates shall not be permanently deferrable by the user where required to maintain system integrity or security.

### **5.7 Update failure protection**

The TV box shall maintain system integrity and security protections during firmware update failure and shall be capable of recovering to a secure and functional state.

## **6. Secure boot and trusted execution**

This clause specifies the requirements for secure boot and trusted execution to ensure the TV box boots using trusted software and operates in a protected environment against unauthorised code and tampering. Detailed test procedures are provided in Annex D.

### **6.1 Hardware root of trust**

A hardware root of trust shall be implemented to establish a secure foundation for system operation and trust establishment. The hardware root of trust shall:

- a) securely anchor the secure boot process,
- b) protect cryptographic keys from unauthorised access and modification, and
- c) establish an immutable trust boundary for all subsequent stages of system execution.

#### **6.1.1 Secure boot verification**

Secure boot verification shall ensure the authenticity and integrity of all boot components during system startup. The verification steps are as follows.

- a) All boot components, including the initial bootloader, operating system, and system firmware, shall be verified for authenticity and integrity prior to execution.
- b) Only boot components that are successfully verified as trusted shall be permitted to execute.

#### **6.1.2 Secure boot validation**

Secure boot validation shall be cryptographically enforced from a hardware-based root of trust and shall apply to all stages of the boot process.

The requirements are as follows.

- a) Secure boot validation shall cover all boot stages, including the primary bootloader, secondary boot stages, operating system kernel, and system firmware.
- b) Boot components that fail secure boot validation shall not be permitted to execute.

## **6.2 Boot failure protection**

Boot failure protection shall ensure the system remains secure in the event of boot verification failure. The handling mechanisms are as follows.

- a) TV box shall prevent normal startup if verification of boot components fails or if unauthorised system images are detected.
- b) TV box shall transition to a defined secure failure state in accordance with the device security policy.
- c) The secure failure state shall be recoverable through a firmware recovery mechanism.

## **6.3 Trusted Execution Environment (TEE)**

The device shall provide an isolated Trusted Execution Environment (TEE) for security sensitive operations including Digital Rights Management (DRM) processing and cryptographic key handling.

## **6.4 Secure cryptographic key storage**

Secure cryptographic key storage shall protect sensitive keys from unauthorised access and exposure. The protection measures are as follows:

- a) Cryptographic keys used for secure boot, firmware authentication, DRM, and other security-sensitive functions shall be securely generated, stored, and used within hardware-protected storage.
- b) Where hardware-protected storage is not used, cryptographic keys shall be encrypted using a hardware-based key prior to storage.
- c) Cryptographic keys shall not be directly accessible by normal system software.

## **6.5 Secure media pipeline**

A secure media pipeline shall be implemented to ensure that decoded media content is protected from unauthorised access or exposure during decoding, processing, and output.

# **7. Application access control**

This clause specifies the requirements for application access control to prevent the installation, execution, and operation of applications that enable unauthorised access to copyrighted content. Detailed test suite specifications are provided in Annex E.

## **7.1 Pre-loaded applications**

To ensure transparency and security, the manufacturer shall declare the following during the certification process.

- a) All pre-loaded applications.
- b) All hidden applications.
- c) All background services.

All declared applications shall be identifiable and traceable for verification purposes.

## **7.2 Trusted application sources**

Application installation shall be restricted to ensure that only trusted and authorised sources are used, with the following requirements.

- a) Applications shall only be downloaded and installed from trusted and verified application repositories approved by official digital platforms and official Over-The-Top (OTT) partners.
- b) Sideload capabilities shall be disabled by default. This includes, but is not limited to:
  - i) installation using Universal Serial Bus (USB);
  - ii) unauthorised network sources; and
  - iii) third-party package installers.
- c) Applications that enable end users to configure, add, edit, or modify content source Uniform Resource Locators (URLs), servers, hosts, or playlists for accessing audiovisual streaming content shall be restricted, unless explicitly authorised and controlled by the service provider.
- d) The restrictions shall apply to:
  - i) pre-loaded applications; and
  - ii) applications installed from any authorised application store or application distribution mechanism supported by the device.

## **7.3 Application signature verification**

Application signature verification shall be enforced by the TV box operating system, which are as below.

- a) All application packages shall undergo cryptographic signature verification prior to installation and execution.
- b) Applications without a valid digital certificate issued by a recognised and trusted Certificate Authority (CA) or the manufacturer's secure key infrastructure shall be blocked from installation.

## **7.4 Application installation control and permission management**

The TV box shall enforce the principle of least privilege. The permission controls are as follows.

- a) Applications shall be granted only the minimum system permissions necessary for their declared functions.
- b) Applications shall not obtain root access or administrative privileges.
- c) Applications shall not modify core system networking parameters, including but not limited to Domain Name System (DNS) configurations for unauthorised routing.

## **7.5 Developer mode**

Access to developer mode shall be restricted.

The following shall apply.

- a) Developer mode shall be accessible only through authorised and controlled mechanisms.

- b) Application sideloading or installation shall be permitted only through authorised and securely controlled mechanisms.
- c) Unauthorised access to developer mode shall be prevented.

## 8. System integrity and tamper protection

This clause specifies the requirements for system integrity and tamper protection to detect and prevent unauthorised modifications, including root or jailbreak attempts, bootloader compromise, and debugging or instrumentation abuse. Detailed test suite specifications are provided in Annex F.

### 8.1 Root or jailbreak detection

Root or jailbreak detection shall be implemented to identify compromise of system integrity, with the following controls.

- a) The device shall detect, at boot time, whether the system has been rooted, jailbroken, or otherwise modified to obtain elevated privileges.
- b) Such conditions shall be treated as a compromise of system integrity.

### 8.2 Bootloader protection

Bootloader protection shall be implemented to detect and manage unauthorised or non-secure bootloader states.

Bootloader states and corresponding controls are as follows.

- a) The TV box shall detect and report any unlocked, modified, or non-verified bootloader state prior to enabling protected content playback, firmware update or recovery operations, DRM services, or other security-sensitive system functions.
- b) Protected content playback and other security-sensitive system functions shall be restricted when an unlocked or non-verified bootloader is detected.

### 8.3 Debugging and instrumentation detection

Debugging and instrumentation controls shall be implemented to prevent bypass of system protections.

The presence of such tools and corresponding controls are as follows.

- a) The TV box shall detect or restrict the use of debugging tools, runtime instrumentation frameworks, or other tools that may be used to bypass system protections.
- b) Security-sensitive functions shall be restricted when such tools are detected.

Security-sensitive functions include features that depend on system integrity and trust, such as content protection, cryptographic key usage, firmware management, and trusted execution services.

## 9. Digital Rights Management (DRM)

The device shall support at least one industry-recognised DRM system as specified in Table 1.

**Table 1. Industry recognised DRM.**

Type of DRM	Version (minimum)	Device Security Level (minimum)
Google Widevine	Provisioning 2.0	L1
Microsoft PlayReady	3.0	SL2000
Apple FairPlay	As specified in Apple Developer Community	As specified in Apple Developer Community
Marlin Simple Secure Streaming	As specified in Marlin Developer Community	As specified in Marlin Developer Community

In addition to the above, the TV box may support other DRM systems, provided they meet security requirements equivalent to or exceeding the minimum mandated security levels.

The TV box supplier shall provide evidence of certification indicating that the TV box is certified for the stated DRM system. Such certification shall be issued by the DRM provider or an authorised Third-Party Laboratory (3PL) recognised by the respective DRM provider.

DRM-protected content shall comply with ISO/IEC 14496-12, and common encryption shall comply with ISO/IEC 23001-7. Any additional requirements specified by the DRM vendor shall also be complied with.

**Annex A**  
(normative)

**Normative References**

ISO/IEC 14496-12:2026, Information technology - Coding of audio-visual objects - Part 12: ISO base media file format

ISO/IEC 23001-7:2023, Information technology - MPEG systems technologies - Part 7: Common encryption in ISO base media file format files

Existing Cryptographic Algorithm for MySEAL (AKSA MySEAL)

<https://mykripto.cybersecurity.my/index.php/services/myseal/myseal-category/aksa-myseal>

PUBLIC COMMENT

**Annex B**  
(normative)

**Abbreviations**

3PL	Third-Party Laboratory
AOSP	Android Open-Source Project
CA	Certificate Authority
DRM	Digital Rights Management
HDMI	High-Definition Multimedia Interface
OTT	Over-The-Top
RAM	Random-Access Memory
TEE	Trusted Execution Environment
TLS	Transport Layer Security
TV	Television
URLs	Uniform Resource Locators
USB	Universal Serial Bus

PUBLIC COMMENT

**Annex C**  
**Requirements for test suite for firmware control and update management**

**Table C.1: Firmware control and update management**

Sub-clause	Objective	Expected Test Result	Information requires for Declaration form
<b>5.1</b> <b>Firmware authenticity and integrity protection</b>	To verify that the device enforces cryptographic authentication and integrity verification of firmware using MySEAL AKBA & AKSA-approved cryptographic algorithms, ensuring that only authentic, untampered firmware from authorised entities is installed and execute.	Only authorised, using MySEAL AKBA & AKSA-approved cryptographic algorithms and integrity verified firmware is accepted and executed; invalid or tampered firmware is rejected.	The manufacturer shall also declare: <ul style="list-style-type: none"> <li>a) When firmware authentication and integrity verification are performed (update, boot, execution, recovery).</li> <li>b) How firmware verification trust anchors (public keys/certificates) are.</li> <li>c) Secure device behaviour after verification failure (e.g: fallback, rollback, or recovery).</li> <li>d) Cryptographic Algorithms Used (Confirmation that all cryptographic algorithms used MySEAL AKBA &amp; AKSA approved cryptographic algorithm lists).</li> </ul>
<b>5.2</b> <b>Firmware access control</b>	To verify that firmware access controls prevent unauthorised access to firmware, memory, or RAM and prevent unauthorised firmware modification.	Any unauthorised attempt to read, write, or modify firmware, memory, or RAM is detected and blocked by the device, and the firmware remains unchanged and protected from unauthorised access or modification.	The manufacturer shall declare: <p>Firmware access control mechanism description and Identification of interface, user (e.g: secure boot, memory protection, privilege level, Secure execution environment)</p>

**Table C.1: Firmware control and update management** (continued)

Sub-clause	Objective	Expected Test Result	Information requires for Declaration form
5.2.1	<b>Firmware downgrade protection</b>	To verify that the device enforces firmware version control mechanisms that prevent rollback to older firmware versions during installation or execution.	<p>Any attempt to install or execute a firmware version older than the currently installed version is detected and rejected by the device, and the downgrade firmware is not installed or executed.</p> <p>The manufacturer shall declare:</p> <ul style="list-style-type: none"> <li>a) Description of the firmware versioning scheme (e.g. version number format,).</li> <li>b) Mechanism used to prevent firmware rollback (e.g. version check, anti-rollback counter, secure storage).</li> </ul>
5.2.2	<b>Firmware recovery protection</b>	To verify that the device's firmware recovery mechanism maintains all security controls and restores the device only to a secure and trusted firmware state, without allowing bypass of firmware authentication, version control, or other system security protections.	<p>The firmware recovery mechanism restores the device to a secure and trusted state while maintaining all security controls and preventing installation or execution of unsigned, unauthorised, or insecure firmware.</p> <p>The manufacturer shall provide:</p> <ul style="list-style-type: none"> <li>a) Description of supported firmware recovery mechanisms (e.g. factory reset, recovery mode, system recovery).</li> <li>b) Conditions under which recovery is triggered (manual, automatic, failure-based).</li> <li>c) What user data is erased during factory reset.</li> <li>d) What data remains after factory reset (e.g. factory firmware, certificates).</li> </ul>

**Table C.1: Firmware control and update management** (continued)

Sub-clause	Objective	Expected Test Result	Information requires for Declaration form
<b>5.3</b> <b>Secure firmware update delivery</b>	To verify that firmware updates are delivered exclusively through secure, authenticated, and encrypted communication channels that ensure confidentiality, integrity, and server authentication, regardless of the update delivery mechanism used.	The device accepts firmware updates only over authenticated and encrypted channels and rejects updates delivered via insecure communication mechanisms.	The manufacturer shall declare: <ul style="list-style-type: none"> <li>a) Transport protocols used for firmware updates (e.g. TLS 1.2, TLS 1.3).</li> <li>b) Cryptographic parameters (e.g. cipher suites, key exchange, hash algorithms).</li> <li>c) Method used for server authentication (e.g. X.509 certificates, certificate chains).</li> </ul>
<b>5.4</b> <b>Firmware update authorisation</b>	To verify that the device enforces authorised firmware update mechanisms and accepts and installs firmware updates only when they are cryptographically authenticated and originate from the manufacturer or explicitly authorised entities.	Only cryptographically authenticated firmware from authorised entities delivered via authorised update mechanisms is accepted and installed by the device.	The manufacturer shall provide: List and description of authorised firmware update mechanisms (e.g. OTA/IP update, user-initiated update, managed update, rollback, recovery).
<b>5.5</b> <b>Firmware version control management</b>	To verify that the device maintains clearly identifiable firmware version information and provides traceability of the installed firmware version to support security management, firmware update control, and operational support.	The device displays or provides access to accurate and uniquely identifiable firmware version information, allowing the installed firmware version to be traced and verified for security management, update control, and support purposes.	The manufacturer shall provide: <ul style="list-style-type: none"> <li>a) Description of the firmware version format (e.g. major/minor/build, semantic versioning).</li> <li>b) Explanation of how firmware versions are uniquely identified.</li> <li>c) Where firmware version information is stored (e.g. firmware header, secure storage, bootloader).</li> </ul>

**Table C.1: Firmware control and update management (concluded)**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
<b>5.6</b>	<b>Mandatory security updates</b>	To verify that the device supports the secure deployment and installation of mandatory security updates and enforces their installation when required to maintain system integrity or security, without allowing permanent user deferral.	Mandatory security updates are securely installed and cannot be permanently deferred by the user.	The manufacturer shall provide: a) Description of the security update policy during the supported lifecycle. b) Criteria used to classify updates as mandatory security updates.
<b>5.7</b>	<b>Update failure protection</b>	To verify that the device preserves system integrity and security protections when a firmware update fails, and is able to recover to a secure and functional state without executing incomplete, corrupted, or unauthorised firmware.	Firmware update failures do not compromise system security, and the device recovers to a secure and functional state.	Expected device behaviour in each failure scenario

**Annex D**  
**Requirements for test suite for secure boot and trusted execution**

**Table D.1: Requirements for test suite for secure boot and trusted execution**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
<b>6.1</b>	<b>Hardware root of trust</b>	To verify that the device implements a hardware-based root of trust that: <ul style="list-style-type: none"> <li>1) Anchors the secure boot chain.</li> <li>2) Protects cryptographic keys (e.g., public key, hash, fuses)</li> <li>3) Provides an immutable trust boundary (cannot be altered post-manufacturing)</li> </ul>	The device hardware-based root is implemented in dedicated hardware.	Manufacturer may provide: <ul style="list-style-type: none"> <li>a) Description of implementation.</li> <li>b) Location of implementation (e.g ROM, eFuse, TPM, Secure Enclave, etc.)</li> <li>c) Evidence to prove the implementation of hardware root of trust.</li> </ul>
<b>6.1.1</b>	<b>Secure boot verification</b>	To verify that the device ensures authenticity and integrity of all boot components before execution.	The device ensures authenticity and integrity of boot components	Manufacturer may provide: <ul style="list-style-type: none"> <li>a) Secure Boot Architecture <ul style="list-style-type: none"> <li>i) Description of boot chain</li> <li>ii) Components included in verification chain</li> </ul> </li> <li>b) Type of hardware protection used. (e.g) eFuse / OTP / secure storage</li> </ul>

**Table D.1: Requirements for test suite for secure boot and trusted execution** (continued)

Sub-clause	Objective	Expected Test Result	Information requires for Declaration form	
6.1.2	<b>Secure boot validation</b>	To verify that the device enforces cryptographic validation of all boot components from a hardware root of trust and blocks execution of any invalid components.	The device cryptographically validates the boot chain before execution	Manufacture may provide: <ul style="list-style-type: none"> <li>a) Architecture Documentation/any information that contain the following:                             <ul style="list-style-type: none"> <li>i) Secure Boot architecture diagram/flow</li> <li>ii) cryptography used / algorithm used (e.g RSA-2048, ECDSA P-256)</li> <li>iii) certificate/signature format (e.g custom header)</li> <li>iv) Description on chain of trust implementation</li> </ul> </li> </ul>
6.2	<b>Boot failure protection</b>	To verify that the device prevents normal startup when boot component verification fails or unauthorised firmware is detected.	The device enters a controlled secure state, such as: <ul style="list-style-type: none"> <li>1) Recovery mode or,</li> <li>2) Minimal trusted environment or,</li> <li>3) Boot halt with error indication or, any secure state defined by manufacturer which align with device security policy.</li> </ul>	Manufacturer may provide: <ul style="list-style-type: none"> <li>a) Manufacturer recovery utility (if any)</li> <li>b) Description of secure boot state (e.g normal, failure, recovery)</li> </ul>

**Table D.1: Requirements for test suite for secure boot and trusted execution (continued)**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
6.3	<b>Trusted execution environment</b>	To verify that the device implements an isolated Trusted Execution Environment (TEE)	The device enforces TEE Isolation using: Hardware-backed isolation	Manufacturer may provide: <ul style="list-style-type: none"> <li>a) TEE Architecture <ul style="list-style-type: none"> <li>i) Type of TEE implementation: (e.g ARM TrustZone, Secure Enclave, or equivalent)</li> </ul> </li> <li>b) DRM Implementation <ul style="list-style-type: none"> <li>i) DRM scheme used. (e.g., Widevine (L1/L2/L3))</li> <li>ii) Location of DRM processing</li> </ul> </li> </ul>
6.4	<b>Secure cryptographic key storage</b>	To verify that the device cryptographic keys are securely generated, stored, and used within protected hardware mechanisms.	The device cryptographic keys generated comply with Approved Algorithms in MySEAL recommended cryptographic standards.  Examples: AES ( $\geq 128$ -bit) SHA-256 or higher RSA/ECC with approved key lengths Weak/obsolete algorithms (e.g., MD5, SHA-1 for security) are not used.	Manufacturer may provide: <ul style="list-style-type: none"> <li>a) Key Types and purpose of each key <ul style="list-style-type: none"> <li>i) Secure boot key</li> <li>ii) Firmware signing verification key</li> <li>iii) DRM keys</li> </ul> </li> <li>b) Cryptographic Algorithms used <ul style="list-style-type: none"> <li>i) Algorithms and key lengths used</li> <li>ii) compliance with approved algorithm guideline</li> </ul> </li> </ul>

**Table D.1: Requirements for test suite for secure boot and trusted execution (concluded)**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
				<ul style="list-style-type: none"> <li>iii) compliance with approved algorithm guideline</li> <li>c) Secure storage of key generated in the firmware</li> <li>i) Description of Hardware-protected storage (e.g., eFuse, OTP, TEE secure storage)</li> </ul>
<b>6.5</b>	<b>Secure media pipeline</b>	To verify that the device implements a protected media processing path	The device implemented protected media pipeline by isolating and protecting across media decoding, processing and rendering input.	Manufacturer may provide: <ul style="list-style-type: none"> <li>a) Architecture and design of the media pipeline used.</li> <li>b) DRM &amp; Content Protection Mechanisms.</li> </ul>

**Annex E**  
**Requirements for test suite for application access control**

**Table E.1: Requirements for test suite for application access control**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
7.1	<b>Pre Load application</b>	<p>To ensure that the manufacturer:</p> <ol style="list-style-type: none"> <li>1) Fully discloses all pre-installed applications on the device</li> <li>2) Includes visible apps, hidden apps, system apps, and background services</li> <li>3) Prevents undisclosed software that may introduce security, privacy, or integrity risks</li> </ol>	<p>The manufacturer declared all pre-loaded application, hidden and background services.</p>	<p>Manufacturer may provide: Full Application Inventory.</p> <p>a) Complete list of:</p> <ol style="list-style-type: none"> <li>i) All installed applications (system + user) Include:               <ol style="list-style-type: none"> <li>1) Version numbers</li> <li>2) Package names</li> <li>3) Function descriptions</li> </ol> </li> <li>ii) Hidden Components Declaration Any: (example)               <ol style="list-style-type: none"> <li>1) Hidden apps</li> <li>2) Non-UI services</li> <li>3) Justification for existence</li> </ol> </li> </ol>

**Table E.1: Requirements for test suite for application access control** (continued)

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
<b>7.2</b>	<b>Trusted application sources</b>	To verify that the device restricts application installation and download exclusively to trusted and verified repositories.	The device allows installation only from trusted sources/Official app store and all other sources is blocked by default	<p>Manufacturer may provide:</p> <ul style="list-style-type: none"> <li>a) Approved Application Sources                             <ul style="list-style-type: none"> <li>List of allowed sources:                                     <ul style="list-style-type: none"> <li>i) Official app store (e.g., Google Play)</li> </ul> </li> </ul> </li> <li>b) OTT Platform Approval Requirement                             <ul style="list-style-type: none"> <li>Applications must be approved by official                                     <ul style="list-style-type: none"> <li>i) OTT provider platform (e.g., certified streaming ecosystem)</li> </ul> </li> </ul> </li> </ul>
<b>7.3</b>	<b>Application signature verification</b>	To verify the device enforces cryptographic signature verification for all application packages before Installation and execution	The device verifies the Trusted Certificates and allows only applications signed with: <ul style="list-style-type: none"> <li>1) Trusted developer certificates</li> <li>2) Platform-recognised certificate authorities</li> </ul>	<p>Manufacturer to provide:</p> <ul style="list-style-type: none"> <li>a) Source of trust:                             <ul style="list-style-type: none"> <li>Platform CA store / OEM-managed certificates</li> </ul> </li> <li>b) Policy for:                             <ul style="list-style-type: none"> <li>Accepting/rejecting certificates</li> </ul> </li> </ul>

**Table E.1: Requirements for test suite for application access control (concluded)**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
<b>7.4</b>	<b>Application installation control</b>	To verify that the device restricts installation of applications from unknown or unauthorised sources.	The device restricts application from Unknown Sources and application Installation from: 1) USB 2) Browser download 3) Third-party stores	Manufacturer to provide Authorisation Mechanism  Steps required to: a) Enable installation from unknown sources b) Whether authentication is required: c) PIN / password / developer mode
<b>7.5</b>	<b>Developer Mode</b>	To verify the the application sideloading is only possible through:  1) Explicitly authorised access to Developer Mode. 2) Secure and controlled activation mechanisms.	The device ensures that the application sideloading in the device is not available for normal mode.	Developer Mode must require:  a) Explicit user action (menu/settings activation)  b) Optional authentication (PIN/password depending on OEM design) in normal user mode

## Annex F Requirements for test suite for system integrity and tamper protection

**Table F.1: Requirements for test suite for system integrity and tamper protection**

Sub-clause		Objective	Expected Test Result	Information requires for Declaration form
8.1	<b>Root or jailbreak detection</b>	The device shall detect at boot time whether the system has been rooted, jailbroken, or otherwise modified to obtain elevated privileges, and shall treat such conditions as a compromise of the system integrity.	To verify that the device detects rooting, jailbreaking, or unauthorised privilege escalation at boot time and/or during runtime, and appropriately treats such conditions as a compromise of system integrity.	Upon detection of rooting or jailbreaking, the device prevents normal operation and/or restricts functionality to protect system integrity.
8.2.1	<b>Bootloader protection</b>	To verify that the device detects and reports an unlocked, modified, or non-verified bootloader state and prevents the use of security-sensitive system functions until system integrity and trust are ensured.	An insecure bootloader state is detected, reported, and results in restriction of security-sensitive system functions	<p>a) How the bootloader state is reported or made observable (e.g. system status flag, user notification, logs, management interface).</p> <p>b) Whether reports are accessible for testing and audit purposes.</p>
8.2	<b>Bootloader protection</b>	To verify that the device detects an unlocked bootloader state and restricts protected content playback in order to preserve system integrity and content protection	Protected content playback is restricted whenever an unlocked bootloader state is detected.	Not required
8.3	<b>Debugging and instrumentation detection</b>	To verify that the device is able to detect or restrict the presence of debugging tools, runtime instrumentation frameworks, or other bypass tools, and enforce appropriate protections to prevent compromise of security-sensitive system functions.	When a runtime debugging tool is detected, the device disables DRM-protected content playback and blocks access to cryptographic keys, protecting security-sensitive functions from compromise	<p>The manufacturer shall provide:</p> <p>1) Actions taken when such tools are detected (e.g. blocking execution, disabling features, restricting access).</p>

## Bibliography

- [1] MCMC MTSFB TC G044, Internet of Things (IOT) Baseline Security Requirements For Consumer Devices
- [2] ETSI EN 303 645, CYBER; Cyber Security for Consumer Internet of Things: Baseline Requirements.
- [3] NIST SP 800-193, Platform Firmware Resiliency Guidelines
- [4] NIST IR 8259, Foundational Cybersecurity Activities for IoT Device Manufacturers
- [5] NIST Special Publication 800-57 Part 1 Revision 5, Recommendation for Key Management: Part 1, General
- [6] NIST Special Publication 800-95, Guide to Secure Web Services

## **Acknowledgements**

### **Members of the Broadcast Technology Working Group**

#### **Working Group Leaders**

Ts Azhar Abdul Latiff (Chair)	Medialab Alliance Sdn Bhd
Ms Imaliana Muzni (Vice Chair I)	Media Prima Berhad
Prof Ir Ts Dr Muzammil Jusoh (Vice Chair II)	Universiti Malaysia Perlis

#### **Drafting Committee Members**

Mr Afzel Mohd Hakimi (Draft Lead)	Measat Broadcast Network Systems Sdn Bhd
Ms Nurul Amirah Zarifah Norazaruddin (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Nur Sharifah Idayu Mat Roh	CyberSecurity Malaysia
Ms Nurul Syahirah Aspawi	CyberSecurity Malaysia
Mr Wan Mohd Hafeez Wan Mohd Salleh	Measat Broadcast Network Systems Sdn Bhd
Ts Azhar Abdul Latiff	Medialab Alliance Sdn Bhd
Mr Al Hafiz Abu Bakar	SIRIM Berhad
Mr Mohamad Nurhakim Rajaie	Sony EMCS Malaysia Sdn Bhd
Mr Mohd Hafizuddin Shaharom	TM Technology Services Sdn Bhd
Mr Mohd Shazni Suhairy	TM Technology Services Sdn Bhd
Dr Megat Syahirul Amin Megat Ali	Universiti Teknologi MARA
Gs Dr Muhammad Hasif Azami	Universiti Teknologi MARA

#### **Contributors**

Mr Muhammad Nazmi Md Radzi	MYTV Broadcasting Sdn Bhd
Mr Tharsvin Kumar Thayalan	SIRIM Berhad
Prof Ir Ts Dr Muzammil Jusoh	Universiti Malaysia Perlis