

MCMC MTSFB TC G050:2025

TECHNICAL CODE

INTERNET OF THINGS (IOT) - BASELINE SECURITY ASSESSMENT FOR CONSUMER DEVICES

Developed by



Registered by



Registered date: 27 February 2025

© Copyright 2025

MCMC MTSFB TC G050:2025

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
Website: 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
Website: www.mtsfb.org.my

Contents

	Page
Committee representation.....	ii
Foreword	iii
0. Introduction.....	1
1. Scope	1
2. Normative references	1
3. Abbreviations.....	2
4. Terms and definitions.....	2
5. Assessment method.....	4
5.1 Roles and Documentation	4
5.2 Assessment checklist	5
5.3 Assignment of verdicts.....	6
6. Test Scenarios (TSO) for consumer IoT	6
6.1 TSO-1 - No universal default passwords.....	7
6.2 TSO-2 - Managing reports of vulnerabilities	8
6.3 TSO-3 - Keep software updated.....	10
6.4 TSO-4 - Securing sensitive security parameters.....	22
6.5 TSO-5 - Communicate securely	25
6.6 TSO-6 - Minimising attack surfaces.....	31
6.7 TSO-7 - Ensure software integrity	36
6.8 TSO-8 - Ensure secure personal data.....	38
6.9 TSO-9 - Systems resilient to outages.....	39
6.10 TSO-10 - Secure telemetry data.....	42
6.11 TSO-11 - Deleting user data.....	42
6.12 TSO-12 - Installation and maintenance of devices.....	45
6.13 TSO-13 - Validate input data	46
6.14 TSO-14 - Data protection requirements for consumer IoT	48
Annex A Abbreviations.....	51
Annex B Forms for the Supplier Organisation (SO).....	53
Annex C Overview of required CTIF entries per requirement.....	64
Annex D Sample of Comprehensive Testing Information File (CTIF)	82
Annex E Sample of complete forms for the Supplier Organisation (SO).....	84
Annex F Key secure by design principles of Internet of Things.....	105
Bibliography	107

MCMC MTSFB TC G050:2025

Committee representation

This technical code was developed by the Internet of Things and Smart Sustainable Cities Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB), which consists of representatives from the following organisations:

CyberSecurity Malaysia

Cyberview Sdn Bhd

Favoriot Sdn Bhd

SIRIM Berhad

Sunway University College Sdn Bhd

TM Technology Services Sdn Bhd

UCSI Education Sdn Bhd

Universiti Malaya

Universiti Sains Malaysia

Universiti Teknologi MARA

Foreword

This technical code for Internet of Things (IoT) - Baseline Security Assessment for Consumer Devices ('Technical Code') was developed pursuant to Section 185 of the Communications and Multimedia Act 1998 (Laws of Malaysia Act 588) by the Internet of Things and Smart Sustainable Cities Working Group of the Malaysian Technical Standards Forum Bhd (MTSFB).

This Technical Code shall continue to be valid and effective from the date of its registration until it is replaced or revoked.

(THIS PAGE IS INTENTIONALLY LEFT BLANK)

INTERNET OF THINGS (IOT) - BASELINE SECURITY ASSESSMENT FOR CONSUMER DEVICES

0. Introduction

In today's interconnected world, the rapid proliferation of Internet of Things (IoT) devices has dramatically expanded the potential attack surface for cyber threats. From basic fitness trackers to advanced smart home automation systems, each IoT device introduces unique vulnerabilities that malicious actors could exploit. Recognizing these risks, MCMC MTSFB TC G044 establishes essential security requirements to safeguard consumer IoT devices, providing a benchmark for best practices in IoT security.

This Technical Code has been developed to provide detailed testing guidelines for each requirement in MCMC MTSFB TC G044, helping Supplier Organisation (SO) to understand the specific items that need to be evaluated. By following this Technical Code, which operates independently of specific assurance schemes, SO can conduct thorough assessments to ensure that their devices meet the established security requirements. This unified approach aims to enhance the overall security of IoT products and build greater consumer confidence in connected technologies.

This Technical Code also serves as a voluntary assessment of the security baseline for consumer IoT devices, promoting best practices and enhancing product security. It is not mandatory, allowing suppliers to tailor security measures to their product design, market needs, and risk profiles. The content requirements encourage the adoption of secure devices, fostering greater consumer confidence in IoT products.

By integrating security into the development process, this approach addresses the unique challenges and vulnerabilities of IoT ecosystems, ensuring that security remains a fundamental consideration in device design and deployment.

1. Scope

This Technical Code establishes the methodology for evaluating consumer IoT devices and their associated services to meet the requirements of MCMC MTSFB TC G044. It specifies test cases and assessment criteria for meeting the recommended requirements, conditions, and supplements of the standards. It does not encompass the establishment of any certification or conformance declaration schemes.

The focus of this Technical Code is on evaluating the security requirements of consumer IoT devices. It assumes that these devices are connected to a secure network. However, the security of the network itself falls outside the scope of this document.

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.

MCMC MTSFB TC G044, *Internet of Things (IoT) - Baseline Security Requirements for Consumer Devices*

ETSI TS 103 701 V1.1.1 (2021-08), *Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements*

MCMC MTSFB TC G050:2025

AKSA MySEAL, *National Trusted Cryptographic Algorithm List (Senarai Algoritma Kriptografi Terpercaya Negara)*

Senior Officials Group Information System Security (SO-GIS): SOG-IS Crypto Working Group, *SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms*

3. Abbreviations

For the purposes of this Technical Code, the abbreviations in Annex A apply.

4. Terms and definitions

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

4.1 Assess

Generate a result by analysis using evaluator expertise. This includes practical analysis using the Device Under Test (DUT).

4.2 Assessment criteria

Complete and independent specification of the test units required to achieve a specific test purpose.

NOTE: The specification is complete if it is sufficient to enable a test case verdict to be assigned unambiguously to each potentially observable test outcome. The specification is independent if it is sufficient to execute the test units in isolation from other test cases.

4.3 Associated services

Software-based application services that support, enhance, or extend the functionality of IoT devices within a smart home ecosystem.

NOTE: These services typically operate through applications, cloud platforms, and integration systems, enabling users to manage, monitor, and interact with smart home devices remotely or through automation.

4.4 Check

Generate a result by a simple comparison. This may include practical analysis on the DUT.

4.5 Comprehensive Testing Information File (CTIF)

Extra information (in addition to that given in the Self-Assessment Statement (SAS) related to the DUT and its assessment environment, which will enable the Test Laboratory (TL) to perform appropriate test activities.

4.6 Comprehensive Testing Information File (CTIF) form

Document, in the form of a questionnaire, which when completed for a DUT becomes the Comprehensive Testing Information File (CTIF).

4.7 Device Under Test (DUT)

Consumer IoT device (as defined in MCMC MTFSB TC G044) that is the target of the assessment.

4.8 Self-Assessment Statement (SAS)

Statement, made by the Supplier Organisation (SO), of the capabilities implemented in or supported by the DUT.

4.9 Self-Assessment Form (SAF)

Document, in the form of a questionnaire, which when completed for a DUT becomes the SAS.

4.10 Indication

Documented finding by the TL used inside the assessment to assign a verdict.

4.11 Security guarantee

Statement of the addressed security objectives.

NOTE: In the present document security guarantees, are used in CTIF to describe the security objectives (e.g. confidentiality) which are realized by an implementation or process.

4.12 Supplier Organisation (SO)

Entity that is responsible for any part in the supply chain of the DUT. It includes manufacturers, vendors, system developer, IoT implementers, etc.

4.13 Test group

Related test cases that describe how to assess the DUT to a single requirement as specified in MCMC MTSFB TC G044.

NOTE: The naming of test groups and their corresponding requirements coincide.

4.14 Test Laboratory (TL)

Entity such as an independent testing organisation, a user organisation, or an identifiable part of a SO that carries out assessment of a DUT.

4.15 Test Scenario (TSO)

Named set of related test groups that describe how to assess the conformance of the DUT to a corresponding set of guidelines as specified in MCMC MTSFB TC G044.

NOTE: The names of Test Scenario (TSO) (sets of test groups) align with their corresponding sets of requirements.

4.16 Test unit

Indivisible unit of a specification of test activities processes.

4.17 User organisation

Person or organisation that represents user' interest with respect to DUT.

NOTE: This includes, for example, purchasers or users of products, or potential customers seeking to rely on a supplier's management system, or organizations representing those interests. A user organisation typically carries out a second party assessment.

5. Assessment method

This clause focuses on the overview and structure of the document for the method, which comprises of relevant roles, objects and assessments involving Self-Assessment Statement (SAS) & Comprehensive Testing Information File (CTIF).

Figure 1 illustrates the assessment method for the DUT. This Technical Code is develop based on MCMC MTSFB TC G044 and ETSI TS 103 701. The Self-Assessment Form (SAF) and CTIF forms were to be fill up by SO to produce a complete SAS and CTIF evaluation report. It is recommended that the outcome document can be published at the SO website to promote best practice in product security.

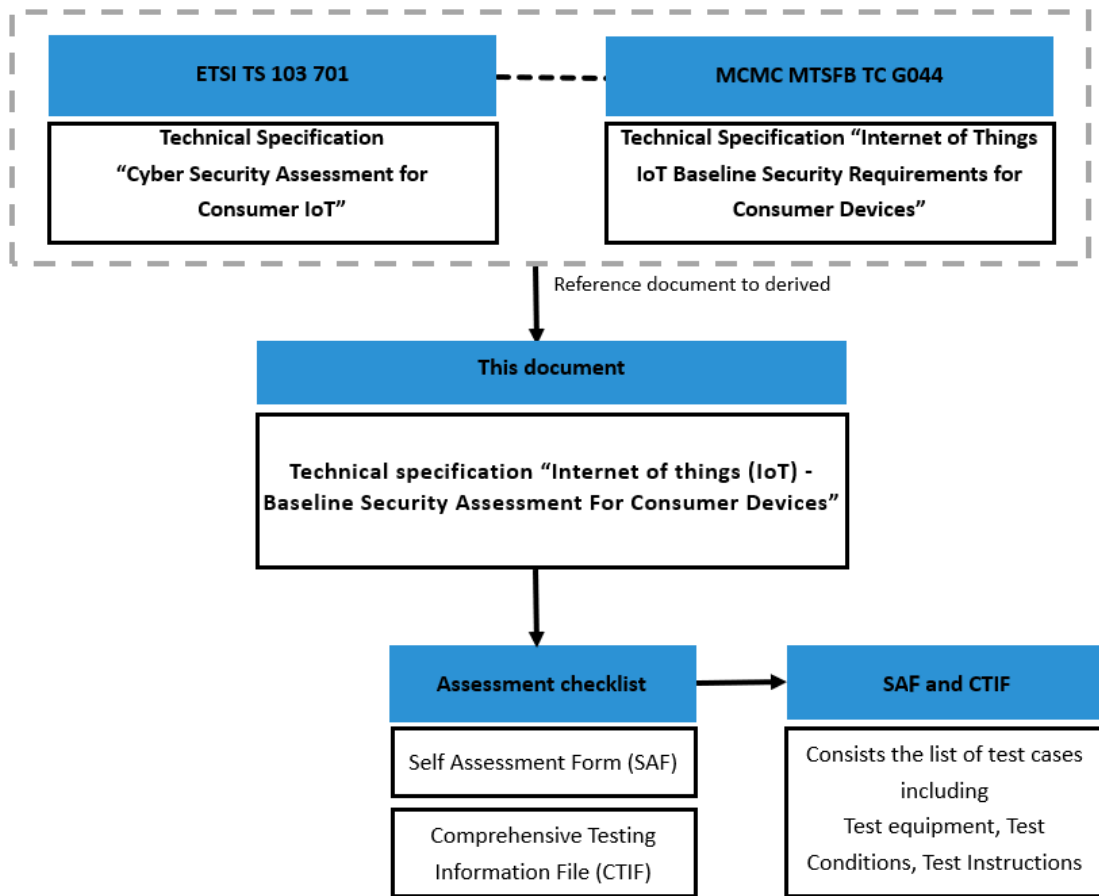


Figure 1. Relations of the present document with respect to the assessment structure

5.1 Roles and Documentation

This clause describes the relevant roles and documentations for the assessment procedure, i.e. DUT and SO.

5.1.1 Device Under Test (DUT)

As illustrated in Figure 2, the present document intends to provide TSOs for a wide variety of consumer IoT devices with different interfaces. Thus, the formulation of TSOs provides a certain level of abstraction as it is not feasible to describe a specific testing procedure for every kind of consumer IoT device. Explanation of Figure 2 in MCMC MTSFB TC G044 shall apply.

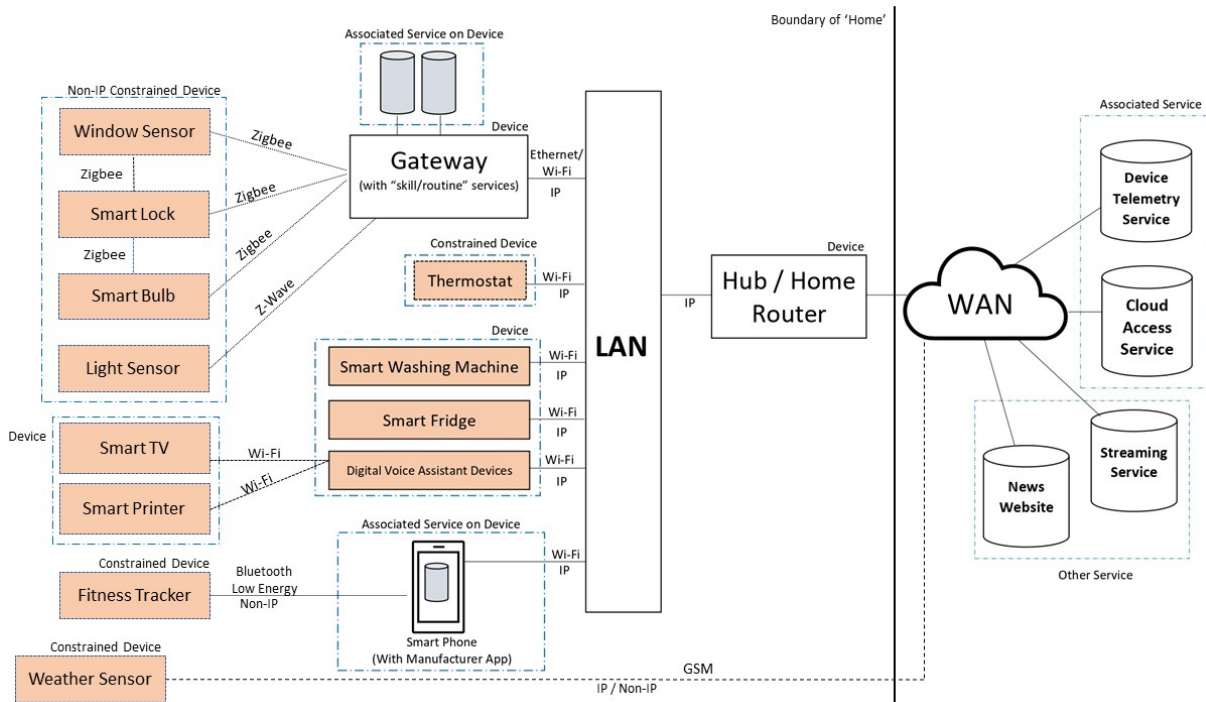


Figure 2. Examples for the heterogeneity of IoT implementations.

5.1.2 Supplier Organisation (SO) Role

The SO requests a specific DUT to be tested against the requirement in MTSFB TC G044. The SO is supposed to have all necessary knowledge about the security measures of the DUT to fill up the SAF and CTIF forms.

5.1.3 Test Laboratory (TL) Role

The TL is an entity that conducts the assessment of a DUT, which is either of the following entities.

- a) SO - self-assessment
- b) Independent testing laboratory appointed by the SO

5.2 Assessment checklist

The SO may use the following documents to evaluate their devices.

- i) DUT identification

The identification of the DUT provides information, as detailed as possible, e.g., about the DUT version numbering and configuration options. Furthermore, a declaration concerning constrained devices and contact information of the SO are included in the form. Table B.1 Annex B provide sample of DUT form to be filled up by the SO.

- ii) SAF form

The SO may indicate which capabilities are supported in the product according to MCMC MTSFB TC G044. The SO should confirm all requirements intended for assessment by

MCMC MTSFB TC G050:2025

marking 'YES' or 'NO' in the support column in Table B.1 Annex B. This form to be used together with TSO.

- iii) CTIF form

This document contains additional necessary information to assess the product. SO shall complete the CTIF entries to all requirements that indicates as "YES".

5.3 Assignment of verdicts

The test verdicts are achieved by evaluating the TSO marked as "YES" in the SAF. The verdicts for PASS and FAIL are assigned to each test case in the TSO.

Table 1 below describes the instructions for the assignment of test group verdict.

Table 1. Assignment test verdict

Test verdict	Instruction
PASS	This verdict is assigned when each test case of the TSO is assigned a PASS verdict
FAIL	This verdict is assigned when at least one test case of the TSO is assigned a FAIL verdict.
INCONCLUSIVE	The verdict is assigned when the required elements (e.g. evaluation tools and CITF information) for the test case performance are not present or are not sufficient to allow a proper execution of the test case and therefore no conclusive PASS or FAIL verdict can be assigned

6. Test Scenarios (TSO) for consumer IoT

This clause presents the assessment criteria for the baseline security requirements as presented in the MCMC MTSFB TC G044. TSO-1 until TSO-13 represents the TSO for Clause 6.1 until 6.13 in MCMC MTSFB TC G044. TSO-14 represents TSO for Clause 7 in MCMC MTSFB TC G044.

The TSO consists of the following information.

- a) Status - Security categories are classified into Mandatory, Mandatory Conditional, Recommended, and Recommended Conditional as defined in ETSI TS 103 701 V1.1.1.
- b) Requirement - specifies the clause number and the baseline security requirements in MCMC MTSFB TC G044. This represents the test group for each requirement.
- c) Assessment criteria - The TL should assess the security requirements based on the assessment criteria.
- d) CTIF Number – The TL should refer to the CTIF number for the detail methods or specification.
- e) PASS Assignment of verdict – The TL should assess the specific test cases for the specific test group in the assessment criteria.

The legend below is applicable for the Clause 6.1 until 6.13.

Legend

- M Mandatory
- MC Mandatory Conditional
- R Recommended
- RC Recommended Conditional

NOTE: MC (x) or RC (x): The 'x' is referring to the condition value as listed in Table B.2 in Annex B.

6.1 TSO-1 - No universal default passwords

The objective of this assessment is to verify that consumer IoT devices do not utilise universal default passwords. This measure is crucial for enhancing the security of IoT devices by preventing unauthorised access that could be facilitated through easily guessable default credentials. Table 2 below outlines the assessment criteria and assignment verdicts for TSO-1.

Table 2. TSO-1 - No universal default passwords

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (1)	6.1 No Universal Default Passwords	a) The TL should assess for all password-based user authentication mechanisms in the corresponding CTIF where passwords are not defined by the user according to "Authentication Factor" and used in any state other than the factory default whether the "Password Generation Mechanism" ensures that passwords are unique per device.	CTIF 1-AuthMech	<ul style="list-style-type: none"> • Each password of a password-based authentication mechanism being used in any state other than the factory default, that is not defined by the user, is unique per device. • Every discovered password-based authentication mechanism is documented in the CTIF. • The user is required to define all passwords, as indicated in the CTIF, before they are used. • There is no evidence of a non-user-defined password being generated by the DUT.
MC (2)		b) Where pre-installed unique per device passwords are used, these should be generated with a mechanism that reduces the risk of automated attacks against a class or type of device.	CTIF 1-AuthMech	<ul style="list-style-type: none"> • No obvious regularities in pre-installed passwords are found. • No common strings or other common patterns in pre-installed passwords are found. • The generation mechanisms for pre-installed passwords do not induce passwords, that are related in an obvious way to public information. • The generation mechanisms for pre-installed passwords are considered appropriate in terms of complexity. • For each pre-installed password, there is no evidence that it was generated in a way different from the method outlined in the CTIF.

MCMC MTSFB TC G050:2025

Table 2. TSO-1 - No universal default passwords (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (8)	6.1 No Universal Default Passwords	c) Authentication mechanisms used to authenticate users against a device should use best-practice cryptography, appropriate to the properties of the technology, risk and usage. Refer to the authentication mechanism in the corresponding CTIF. The "Cryptographic Details" are provided by the SO based on the reference catalogue used.	CTIF 1-AuthMech	<ul style="list-style-type: none"> The security guarantees are appropriate for the use case of user authentication. The mechanism is appropriate to achieve the security guarantees for the use case. All cryptographic details used are considered best practice for the use case. All cryptographic details used are not known to be vulnerable to feasible attacks concerning the desired security property.
MC (8)		d) Where a user can authenticate against a device, the device should provide to the user or an administrator a simple and workable mechanism to change the authentication value used.	CTIF 1- AuthMech	<ul style="list-style-type: none"> For all user-based authentication mechanisms the published resource describes how to change the authentication value with a simple mechanism. All mechanisms for the user to change authentication values for user authentication mechanisms work as described.
MC (5)		e) When the device is not a constrained device, it should have a mechanism available which makes brute-force attacks on authentication mechanisms via network interfaces impracticable.	CTIF 1- AuthMech	<ul style="list-style-type: none"> The documented mechanisms make brute force attacks via network interfaces impracticable. Every discovered network-based authentication mechanism is documented in the CTIF; and For all authentication mechanism via network interfaces there is no indication that the implementation of brute force prevention differs from its CTIF documentation.

6.2 TSO-2 - Managing reports of vulnerabilities

The objective of this assessment is to determine if access to the publication, as outlined in "Publication of Vulnerability Disclosure Policy" within CTIF 2-UserInfo, is made publicly available to everyone. A website of the manufacturer is sufficient. Table 3 below outlines the assessment procedure and assignment verdicts for TSO-2.

Table 3. TSO-2 - Managing reports of vulnerabilities

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.2.1 Disclosure policy publicly available	a) The TL should check whether the vulnerability disclosure policy is publicly accessible as described in "Publication of Vulnerability Disclosure Policy" in the corresponding CTIF.	CTIF 2-UserInfo.	The publication of the vulnerability disclosure policy is available for anybody
		b) The TL should check whether The TL shall functionally check whether the vulnerability disclosure policy is publicly accessible as described in "Publication of Vulnerability Disclosure Policy" in IXIT 2-UserInfo.	CTIF 2-UserInfo.	The vulnerability disclosure policy is publicly accessible
		c) The TL should check whether the policy contains contact information and information on timelines regarding acknowledgement of receipt and status updates.	N/A	The vulnerability disclosure policy contains contact information and information on timelines regarding acknowledgement of receipt and status updates
R	6.2.2 Disclosed vulnerabilities rectification time	d) The TL should assess whether the "Action" and the "Time Frame" of each disclosed vulnerability in the corresponding CTIF(i) facilitate that vulnerabilities are acted on in a timely manner under consideration of the vulnerability disclosure policy according to "Publication of Vulnerability Disclosure Policy" in the corresponding CTIF(ii).	i) CTIF 3-VulnTypes ii) CTIF 2-UserInfo	There is no indication that any described kind of vulnerability is not acted on timely;
		e) The TL should check whether "Confirmation of Vulnerability Actions" in the corresponding CTIF states a confirmation.	CTIF 4-Conf	A confirmation for the implementation is given.

MCMC MTSFB TC G050:2025

Table 3. TSO-2 - Managing reports of vulnerabilities *(continued)*

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.2.3 Vulnerabilities Monitoring	a) The TL should assess whether the way of continuously monitoring for security vulnerabilities documented in the corresponding CTIF is suited to systematically gather information about security vulnerabilities that potentially can affect the DUT.	CTIF 5-VulnMon	The described way is suited for continuously monitoring for security vulnerabilities;
		b) The TL should assess whether the way of identifying security vulnerabilities documented in the corresponding CTIF is suited to determine if and how a security vulnerability can affect the DUT.	CTIF 5-VulnMon	The described way is suited for identifying security vulnerabilities;
		c) The TL should assess whether the way of rectifying security vulnerabilities documented in the corresponding CTIF is suited to address and mitigate the susceptibility of a DUT against a security vulnerability.	CTIF 5-VulnMon	The described way is suited for rectifying security vulnerabilities;
		d) The TL should check whether "Confirmation of Vulnerability Monitoring" in the corresponding CTIF states a confirmation.	CTIF 4-Conf	A confirmation for the implementation is given.

6.3 TSO-3 - Keep software updated

This TSO handles the updatability of each software components except software updates that are beyond practicability or absent for a security reason. It assesses the updatability of software components concerning the absence of software updates and the update mechanisms. Table 4 below outlines the assessment procedure and assignment verdicts for TSO-3.

NOTE: Clause 6.3.3 to 6.3.12 is dependent upon an update mechanism being implemented, as per Clause 6.3.1 or 6.3.2.

Table 4. TSO-3 - Keep software updated

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.3.1 Updating software components	a) For each software component in the corresponding CTIF with an empty list in "Update Mechanism", the TL should assess whether the implementation of software updates is beyond practicability or for a security reason as described in the justification for the absence of software updates.	CTIF 6-SoftComp	For all software components without the ability for software updates, a software update is not possible for practicability reasons or security reasons
		b) The TL should apply all test units as specified in the Test case 6.3.2(a) to every referenced "Update Mechanism" in the corresponding CTIF.	CTIF 6-SoftComp	No update mechanism can be misused by an attacker.
		c) The TL should apply all test units as specified in the Test case 6.3.2(b) to every referenced "Update Mechanism" in the corresponding CTIF.	CTIF 6-SoftComp	There is no indication that a misuse of any update mechanism is possible.
MC (5)	6.3.2 Secure installation of updates	a) For each update mechanism in the corresponding CTIF, the TL should assess whether the design of the update mechanism prevents misuse from an attacker according to the "Security Guarantees", the corresponding "Description", "Cryptographic Details" and "Initiation and Interaction".	CTIF 7-UpdMech	The update mechanism of the DUT cannot be misused by an attacker.
		b) For each update mechanism in the corresponding CTIF, the TL should devise functional attacks to misuse the update mechanism based on the "Description".	CTIF 7-UpdMech	There is no indication that a misuse of one update mechanism of the DUT is possible.

MCMC MTSFB TC G050:2025

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (5)	6.3.2 Secure installation of updates	c) The TL should attempt to misuse each update mechanism on the base of the devised adverse actions and assess whether the design of the mechanism (see "Description", the "Cryptographic Details" and "Initiation and Interaction") effectively prevents the misuse of software updates as described in the "Security Guarantees".	CTIF 7-UpdMech	There is no indication that a misuse of one update mechanism of the DUT is possible.
MC (12)	6.3.3 Simple update	a) For each software component in the corresponding CTIF(i), the TL should assess whether at least one "Update Mechanism" is described, which is simple for the user to apply according to "Initiation and Interaction" in the corresponding CTIF(ii) based on the following factors: <ul style="list-style-type: none"> • automatically applied without requiring any user interaction; or • initiated via an associated service; or • initiated via a web interface on the device; or • any approach for the user with limited technical knowledge. 	i) CTIF 6-SoftCom ii) CTIF 7-UpdMech	Each software component is covered by at least one update mechanism, which is simple for the user to apply.
RC (12)	6.3.4 Automatic mechanisms for software updates	a) The TL should evaluate if each software component in the corresponding CTIF(i) has an "Update Mechanism" described in the corresponding CTIF(ii) that allows updates without user interaction for both "Initiation and Interaction" and "Update Checking".	i) CTIF 6-SoftCom ii) CTIF 7-UpdMech	Each software component is covered by at least one update mechanism that does not require any user interaction for performing an update and for checking the availability of an update

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (12)	6.3.4 Automatic mechanisms for software updates	b) The TL should verify if any automatic mechanisms are enabled by default for each software components in the corresponding CTIF(i) covered by an "Update Mechanism" in corresponding CTIF(ii) with the capability to configure the automation based on "Configuration".	i) CTIF 6-SoftCom ii) CTIF 7-UpdMech	For each software component covered by a configurable update mechanism at least one of the automatic mechanisms is enabled by default.
RC (12)	6.3.5 Periodic security updates	a) For each software component in the corresponding CTIF(i), the TL should assess whether at least one "Update Mechanism" is described in corresponding CTIF(ii), that checks the availability of security updates according to the schedule for querying for security updates in "Update Checking": <ul style="list-style-type: none"> • after initialization of the DUT; and • periodically. 	i) CTIF 6-SoftCom ii) CTIF 7-UpdMech	<ul style="list-style-type: none"> • The checking of the availability of software updates is triggered by the DUT itself; • The availability of software updates is checked after initialization of the DUT; and • The availability of software updates is checked periodically.
RC (9,12)	6.3.6 Automatic updates	a) The TL should identify and functionality assess all automatic update mechanisms in the corresponding CTIF by assessing whether the mechanism allows the performance of updates without requiring any user interaction according to "Initiation and Interaction".	CTIF 7-UpdMech	<ul style="list-style-type: none"> • The DUT supports automatic updates and the configuration for all update mechanisms the user is provided with the ability to enable, disable or postpone automatic installation of security updates and automatic updates are enabled in the initialized state; or • The DUT does not support automatic updates;
		b) For each update mechanism in the corresponding CTIF that provides automatic software updates, the TL should check and perform modification of the configuration whether it provides the user with the ability to enable, disable or postpone the automatic installation of security updates according to "Configuration" in the corresponding CTIF.	CTIF 7-UpdMech	

MCMC MTSFB TC G050:2025

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (9,12)	6.3.6 Automatic updates	c) For each update mechanism in the corresponding CTIF that provides automatic software updates, the TL should check whether automatic software updates are enabled in the initialized state according to "Configuration".	CTIF 7-UpdMech	<ul style="list-style-type: none"> The DUT supports automatic updates and the configuration for all update mechanisms the user is provided with the ability to enable, disable or postpone automatic installation of security updates and automatic updates are enabled in the initialized state; or The DUT does not support automatic updates;
		d) For each update mechanism in the corresponding CTIF that provides update notifications according to "User Notification" the TL should check and perform modification whether it provides the user with the ability to enable, disable or postpone update notifications according to "Configuration" in the corresponding CTIF.	CTIF 7-UpdMech	<ul style="list-style-type: none"> The DUT supports update notifications and configuration for all update mechanisms the user is provided with the ability to enable, disable or postpone update notifications and update notifications are enabled in the initialized state; or The DUT does not support update notifications.
		e) For each update mechanism in the corresponding CTIF that provides update notifications according to "User Notification", the TL should check functionality assess whether update notifications are enabled in the initialized state according to "Configuration".	CTIF 7-UpdMech	
MC (12)	6.3.7 Secure update mechanism	a) For each update mechanism in corresponding CTIF, the TL should assess whether the "Security Guarantees" are appropriate for the use case of secure updates, at least integrity and authenticity are required to be fulfilled.	CTIF 7-UpdMech	The security guarantees are appropriate for the use case of secure updates.
		b) For each update mechanism in corresponding CTIF, the TL should assess whether the mechanism according to "Description" is appropriate to achieve the "Security Guarantees".	CTIF 7-UpdMech	The mechanism is appropriate to achieve the security guarantees with respect to the use case

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (12)	6.3.7 Secure update mechanism	<p>c) For each update mechanism in the corresponding CTIF, the TL should assess whether the "Cryptographic Details" are considered as best practice cryptography for the use case of secure updates based on a reference catalogue. If "Cryptographic Details" are not included in a reference catalogue for the corresponding use case (e.g. novel cryptography), the SO should provide evidences, e.g. a risk analysis, to justify the cryptography is appropriate as best practice for the use case. In such cases the TL should assess whether the evidence is appropriate and reliable for the use case.</p> <p>General reference catalogues of best practice cryptography are available, for example:</p> <ul style="list-style-type: none"> • AKSA MySEAL • SOGIS Agreed Cryptographic Mechanisms 	CTIF 7-UpdMech	All used cryptographic details are considered as best practice for the use case.
		<p>d) For each update mechanism in corresponding CTIF, the TL should assess whether the "Cryptographic Details" are not known to be vulnerable to a feasible attack for the desired security property on the base of the "Security Guarantees" by reference to competent cryptanalytic reports.</p>	CTIF 7-UpdMech	All used cryptographic details are not known to be vulnerable to a feasible attack for the desired security property.
MC (12)	6.3.8 Timeliness of security updates	<p>a) The TL should assess whether the "Description" and the "Time Frame" of each security update procedure in corresponding CTIF facilitate that security updates are deployed in a timely manner.</p>	CTIF 8-UpdProc	There is an indication that the described management procedure allows a timely deployment of security updates.

MCMC MTSFB TC G050:2025

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (12)	6.3.8 Timeliness of security updates	b) The TL should check whether "Confirmation of Update Procedures" in the corresponding CTIF states a confirmation.	CTIF 4-Conf	A confirmation for the implementation is given
RC (12)	6.3.9 Authenticity and integrity verification	a) For each update mechanism in corresponding CTIF, the TL should assess whether the authenticity of software updates is suitably verified according to "Security Guarantees" and the corresponding "Cryptographic Details", including, in particular, the originality of the software update in regard to its source (manufacturer) and target (DUT) prior to the installation.	CTIF 7-UpdMech	Each update mechanism is effective for the verification of authenticity of software updates.
		b) For each update mechanism in corresponding CTIF, the TL should assess whether the integrity of software updates is suitably verified according to "Security Guarantees" and the corresponding "Cryptographic Details".	CTIF 7-UpdMech	Each update mechanism is effective for the verification of integrity of software updates.
		c) For each update mechanism in corresponding CTIF, the TL should check whether the authenticity AND the integrity verification is performed by the DUT itself according to "Security Guarantees".	CTIF 7-UpdMech	The verification of authenticity AND integrity of software updates is performed by the DUT itself.
MC (11,12)	6.3.10 Software updates network interface	a) The TL should apply the test units a-b as specified in the Clause 6.3.9.2.	CTIF 7-UpdMec	<ul style="list-style-type: none"> • Each update mechanism is effective for the verification of authenticity of software updates; • Each update mechanism is effective for the verification of integrity of software updates; and • The verification of authenticity and integrity of software updates is based on a valid trust relationship.

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (11,12)	6.3.10 Software updates network interface	b) For each network-based update mechanism in corresponding CTIF, the TL should assess whether the verification of integrity and authenticity relies on a valid trust relationship according to "Description" and "Security Guarantees". A valid trust relationship includes: <ul style="list-style-type: none"> • authenticated communication channels; • presence on a network that requires the device to possess a critical security parameter or password to join; • digital signature verification of the update; • confirmation by the user; or • a comparable secure functionality. 	CTIF 7-UpdMech	<ul style="list-style-type: none"> • Each update mechanism is effective for the verification of authenticity of software updates; • Each update mechanism is effective for the verification of integrity of software updates; and • The verification of authenticity and integrity of software updates is based on a valid trust relationship.
		c) The TL should functionally assess whether update mechanisms that are not documented in CTIF 7-UpdMech are available via a network interface on the DUT.	CTIF 7-UpdMech	Every discovered network-based update mechanism is documented in the CTIF.
RC (12)	6.3.11 Software update risks mitigation	a) For each update mechanism in corresponding CTIF the TL should assess whether the method to inform the user about the availability of required security updates is recognizable and apparent according to "User Notification".	CTIF 7-UpdMech	The method to inform the user about required security updates is recognizable and apparent.
		b) For each update mechanism in corresponding CTIF the TL should assess whether the user notification on required security updates includes information about the risks mitigated by the update according to "User Notification".	CTIF 7-UpdMech	The notification on required security updates includes information about the risks mitigated by the update.

MCMC MTSFB TC G050:2025

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (12)	6.3.12 Software update disruption	a) The TL should check whether each update mechanism in corresponding CTIF supports user notification in case of disruptive software updates according to "User Notification" and it is indicated as realized on the DUT itself.	CTIF 7- UpdMech supports	<ul style="list-style-type: none"> The user is appropriately notified about the disruption of basic functioning during the software update; and The user notification is realized on the DUT itself.
M	6.3.13 Software update support	a) The TL should assess whether access to the "Publication of Support Period" in corresponding CTIF is understandable and comprehensible for a user with limited technical knowledge.	CTIF 2-UserInfo	The publication of software update support period is understandable and comprehensible for a user with limited technical knowledge.
		b) The TL should functionally check whether the user information on accessing the resource for publishing the defined support period according to "Publication of Support Period" in corresponding CTIF is provided as described.	CTIF 2-UserInfo	The access to the resource for publishing the defined support period to the user is provided as described in the CTIF.
		c) The TL should functionally check whether the resource for publishing the defined support period according to "Publication of Support Period" in corresponding CTIF is accessible without restrictions (like e.g. a registration prior to the access).	CTIF 2-UserInfo	The access to the resource for publishing the defined support period is unrestricted.
		d) The TL should functionally check whether the published support period according to "Publication of Support Period" in corresponding CTIF actually defines the support period with respect to the updateable software components as described in "Support Period" in corresponding CTIF.	CTIF 2-UserInfo	The defined support period is published.
RC (3,4)	6.3.14 Software update constraint	a) The TL should assess whether the access to the "Publication of Non-Updatable" and "Documentation of Replacement" in corresponding CTIF is understandable for a user with limited technical knowledge.	CTIF 2-UserInfo	The publication of the rationale for absence of updates and hardware replacement support is understandable for a user with limited technical knowledge.

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (3,4)	6.3.14 Software update constraint	b) The TL should functionally check whether the user information on accessing the resource for the rationale for absence of updates and publishing the hardware replacement support according to "Publication of Non-Updatable" and "Documentation of Replacement" in corresponding CTIF is provided as described.	CTIF 2-UserInfo	The access to the resource for publishing the rationale for absence of updates and hardware replacement support to the user is provided as described in the CTIF.
		c) The TL should functionally check whether the resource for publishing the rationale for absence of updates and hardware replacement support according to "Publication of Non-Updatable" and "Documentation of Replacement" in corresponding CTIF is accessible without restrictions (like e.g. a registration prior to the access).	CTIF 2-UserInfo	The access to the resource for publishing the rationale for absence of updates and hardware replacement support is unrestricted.
		d) The TL should functionally check whether the published rationale for absence of updates according to "Publication of Non-Updatable" in corresponding CTIF contains the rationale for the absence of software updates.	CTIF 2-UserInfo	The rationale for the absence of software updates is published.
		e) The TL should functionally check whether the published hardware replacement support according to "Documentation of Replacement" in corresponding CTIF contains the hardware replacement plan in terms of the period and method of hardware replacement support.	CTIF 2-UserInfo	The period and method of hardware replacement support is published.

MCMC MTSFB TC G050:2025

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (3,4)	6.3.14 Software update constraint	f) The TL should functionally check whether the published rationale for absence of updates according to "Publication of Non-Updatable" in corresponding CTIF contains a defined support period.	CTIF 2-UserInfo	A support period is published.
RC (3,4)	6.3.15 Isolable constrained devices product	a) The TL should assess whether the described method in "Isolation" in corresponding CTIF is suitable to isolate the IoT product, i.e. to remove the IoT product from the network it is connected to, or to place the IoT product in a self-contained environment.	CTIF 9-ReplSup	The described method is suited for the isolation of the IoT product.
		b) The TL should assess whether the described method in "Hardware Replacement" in corresponding CTIF is suitable to be able to replace the hardware.	CTIF 9-ReplSup	The described method is suited for the replacement of the hardware.
		c) The TL should set up the IoT product in the intended environment. (Refer to clause 4.7b)	N/A	<ul style="list-style-type: none"> The IoT product can be isolated successfully according to the described method for isolation; and The hardware can be replaced successfully according to the described method for hardware replacement.
		d) The TL should perform the method described in "Isolation" in corresponding CTIF in order to isolate the IoT product, i.e. to remove the IoT product from the network it is connected to, or to place the IoT product in a self-contained environment, as appropriate.	CTIF 9-ReplSup	The hardware can be replaced successfully according to the described method for hardware replacement.

Table 4. TSO-3 - Keep software updated (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (3,4)	6.3.15 Isolable constrained devices product	e) The TL should functionally assess whether on the isolated IoT product: <ul style="list-style-type: none"> in case of removing the IoT product from the network connection: any functionality loss caused is related only to that connectivity and not to the main function of the DUT; or in case of placing the IoT product in a self-contained environment with other devices: the integrity of devices within that environment is ensured. 	N/A	The hardware can be replaced successfully according to the described method for hardware replacement.
		f) The TL should perform the method described in "Hardware Replacement" in corresponding CTIF in order to replace the hardware in the intended environment.	CTIF 9-ReplSup	
		g) The TL should functionally assess whether the connectivity and associated functionality can be regained on the replaced DUT.	N/A	
M	6.3.16 Recognisable model designation	a) The TL should assess whether the model designation of the DUT can be obtained in a clearly recognizable way, either by labelling on the DUT or via a physical interface according to "Model Designation" in corresponding CTIF.	CTIF 2-UserInfo	The model designation of the DUT can be obtained clearly recognizable by labelling on the DUT or via a physical interface.
		b) The TL should functionally check whether the model designation of the DUT can be obtained applying the described way of recognition in "Model Designation" in corresponding CTIF.	CTIF 2-UserInfo	The model designation of the DUT can be extracted according to the described way of recognition.

MCMC MTSFB TC G050:2025

Table 4. TSO-3 - Keep software updated (concluded)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.3.16 Recognisable model designation	c) The TL should functionally assess whether the obtained model designation is available in simple text and corresponds with the expected model designation described in "Model Designation" in corresponding CTIF.	CTIF 2-UserInfo	<ul style="list-style-type: none"> The model designation is available in simple text; and The model designation is corresponding with the expected model designation according to the CTIF.

6.4 TSO-4 - Securing sensitive security parameters

This assessment is crucial for ensuring the robust security of IoT devices. By verifying the secure storage and management of sensitive security parameters, resisting tampering of unique device identities, avoiding hard-coded credentials, and implementing unique critical security parameters, the assessment aims to protect devices from unauthorized access and various types of attacks. These measures will significantly enhance the overall security and reliability of IoT devices, safeguarding user data and maintaining the integrity of device operations. Table 5 below outlines the assessment procedure and assignment verdicts for TSO-4.

Table 5. TSO-4 - Securing sensitive security parameters

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (14)	6.4.1 Storing sensitive security parameters	a) The TL should assess whether the declaration in "Type" of each sensitive security parameter provided in the corresponding CTIF is consistent with the "Description".	CTIF 10-SecParam	For every sensitive security parameter, the declaration is consistent with its description.
		b) The TL should assess whether the "Security Guarantees" of each sensitive security parameter provided in corresponding CTIF matches at least the protection needs indicated by "Type".	CTIF 10-SecParam	For every sensitive security parameter, the claimed security guarantees match their minimal protection needs.
		c) The TL should assess whether the "Protection Scheme" of each sensitive security parameter provided in corresponding CTIF provides the claimed "Security Guarantees".	CTIF 10-SecParam	Every sensitive security parameter has a suitable protection mechanism for the claimed security guarantees.

Table 5. TSO-4 - Securing sensitive security parameters (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (14)	6.4.1 Storing sensitive security parameters	d) The TL should assess the completeness of the sensitive security parameters in corresponding CTIF by considering indications for sensitive security parameters in the provided information in all other CTIFs.	CTIF 10-SecParam	There is no indication, that the listed sensitive security parameters are incomplete.
		e) The TL should functionally assess whether for all sensitive security parameters provided in corresponding CTIF "Protection Scheme" is implemented according to the CTIF documentation.	CTIF 10-SecParam	For every sensitive security parameter there is no indication that the implementation of the corresponding protection scheme differs from its CTIF documentation.
MC (10)	6.4.2 Hard-coded unique device identity	a) The TL should check whether for each sensitive security parameter in corresponding CTIF where the "Description" indicates that it is used as an hard-coded identity, a corresponding explicit statement is provided.	CTIF 10-SecParam	There is no indication that any hard-coded identity is not documented as such.
		b) The TL should assess whether for each hard-coded identity as indicated in "Description" in corresponding CTIF the corresponding "Security Guarantees" provide tamper-resistance.	CTIF 10-SecParam	For all hard-coded identities the security guarantee includes tamper-resistance.
		c) The TL should assess whether the "Protection Scheme" of each hard-coded identity as indicated in "Description" in corresponding CTIF provides the claimed "Security Guarantees" with respect to tamper-resistance.	CTIF 10-SecParam	Every hard-coded identity has a suitable protection mechanism for tamper-resistance
		d) The TL should functionally assess whether each hard-coded identity as indicated in "Description" in corresponding CTIF the "Protection Scheme" with respect to tamper-resistance is implemented according to the CTIF documentation.	CTIF 10-SecParam	For every hard-coded identity, there is no indication that the implementation of any protection scheme with respect to tamper-resistance differs from its CTIF documentation.

MCMC MTSFB TC G050:2025

Table 5. TSO-4 - Securing sensitive security parameters (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.4.3 Hard-coded critical security parameters	a) The TL should check whether for all critical security parameters provided in corresponding CTIF where "Provisioning Mechanism" indicates that it is hard coded in device software source code, the fact is reflected in "Description".	CTIF 10-SecParam	There is no indication that any critical security parameter hard-coded in device software source code is not documented as such.
		b) The TL should assess whether for all critical security parameters in corresponding CTIF, which are hard coded in device software source code according to "Description", the corresponding "Provisioning Mechanism" ensures that it is not used during the operation of the DUT.	CTIF 10-SecParam	The DUT meets the specific requirements outlined in the assessment criteria.
		c) The TL should functionally assess whether for all critical security parameters hard-coded in device software source code documented in "Description" of corresponding CTIF, the "Provisioning Mechanism" is indeed applied during the operation of the DUT.	CTIF 10-SecParam	The DUT meets the specific requirements outlined in the assessment criteria.
MC (15)	6.4.4 Unique critical security parameters	a) The TL should check whether all critical security parameter provided in corresponding CTIF, where "Description" indicates that the critical security parameters are used for integrity and authenticity checks of software updates or for protection of communication with associated services are documented as such in "Generation Mechanism".	CTIF 10-SecParam	The DUT meets the specific requirements outlined in the assessment criteria.

Table 5. TSO-4 - Securing sensitive security parameters (concluded)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (15)	6.4.4 Unique critical security parameters	b) The TL should assess for all critical security parameters provided in corresponding CTIF, whether the "Generation Mechanism" ensures that the critical security parameter is unique per device and produced with a mechanism that reduces the risk of automated attacks against classes of devices.	CTIF 10-SecParam	The DUT meets the specific requirements outlined in the assessment criteria.

6.5 TSO-5 - Communicate securely

The assessment aims to ensure secure communication in consumer IoT devices by verifying the use of best practice cryptography, evaluating and updating cryptographic implementations, ensuring authenticated access to device functionality and security-relevant configurations, encrypting critical security parameters in transit, protecting their confidentiality, and confirming that secure management processes are followed by the manufacturer. Table 6 below outlines the assessment procedure and assignment verdicts for TSO-5.

Table 6. TSO-5 - Communicate securely

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.5.1 Cryptography for secure communication	a) For each communication mechanism in corresponding CTIF, the TL should assess whether the "Security Guarantees" are appropriate for the use case of the communication.	CTIF 11-ComMech	The security guarantees are adequate to meet the secure communication.
		b) For each communication mechanism in corresponding CTIF, the TL should assess whether the mechanism according to "Description" is appropriate to achieve the "Security Guarantees".	CTIF 11-ComMech	The communication mechanism is adequate to meet the security guarantees.
		c) For each communication mechanism in its corresponding CTIF, the TL should evaluate whether the "Cryptographic Details": <ul style="list-style-type: none"> • Follow best practice cryptography suitable for secure communication, as outlined in a standard reference, e.g. AKSA MySEAL: Deterministic Random Bit Generator; or 	CTIF 11-ComMech	All used cryptographic details are considered as best practice.

MCMC MTSFB TC G050:2025

Table 5. TSO-5 - Communicate securely (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.5.1 Cryptography for secure communication	<ul style="list-style-type: none"> If the "Cryptographic Details" are not listed in a reference for that use case (e.g., using new cryptography), the SO must provide evidence such as a risk analysis to justify its suitability as best practice. In such cases, the TL evaluates the adequacy and reliability of the evidence for the specific use case. 	CTIF 11-ComMech	All used cryptographic details are considered as best practice.
		d) For each communication mechanism in the corresponding CTIF, the TL should evaluate whether the "Cryptographic Details" are resilient against known feasible attacks that could compromise the desired security properties, based on "Security Guarantees" referenced from reliable cryptanalytic reports.	CTIF 11-ComMech	All cryptographic details used in the communication mechanism are resilient to feasible attack of the desired security properties.
		e) For each communication mechanism in the corresponding CTIF, the TL should functionally evaluate whether the described "Cryptographic Details" are implemented by the DUT.	CTIF 11-ComMech	All cryptographic settings meet the CTIF documentation.
R	6.5.2 Cryptography for consumer IoT device	a) For each implementation in corresponding CTIF, the TL should check whether it has been reviewed or evaluated according to "Review/Evaluation Method".	CTIF 12-NetSecImpl	All implementations of network and security functionalities are reviewed or evaluated.
		b) For each review or evaluation method associated to an implementation in corresponding CTIF, the TL should assess whether the "Review/Evaluation Method" and its "Report" covers the related implementation scope as described in "Description".	CTIF 12-NetSecImpl	All review and evaluation methods cover the scope of the related implementation.

Table 5. TSO-5 - Communicate securely (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.5.2 Cryptography for consumer IoT device	c) For each implementation associated with a review or evaluation method in corresponding CTIF, the TL should functionally check whether the identification of the implementation (name and version) on the DUT matches the identification of the implementation provided in the "Report".	CTIF 12-NetSecImpl	<ul style="list-style-type: none"> The name and version of every provided implementation matches the name and version provided in the related report; or The necessary information is not obtainable, because the DUT does not provide any information on the implementation name and version.
R	6.5.3 Updateable cryptographic algorithms and primitives	a) For each software component in corresponding CTIF indicating "Cryptographic Usage", the TL should check whether an "Update Mechanism" to update the software component is referenced.	CTIF 6-SoftComp	For every software component indicating cryptographic usage an update mechanism is referenced.
		b) For each software component in corresponding CTIF indicating "Cryptographic Usage", the TL should check whether side effects of updating those algorithms and primitives are considered by the manufacturer.	CTIF 6-SoftComp	Side effects of updating those algorithms and primitives are considered by the manufacturer.
RC (16)	6.5.4 Access to device functionality	a) For each device functionality in corresponding CTIF indicated as accessible via network interface in the initialized state according to "Description", the TL should check whether there is at least one "Authentication Mechanism" referenced.	CTIF 13-SoftServ	At least one authentication mechanism is referenced for every device functionality accessible via network interface in the initialized state.
		b) For each "Authentication Mechanism" referenced in corresponding CTIF(i), the TL should assess whether the authentication mechanism described in corresponding CTIF(ii) allows to discriminate between multiple authentication subjects and can reject authentication attempts based on invalid identities and/or authentication factors.	i) CTIF 13-SoftServ ii) CTIF 1-AuthMech	Every authentication mechanism allows to discriminate between multiple authentication subjects and to reject authentication attempts based on invalid identities and/or authentication factors. Every authorization mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects.

MCMC MTSFB TC G050:2025

Table 5. TSO-5 - Communicate securely (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (16)	6.5.4 Access to device functionality	c) For each "Authentication Mechanism" referenced in corresponding CTIF(i), the TL should assess whether the means protecting the authentication mechanism in "Cryptographic Details" in corresponding CTIF(ii) provide the "Security Guarantees" identified for the mechanism and are resistant to attempts at compromising the mechanism.	i) CTIF 13-SoftServ ii) CTIF 1-AuthMech	The means used to protect an authentication mechanism provide the expected security guarantees and are resistant at attempts to compromise the mechanism.
		d) For each "Authentication Mechanism" referenced in corresponding CTIF(i), the TL should assess whether the authorization process described in "Description" in corresponding CTIF(ii) allows authenticated subjects with proper access rights to be granted access and denies authenticated subjects with inadequate access rights or unauthenticated subjects to be granted access.	i) CTIF 13-SoftServ ii) CTIF 1-AuthMech	Every authorization mechanism allows access to authenticated subjects with proper access rights.
		e) For each "Authentication Mechanism" referenced in corresponding CTIF, the TL should functionally assess whether an unauthenticated subject and a subject with invalid identity or credentials and an authenticated subject without appropriate access rights cannot access the device functionality in the initialized state.	CTIF 13-SoftServ	An unauthenticated subject, a subject with invalid identity or invalid credentials and an authenticated subject without appropriate access rights cannot access the functionality in the initialized state.
		f) For each "Authentication Mechanism" referenced in corresponding CTIF, the TL should functionally assess whether an authenticated subject with appropriate access rights can access the device functionality in the initialized state.	CTIF 13-SoftServ	An authenticated subject with appropriate access rights can access the device functionality in the initialized state.

Table 5. TSO-5 - Communicate securely (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (16)	6.5.4 Access to device functionality	g) For each "Authentication Mechanism" referenced in corresponding CTIF(i), the TL should functionally assess whether the protection of the authentication mechanism conforms to the description in "Security Guarantees" and "Cryptographic Details" in corresponding CTIF(ii).	i) CTIF 13-SoftServ ii) CTIF 1-AuthMech	There is no indication that the mechanism to secure the authentication differs from its CTIF documentation.
MC (17)	6.5.5 Access to security-relevant configurations	a) The TL should apply all test units as specified in the Test case 5.5-4-1 for all states of the DUT with restriction to the functionalities that allow security-relevant changes according to "Allows Configuration" in Corresponding CTIF. Network service protocols that are relied upon by the DUT and where the manufacturer cannot guarantee what configuration will be required for the DUT to operate are excluded.	CTIF 13-SoftServ	<ul style="list-style-type: none"> At least one authentication mechanism is referenced for every device functionality accessible via network interface that allows security-relevant changes; Every authentication mechanism allows to discriminate between multiple authentication subjects and to reject authentication attempts based on invalid identities and/or authentication factors; The means used to protect an authentication mechanism provide the expected security guarantees and are resistant at attempts to compromise the mechanism; Every authorisation mechanism allows access to authenticated subjects with proper access rights; and Every authorization mechanism denies access to authenticated subjects with inadequate access rights and to unauthenticated subjects.
		b) The TL should apply all test units as specified in the Test case 5.5-4-2 for all states of the DUT with restriction to the functionalities that allow security-relevant changes according to "Allows Configuration" in Corresponding CTIF. Network service protocols that are relied upon by the DUT and where the manufacturer cannot guarantee what configuration will be required for the DUT to operate are excluded.	CTIF 13-SoftServ	<ul style="list-style-type: none"> An unauthenticated subject, a subject with invalid identity or invalid credentials and an authenticated subject without appropriate access rights cannot access the functionality; and An authenticated subject with appropriate access rights can access the device functionality.

MCMC MTSFB TC G050:2025

Table 5. TSO-5 - Communicate securely (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (17)	6.5.5 Access to security-relevant configurations	c) The TL should functionally assess whether communication mechanisms that are not documented in Corresponding CTIF are available via a network interface on the DUT.	CTIF 11-ComMech	<ul style="list-style-type: none"> There is no indication that the mechanism to secure the authentication differs from its CTIF documentation; and Every discovered network-based communication mechanism is documented in the CTIF.
RC (18)	6.5.6 Encryption of critical security parameters	a) For all "Communication Mechanisms" in corresponding CTIF(i) referenced in any critical security parameter in corresponding CTIF(ii), the TL should apply all test units as specified in the Test case 5.5-1-1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.	i) CTIF 11-ComMech ii) CTIF 10-SecParam	<ul style="list-style-type: none"> The security guarantees are appropriate for the use case of secure communication; The mechanism is appropriate to achieve the security guarantees with respect to the use case; All used cryptographic details are considered as best practice for the use case; and All used cryptographic details are not known to be vulnerable to a feasible attack.
		b) For all "Communication Mechanisms" in corresponding CTIF(i) referenced in any critical security parameter in corresponding CTIF(ii), the TL should apply all test units as specified in the Test case 5.5-1-2.	i) CTIF 11-ComMech ii) CTIF 10-SecParam	There is no indication that any used cryptographic setting differs from its CTIF documentation.
MC (19)	6.5.7 Protection of critical security parameters	a) For all "Communication Mechanisms", that are remotely accessible according to their "Description" in corresponding CTIF(i) referenced in any critical security parameter in corresponding CTIF(ii), the TL should apply all test units as specified in the Test case 5.5-1-1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.	i) CTIF 11-ComMech ii) CTIF 10-SecParam	<ul style="list-style-type: none"> The security guarantees are appropriate for the use case of secure communication; The mechanism is appropriate to achieve the security guarantees with respect to the use case; All used cryptographic details are considered as best practice for the use case; and All used cryptographic details are not known to be vulnerable to a feasible attack.
		b) For all "Communication Mechanisms", that are remotely accessible according to their "Description" in corresponding CTIF(i) referenced in any critical security parameter in corresponding CTIF(ii), the TL should apply all test units as specified in the Test case 5.5-1-2.	i) CTIF 11-ComMech ii) CTIF 10-SecParam	There is no indication that any used cryptographic setting differs from its CTIF documentation.

Table 5. TSO-5 - Communicate securely (concluded)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (20)	6.5.8 Secure management process	a) The TL should assess whether the secure management of critical security parameters covers the whole life cycle of a critical security parameter considering its: <ul style="list-style-type: none"> • generation; • provisioning; • storage; • updates; • decommissioning, archival, and destruction; and • processes to handle the expiration and compromise. <p>All parameters above should according to the processes in corresponding CTIF.</p>	CTIF 14-SecMgmt	The secure management covers the whole life cycle of a critical security parameter according to its processes.
		b) The TL should check whether "Confirmation of Secure Management" in corresponding CTIF states a confirmation.	CTIF 4-Conf	A confirmation for the implementation is given

6.6 TSO-6 - Minimising attack surfaces

The objective of this assessment is to validate input data, as stipulated in Clause 6.6 of the MCMC MTSFB TC G044. The assessment aims to minimize attack surfaces in IoT devices by ensuring unused interfaces are disabled, limiting unauthenticated information disclosure, reducing exposure of physical interfaces, disabling accessible debug interfaces, enabling only necessary software services, minimizing code and privilege levels, implementing hardware-level access controls, and following secure software development processes. Table 7 below outlines the assessment procedure and assignment verdicts for TSO-6.

Table 7. TSO-6 - Minimising attack surfaces

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.6.1 Unused network and logical interfaces	a) a) For each network and logical interface in corresponding CTIF that is described as enabled according to "Status", the TL should assess whether the purpose of the interface in "Description" provides a valid justification for being enabled.	CTIF 15-Intf	For every network or logical interface that is marked as enabled in the CTIF documentation, there is a purpose that provides a valid justification for the interface to be enabled.

MCMC MTSFB TC G050:2025

Table 7. TSO-6 - Minimising attack surfaces (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
M	6.6.1 Unused network and logical interfaces	b) For each network and logical interface in corresponding CTIF, the TL should functionally check whether the status of the interface matches the "Status" in the CTIF documentation.	CTIF 15-Intf	Every documented network or logical interface that is marked as disabled in the CTIF documentation is found to be disabled or not accessible on the DUT.
		c) The TL should functionally assess whether network or logical interfaces that are not documented in corresponding CTIF are available via a network interface on the DUT.	CTIF 15-Intf	Every discovered network and logical interface is documented in the CTIF.
M	6.6.2 Minimise unauthenticated disclosure	a) For each network interface in corresponding CTIF, the TL should assess whether the "Disclosed Information" disclosed by the interface without authentication in the initialized state and indicated as not security-relevant, is however security-relevant.	CTIF 15-Intf	Every security-relevant information disclosed by the interface without authentication in the initialized state is documented as such.
		b) For each network interface in corresponding CTIF, the TL should assess whether the "Disclosed Information" disclosed by the interface without authentication in the initialized state and indicated as security-relevant, is necessary for the operation of the DUT.	CTIF 15-Intf	All security-relevant information disclosed by the interface without authentication in the initialized state is necessary for the operation of the DUT.
		c) For each network interface in corresponding CTIF, the TL should functionally assess whether security-relevant information can be observed from the interface without authentication in the initialized state, that is not described in "Disclosed Information".	CTIF 15-Intf	For every network interface, only security-relevant information can be observed that is described in the CTIF documentation.
R	6.6.3 Exposure of physical interfaces	a) For each physical interface in corresponding CTIF that does not require exposure according to "Description", the TL should assess whether the protection means of the interface in "Protection" include protection by the device casing or similar measures.	CTIF 15-Intf	For every physical interface that does not require exposure, the protection means of the interface includes protection by the device casing or similar measures.

Table 7. TSO-6 - Minimising attack surfaces (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.6.3 Exposure of physical interfaces	b) For each air interface in corresponding CTIF that does not require exposure according to "Description", the TL should check whether the interface is disabled according to "Status".	CTIF 15-Intf	For every air interface that does not require exposure, the interface is disabled.
		c) For each physical interface in corresponding CTIF that does not require permanent exposure according to "Description", the TL should check whether the interface is disabled according to "Status" for all periods in which the use of the interface is not required.	CTIF 15-Intf	For every physical interface that does not require permanent exposure, the interface is disabled for all periods in which the use of the interface is not required.
		d) For each physical interface identified on the DUT the TL should functionally check whether exposed physical interfaces on the DUT are contained in corresponding CTIF and described as required or intermittently required in "Description".	CTIF 15-Intf	All exposed physical interfaces on the DUT are described as "required" or "intermittently required" in the CTIF documentation.
		e) For each physical interface identified on the DUT that does not require exposure according to "Description" the TL should functionally assess whether physical interfaces on the DUT are protected by device casing or similar measures.	N/A	All physical interfaces that are identified as never requiring exposure in the CTIF documentation, the interface is protected by the device casing or similar measures.
		f) For each air interface identified on the DUT the TL should functionally check whether it is enabled or disabled as indicated in "Status" in corresponding CTIF.	CTIF 15-Intf	All air interfaces that are enabled on the DUT are marked as "required" or "intermittently required" in the CTIF documentation.
		g) For each physical interface identified on the DUT the TL should functionally assess whether the physical interfaces that are not permanently required are disabled for all periods in which the use of the interface is not required.	N/A	For all physical interfaces that are marked as "intermittently required" in the CTIF documentation, the interface is disabled for all periods in which the use of the interface is not required.

MCMC MTSFB TC G050:2025

Table 7. TSO-6 - Minimising attack surfaces *(continued)*

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (13)	6.6.4 Existence of debug interface	a) For each physical interface in corresponding CTIF that is described as an accessible debug interface according to "Debug Interface", the TL should assess whether the protection means for the interface in "Protection" include a software mechanism to disable the interface.	CTIF 15-Intf	For every accessible physical debug interface, there is a software mechanism described to disable the interface.
		b) For each physical interface in corresponding CTIF that is described as an accessible debug interface, that is not indicated as intermittently required according to "Description", the TL should check whether the interface is disabled permanently according to "Status".	CTIF 15-Intf	For every accessible physical debug interface that is not indicated as intermittently required, the interface is permanently disabled.
		c) For each physical interface in corresponding CTIF that is described as an accessible debug interface, that is indicated as intermittently required according to "Description", the TL should check whether the interface is disabled by default according to "Status".	CTIF 15-Intf	For every accessible physical debug interface that is indicated as intermittently required, the interface is disabled by default.
		d) For each accessible physical interface on the DUT indicated as "Debug Interface" in corresponding CTIF, the TL should functionally check whether the interface is disabled.	CTIF 15-Intf	Every accessible physical debug interface is disabled.
		e) For each accessible physical interface on the DUT the TL should functionally assess whether the interface can be used for debugging purposes although it is not indicated as "Debug Interface" in corresponding CTIF.	CTIF 15-Intf	Every physical debug interface is indicated as such in the CTIF.

Table 7. TSO-6 - Minimising attack surfaces (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.6.5 Enabling software services	For each software service in corresponding CTIF that is enabled by default according to "Status", the TL should assess whether the service is necessary for the intended use or operation of the DUT according to the purpose in "Description" and the "Justification" for enabling the service.	CTIF 13-SoftServ	For every enabled by default software service, the service is necessary for the intended use or operation of the DUT.
R	6.6.6 Minimise code	The TL should assess whether the code minimization techniques in corresponding CTIF are appropriate for reducing code to the necessary functionality.	CTIF 16-CodeMin	The described code minimization techniques are appropriate for reducing code to the necessary functionality.
R	6.6.7 Running software	The TL should assess whether all mechanisms to control privileges of software on the DUT in corresponding CTIF together facilitate the principles of separation of duty, need to know and minimization of privilege.	CTIF 17-PrivCtrl	The described privilege control mechanisms are adequate to facilitate the principles of separation of duty, need to know and minimization of privilege.
R	6.6.8 Hardware-level access control mechanism	a) For each hardware-level access control mechanism for memory in corresponding CTIF, the TL should assess whether the mechanism is implemented at the level of the hardware.	CTIF 18-AccCtrl	For every hardware-level access control mechanism for memory, the mechanism is implemented at the level of the hardware.
		b) For each hardware-level access control mechanism for memory in corresponding CTIF, the TL should assess whether the mechanism allows to control access to memory.	CTIF 18-AccCtrl	For every hardware-level access control mechanism for memory, the mechanism allows to control access to memory.

MCMC MTSFB TC G050:2025

Table 7. TSO-6 - Minimising attack surfaces (concluded)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.6.9 Development of software	a) The TL should assess whether the secure development of software covers: <ul style="list-style-type: none"> • security training of developers; • the requirement and design phases of the software; • secure coding techniques; • security tooling for the implementation phase; • security testing; • security review. • archival of assets and information relevant to maintaining security of the software; • secure deployment; and • handling of third-party software providers according to the processes in corresponding CTIF. 	CTIF 19-SecDev	<ul style="list-style-type: none"> • Security training of developers; • The requirement and design phases of the software; • Secure coding techniques; • Security tooling for the implementation phase; • Security testing; • Security reviews; • Archival of assets and information relevant to maintaining security of the software; • Secure deployment; and • If applicable, handling of third-party software providers;
		b) The TL should check whether "Confirmation of Secure Development" in corresponding CTIF states a confirmation.	CTIF 4-Conf	A confirmation for the implementation is given.

6.7 TSO-7 - Ensure software integrity

The objective of this assessment is to validate input data, as stipulated in Clause 6.7 of the MCMC MTSFB TC G044. The assessment aims to ensure software integrity in consumer IoT devices by verifying the implementation of secure boot mechanisms that check software integrity, and by confirming that the device can detect unauthorized software changes, alert users or administrators, and limit network connectivity to essential alerting functions. Table 8 below outlines the assessment procedure and assignment verdicts for TSO-7.

Table 8. TSO-7 - Ensure software integrity

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.7.1 Secure boot mechanisms	a) The TL should assess whether the "Security Guarantees" of each secure boot mechanism in corresponding CTIF provide at least verification of integrity and authenticity of device software.	CTIF 20-SecBoot	Every secure boot mechanism provides the security guarantees of integrity and authenticity of the device software.

Table 8. TSO-7 - Ensure software integrity (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.7.1 Secure boot mechanisms	b) The TL should assess whether for each secure boot mechanism in corresponding CTIF, the "Description" and corresponding "Detection Mechanisms" are suitable to provide the "Security Guarantees" it is used.	CTIF 20-SecBoot	Every secure boot mechanism and its detection mechanisms is suitable to provide the described security guarantee.
		c) The TL should functionally assess whether the verification of the device software is implemented according to the information in corresponding CTIF.	CTIF 20-SecBoot	There is no indication, that the implementation of any secure boot mechanism differs from its CTIF documentation.
R	6.7.2 Unauthorized change	a) The TL should assess whether the method for "User Notification" including its contained information is sufficient to inform the user and/or administrator about unauthorized changes in device software.	N/A	The described way of user notification is sufficient to inform the user and/or administrator about unauthorized changes in device software.
		b) The TL should assess whether every "Notification Functionality" in corresponding CTIF is necessary for the described method of "User Notification".	CTIF 20-SecBoot	Every described notification functionality is necessary for the user notification in case of detecting unauthorized software changes.
		c) The TL should functionally assess whether alerting takes place as described in "User Notification" in corresponding CTIF after the detection of an unauthorized change in device software.	CTIF 20-SecBoot	There is no indication that the implementation of any alerting mechanism of the DUT differs from its CTIF documentation.
		d) The TL should functionally assess whether the communication capabilities of the DUT to wider networks are restricted to the ones described in "Notification Functionality" in corresponding CTIF after the detection of an unauthorized change in device software.	CTIF 20-SecBoot	Only communication to wider networks is detected after detection of unauthorized changes, that is described as necessary.

MCMC MTSFB TC G050:2025

6.8 TSO-8 - Ensure secure personal data

The objective of this assessment is to validate input data, as stipulated in Clause 6.8 of the MCMC MTSFB TC G044. The assessment aims to ensure secure personal data in IoT devices by evaluating the protection of transiting personal data with best practice cryptography, safeguarding sensitive data with appropriate cryptographic methods, and verifying that all external sensing capabilities are clearly documented and accessible to users. Table 9 below outlines the assessment procedure and assignment verdicts for TSO-8.

Table 9. TSO-8 - Ensure secure personal data

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (21)	6.8.1 Confidentiality of transiting data	a) For all "Communication Mechanisms" in corresponding CTIF(i) referenced in any personal data in corresponding CTIF(ii), the TL should apply all test units as specified in the clause 6.5.1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.	i) CTIF 11-ComMec ii) CTIF 21-PersData	<ul style="list-style-type: none"> The security guarantees are appropriate for the use case of communicating personal data; The mechanism is appropriate to achieve the security guarantees with respect to the use case; All used cryptographic details are considered as best practice for the use case; and All used cryptographic details are not known to be vulnerable to a feasible attack.
		b) For all "Communication Mechanisms" in corresponding CTIF(i) referenced in any personal data in corresponding CTIF(ii), the TL should apply all test units as specified in the Test case 6.5-1(e).	i) CTIF 11-ComMec ii) CTIF 21-PersData	There is no indication that any used cryptographic setting differs from its CTIF documentation.
MC (22)	6.8.2 Confidentiality of sensitive data	ii) For all "Communication Mechanisms" in corresponding CTIF(i) referenced in any sensitive personal data in corresponding CTIF(ii) according to "Sensitive", where the communication partner is an associated service, the TL should apply all test units as specified in the Test case 6.5.1 with restriction, that at least the security guarantee of confidentiality is required to be fulfilled.	i) CTIF 11-ComMec ii) CTIF 21-PersData	<ul style="list-style-type: none"> The security guarantees are appropriate for the use case of communicating sensitive personal data between the device and an associated service; The mechanism is appropriate to achieve the security guarantees with respect to the use case; All used cryptographic details are considered as best practice for the use case; and All used cryptographic details are not known to be vulnerable to a feasible attack.
		iii) For all "Communication Mechanisms" in corresponding CTIF(i) referenced in any sensitive personal data in corresponding CTIF according to "Sensitive", where the communication partner is an associated service, the TL should apply all test units as specified in the Test case 6.5.1(e).	i) CTIF 11-ComMec ii) CTIF 21-PersData	There is no indication that any used cryptographic setting differs from its CTIF documentation.

Table 9. TSO-8 - Ensure secure personal data (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (23)	6.8.3 External sensing capabilities	a) The TL should functionally check whether the documentation of external sensing capabilities is accessible as documented in "Documentation of Sensors" in corresponding CTIF.	CTIF 2-UserInfo	The documentation is accessible according to the CTIF.
		b) The TL should functionally assess whether the documentation of external sensing capabilities as documented in "Documentation of Sensors" in corresponding CTIF is understandable for a user with limited technical knowledge.	CTIF 2-UserInfo	The documentation is understandable for a user with limited technical knowledge.
		c) The TL should functionally assess whether all obvious sensing capabilities of the DUT are documented in corresponding CTIF.	CTIF 22-ExtSens	Each obvious sensing capability of the DUT is documented for the user.

6.9 TSO-9 - Systems resilient to outages

The objective of this assessment is to validate input data, as stipulated in Clause 6.9 of the MCMC MTSFB TC G044. This assessment aims to evaluate the resilience of consumer IoT devices to data network and power outages by reviewing design integration, testing local functionality during network losses, ensuring clean recovery post-power restoration, verifying orderly network reconnection, and assessing measures against DDoS attacks and signalling storms. Additionally, it ensures that resilience measures are proportionate to usage and consider the broader impact on related systems and services. Table 10 below outlines the assessment procedure and assignment verdicts for TSO-9.

Table 10. TSO-9 - Systems resilient to outages

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.9.1 Building resilience	a) The TL should assess whether the combination of the resilience mechanisms in corresponding CTIF are appropriate to protect against network connectivity and power outages according to the "Security Guarantees".	CTIF 23-ResMech	The resilience mechanisms are appropriate to protect against network connectivity and power outages.
		b) For each resilience mechanism in corresponding CTIF the TL should assess whether the mechanism according to the "Description" is appropriate to achieve the "Security Guarantees".	CTIF 23-ResMech	Every resilience mechanism is appropriate to achieve its security guarantees.

MCMC MTSFB TC G050:2025

Table 10. TSO-9 - Systems resilient to outages (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.9.1 Building resilience	c) The TL should interrupt the DUT's connection to the network and functionally assess whether the resilience mechanisms operate as described in corresponding CTIF.	CTIF 23-ResMech	There is no indication that the operation of the resilience mechanisms during network connectivity and power outages differs from its CTIF documentation.
		d) The TL should interrupt the DUT's power supply and functionally assess whether the resilience mechanisms operate as described in corresponding CTIF.	CTIF 23-ResMech	
R	6.9.2 Remain functioning	a) The TL should apply all test units as specified in the Test case 6.9.1 for the resilience mechanisms in corresponding CTIF.	CTIF 23-ResMech	<ul style="list-style-type: none"> • The resilience mechanisms are appropriate to protect against network connectivity and power outages; and • Every resilience mechanism is appropriate to achieve its security guarantees.
		b) The TL should assess whether the resilience mechanisms in corresponding CTIF, protecting against network connectivity outages according to "Type" are appropriate to ensure, that the DUT remains operating and locally functional in the case of a loss of network connectivity.	CTIF 23-ResMech	The resilience mechanisms are appropriate to ensure that the DUT remains operating and locally functional in the case of a loss of network connectivity.
		c) The TL should assess whether the resilience mechanisms in corresponding CTIF protecting against power outages according to "Type" are appropriate to ensure, that the DUT resumes the connectivity and functionality after a loss of power in the same or improved state as before.	CTIF 23-ResMech	The resilience mechanisms are appropriate to ensure that the DUT recovers cleanly after a loss of power.

MCMC MTSFB TC G050:2025

Table 10. TSO-9 - Systems resilient to outages (concluded)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.9.2 Remain functioning	d) The TL should interrupt the DUT's connection to the network and functionally assess whether the resilience mechanisms operate as described in corresponding CTIF and the DUT remains operating and locally functional after the loss of network connectivity.	CTIF 23-ResMech	<ul style="list-style-type: none"> There is no indication that the operation of the resilience mechanisms during network connectivity or power outages differs from its CTIF documentation; There is no indication that the DUT does not remain operating and locally functional after the loss of network connectivity; and There is no indication that the DUT does not resume the connectivity and functionality after a loss of power in the same or improved state as before.
		e) The TL should interrupt the DUT's power supply and functionally assess whether the resilience mechanisms operate as described in corresponding CTIF and the DUT resumes the connectivity and functionality after a loss of power in the same or improved state as before.	CTIF 23-ResMech	
R	6.9.3 Connection to networks	a) For each communication mechanism in corresponding CTIF the TL should assess whether the "Resilience Measures" are appropriate to achieve a connection to a network in an orderly fashion taking the capability of the infrastructure into consideration.	CTIF 11-ComMech	Every communication mechanism provides appropriate measures to achieve a connection to a network in an orderly fashion
		b) For each communication mechanism in corresponding CTIF the TL should assess whether the "Resilience Measures" are appropriate to support the operation of a stable network taking the capability of the infrastructure into consideration.	CTIF 11-ComMech	Every communication mechanism provides appropriate measures to support the operation of a stable network.
		c) The TL should functionally assess whether the implemented "Resilience Measures" for each communication method in corresponding CTIF are implemented as described, especially considering the protection against simultaneous mass-reconnections.	CTIF 11-ComMech	There is no indication that the operation of any implemented resilience measure differs from its CTIF documentation.

MCMC MTSFB TC G050:2025

6.10 TSO-10 - Secure telemetry data

The objective of this assessment is securing telemetry data, as stipulated in Clause 6.10 of the MCMC MTSFB TC G044. The purpose of this assessment is to ensure that telemetry data collected from consumer IoT devices, such as usage and measurement data, is checked for security issues. By analyzing this data, the assessment aims to spot unusual activities early, reduce security risks, and quickly address any problems. This helps improve the overall security of IoT devices. Table 11 below outlines the assessment procedure and assignment verdicts for TSO-10.

Table 11. TSO-10 - Secure telemetry data

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (6)	6.10.1 Examine for security anomalies	a) The TL should check whether at least one "Security Examination" is provided in corresponding CTIF for examining for security anomalies.	CTIF 24-TelData	At least one security anomaly examination is provided.
		b) For each "Security Examination" of telemetry data in corresponding CTIF, the TL should assess whether the associated telemetry data in "Description" are suited for the described security examination and for examining the data for security anomalies.	CTIF 24-TelData	Each security anomaly examination is suited for examining the associated telemetry data for a security anomaly.

6.11 TSO-11 - Deleting user data

The objective of this assessment is deleting user data, as stipulated in Clause 6.11 of the MCMC MTSFB TC G044. This assessment is critical for verifying that IoT devices offer straightforward, secure, and compliant functionalities for deleting user data. By ensuring ease of data deletion, effective removal from associated services, and providing clear instructions and confirmations, the assessment aims to protect user privacy, enhance user experience, and adhere to data protection regulations such as Personal Data Protection Act (PDPA). Table 12 below outlines the assessment procedure and assignment verdicts for TSO-11.

Table 12. TSO-11 - Deleting user data

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (24)	6.11.1 User-friendly deletion	a) The TL should assess whether at least one functionality is provided according to corresponding CTIF, which can be performed by the user with limited technical knowledge according to "Description" and "Initiation and Interaction" to erase user data from the device according to "Target Type".	CTIF 25-DelFunc	At least one simple functionality to erase user data from the device is provided to the user.
		b) The TL should assess whether each functionality in corresponding CTIF is adequate to erase the targeted user data from the device.	CTIF 25-DelFunc	The described functionality is adequate to erase the targeted user data from the device

Table 12. TSO-11 - Deleting user data (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (24)	6.11.1 User-friendly deletion	c) The TL should assess whether the functionalities to erase user data corresponding CTIF cover personal data, user configuration and user-related cryptographic material.	CTIF 25-DelFunc	Personal data, user configuration and cryptographic material is covered by the functionalities to erase user data from the device.
		d) The TL should create typical user data on the DUT with regards to the usage of the device.	CTIF 25-DelFunc	The initiation and interaction of the user is consistent with the CTIF.
		e) The TL should perform each functionality to erase user data from the device according to "Target Type" in corresponding CTIF and functionally assess whether the "Initiation and Interaction" is consistent with the CTIF.	CTIF 25-DelFunc	
		f) The TL should perform each functionality to erase user data from the device according to "Target Type" in corresponding CTIF and functionally assess whether the corresponding user data still exists after completing the operation.	CTIF 25-DelFunc	There is no indication that the corresponding user data is not erased successfully.
RC (25)	6.11.2 Removal of personal data from associated services	a) For all deletion functionalities in corresponding CTIF the TL should assess whether at least one functionality is provided, which can be performed by the user with limited technical knowledge according to "Description" and "Initiation and Interaction" to remove all personal data stored on the associated services according to "Target Type".	CTIF 25-DelFunc	At least one simple functionality to remove personal data from associated services is provided to the user.
		b) The TL should assess whether all associated services storing personal data according to "Processing Activities" in corresponding CTIF(i) are covered by the combination of all deletion functionalities in corresponding CTIF(ii).	i) CTIF 21-PersDat a ii) CTIF 25-DelFunc	Every associated service storing personal data is covered by a simple deletion functionality.
		c) The TL should create typical personal data on associated services with regards to the usage of the DUT.	N/A	The initiation and interaction of the user is consistent with the CTIF.

MCMC MTSFB TC G050:2025

Table 12. TSO-11 - Deleting user data (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (25)	6.11.2 Removal of personal data from associated services	d) The TL should perform each functionality to remove personal data according to "Target Type" in corresponding CTIF and functionally assess whether the "Initiation and Interaction" is consistent with in the CTIF.	CTIF 25- DelFunc	There is no indication that the corresponding personal data stored on the associated service is not removed successfully.
		e) The TL should perform each functionality to remove personal data according to "Target Type" in corresponding CTIF and functionally assess whether the corresponding personal data still exists on the associated services after completing the operation.	CTIF 25- DelFunc	
RC (26)	6.11.3 Instruction to delete data	a) The TL should create typical personal data with regard to the usage of the DUT. The information from "Processing Activities" in corresponding CTIF can be helpful to create personal data which are stored on the DUT and on associated services.	CTIF 21-PersData	Is covered by the documentation.
		b) The TL should functionally assess whether all deletion functionalities in corresponding CTIF(i) are covered by the "Documentation of Deletion" in corresponding CTIF(ii).	i) CTIF 25- DelFunc ii) CTIF 2-UserInfo	Is documented in a concise manner and includes the necessary steps to be taken to delete personal data.
		c) For each deletion functionality in corresponding CTIF(i) the TL should perform the functionality according to the "Documentation of Deletion" in corresponding CTIF(ii) and functionally assess whether it is described in a concise manner and includes all necessary steps to delete the personal data from the device or associated service according to "Target Type" in corresponding CTIF(i).	i) CTIF 25- DelFunc ii) CTIF 2-UserInfo	
RC (26)	6.11.4 Confirmation on data deletion	a) The TL should perform each deletion functionality in corresponding CTIF(i) according to "Documentation of Deletion" in corresponding CTIF(ii).	i) CTIF 25- DelFunc ii) CTIF 2-UserInfo	For every deletion functionality a clear confirmation is provided, that the corresponding data is deleted.
		b) For each deletion functionality in corresponding CTIF the TL should functionally assess whether the user is provided with a clear "Confirmation", that the corresponding data is deleted.	CTIF 25- DelFunc	

6.12 TSO-12 - Installation and maintenance of devices

The objective of this assessment is to, as stipulated in Clause 6.12 of the MCMC MTSFB TC G044. The aim of this assessment is to offer guidance on evaluating the installation and maintenance of devices. Table 13 below outlines the assessment procedure and assignment verdicts for TSO-12.

Table 13. TSO-12 - Installation and maintenance of devices

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.12.1 User-friendly installation and maintenance	a) For each decision in corresponding CTIF the TL should assess whether it is necessary regarding the usage in the operational environment.	CTIF 26-UserDec	Every decision taken by the user is necessary regarding the usage in the operational environment.
		b) For each decision in corresponding CTIF the TL should assess whether the default value for the decision according to "Options" follows security best practice.	CTIF 26-UserDec	Every default value for a decision taken by the user follows security best practice.
		c) The TL should trigger all user-based decisions in corresponding CTIF according to "Triggered By".	CTIF 26-UserDec	Every decision taken by the user is prominently requested during the installation and maintenance flows.
		d) For each decision in corresponding CTIF the TL should functionally assess whether it is prominently requested from the user during the installation and maintenance flows.	CTIF 26-UserDec	Every decision taken by the user is understandable for a user with limited technical knowledge.
		e) For each decision in corresponding CTIF the TL should functionally assess whether the decision and its "Options" are understandable for a user with limited technical knowledge.	CTIF 26-UserDec	
		f) The TL should functionally assess whether the decisions to be taken by the user during installation and maintenance on the DUT are conformant to their "Description" and "Options" in corresponding CTIF.	CTIF 26-UserDec	Every decision taken by the user during installation or maintenance on the DUT is as described in the CTIF.
R	6.12.2 Users' guidance to set up device	a) The TL should set up the DUT using the "Documentation of Secure Setup" described in corresponding CTIF.	CTIF 2-UserInfo	<ul style="list-style-type: none"> • Every security-relevant user decision is covered by the documentation; and • For every security-relevant user decision a recommendation on how to achieve a secure setup is given.

MCMC MTSFB TC G050:2025

Table 13. TSO-12 - Installation and maintenance of devices (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
R	6.12.2 Users' guidance to set up device	b) The TL should functionally assess whether in the "Documentation of Secure Setup" described in corresponding CTIF(i) each security-relevant user decision in corresponding CTIF(ii) is covered by the documentation.	i) CTIF 2-UserInfo ii) CTIF 26-UserDec	<ul style="list-style-type: none"> • Every security-relevant user decision is covered by the documentation; and • For every security-relevant user decision a recommendation on how to achieve a secure setup is given.
		c) The TL should functionally assess whether the "Documentation of Secure Setup" described in corresponding CTIF includes recommendations on how to take the security-relevant user decisions to achieve a secure setup.	CTIF 2-UserInfo	
R	6.12.3 Users' guidance to check device set up	a) The TL should set up the DUT using an example configuration.	N/A	Every step for checking the securely set up is covered by the documentation.
		b) The TL should functionally assess whether in the "Documentation of Setup Check" described in corresponding CTIF each step for checking whether the DUT is securely set up is covered by the documentation.	CTIF 2-UserInfo	
		c) The TL should functionally assess whether the check applied to the example configuration results in a reasonable outcome.	N/A	The application of the check for securely set up according to the documentation results in an outcome and there is an indication that the result is reasonable.

6.13 TSO-13 - Validate input data

The objective of this assessment is to validate input data, as stipulated in Clause 6.13 of the MCMC MTSFB TC G044. Input data validation ensures data is processed correctly by verifying it meets required criteria. This involves checking the data type, value, structure, cardinality, and order. For short lists, this can be done against a predefined list of acceptable values. Table 14 below outlines the assessment procedure and assignment verdicts for TSO-13.

NOTE: Short list identifies the appropriate data type output from the sensor, as an example.

Table 14. TSO-13 - Validate input data

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (27)	6.13.1 Validate data input	a) The TL should assess whether the combination of data input validation methods in corresponding CTIF(i) covers all sources for data input including: <ul style="list-style-type: none"> • The user interfaces, which enable data input from the user in corresponding CTIF(ii); • The Application Programming Interfaces (APIs), which enable data input from external sources in corresponding CTIF(iii); and • The network communications, which enable data input according to the corresponding remotely accessible communication methods in corresponding CTIF(iv). 	i) CTIF 29- InpVal ii) CTIF 27- UserIntf iii) CTIF 28- ExtAPI iv) CTIF 11- ComMech	The data input validation methods cover data input via user interfaces, transmitted via APIs and between networks in services and devices.
		b) For each data input validation method in corresponding CTIF, the TL should assess whether it is effective for validating the corresponding data input.	CTIF 29- InpVal	Every described data input validation method is effective for validating the corresponding data input.
		c) The TL should functionally assess whether each data input validation method in corresponding CTIF prevents the processing of unexpected data input.	CTIF 29- InpVal	There is no indication that any data input validation does not protect against the processing of unexpected data input.
		d) The TL should functionally assess whether all user interfaces of the DUT are described in corresponding CTIF according to the documentation for the user, e.g. user manual.	CTIF 27- UserIntf	Every discovered user interface is documented in the CTIF.
		e) The TL should functionally assess whether all remotely accessible APIs of the DUT are described in corresponding CTIF.	CTIF 28- ExtAPI	Every discovered remotely accessible API is documented in the CTIF.

MCMC MTSFB TC G050:2025

6.14 TSO-14 - Data protection requirements for consumer IoT

The objective of this assessment is to verify data protection requirements for consumer IoT, as stipulated in Clause 7 of the MCMC MTSFB TC G044. Protecting consumer IoT data is essential for preserving privacy, preventing security threats, fostering trust, and complying with legal requirements, ultimately contributing to a safer and more secure digital ecosystem. Table 15 below outlines the assessment procedure and assignment verdicts for TSO-14.

Table 15. TSO-14 - Data protection requirements for consumer IoT

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (28)	7 (a)	a) The TL should assess whether the "Documentation of Personal Data" in corresponding CTIF is suitable for the consumer to obtain the information about processing personal data.	CTIF 2-Userinfo	The information about processing personal data is suitably provided to the consumer.
		b) The TL should functionally assess whether the provided information about processing personal data (obtained information) is consistent to the description in "Documentation of Personal Data" in corresponding CTIF.	CTIF 2-Userinfo	The information about processing personal data can be obtained as described.
		c) The TL should functionally assess whether the obtained information about processing personal data accessing the "Documentation of Personal Data" in corresponding CTIF(i) match their description in "Processing Activities" in corresponding CTIF(ii).	i) CTIF 2-Userinfo ii) CTIF 21-Persdat	The obtained information about processing personal data match their description.
		d) The TL should functionally assess whether the obtained information describes what personal data is processed in a way understandable for a user with limited technical knowledge	N/A	The personal data being processed is clearly and transparently described.
		e) The TL should functionally assess whether the obtained information describe how personal data is being used, by whom, and for what purposes in a way understandable for a user with limited technical knowledge.	N/A	It is clearly and transparently described how personal data is being used, by whom, and for what purposes.

MCMC MTSFB TC G050:2025

Table 15. TSO-14 - Data protection requirements for consumer IoT (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
MC (7)	7 (b)	a) For each personal data in corresponding CTIF that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL should assess whether the opt-in choice: <ul style="list-style-type: none"> • is given freely; • is given obviously; and • is given explicitly according to the description of "Obtaining Consent". 	CTIF 21-PersData	<ul style="list-style-type: none"> • It is described how to express consent (opt-in choice) to the processing of personal data for specific purposes; and • The opt-in choice is given freely, obviously and explicitly.
		b) For each personal data in corresponding CTIF that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL should functionally assess whether consumers' consent to processing personal data is obtained as described in the CTIF.	CTIF 21-PersData	The way of obtaining consumers' consent matches the description.
MC (7)	7 (c)	a) For each personal data in corresponding CTIF that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL should assess whether the information on "Withdrawing Consent" describes how to withdraw consent to the processing of personal data at any time by configuring IoT device and service functionality appropriately.	CTIF 21-PersData	It is described how to withdraw consent to the processing of personal data at any time.
		b) For each personal data in corresponding CTIF that is processed on the basis of consumers' consent according to "Obtaining Consent", the TL should functionally assess whether consumers' consent to processing personal data can be withdrawn as described in "Withdrawing Consent".	CTIF 21-PersData	The way of withdrawing consumers' consent matches the description.

MCMC MTSFB TC G050:2025

Table 15. TSO-14 - Data protection requirements for consumer IoT (continued)

Status	Requirement	Assessment criteria	CTIF number	PASS assignment of verdicts
RC (6)	7 (d)	a) The TL should assess whether the personal data in corresponding CTIF(i) that are referenced in "Personal Data" in corresponding CTIF(ii) is necessary for the intended functionality as described in the "Purpose" of collecting the data.	i) CTIF 21- PersData ii) CTIF 24- TelData	Their processing is necessary for the intended functionality.
MC (6)	7 (e)	a) The TL should assess whether the "Documentation of Telemetry Data" in corresponding CTIF is suitable for the consumer to obtain the information about processing telemetry data.	CTIF 2- UserInfo	The information about processing telemetry data is suitably provided to the consumer.
		b) The TL should functionally assess whether the provided information about processing telemetry data (obtained information) is consistent with the description in "Documentation of Telemetry Data" in corresponding CTIF.	CTIF 2- UserInfo	The information about processing telemetry data can be obtained as described.
		c) The TL should functionally assess whether the obtained information about processing telemetry data accessing the "Documentation of Telemetry Data" in corresponding CTIF(i) match their "Purpose" described in corresponding CTIF(ii).	i) CTIF 2- UserInfov ii) CTIF 24- TelData	The obtained information about processing telemetry data match their description.
		f) The TL should functionally check whether the obtained information describes what telemetry data is collected.	N/A	The telemetry data being collected is described.
		g) The TL should functionally check whether the obtained information describes how telemetry data is being used, by whom, and for what purposes.	N/A	It is completely described how telemetry data is being used, by whom, and for what purposes.
R	7 (f)	The TL should assess whether adequate anti-virus software is installed.	N/A	Adequate antivirus software is installed.
R	7 (g)	The TL should ensure that the procedure for data cleansing on backup data is documented based on the retention policy in PDPA or data retention laws for regulated industries if exist.	N/A	The procedure is available and documented.

Annex A
(informative)

Abbreviations

AES	Advanced Encryption Standard
API	Application Programming Interface
ARM	Advanced RISC Machines
BL	Boot Loader
CPU	Central Processing Unit
CVE	Common Vulnerabilities and Exposures
CTIF	Comprehensive Testing Information File
DUT	Device Under Test
GDB	GNU Debugger
GPS	Global Positioning System
HSM	Hardware Security Module
HTML	Hyper Text Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
SAS	Self-Assessment Statement
IoT	Internet of Things
JTAG	Joint Test Action Group
LAN	Local Area Network
MAC	Media Access Control
OAEP	Optimal Asymmetric Encryption Padding
OS	Operating System
PC	Personal Computer
PHP	Hypertext Preprocessor
PKCS	Public-Key Cryptography Standards
PSA	Platform Security Architecture
RAM	Random Access Memory
ROM	Read Only Memory
SO	Supplier Organisation
SOAP	Simple Object Access Protocol

MCMC MTSFB TC G050:2025

SSH	Secure Shell
TBB	Trusted Board Boot
TL	Test Laboratory
TLS	Transport Layer Security (Protocol)
TSO	Test Scenario
WLAN	Wireless Local Area Network

Annex B
(normative)

Forms for the Supplier Organisation (SO)

B.1 Identification of the DUT form

The identification of the DUT provides information, as detailed as possible, e.g., about the DUT version numbering and configuration options. Furthermore, a declaration concerning constrained devices and contact information of the TL are included in the form. Table B.1 provide sample of DUT form to be filled up by the SO.

Table B.1 Sample of DUT form

Date of the statement	
Date of the statement	:
DUT identification	
DUT name	:
Brand/Trade Names: The devices with alternative brand/trade names are expected to be functionally equivalent to the DUT	:
Hardware configuration (including Release Number and Serial Number)	:
Runtime environment/Operating System (OS), if applicable	:
Firmware version in factory setting	:
Associated services necessary for the assessment (including e.g. Release Number, URL)	:
Constrained Device	
Constrained Device (According to MCMC MTSFB TC G044)	:
Justification	:
Supplier Organisation (SO)	
Name	:
Address	:
Telephone number	:
SO contact person	
Name	:
Telephone number	:
E-mail address	:
Additional information	:

MCMC MTSFB TC G050:2025

B.2 Self-Assessment Form

Table B.2 provides a mechanism for the user of the present document (who is expected to be an entity involved in the development or manufacturing of consumer IoT) to give information about the implementation of the requirement within MCMC MTSFB TC G044.

The requirement column gives reference to the requirement in MCMC MTSFB TC G044.

The status column indicates the status of a provision. The following notations are used:

- a) M represent the requirement is a mandatory requirement.
- b) R represent the requirement is a recommendation.
- c) MC represent the requirement is a mandatory requirement and conditional.
- d) RC represent the requirement is a recommendation and conditional.

NOTE: Where the conditional notation is used, this is conditional on the text of the requirement. The conditions are provided at the bottom of the table with references provided for the relevant provisions to help with clarity.

The support column can be filled in by the user of the present document. The following notations are used:

- a) Y represent supported by the implementation.
- b) N represent not supported by the implementation.
- c) N/A represent the requirement is not applicable (allowed only if a provision is conditional as indicated in the status column and if it has been determined that the condition does not apply for the product in question).

The detail column can be filled in by the user of the present document by referring to the below information.

- a) If a requirement is supported by the implementation, the entry in the detail column is to contain information on the measures that have been implemented to achieve support.
- b) If a requirement is not supported by the implementation, the entry in the detail column is to contain information on the reasons why implementation is not possible or not appropriate.
- c) If a requirement is not applicable, the entry in the detail column is to contain the rationale for this determination.

Table B.2 Sample of SAF form

Clause number and title			
Requirement	Status	Support	Detail
6.1 No Universal Default Passwords			
6.1a	MC (1)		
6.1b	MC (2)		
6.1c	MC (8)		
6.1d	MC (8)		
6.1e	MC (5)		

Table B.2 Sample of SAF form (continued)

Clause number and title			
Requirement	Status	Support	Detail
6.2 – Managing Reports of Vulnerabilities			
6.2.1	M		
6.2.2	R		
6.2.3	R		
6.3 Keep software updated			
6.3.1	R		
6.3.2	MC (5)		
6.3.3	MC (12)		
6.3.4	RC (12)		
6.3.5	RC (12)		
6.3.6	RC (9, 12)		
6.3.7	MC (12)		
6.3.8	MC (12)		
6.3.9	RC (12)		
6.3.10	MC (11, 12)		
6.3.11	RC (12)		
6.3.12	RC (12)		
6.3.13	M		
6.3.14	RC (3, 4)		
6.3.15	RC (3, 4)		
6.3.16	M		
6.4 Securing sensitive security parameters			
6.4.1	MC (14)		
6.4.2	MC (10)		
6.4.3	M		
6.4.4	MC (15)		
6.5 Communicate securely			
6.5.1	M		
6.5.2	R		
6.5.3	R		
6.5.4	RC (16)		
6.5.5	MC (17)		
6.5.6	RC (18)		
6.5.7	MC (19)		
6.5.8	MC (20)		
6.6 Minimize attack surfaces			
6.6.1	M		
6.6.2	M		
6.6.3	R		
6.6.4	MC (13)		
6.6.5	R		

MCMC MTSFB TC G050:2025

Table B.2 Sample of SAF form (continued)

Clause number and title			
Requirement	Status	Support	Detail
6.6.6	R		
6.6.7	R		
6.6.8	R		
6.6.9	R		
6.7 Ensure software integrity			
6.7.1	R		
6.7.2	R		
6.8 Ensure secure personal data			
6.8.1	RC (21)		
6.8.2	MC (22)		
6.8.3	MC (23)		
6.9 Systems resilient to outages			
6.9.1	R		
6.9.2	R		
6.9.3	R		
6.10 Secure telemetry data			
6.10.1	RC (6)		
6.11 Deleting user data			
6.11.1	MC (24)		
6.11.2	RC (25)		
6.11.3	RC (26)		
6.11.4	RC (26)		
6.12 Installation and maintenance of devices			
6.12.1	R		
6.12.2	R		
6.12.3	R		
6.13 Validate input data			
6.13.1	MC (27)		
7 Data protection requirements for consumer IoT			
7a	MC (28)		
7b	MC (7)		
7c	MC (7)		
7d	RC (6)		
7e	MC (6)		
7f	R		
7g	R		

Table B.2 Sample of SAF form (concluded)

Conditions	
1) passwords are used;	
2) pre-installed unique per device passwords are used;	
3) software components are not updateable;	
4) the device is constrained;	
5) the device is not constrained;	
6) telemetry data being collected;	
7) personal data is processed on the basis of consumers' consent;	
8) the device allowing user authentication;	
9) the device supports automatic updates and/or update notifications;	
10) a hard-coded unique per device identity is used for security purposes;	
11) updates are delivered over a network interface;	
12) an update mechanism is implemented;	
13) a debug interface is physically accessible;	
14) sensitive security parameters are stored persistently;	
15) critical security parameters used for integrity and authenticity checks of software updates in device software or for protection of communication with associated services in device software exist;	
16) access to device functionality via a network interface in the initialized state is possible;	
17) device functionality that allows security-relevant changes in configuration via a network interface exists;	
18) critical security parameters are transmitted;	
19) critical security parameters are transmitted via remotely accessible network interfaces;	
20) critical security parameters relating to the device exist;	
21) personal data is transmitted between a device and a service;	
22) sensitive personal data is transmitted between a device and a service;	
23) external sensing capabilities exist;	
24) user data is stored on the device;	
25) personal data is stored on associated services;	
26) personal data is stored;	
27) data input via user interfaces or transferred via APIs or between networks in services and devices is supported;	
28) personal data is processed.	

B.3 CTIF form

Table B.3 Sample CTIF 1-AuthMech (Authentication Mechanisms)

ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention

MCMC MTSFB TC G050:2025

Table B.4 Sample CTIF 2-UserInfo (User Information)

Documentation of Change Mechanisms	
Documentation of Replacement	
Documentation of Sensors	
Documentation of Secure Setup	
Documentation of Setup Check	
Documentation of Personal Data	
Documentation of Telemetry Data	
Documentation of Deletion	
Model Designation	
Support Period	
Publication of Support Period	
Publication of Vulnerability Disclosure Policy	
Publication of Non-Updatable	

Table B.5 Sample CTIF 3-VulnTypes (Relevant Vulnerabilities)

ID	Description	Action	Time Frame

Table B.6 Sample CTIF 4-Conf (Confirmations)

Confirmation of Vulnerability Actions	
Confirmation of Vulnerability Monitoring	
Confirmation of Update Procedures	
Confirmation of Secure Management	
Confirmation of Secure Development	

Table B.7 Sample CTIF 5-VulnMon (Vulnerability Monitoring)

ID	Description

Table B.8 Sample CTIF 6-SoftComp (Software Components)

ID	Description	Update Mechanism	Cryptographic Usage

Table B.9 Sample CTIF 7-UpdMech (Update Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Initiation and Interaction	Configuration	Update Checking	User Notification

Table B.10 Sample CTIF 8-UpdProc (Update Procedures)

ID	Description	Time Frame

NOTE: CTIF 9-RepISup is only applicable for constrained devices.

Table B.11 Sample CTIF 9-RepISup (Replacement Support)

Isolation	
Hardware Replacement	

MCMC MTSFB TC G050:2025

Table B.12 Sample CTIF 10-SecParam (Security Parameters)

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism

Table B.13 Sample CTIF 11-ComMech (Communication Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Resilience Measures

Table B.14 Sample CTIF 12-NetSecImpl (Network and Security Implementations)

ID	Description	Review/Evaluation Method	Report

Table B.15 Sample CTIF 13-SoftServ (Software Services)

ID	Description	Status	Justification	Allows Configuration	Authentication Mechanism

Table B.16 Sample CTIF 14-SecMgmt (Secure Management Processes)

ID	Description

Table B.17 Sample CTIF 15-Intf (Interfaces)

ID	Description	Type	Status	Disclosed Information	Debug Interface	Protection

Table B.18 Sample CTIF 16-CodeMin (Code Minimization)

ID	Description

Table B.19 Sample CTIF 17-PrivlCtrl (Privilege Control)

ID	Description

Table B.20 Sample CTIF 18-AccCtrl (Access Control)

ID	Description

Table B.21 Sample CTIF 19-SecDev (Secure Development Processes)

ID	Description

MCMC MTSFB TC G050:2025

Table B.22 Sample CTIF 20-SecBoot (Secure Boot Mechanisms)

ID	Description	Security Guarantees	Detection Mechanisms	User Notification	Notification Functionality

Table B.23 Sample CTIF 21-PersData (Personal Data)

ID	Description	Processing Activities	Communication Mechanisms	Sensitive	Obtaining Consent	Withdrawing Consent

Table B.24 Sample CTIF 22-ExtSens (External Sensors)

ID	Description

Table B.25 Sample CTIF 23-ResMech (Resilience Mechanisms)

ID	Description	Type	Security Guarantees

Table B.26 Sample CTIF 24-TeIData (Telemetry Data)

ID	Description	Purpose	Security Examination	Personal Data

Table B.27 Sample CTIF 25-DelFunc (Deletion Functionalities)

ID	Description	Target Type	Initiation and Interaction	Confirmation

Table B.28 Sample CTIF 26-UserDec (User Decisions)

ID	Description	Options	Triggered By

Table B.29 Sample CTIF 27-UserIntf (User Interfaces)

ID	Description

Table B.30 Sample CTIF 28-ExtAPI (External APIs)

ID	Description

Table B.31 Sample CTIF 29-InpVal (Data Input Validation)

ID	Description

Annex C (normative)

Overview of required CTIF entries per requirement

C.1 CTIF entries per requirement

As described in the assessment procedure in Clause 5.2, Table C.1 describes the required CTIF entries to be performed for the corresponding test group, following the requirements in MCM MTSFB TC G044

Table C.1 Required CTIF entries per requirement

Requirement	Required CTIF entries
6.1 TSO-1 No universal default passwords	
6.1a	CTIF 1-AuthMech: ID, Description, Authentication Factor, Password Generation Mechanism
6.1b	CTIF 1-AuthMech: ID, Description, Authentication Factor, Password Generation Mechanism
6.1c	CTIF 1-AuthMech: ID, Description, Security Guarantees, Cryptographic Details
6.1d	CTIF 1-AuthMech: ID, Description CTIF 2-UserInfo: Documentation of Change Mechanisms
6.1e	CTIF 1-AuthMech: ID, Description, Brute Force Prevention
6.2 TSO-2 Managing reports of vulnerabilities	
6.2.1	CTIF 2-UserInfo: Publication of Vulnerability Disclosure Policy
6.2.2	CTIF 2-UserInfo: Publication of Vulnerability Disclosure Policy CTIF 3-VulnTypes: ID, Description, Action, Time Frame CTIF 4-Conf: Confirmation of Vulnerability Actions
6.2.3	CTIF 4-Conf: Confirmation of Vulnerability Monitoring CTIF 5-VulnMon: ID, Description
6.3 TSO-3 Keep software updated	
6.3.1	CTIF 6-SoftComp: ID, Description, Update Mechanism
6.3.2	CTIF 7-UpdMech: ID, Description, Security Guarantees, Cryptographic Details, Initiation and Interaction
6.3.3	CTIF 6-SoftComp: ID, Description, Update Mechanism CTIF 7-UpdMech: ID, Description, Initiation and Interaction
6.3.4	CTIF 6-SoftComp: ID, Description, Update Mechanism CTIF 7-UpdMech: ID, Description, Initiation and Interaction, Configuration
6.3.5	CTIF 6-SoftComp: ID, Description, Update Mechanism CTIF 7-UpdMech: ID, Description, Update Checking
6.3.6	CTIF 7-UpdMech: ID, Description, Initiation and Interaction, Configuration, User Notification
6.3.7	CTIF 7-UpdMech: ID, Description, Security Guarantees, Cryptographic Details
6.3.8	CTIF 4-Conf: Confirmation of Update Procedures CTIF 8-UpdProc: ID, Description, Time Frame
6.3.9	CTIF 7-UpdMech: ID, Description, Security Guarantees, Cryptographic Details
6.3.10	CTIF 7-UpdMech: ID, Description, Security Guarantees, Cryptographic Details
6.3.11	CTIF 7-UpdMech: ID, Description, User Notification
6.3.12	CTIF 7-UpdMech: ID, Description, User Notification

Table C.1 Required CTIF entries per requirement (continued)

Requirement	Required CTIF entries
6.3.13	CTIF 2-UserInfo: Support Period, Publication of Support Period
6.3.14	CTIF 2-UserInfo: Documentation of Replacement, Publication of Non-UpdaCTIF
6.3.15	CTIF 9-ReplSup: Isolation, Hardware Replacement
6.3.16	CTIF 2-UserInfo: Model Designation
6.4 TSO-4 Securing sensitive security parameters	
6.4.1	CTIF 10-SecParam: ID, Description, Type, Security Guarantees, Protection Scheme
6.4.2	CTIF 10-SecParam: ID, Description, Type, Security Guarantees, Protection Scheme
6.4.3	CTIF 10-SecParam: ID, Description, Type, Provisioning Mechanism
6.4.4	CTIF 10-SecParam: ID, Description, Type, Generation Mechanism
6.5 TSO-5 Communicate securely	
6.5.1	CTIF 11-ComMech: ID, Description, Security Guarantees, Cryptographic Details
6.5.2	CTIF 12-NetSecImpl: ID, Description, Review/Evaluation Method, Report
6.5.3	CTIF 6-SoftComp: ID, Description, Update Mechanism, Cryptographic Usage
6.5.4	CTIF 1-AuthMech: ID, Description, Security Guarantees, Cryptographic Details CTIF 13-SoftServ: ID, Description, Authentication Mechanism
6.5.5	CTIF 11-ComMech: ID, Description, Security Guarantees, Cryptographic Details CTIF 13-SoftServ: ID, Description, Allows Configuration, Authentication Mechanism
6.5.6	CTIF 10-SecParam: ID, Description, Type, Communication Mechanisms CTIF 11-ComMech: ID, Description, Security Guarantees, Cryptographic Details
6.5.7	CTIF 10-SecParam: ID, Description, Type, Communication Mechanisms CTIF 11-ComMech: ID, Description, Security Guarantees, Cryptographic Details
6.5.8	CTIF 4-Conf: Confirmation of Secure Management CTIF 14-SecMgmt: ID, Description
6.6 TSO-6 Minimize attack surfaces	
6.6.1	CTIF 15-Intf: ID, Description, Type, Status
6.6.2	CTIF 15-Intf: ID, Description, Type, Disclosed Information
6.6.3	CTIF 15-Intf: ID, Description, Type, Status, Protection
6.6.4	CTIF 15-Intf: ID, Description, Type, Status, Debug Interface, Protection
6.6.5	CTIF 13-SoftServ: ID, Description, Status, Justification
6.6.6	CTIF 16-CodeMin: ID, Description
6.6.7	CTIF 17-PrivlCtrl: ID, Description
6.6.8	CTIF 18-AccCtrl: ID, Description
6.6.9	CTIF 4-Conf: Confirmation of Secure Development CTIF 19-SecDev: ID, Description
6.7 TSO-7 Ensure software integrity	
6.7.1	CTIF 20-SecBoot: ID, Description, Security Guarantees, Detection Mechanisms
6.7.2	CTIF 20-SecBoot: ID, Description, User Notification, Notification Functionality
6.8 TSO-8 Ensure secure personal data	
6.8.1	CTIF 11-ComMech: ID, Description, Security Guarantees, Cryptographic Details CTIF 21-PersData: ID, Description, Communication Mechanisms

MCMC MTSFB TC G050:2025

Table C.1 Required CTIF entries per requirement (concluded)

Requirement	Required CTIF entries
6.8.2	CTIF 11-ComMech: ID, Description, Security Guarantees, Cryptographic Details CTIF 21-PersData: ID, Description, Processing Activities, Communication Mechanisms, Sensitive
6.8.3	CTIF 2-UserInfo: Documentation of Sensors CTIF 22-ExtSens: ID, Description
6.9 TSO-9 Systems resilient to outages	
6.9.1	CTIF 23-ResMech: ID, Description, Security Guarantees
6.9.2	CTIF 23-ResMech: ID, Description, Type, Security Guarantees
6.9.3	CTIF 11-ComMech: ID, Description, Resilience Measures
6.10 TSO-10 Secure telemetry data	
6.10.1	CTIF 24-TelData: ID, Description, Security Examination
6.11 TSO-11 Deleting user data	
6.11.1	CTIF 25-DelFunc: ID, Description, Target Type, Initiation and Interaction
6.11.2	CTIF 21-PersData: ID, Description, Processing Activities CTIF 25-DelFunc: ID, Description, Target Type, Initiation and Interaction
6.11.3	CTIF 2-UserInfo: Documentation of Deletion CTIF 21-PersData: ID, Description, Processing Activities CTIF 25-DelFunc: ID, Description, Target Type
6.11.4	CTIF 2-UserInfo: Documentation of Deletion CTIF 25-DelFunc: ID, Description
6.12 TSO-12 Installation and maintenance of devices	
6.12.1	CTIF 26-UserDec: ID, Description, Options, Triggered By
6.12.2	CTIF 2-UserInfo: Documentation of Secure Setup CTIF 26-UserDec: ID, Description, Options
6.12.3	CTIF 2-UserInfo: Documentation of Setup Check
6.13 TSO-13 Validate input data	
6.13.1	CTIF 11-ComMech: ID, Description CTIF 27-UserIntf: ID, Description CTIF 28-ExtAPI: ID, Description CTIF 29-InpVal: ID, Description
7 TSO-14 Data protection requirements for consumer IoT	
7a	CTIF 2-UserInfo: Documentation of Personal Data CTIF 21-PersData: ID, Description, Processing Activities
7b	CTIF 21-PersData: ID, Description, Obtaining Consent
7c	CTIF 21-PersData: ID, Description, Obtaining Consent, Withdrawing Consent
7d	CTIF 21-PersData: ID, Description CTIF 24-TelData: ID, Description, Purpose, Personal Data
7e	CTIF 2-UserInfo: Documentation of Telemetry Data CTIF 24-TelData: ID, Description, Purpose
7f	N/A
7g	N/A

C.2 CTIF description

1) CTIF 1-AuthMech: Authentication Mechanisms

The completed CTIF lists all authentication mechanisms of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("AuthMech-1") or labelling scheme ("AuthMech-PswdWebIf").

- b) **Description:** Brief description of the authentication mechanism and its corresponding authorization process. It is indicated additionally whether the mechanism is used for user or machine-to-machine authentication and whether it is directly addressable from a network interface.

- c) **Authentication Factor:** The type of attribute used for authentication. For passwords it is indicated additionally whether the password is set by the user and used in the initialized state.

EXAMPLE: Password (set by user), password (pre-installed), biometric fingerprint.

- d) **Password Generation Mechanism:** If the authentication factor is a password, which is not set by the user: Description of the mechanism to generate the password. It is indicated additionally whether the password is unique per device and whether it is pre-installed.

NOTE: A detailed specification of the password generation mechanism is not necessary. It is considered as sufficient when the description explains the measures to ensure that the passwords are unique per device in any state other than the factory default and to reduce the risks of automated attacks based on obvious regularities, common strings, public available information or inappropriate complexity when used as pre-installed and unique per device password.

- e) **Security Guarantees:** Description of the realized security objectives and the threats the mechanism is protected against.

EXAMPLE: The mechanisms attests that the authenticated entity is in possession of a valid password. The confidentiality and integrity protection of the password during transfer is also guaranteed within the session.

- f) **Cryptographic Details:** Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the authentication mechanism considering key management, and to facilitate the described "Security Guarantees".

EXAMPLE: Authentication is performed via http authentication framework (IETF RFC 7235 [i.8]). Integrity and confidentiality of the password transfer to the DUT is realized with the Secure Shell (SSH) cipher suite TLS_DHE_RSA_WITH_AES_128_CBC_SHA256.

- g) **Brute Force Prevention:** If the authentication mechanism is directly addressable from a network interface: Description of the method to prevent an attacker from brute forcing credentials via network interfaces.

EXAMPLE: A time delay of 5 seconds after an unsuccessful login before a new login can follow.

MCMC MTSFB TC G050:2025

2) CTIF 2-UserInfo: User Information

The completed CTIF lists documentations, publications and information provided to users. The form contains the following entries, which are independent from each other, and is typically filled out in form of a list.

- a) **Documentation of Change Mechanisms:** Description of the way the mechanisms to change the authentication values are documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- b) **Documentation of Replacement:** If the DUT is not updatable: Description of the way the guidance to isolate the DUT and the hardware replacement plan is documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- c) **Documentation of Sensors:** Description of the way the information about external sensing capabilities is documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- d) **Documentation of Secure Setup:** Description of the way the method for securely setting up the DUT is documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- e) **Documentation of Setup Check:** Description of the way the method for checking the secure setup of the DUT is documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- f) **Documentation of Personal Data:** Description of the way the information about processing personal data is documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- g) **Documentation of Telemetry Data:** Description of the way the information about collecting telemetry data is documented for the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- h) **Documentation of Deletion:** Description of the way the methods for deletion of personal data documented to the user, including all information to access the documentation.

NOTE: Possible ways of documentation are the website of the manufacturer and the corresponding URL, the user manual or built-in help.

- i) **Model Designation:** Model designation of the DUT and a brief description of how the user can recognize the model designation of the DUT.

NOTE: API call for or labelling sticker on the DUT are options to inform the user about the model designation.

- j) **Support Period:** Time during which the product or service is maintained by the manufacturer, e.g. in terms of updates.
- k) **Publication of Support Period:** Description of the way the defined "Support Period" is published and documented to the user, including all information to access the publication.

NOTE: Possible way of publication is the website of the manufacturer and the corresponding URL.

- l) **Publication of Vulnerability Disclosure Policy:** Description of the way the vulnerability disclosure policy is published, including all information to access the publication.

NOTE: Possible way of publication is the website of the manufacturer and the corresponding URL.

- m) **Publication of Non-Updatable:** If the DUT is not updatable: Description of the way the rationale for the absence of software updates is published, including all information to access the publication.

NOTE: Possible way of publication is the website of the manufacturer and the corresponding URL.

3) CTIF 3-VulnTypes: Relevant Vulnerabilities

The completed CTIF lists all types of vulnerabilities that are relevant for the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("VulnTypes-1") or labelling scheme ("VulnTypes-Firmw").

- b) **Description:** Brief description of the kind of vulnerability that is relevant for the DUT.

NOTE: Hardware, software and firmware are possible kinds of vulnerabilities. If all vulnerabilities are covered by a single process a separation is not necessary.

- c) **Action:** Description of the way of acting on this kind of vulnerability in case of a vulnerability disclosure including all entities and responsibilities.

NOTE: Rolling out patches and publishing advisories are possible actions in this case.

- d) **Time Frame:** Targeted time frame in which the given steps of the action in case of a vulnerability are scheduled.

EXAMPLE: 5 days for initial response and 90 days until publication of the patch.

4) CTIF 4-Conf: Confirmations

The completed CTIF lists confirmations for the establishment of processes. The form contains the following entries, which are independent from each other, and is typically filled out in form of a list.

- a) **Confirmation of Vulnerability Actions (Yes/No):** Confirmation that for every "Action" described in CTIF 3-VulnTypes the required infrastructure is in place and operators are briefed in order to achieve the targeted "Time Frame".

- b) **Confirmation of Vulnerability Monitoring (Yes/No):** Confirmation that for every vulnerability monitoring, identifying and rectifying described in CTIF 5-VulnMon the required infrastructure is in place and operators are briefed.

- c) **Confirmation of Update Procedures (Yes/No):** Confirmation that for every update procedure described in CTIF 8-UpdProc the required infrastructure is in place and operators are briefed in order to achieve the targeted "Time Frame".

MCMC MTSFB TC G050:2025

- d) **Confirmation of Secure Management (Yes/No):** Confirmation that the secure management processes described in CTIF 14-SecMgmt are established.
- e) **Confirmation of Secure Development (Yes/No):** Confirmation that the secure development processes described in CTIF 19-SecDev are established.

5) CTIF 5-VulnMon: Vulnerability Monitoring

The completed CTIF lists all procedures for monitoring, identifying and rectifying vulnerabilities. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("VulnMon-1") or labelling scheme ("VulnMon-Rectf").
- b) **Description:** Description of the way security vulnerabilities are monitored, identified and rectified in products and services.

NOTE: Procedures for identifying vulnerabilities commonly include assessments whether a potential vulnerability is relevant for a certain product, responsible persons, an approach to gather information and a workflow to perform in case a vulnerability is discovered.

6) CTIF 6-SoftComp: Software Components

The completed CTIF lists all software components of the DUT. The form contains the following entries and is typically filled out in form of a table.

NOTE: The used level of detail concerning the division of the DUT software into software components serves for the fact that the TL can identify which components are updatable and which are not.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("SoftComp-1") or labelling scheme ("SoftComp-Firmw").
- b) **Description:** Brief description of the software component.

NOTE: BIOS, firmware and Boot Loader (BL) are possible software components of the DUT.
- c) **Update Mechanism:** Reference to update mechanisms in CTIF 7-UpdMech that are used for updating the software component. An empty list of update mechanisms indicates the absence of updates for the software component and in this case a justification is provided.
- d) **Cryptographic Usage:** Indicates, if the software component makes use of cryptographic algorithms or primitives (Yes/No) and if so, it is included additionally, whether side effects of updating those algorithms and primitives are considered by the manufacturer (Yes/No).

7) CTIF 7-UpdMech: Update Mechanisms

The completed CTIF lists all update mechanisms of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("UpdMech-1") or labelling scheme ("UpdMech-Firmw").

- b) **Description:** Brief description of the update mechanism including its major characteristics. It is indicated additionally whether the delivery of an update is network-based.

NOTE: Depending on the complexity it may be useful to divide the description into the steps in which the update is performed.

EXAMPLE: Update step

- i) DUT queries server X to verify if an update is available, initiated by the user;
- ii) Server delivers the update to the DUT (network-based);
- iii) DUT verifies authenticity and integrity of the update;
- iv) After successful validation the installation of the update is performed.

- c) **Security Guarantees:** Description of the realized security objectives and the threats the mechanism is protected against. For authenticity and integrity is indicated additionally whether the security guarantee is given by the DUT itself.

EXAMPLE: The mechanism validates the integrity and authenticity before the installation of an update on the DUT itself.

- d) **Cryptographic Details:** Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the update mechanism considering key management, and to facilitate the described "Security Guarantees".

EXAMPLE: Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 3852 [i.9]. For the signature SHA-256 with RSA 2048 and PSS padding is used. The signing of the firmware package is performed with the private key of the manufacturer. The public key for the update validation is integrated during the manufacturing process of the DUT.

- e) **Initiation and Interaction:** Brief description of the procedure how an update is initiated and a brief description of the user interaction, which is necessary to initiate and apply an update.

NOTE: This entry serves also for the indication whether it is an automatic update mechanism.

- f) **Configuration:** Brief description of how automation and notification of software updates can be configured by the user, and which options the user can choose from. The default configuration is indicated additionally.

NOTE: Enable, disable and/or postpone automatic updates and enable, disable and/or postpone notifications are possible configurations or options to choose from.

- g) **Update Checking:** Brief description of the mechanism and the schedule for querying for security updates. It is indicated additionally whether the availability check is performed by the DUT itself.

EXAMPLE: HyperText Transfer Protocol Secure (HTTPS) query for latest stable Firmware version to EXAMPLE.ORG and comparison to installed version after initialization and every day at 2 am (initiated and performed by the DUT).

- h) **User Notification:** Brief description of how the user is informed about an available update and about disruptions caused by the update mechanism, e.g. limited availability of certain features. It is indicated additionally which information are contained in the notification and if the notification is realized by the DUT itself.

NOTE: Notifications via user interfaces and push messages are possible ways to inform the user.

8) CTIF 8-UpdProc: Update Procedures

This completed CTIF lists procedures of the manufacturer for the management of security updates. The form contains the following entries and is typically filled out in form of a table.

MCMC MTSFB TC G050:2025

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("UpdProc-1") or labelling scheme ("UpdProc-SecUpd").

- b) **Description:** Brief description of the procedure for deploying security updates including all entities and responsibilities.

- c) **Time Frame:** Targeted time frame for completing the procedure.

9) CTIF 9-RepISup: Replacement Support

The completed CTIF lists information about the isolation and hardware replacement of the DUT. The form contains the following entries, which are independent from each other, and is typically filled out in form of a list.

- a) **Isolation:** Description of the method including the steps to isolate the DUT.
- b) **Hardware Replacement:** Method's description including steps to replace the hardware of the DUT.

10) CTIF 10-SecParam: Security Parameters

The completed CTIF lists all sensitive (public and critical) security parameters that are persistently stored on the DUT during intended usage. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("SecParam-1") or labelling scheme ("SecParam-Pswd").

- b) **Description:** Brief description of the security parameter, including its purpose. It is indicated additionally whether the parameter is a hard-coded unique per device identity used in a device for security purposes (hard-coded identity) and/or hard-coded in device software source code.

- c) **Type:** Indication whether the security parameter is public or critical.

NOTE: Public and critical security parameters are defined in MCMC MTSFB TC G044.

- d) **Security Guarantees:** Description of the realized baseline security objectives and threats the security parameter is protected against during persistent storage.
- e) **Protection Scheme:** Description of the measures that are applied to achieve the Security Guarantees. This includes the principals and roles through which access to the parameter is possible, including the privileges associated to each role.
- f) **Provisioning Mechanism:** If the "Type" indicates that the parameter is critical: Description of the mechanism through which the parameter is assigned its value for the operation of the DUT.

NOTE:

1. Such assignment can happen during initialization or in initialized state (e.g. when a device functionality relying on the parameter is activated by the user).
2. Persistent configuration data, runtime configuration data, protocol negotiation and assignment to a default value are potentially possible provisioning mechanisms.

- g) **Communication Mechanisms:** Reference to communication mechanisms in CTIF 11-ComMech that are used for communicating the parameter and an indication whether the communication is done via remotely accessible interfaces.

- h) **Generation Mechanism:** If the "Type" indicates that the parameter is critical and used for integrity and authenticity checks of software updates or for protection of communication with associated services: Description of the mechanism used to generate the values of the parameter and it is indicated additionally that the parameter is used for integrity and authenticity checks of software updates or for protection of communication with associated services.

EXAMPLE: References to a standard random number generator and applicable design documents.

MCMC MTSFB TC G050:2025

11) CTIF 11-ComMech: Communication Mechanisms

The completed CTIF lists all communication mechanisms of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("ComMech-1") or labelling scheme ("ComMech-IP").

- b) **Description:** Brief description of the communication mechanism, including its purpose and a description of the used protocol. For standardized protocols a reference is sufficient. It is indicated additionally whether the mechanism is remotely accessible.

NOTE: A possible communication mechanism is the use of Bluetooth®, WiFi® or NFC for a local connection between a mobile application and the DUT.

- c) **Security Guarantees:** Description of the realized security objectives and the threats the mechanism is protected against.

NOTE: The most common security guarantees to be considered include authentication of peers, authentication of origin, integrity protection, confidentiality protection, and anti-replay.

- d) **Cryptographic Details:** Description of the cryptographic methods (protocols, operations, primitives, modes and key-sizes) used to secure the communication mechanism considering key management, and to facilitate the described "Security Guarantees".

NOTE: Cryptographic Details contain information such as: the protocol Z-Wave® with Security 2 Command Class v1 is used for the communication. The transferred data is authenticated encrypted with AES-128 CCM to facilitate confidentiality and integrity. The key exchange is based on an out-of-band mechanism.

- e) **Resilience Measures:** Description of the measures to ensure that the connection establishment is performed in an orderly fashion including an expected, operational and stable state to achieve a stable connection.

NOTE: Resilience measures consider the sequence of the used protocol, the capability of the infrastructure, reset and initialization of the protocol and problems caused by mass reconnections.

12) CTIF 12-NetSecImpl: Network and Security Implementations

The completed CTIF lists all implementations of network and security functionalities of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("NetSecImpl-1") or labelling scheme ("NetSecImpl-SecLib").

- b) **Description:** Brief description of the implementation of the network or security functionality, including its purpose and scope.

NOTE 30: The kind of implementation (e.g. software library or separate microcontroller) is helpful to determine the relevant functionality for an evaluation or review.

- c) **Review/Evaluation Method:** Description of the method used to review or evaluate the implementation, including the principles it is based on (e.g. audit, peer review, automated code analysis). Additionally, the implementation scope is described, that is covered by the method.

- d) **Report:** Outcome of the review or evaluation or a reference to the certificate or the evaluation report that proves that the implementation has been successfully evaluated.

NOTE: The outcome of the review or evaluation does not need to be a single document. For instance, it is also possible to use the documentation of bug tracking in a software management tool to demonstrate that the implementation is reviewed.

13) CTIF 13-SoftServ: Software Service

This completed CTIF lists all software services of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("SoftServ-1") or labelling scheme ("SoftServ-WebServ").

- b) **Description:** Brief description of the service, including its purpose. It is indicated additionally whether the service is accessible via network interface and whether this is the case in the initialized state.

NOTE 32: A SSH daemon not started by default (disabled), because it was used only for development purposes, is such a service.

- c) **Status:** Indication whether the service is enabled or disabled in the initialized state.
- d) **Justification:** If the service is enabled: Justification why the service is necessary for the intended use or operation of the DUT.
- e) **Allows Configuration (Yes/No):** If the service is accessible via network interface: Indication whether the service allows security-relevant changes in configuration and if so, a brief description of the possible configuration.
- f) **Authentication Mechanism:** If the service is accessible via network interface: Reference to authentication mechanisms in CTIF 1-AuthMech that are used for authentication prior the use of the service.

14) CTIF 14-SecMgmt: Secure Management Processes

The completed CTIF lists all secure management processes for critical security parameters implemented by the SO for the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE 21: Sequential numbering ("SecMgmt-1") or labelling scheme ("SecMgmt-Passwd").

- b) **Description:** Brief description of the secure management process regarding the whole life cycle for critical security parameters. If an existing standard is used, a reference to the corresponding standard is provided.

NOTE: The life cycle of a critical security parameters typically considers generation, provisioning, storage, updates, decommissioning, archival, destruction, processes to handle the expiration and compromise of the parameter.

MCMC MTSFB TC G050:2025

15) CTIF 15-Intf: Interfaces

The completed CTIF lists all network, physical and logical interfaces of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("Intf-1") or labelling scheme ("Intf-LanPort").

- b) **Description:** Brief description of the interface, including its purpose. For physical interfaces, it is described additionally whether the interface is always required, never required or required only in specific cases (e.g. intermittently usage), which are briefly described then.

- c) **Type:** Indication whether the interface is network, physical (includes also air interfaces), logical or several types.

NOTE: The provisions of ETSI TS 103 645 [1]/ETSI EN 303 645 [2] distinguish between network and logical interfaces, but typically both types are equivalent. Therefore, in this case both types are to be indicated.

- d) **Status:** Indication whether the interface is enabled or disabled in the initialized state. For enabled interfaces a justification is given.

- e) **Disclosed Information:** If the interface is a network interface: Description of the information disclosed without authentication in the initialized state and the reason for the disclosure. It is indicated additionally whether the information is security relevant.

NOTE: Disclosed information can be used by an attacker to identify a vulnerable device, e.g. software version.

- f) **Debug Interface:** If the interface is a physical interface: Indication whether the interface can be used as debug interface.

- g) **Protection:** If the interface is a physical interface: Description of the protection methods necessary to limit exposure of the interface.

NOTE:

1. For debug interfaces a description of the software mechanism used to disable the interface is expected (see Test group 5.6-4).

2. For non-radio interfaces a device casing is a protection method.

16) CTIF 16-CodeMin: Code Minimization

The completed CTIF lists all methods for minimizing code. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("CodeMin-1") or labelling scheme ("CodeMin-DeadCode").

- b) **Description:** Brief description of the method used to minimize code to the necessary functionality.

17) CTIF 17-PrivCtrl: Privilege Control

The completed CTIF lists all privilege control mechanisms. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("PrivCtrl-1") or labelling scheme ("PrivCtrl-OS").

- b) **Description:** Brief description of the mechanism to control privileges of software on the DUT.

18) CTIF 18-AccCtrl: Access Control

The completed CTIF lists all access control mechanisms for memory on hardware-level. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("AccCtrl-1") or labelling scheme ("AccCtrl-TEE").

- b) **Description:** Brief description of the hardware-level access control mechanism. It is described additionally how it is supported by the OS of the DUT.

19) CTIF 19-SecDev: Secure Development Processes

The completed CTIF lists all secure development processes implemented by the SO for the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("SecDev-1") or labelling scheme ("SecDev-Testing").

- b) **Description:** Brief description of the secure development process. If an existing standard is used, a reference to the corresponding standard is provided.

20) CTIF 20-SecBoot: Secure Boot Mechanisms

The completed CTIF lists all secure boot mechanisms of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("SecBoot-1") or labelling scheme ("SecBoot-TEE").

- b) **Description:** Brief description of the mechanism (including trust assumptions) used for the secure boot process of the DUT and the part of the software that is protected.

- c) **Security Guarantees:** Description of the realized security objectives of the mechanism.

EAMPLE 28: The mechanisms realize authenticity and integrity of the OS kernel.

- d) **Detection Mechanisms:** Description of the mechanism detecting an unauthorized change in the software of the DUT.

MCMC MTSFB TC G050:2025

- e) **User Notification:** Brief description of how the user is informed about an unauthorized change in the software. It is indicated additionally which information are contained in the notification.

NOTE: Email address of a user account, communication endpoint (e.g. network address or link address) of a user device (e.g. smart phone, smart watch) or status LED are possible ways to inform the user.

- f) **Notification Functionality:** Brief description of the network functionalities necessary to notify a user.

EXAMPLE: SMTP protocol (in case of email notifications), RFCOMM protocol details (in case of Bluetooth® notifications).

21) CTIF 21-PersData: Personal Data

The completed CTIF lists all personal data processed by the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("PersData-1") or labelling scheme ("PersData-PayInfo").

- b) **Description:** Brief description of the category of personal data processed by the DUT.

EXAMPLE: Log data on the usage of the DUT, payment information, timestamped location data, audio input stream or biometric data.

NOTE:

1. According to MCMC MTSFB TC G044, personal data is any information relating to an identified or identifiable natural person. This term is used to align with well-known terminology but has no legal meaning within MCMC MTSFB TC G044 and the present document.
2. Categories of personal data need to be described at a level of detail that provides a general understanding of what kind of data is being processed. This includes a general understanding of the level of sensitivity of personal data aligned with well-known terminology.

- c) **Processing Activities:** Description of how the personal data is being processed, including all involved parties. It is described additionally for what purposes the processing is done.

NOTE: Permanent storage of personal data, also as backup, is a processing activity.

- d) **Communication Mechanisms:** Reference to communication mechanisms in CTIF 11-ComMech that are used for communicating the personal data and an indication whether the communication partner is an associated service (Yes/No). An empty list of communication mechanisms indicates that the personal data is not transmitted.

- e) **Sensitive (Yes/No):** Indication whether the personal data is sensitive according to the definition in the requirement 4.28 in MCMC MTSFB TC G044.

- f) **Obtaining Consent:** If the personal data is processed on the basis of consumer's consent: Description of how the consent for the processing is obtained from the consumer.

- g) **Withdrawing Consent:** If the personal data is processed on the basis of consumer's consent: Description of how the consumer can withdraw the consent for processing the personal data.

22) CTIF 22-ExtSens: External Sensors

The completed CTIF lists all external sensing capabilities of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("ExtSens-1") or labelling scheme ("ExtSens-Cam").

- b) **Description:** Brief description of the sensing capability.

NOTE: Such sensing capabilities can be a microphone or camera.

23) CTIF 23-ResMech: Resilience Mechanisms

The completed CTIF lists all resilience mechanisms for network connectivity and power outages of the DUT. The form contains the following entries and is typically filled in the form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("ResMech-1") or labelling scheme ("ResMech-Power").

- b) **Description:** Description of the mechanism that contributes to the DUT's resilience to network and/or power outages.

NOTE:

1. Such a resilience mechanism can be a journaling mechanism on ext4 that protects the file system's integrity in case of a power outage.
2. Such a resilience mechanism can be a small battery that enables a clean emergency device shutdown (backup battery). It protects against loss of data in case of power outage.

- c) **Type:** Indication whether the resilience mechanism addresses network connectivity or power outages or both.

- d) **Security Guarantees:** Description of the realised security objectives and the threats the mechanism protects against.

EXAMPLE: The mechanism protects the DUT's data integrity in case of a power outage.

24) CTIF 24-TelData: Telemetry Data

The completed CTIF lists all telemetry data collected by the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("TelData-1") or labelling scheme ("TelData-CrashLog").

- b) **Description:** Brief description of the telemetry data being collected and provided to the manufacturer by the DUT.

- c) **Purpose:** Brief description for what purposes the data is collected.

- d) **Security Examination:** If the data is used for security examination: Description of how and by whom (device or associated service) the telemetry data is examined for security anomalies.

MCMC MTSFB TC G050:2025

NOTE:

1. The security anomaly examination can be realized outside the DUT, i.e. by associated services.
 2. A device telemetry service captures crash logs and data on usage (telemetry data) from the DUT in order to enable the developers to determine security flaws (security anomaly detection).
- e) **Personal Data:** Reference to personal data in CTIF 21-PersData that are processed in the telemetry data.

25) CTIF 25-DelFunc: Deletion Functionalities

The completed CTIF lists all deletion functionalities for data of the user. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("DelFunc-1") or labelling scheme ("DelFunc-CloudServ").

- b) **Description:** Brief description of the functionality used to delete data of the user. If the "Target Type" indicates that an associated service is addressed: The concerning associated service which is covered by the functionality is indicated additionally.

NOTE: The DUT's settings could provide a functionality to remove personal data from a cloud server.

- c) **Target Type:** Indicates whether the functionality addresses user data on the device or personal data on associated services or both.
- d) **Initiation and Interaction:** Brief description of the user interaction, which is necessary to initiate and apply the deletion functionality.
- e) **Confirmation:** Brief description of how the user is given indication that the addressed data has been deleted after applying the deletion functionality.

26) CTIF 26-UserDec: User Decisions

The completed CTIF lists all decisions to be taken by the user during installation and maintenance. The form contains the following entries and is typically filled in the form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("UserDec-1") or labelling scheme ("UserDec-Encrypt").

- b) **Description:** Description of the decision to be taken by the user within the installation and maintenance flows. Its position within the installation or maintenance flow is additionally described.
- c) **Options:** Description of the security-relevant options the user can take and an indication for the default value.
- d) **Triggered By:** Brief description how the decision is triggered. It is indicated additionally whether the decision can be triggered by the user.

27) CTIF 27-UserIntf: User Interfaces

The completed CTIF lists all user interfaces of the DUT, which enable input from the user. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("UserIntf-1") or labelling scheme ("UserIntf-Config").

- b) **Description:** Brief description of the user interface enabling data input from the user. It is indicated additionally how the interface can be accessed by the user.

28) CTIF 28-ExtAPI: External APIs

The completed CTIF lists all APIs of the DUT, which enables data input from external sources. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("ExtAPI-1") or labelling scheme ("ExtAPI-SOAP-Cloud").

- b) **Description:** Description of the API enabling data input from external sources of the DUT.

NOTE: External APIs are typically used for machine-to-machine communication.

29) CTIF 29-InpVal: Data Input Validation

The completed CTIF lists all data input validation methods of the DUT. The form contains the following entries and is typically filled out in form of a table.

- a) **ID:** Unique per CTIF identifier, that may be assigned using a sequential numbering scheme or some other labelling scheme.

EXAMPLE: Sequential numbering ("InpVal-1") or labelling scheme ("InpVal-NetwCom").

- b) **Description:** Description of the method for validating the data input via user interfaces or transferred via APIs and between networks in services and devices including the handling of unexpected data. It is indicated additionally which of the sources for data input are addressed by the method.

NOTE: To validate the data input, it can be checked whether it is of an allowed type (format and structure), of allowed value, an allowed cardinality or an allowed ordering.

Annex D
(normative)

Sample of Comprehensive Testing Information File (CTIF)

To demonstrate the scope and level of details on completing the CTIF form, Annex D provides a brief overview of the sample DUT as seen in Figure D.1 below.

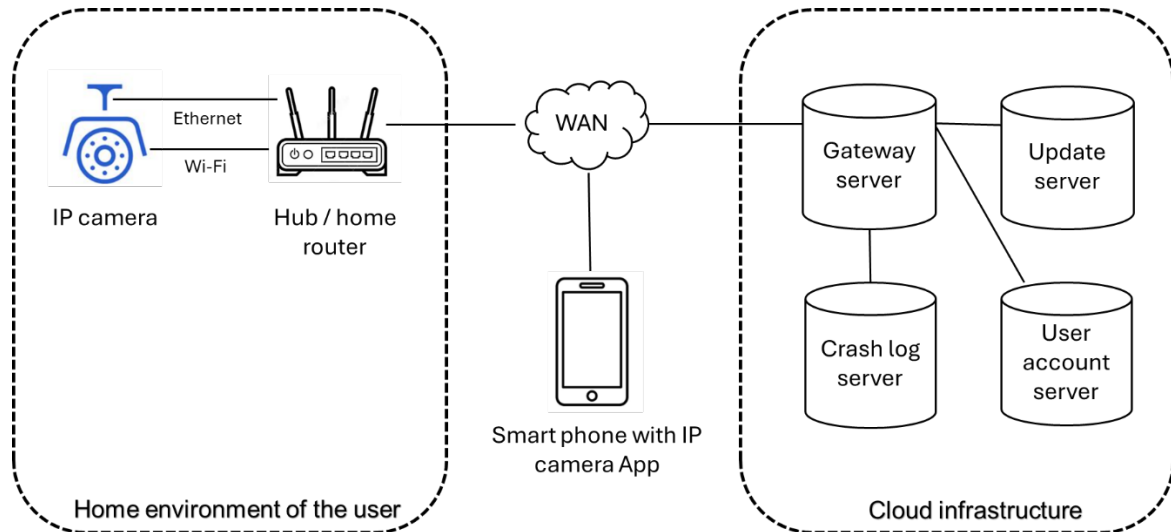


Figure D.1 Infrastructure used for sample CTIF

Main functionalities used in the sample of CTIF demonstrated in 3 main categories as below.

1) Interoperability test examples

The DUT sample of CTIF is a fictional IP camera "IPC 2000" that has real-world functionalities typically and representative for an IoT device. It is functioning to record and playback of video and audio data, e.g. of the user's estate, which can be viewed through the corresponding app "IP camera App" or the web interface. The IP camera is connected via Local Area Network (LAN) or Wireless Local Area Network (WLAN) to the network of the user and can be configured by a local web interface or the app. Web interface and app provide also the capability of performing firmware updates or user management.

2) Exchangeability test examples

To access the web interface, the user has to complete an authentication process before, using username and password. Moreover, the user can connect to the camera via SSH after enabling this functionality in the configuration. This interface can be used to copy video files script based or to check log files. The IP camera also offers a Simple Object Access Protocol (SOAP) interface that can be used by other devices to control the movement of the camera and receive audio and video streams via a direct connection. Connections between IP camera and app are managed by cloud servers of the manufacturer (the cloud infrastructure represents the associated services of the DUT). There is no direct connection between the app and the IP camera itself. This infrastructure is contacted when the user decides to submit crash reports or to contact the developer's support. The cloud servers also provide the firmware updates for the IP camera.

3) Implementation test examples

The IP camera provides different update mechanisms to install software updates. The default way is the user initiation via web interface or app, where the user is also informed about the availability of an update. Alternatively, the user can attach a USB drive with an update file the user downloaded from the manufacturer's website before. In both cases the update package is encrypted, and the integrity and authenticity are verified before an installation.

These examples serve as a reference for conducting CTIF to ensure that IoT devices meet baseline security requirements.

Annex E
(normative)

Sample of complete forms for the Supplier Organisation (SO)

To assist with practical implementation, Table 1 until Table 29 in this Annex E offers a sample with guidance on completing different sections of the CTIF form.

Table E.1 Sample CTIF 1-AuthMech (Authentication Mechanisms)

ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention
AuthMech-1	A user can login over HTTPS at port 443 to gain access to the web frontend. (A user can request a login over HyperText Transfer Protocol (HTTP) at port 80 but is forwarded automatically to HTTPS on port 443.). The authentication on the login page is to be completed before any payload data over HTTPS is exchanged. No payload is readable without logging in first. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	Username and password (pre-installed and used in initialised state).	The username is fixed "admin". The password is generated randomly and is unique per device. The password has a length of 16 and consists of upper case chars, lower case chars and numbers. The password is generated by use of /dev/urandom on a UNIX configuration system during manufacturing phase.	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via a form-based Hyper Text Markup Language (HTML) interface by an internal Hypertext Preprocessor (PHP) script in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over Transport Layer Security (TLS) 1.2. The DUT provides per default the following cipher suites for the TLS handshake: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 3 invalid login attempts the login interface is inaccessible for 5 minutes.

Table E.1 Sample CTIF 1-AuthMech (Authentication Mechanisms) (continued)

ID	Description	Authentication Factor	Password Generation Mechanism	Security Guarantees	Cryptographic Details	Brute Force Prevention
AuthMech-2	A device can exchange data with the DUT over HTTPS/SOAP on port 8085. The authentication via Basic-Auth is confirmed before any payload data over HTTP is exchanged. No payload is readable without providing correct access credentials. The web server authenticates the given credentials against the login information stored in its SQLite database and grants access to the requested resources. The mechanism is used for machine-to-machine authentication. The mechanism is directly addressable from a network interface.	Username and password (set by user and used in initialised state).	N/A (Authentication mechanism is password set by the user)	The username and password are transmitted over an HTTPS channel, so the DUT ensures confidentiality and integrity during the transfer.	Authentication is performed via an HTTP authentication framework (IETF RFC 7235 [i.8]) by the internal Apache Webserver in combination with an SQLite database. Integrity and confidentiality of the password transfer to the DUT is realized over TLS 1.2 with the TLS cipher suites: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	After 10 invalid login attempts user or password combination is disabled for further access.
AuthMech-3	The user can login via SSH at port 22 to gain remote command line access. The authentication via SSH is confirmed before any payload data over SSH is exchanged. No payload is readable without providing correct access credentials. The SSH server authenticates a given signature against the public keys stored on the file system. (The private key is generated on the DUT the key pair can be downloaded over an HTTPS channel via the web interface.) The mechanism is used for user-to-machine authentication. The mechanism is directly addressable from a network interface.	Client private and public key.	N/A (Authentication mechanism is not a password)	With the use of SSH the DUT ensures confidentiality, authenticity and integrity during the transfer.	Authentication is performed via the SSH protocol (IETF RFC 4253 [i.10]) by the internal SSH server of the DUT. The key pair is built on ECDSA 256 bit and is not protected with a password. Integrity and confidentiality of the SSH credentials to the DUT is realized over SSH2 with cipher suites conformant to the following security parameters: Key exchange: diffie-hellman-group-exchange-sha256 (2048-bit), encryption: AEAD_AES_256_GCM, Media Access Control (MAC): hmac-sha2-256.	The DUT uses the "fail2ban" framework as unix daemon that scans the system log files for rejected login attempts and dynamically adjusts the firewall rules to drop packets from an attacker's IP address.

MCMC MTSFB TC G050:2025

Table E.2 Sample CTIF 2-UserInfo (User Information)

Documentation of Change Mechanisms	The user can find information for changing the authentication values in the PDF-File user's manual IPC 2000 downloadable on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 3. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Menus".
Documentation of Replacement	<i>N/A (There are no non-updatable components)</i>
Documentation of Sensors	The microphone functionality, camera functionality (visible spectrum), and camera functionality (infrared spectrum) are explained on the product website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 9. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Functional Overview".
Documentation of Secure Setup	The user is guided through a setup wizard per pre-defined dialogs after the initial password is changed. By these dialogs it is ensured that no insecure configuration can be made by user during the setup. The dialogs are documented on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 1. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Setup".
Documentation of Setup Check	Every user input is checked against validation rules. The only option where the user can make an insecure choice is the password for new user accounts. If the entered password does not comply with the password rules, the user is notified immediately over the web interface or the App and the setup procedure cannot be continued until the user chooses a valid input. The dialogs are documented on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 1. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Setup".
Documentation of Personal Data	The user can find this information in PDF-File user's manual IPC 2000 downloadable on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 6. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Reset".
Documentation of Telemetry Data	The user can find this information in PDF-File user's manual IPC 2000 downloadable on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 6. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Reset".
Documentation of Deletion	The user can find this information on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 7. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Reset" and "Help" -> "Account deletion".
Model Designation	The model designation "IPC 2000" is provided to user on the bottom of the DUT's case in plain text. Also the designation can be read from the app under "Help" -> "About" and from the web interface under "Devices".
Support Period	This DUT is actively maintained concerning security updates for the following 6 years after placing on the market.
Publication of Support Period	The user can find this information on the website of the Example Vendor Inc., accessible under https://example.net/support/devices/ip-camera-example . The printed product information contains this URL in section 4. In addition, the URL can be accessed directly through the IP camera app under "Help" -> "Security Policy".

Table E.3 Sample CTIF 3-VulnTypes (Relevant Vulnerabilities)

ID	Description	Action	Time Frame
VulnTypes-1	Vulnerabilities on the user web frontend regarding HTTP, PHP or HTML and the integration into the related components (web server, database, OS and used libraries).	<p>When a notification about a potential vulnerability is received via the contact form according to the Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw.</p> <p>If the SIT confirms the vulnerability, it proposes a fix for the Software Development Department (SDD). The SDD then implements the fix and verifies the effectiveness within. After confirmation from both teams that the vulnerability is fixed, the new firmware is rolled out and the updated changelog is published with containing a description of the closed vulnerability.</p>	7 days for initial response, 30 days for SIT to investigate and propose a fix, 30 days for SDD to integrate the fix. By no later than 90 days after receiving the vulnerability the fix will be released according to the published vulnerability disclosure policy.
VulnTypes-2	Vulnerabilities concerning the hardware or underlying OS.	<p>When a notification about a potential vulnerability is received via the contact form according to Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw.</p> <p>If the SIT confirms the vulnerability, it contacts the vendors of the underlying OS or hardware via a defined support email address (the responsible contact persons are known) to discuss further steps. If the vulnerability affects the hardware, the SIT will try to mitigate the issue in software in corporation with the external vendor. If the hardware affects the underlying OS, the SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD).</p> <p>Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by Example Vendor Inc. a warning for customers is published on the website under the following URL: https://example.net/support/devices/ip-camera-example.</p>	7 days for initial response are defined according to the published vulnerability disclosure policy. Usually 90 days after receiving the vulnerability a fix will be released or a warning is published. The warning will be withdrawn since a fix is released.

MCMC MTSFB TC G050:2025

Table E.3 Sample CTIF 3-VulnTypes (Relevant Vulnerabilities) (continued)

ID	Description	Action	Time Frame
VulnTypes-3	Vulnerabilities concerning commercially licensed third-party libraries.	<p>When a notification about a potential vulnerability is received via the contact form according to the Vulnerability Disclosure Policy, the notification is forwarded to the Security Incident Team (SIT) where it is investigated. If needed, the team contacts the user who originally submitted the form in order to exchange further information about the flaw. If the SIT confirms the vulnerability, it contacts the vendor of the library via a defined support email address (the responsible contact persons are known) to discuss further steps. The SIT will contact the particular vendor for help on this issue. Any change of software will be handled and released by the Software Development Department (SDD). Depended on the result, a fix is rolled out or in case the vulnerability cannot be fixed by</p> <p>Example Vendor Inc. a warning for customers is published on the website under the following URL: https://example.net/support/devices/ip-camera-example.</p>	7 days for initial response are defined according to the published vulnerability disclosure policy. By no later than 60 days after receiving the vulnerability a fix will be released or a warning is published, as it is assured by contract with the third parties.

Table E.4 Sample CTIF 4-Conf (Confirmations)

Confirmation of Vulnerability Actions	Yes
Confirmation of Vulnerability Monitoring	Yes
Confirmation of Update Procedures	Yes
Confirmation of Secure Management	Yes
Confirmation of Secure Development	Yes

Table E.6 Sample CTIF 6-SoftComp (Software Components)

ID	Description	Update Mechanism	Cryptographic Usage
SoftComp-1	Firmware consisting of a Linux-based OS, the OpenSSL cryptographic library, Apache Web-Server including PHP and SQLite, various libraries.	Firmware can be updated according to UpdMech-1, UpdMech-2, and Upd-Mech-3.	Yes, the firmware includes the cryptographic algorithms available to the DUT. Yes, side effects of updating those algorithms and primitives are considered by the manufacturer through exhaustive testing of the DUT's interfaces by the Software Development Department (SDD), both with negative and positive tests.
SoftComp-2	BL1 according to https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/design/firmware-design.rst that is responsible for booting up the Advanced RISC Machines (ARM) processor.	The BL cannot be updated since this the root component for the boot process and resides in Read Only Memory (ROM).	Yes, the BL contains cryptographic algorithms necessary for checking the signature of the BL2. Since this component cannot be updated, the manufacturer did not consider side effects of updating these algorithms.

Table E.7: Sample CTIF 7-UpdMech (Update Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Initiation and Interaction	Configuration	Update Checking	User Notification
UpdMech-1	User-initiated firmware update over web interface. The DUT queries the update server https://update.example.net to verify if an update is available. This is done automatically once per day. If an update is available, the DUT notifies the user about it or starts the update automatically, depending on its configuration.	The update mechanism provides confidentiality by encrypting the update package. The used encryption key is a hard-coded Advanced Encryption Standard (AES) key (which itself is updatable as well) of the update server.	Confidentiality of a software update is realized by an encrypted firmware package based on 10.6028/NIST.FIPS.197. For the decryption AES-CBC with 128 bits is used, in conformance to SOG-IS Crypto Evaluation Scheme Agreed Cryptographic Mechanisms, Version 1.2.	The DUT checks automatically once a day (the time is chosen randomly for each day) for firmware updates stored at https://update.example.net . The user will be notified when an update is available.	The user can configure the DUT to start an update automatically when available.	The DUT contacts the update server at https://update.example.net once per day (the time is chosen randomly for each day).	The user is notified via the app (by push messages) about a pending update. The user is also informed after login on the web interface.

MCMC MTSFB TC G050:2025

Table E.7: Sample CTIF 7-UpdMech (Update Mechanisms) (continued)

ID	Description	Security Guarantees	Cryptographic Details	Initiation and Interaction	Configuration	Update Checking	User Notification
UpdMech-1	When the user or the DUT itself starts the update mechanism, the server delivers the update to the DUT over its network connection. The update package is encrypted using a static symmetric key. The DUT decrypts the update package and then verifies authenticity and integrity of the decrypted update using an asymmetric key and the installation is initiated. Once the update is finished, the user is notified about the successful update.	The DUT verifies integrity and authenticity of the update file against a hard-coded RSA public key (which itself is updatable as well) of the update server.	Authenticity and integrity of a software update is realized by a signed firmware package based on IETF RFC 8017. For the signature SHA-512 with RSA 4096 bit and Optimal Asymmetric Encryption Padding (OAEP) is used, in conformance to SOG- IS Crypto Evaluation Agreed Cryptographic Mechanisms, Version 1.2. The signing of the firmware package is performed with the private key of the update server. The public key for the update validation is integrated during the manufacturing process of the DUT and is hard-coded in the software. A downgrade attack is prevented by the DUT by verifying that the version of a new firmware package cannot be lower than the version of the currently installed one.	The user then can trigger the update by logging in to the web interface and manually starting the update process by pressing the button "Apply update and restart", or the DUT starts the update itself automatically, depending on its configuration. Once the update is started it proceeds without any further user interaction.	The default option is that the user is only notified about an update and triggers it manually. In this case the user is asked whether the update should be installed now or on a later date ("install now" or "postpone").	If the server is not reachable, the update check is postponed for 2 hours. The DUT initiates and performs the update check.	The notification contains: <ul style="list-style-type: none"> • estimated time needed to apply the update • a warning that during this period the services will be not available • brief changelog of the most important changes The notifications on the web interface are realized by the DUT itself.

Table E.7: Sample CTIF 7-UpdMech (Update Mechanisms) (concluded)

ID	Description	Security Guarantees	Cryptographic Details	Initiation and Interaction	Configuration	Update Checking	User Notification
UpdMech-2	User-initiated firmware update over the app. The description same as UpdMech-1, the only difference is that the update is triggered through the app.	See UpdMech-1.	See UpdMech-1.	See UpdMech-1.	See UpdMech- 1.	See UpdMech-1.	See UpdMech-1.
UpdMech-3	User-initiated firmware update over USB. The user plugs in a USB drive with a firmware file to a local computer and points the DUT to the file via the web interface. This is done manually. When the user starts the update mechanism, the DUT verifies authenticity and integrity of the update file and the installation is initiated. Once the update is finished, the user is notified about the successful update.	See UpdMech-1.	See UpdMech-1.	The user then can trigger the update by logging in to the web interface and manually pointing the DUT to the update file. The update file can be downloaded from https://example.net/updates/devices/ip-camera-example and copied onto an USB stick by the user. Then the user starts the update process by pressing the button "Apply update and restart" on the web interface. Once the update is started it proceeds without any further user interaction.	No configuration options.	The user initiates the update manually.	Since the DUT does not have any meta data about the update, only a warning that during the update period the services will be not available is displayed.

MCMC MTSFB TC G050:2025

Table E.8: Sample CTIF 8-UpdProc (Update Procedures)

ID	Description	Time Frame
UpdProc-1	Every release of the DUT's firmware is under responsibility of the Software Development Team (SDD). The SDD is responsible for integrating security fixes and testing the firmware with positive and negative tests. Once the change was is verified and tested, the SDD rolls out the update over the official update server. To coordinate the handling of security fixes the team uses an internal ticket system, so that no security fix will be overlooked. The changes regarding each firmware release are protocolled in a changelog by the SDD, which is published on the product website.	As mentioned in VulnTypes-1 the time for rolling out a new firmware is 30 days.
NOTE: CTIF 9-ReplSup is only applicable for constrained devices. Since the fictional IP camera is not a constrained device in the sense of ETSI TS 103 645 [1]/ETSI EN 303 645 [2], Table C.9 is filled with exemplary information that is not directly related to the IP camera. Instead, another fictional device is used as an example, namely a window sensor that can detect the opening or closing of a window and submits its state via ZigBee® to a ZigBee® hub		

Table E.9 Sample CTIF 9-ReplSup (Replacement Support)

Isolation	The window sensor can be disconnected from the ZigBee® network in the Smart Hub it is connected to. Afterwards the signals from the window sensor cannot affect the network anymore. In this case the window sensor remains its core functionality to notify a user about the opening or closing of a window by a short acoustical peep sound emitted in case of such an event.
Hardware Replacement	The window sensor can be replaced as a whole by a new window sensor device, which is then connected to the ZigBee® network instead of the old one.

Table E.10: Sample CTIF 10-SecParam (Security Parameters)

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-1	RSA public signature key of update server to verify authenticity and integrity of firmware updates (after decrypting with SecParam-2). The key is not a hard-coded identity The key is hard-coded in device software source code.	Public	The key is not modifiable by an attacker so that its integrity is ensured.	A trustworthy user does not have access to the key through any interfaces. A non-trustworthy user needs root access to stop the update process and change the key. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to read and to modify the key is the software update process which is run under a different account "software-updater" than any of the accounts used for external interfaces.	N/A (The security parameter is not critical)	N/A <i>(The security parameter is not transmitted)</i>	N/A (The security parameter is not critical)

Table E.10: Sample CTIF 10-SecParam (Security Parameters) (continued)

ID	Description	Type	Security Guarantees	Protection Scheme	Provisioning Mechanism	Communication Mechanisms	Generation Mechanism
SecParam-2	AES key for decrypting firmware update packages (prior to verifying with SecParam-1). The key is not a hard-coded identity. The key is hard-coded in device software source code.	Critical	The key is not accessible by an attacker so that its confidentiality is ensured.	An attacker needs access to the file system on the DUT or the firmware package to gain access to the key. The delivered firmware package from the update server is encrypted. Therefore, the key is not extractable. Access to the file system is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify and read the key is the software update process, which is run under a different account "software-updater" than any of the accounts used for external interfaces.	The key is hard-coded in the firmware and is modified only through a verified firmware update package.	N/A (Parameter is not transmitted)	The AES key is generated before a firmware update package is released on a separate offline Linux® Personal Computer (PC) with the most recent OpenSSL version at the time of the key generation. OpenSSL uses its own random number generator, which is seeded by /dev/random of the Linux® machine. /dev/random, in turn, is seeded by an Hardware Security Module (HSM) connected to the machine.
SecParam-3	ECDSA public key in X.509 certificate for authentication in TLS connection over web interface. This key is a hard-coded identity. The key is hard-coded in device software source code.	Public	The key is not modifiable by an attacker so that its integrity is ensured.	An attacker needs access to the file system on the DUT to change the certificate. This is prevented by input validation of data presented to the DUT's interfaces and the access management of the OS. The only user role that has access rights to modify the key is the software update process, which is run under a different account "software-updater" than any of the processes used for external interfaces.	The private key is hard-coded in the firmware and is modified only through a verified firmware update package.	ComMech-1	N/A (Parameter is not used for integrity and authenticity checks of software updates or for protection of communication with associated services)

MCMC MTSFB TC G050:2025

Table E.11 Sample CTIF 11-ComMech (Communication Mechanisms)

ID	Description	Security Guarantees	Cryptographic Details	Resilience Measures
ComMech-1	The DUT offers a connection for its web interface in a LAN environment as server. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: The DUT acts as TLS server which offers the following cipher suites for the connection establishment: ECDHE- ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. Mass reconnections may result in a DoS of the DUT, however the security of its services would be unaffected by this.
ComMech-2	The DUT uses a connection to the associated services (cloud infrastructure) https://cloud.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no potential problems regarding mass connections.
ComMech-3	The DUT uses a connection to the update server https://update.example.net as client. This connection is based on IP/TCP/HTTPS. The mechanism is remotely accessible.	Through TLS the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over TLS 1.2 with the following TLS cipher suites which define all crypto primitives: ECDHE-ECDSA-AES128-GCM-SHA256 or ECDHE-ECDSA-AES256-GCM-SHA384.	The connection uses the well-defined TLS protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. As the DUT is the client there are no potential problems regarding mass connections.
ComMech-4	The DUT offers a connection for its SSH interface in a LAN environment as server. This connection is based on IP/TCP/SSH. The mechanism is remotely accessible.	Through SSH the communication guarantees authenticity of the DUT, integrity and confidentiality of exchanged packets, and anti-replay mechanisms.	All Security Guarantees are realized over the SSH2 protocol keys with cipher suites conformant to the following security parameters: Key exchange: diffie-hellman-group-exchange-sha256 (2048-bit), encryption: AEAD_AES_256_GCM, MAC: hmac-sha2-256	The connection uses the well-defined SSH2 protocol to establish the connection, which covers an ordered protocol sequence, defined state machines, and defined initialization and reset mechanisms. Mass reconnections may result in a DoS of the DUT, however the security of its services would be unaffected by this.

Table E.12: Sample CTIF 12-NetSecImpl (Network and Security Implementations)

ID	Description	Review/Evaluation Method	Report
NetSecImpl-1	The network functionality is implemented by the Linux® network stack. Its purpose is to provide APIs for the application layer to be used by the DUT applications like the internal web server. It is part of the Linux® kernel, version 5.10.30.	The Linux® network stack is widely used on all type of systems all over the world. The Example Vendor Inc. itself did not review the stack. It trusts on the analysis made by security researchers not employed by Example Vendor Inc. The way defects are reported is described on the websites of the Linux® Foundation: https://www.linuxfoundation.org/en/blog/how-to-report-security-vulnerabilities-to-the-linux-foundation/ .	None generated especially for this DUT.
NetSecImpl-2	The cryptographic functionality regarding the web interfaces is provided by the OpenSSL library, version 1.1.1k. Its purpose is to provide all cryptographic functions necessary for operate the web interfaces.	The Example Vendor Inc. did a code review of the OpenSSL parts used by the DUT. The review was done by two people which used an approach of both manual and automated code analysis. The team manually reviewed code responsible for the Diffie-Hellmann key exchange. If vulnerabilities had been discovered, the team would have followed the instructions published on https://www.openssl.org/community/#securityreports . The code was also analysed with a Static Code Analyzing Tool named EXAMPLE TOOL. This tool searches for potential race conditions, buffer overflows, out-of-bound errors, and format-string attacks.	The review team generated an internal code audit report which is attached to this CTIF. Neither the manual nor the automated code analysis found any vulnerabilities.
NetSecImpl-3	The cryptographic functionality regarding the update verification is provided by the Botan library, version 2.18.0. Its purpose is to provide all cryptographic functions necessary for the update verification.	The Botan code was reviewed by Rohde & Schwarz® together with the BSI, see https://www.bsi.bund.de/EN/Topics/Cryptography/CryptoLibrary/cryptolibrary_node.html	The report is available under https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Krypto/Projektzusammenfassung_Botan.pdf?blob=publicationFile&v=1 . The report mentions that all found potential vulnerabilities were fixed, side channel attack resistance was evaluated, missing crypto primitives were implemented according to standards and/or RFCs, and a test specification was implemented.

MCMC MTSFB TC G050:2025

Table E.13: Sample CTIF 13-SoftServ (Software Services)

ID	Description	Status	Justification	Allows Configuration	Authentication Mechanism
SoftServ-1	Web service for providing the HTTP interface. The service is accessible over the network. The service is accessible in the initialized state.	Enabled	The service is necessary to provide the user the possibility to configure the DUT.	Yes. The user can <ul style="list-style-type: none"> configure username/password configurations for web access, configure SSH accounts. 	AuthMech-1, AuthMech-2
SoftServ-2	SSH service for providing a remote command line access. The service is accessible over the network. The service is not accessible in the initialized state and needs to be enabled by the user.	Disabled	N/A <i>(The service is not enabled)</i>	Yes. The user has limited file system access which allows him/her to modify configuration files, read video and audio stream files.	AuthMech-3
SoftServ-3	Update service for downloading and applying firmware updates. The service is not accessible over the network.	Enabled	The service is responsible for checking remote for firmware updates and is enabled by default for security reasons.	No.	N/A <i>(The service is not accessible over the network)</i>
SoftServ-4	Video service for capturing and processing video and audio signal and providing it as a data stream. The service is accessible over the network. The service is accessible in the initialized state.	Enabled	The service represents the core functionality and therefore is enabled by default.	No.	AuthMech-1, AuthMech-2

Table E.14: Sample CTIF 14-SecMgmt (Secure Management Processes)

ID	Description
SecMgmt-1	The Example Vendor Inc. uses ANSI/ISA-62443 to manage its security management processes. This includes all critical security parameters listed in CTIF 10- SecParam. The documentation of the implementation of the standard is attached. In conformance to the standard, it covers the generation and provisioning of security parameters according to sections 5 and 8. The storage is done according to section 5. Updates are handled according to sections 9, 10 and 11. The decommissioning and expiration of the DUT is done according to section 12.

Table C.15: Sample CTIF 15-Intf (Interfaces)

ID	Description	Type	Status	Disclosed Information	Debug Interface	Protection
Intf-1	Ethernet interface required to configure the DUT.	Network, physical, logical	Enabled, because the user needs access to configure the DUT.	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which Common Vulnerabilities and Exposures (CVE) the DUT is vulnerable.	N/A <i>(The interface is not a physical interface)</i>	N/A <i>(The interface is not a physical interface)</i>
Intf-2	WLAN interface to connect the user's wireless environment.	Network, physical, logical	Disabled	This interface discloses the Apache web server version number. This information is security-relevant because it can give an attacker hints to which CVEs the DUT is vulnerable.	N/A <i>(The interface is not a physical interface)</i>	N/A <i>(The interface is not a physical interface)</i>
Intf-3	The board of the DUT has a Joint Test Action Group (JTAG) interface. This interface is not required for the DUT's normal operation.	Physical, logical	Enabled, because it is used to initially flash the DUT. The interface cannot be disabled by the firmware.	The JTAG interface discloses diagnosis information. This information is security-relevant because it can give an attacker complete access to the DUT's software.	Yes, this interface is just used for debug purposes.	The interface is protected by the DUT's casing. The case is adhered, hence it requires a careful and time-consuming approach to access the interface without damaging the casing, which would be visible for the user.
Intf-4	USB interface for manual firmware updates.	Physical	Enabled, because it is used for manual firmware updates in case the DUT is not connected to a network.	None.	No, this interface cannot be used for debug purposes.	There is no need to limit exposure of the interface because its accessibility is necessary to provide its functionality.

MCMC MTSFB TC G050:2025

Table E.16: Sample CTIF 16-CodeMin (Code Minimization)

ID	Description
CodeMin-1	The code is analysed with static code analysis tools during the development phase. The tools list unused functions which are removed according to section 8 of ANSI/ISA-62443.
CodeMin-2	The Example Vendor Inc. uses a code review process according to section 8 of ANSI/ISA-62443. Each code change is reviewed by at least one additional person to ensure that code published in official firmware packages does not contain any unused functions and statements.

Table E.17: Sample CTIF 17-PrivCtrl (Privilege Control)

ID	Description
PrivCtrl-1	The Example Vendor Inc. uses a secure code design process according to section 7 of ANSI/ISA-62443. This includes that for each component of the DUT a list of all technical user accounts and their privileges is maintained. During the design process the privileges are planned to have a minimal configuration so that the DUT's operation is not disturbed. The correct implementation of the defined privileges is then checked by tests according to section 9 of ANSI/ISA-62443 so that it is ensured that each component is operating with at least privileges as possible.

Table E.18: Sample CTIF 18-AccCtrl (Access Control)

ID	Description
AccCtrl-1	The DUT uses an ARM Cortex A8 processor which includes a memory management unit responsible for assigning memory access permissions and memory attributes to separated regions for different processes. The memory management unit controls table walk hardware that accesses translation tables in main memory by enabling a fine-grained memory system control through a set of virtual-to-physical address mappings and memory attributes held in instruction and data TLBs. The OS Arch Linux® ARM depends heavily on use of the memory management unit, especially with its page table management.

Table E.19: Sample CTIF 19-SecDev (Secure Development Processes)

ID	Description
SecDev-1	The Example Vendor Inc. uses a secure development process according to ANSI/ISA-62443. This covers the specification of security requirements by threat models, a defined review process by at least two persons of the security design, the usage of the coding standard MISRA-C for a well-formed implementation representation, the application of pair programming so that every code change is reviewed by at least one additional person, and defined testing strategies including penetration testing and negative testing.

Table E.20: Sample CTIF 20-SecBoot (Secure Boot Mechanisms)

ID	Description	Security Guarantees	Detection Mechanisms	User Notification	Notification Functionality
SecBoot-1	<p>The DUT implements a secure boot process. The bootloader is based on Trusted Board Boot (TBB), which prevents malicious firmware from running on the platform by authenticating all firmware images up to and including the normal world bootloader. It is done by establishing a Chain of Trust using Public-Key Cryptography Standards (PKCS). The root of trust is a hardcoded public key that is initially loaded at the DUT's first configuration. The trust key is immutable and cannot be changed. The root of trust together with the Random Access Memory (RAM) chip is certified according to Platform Security Architecture (PSA) Level 3. A SHA256 of this key is stored into trusted root-key registers. The boot mechanism includes various BLs. The BL1 resides in the ROM so it cannot be tampered with. The succeeding other BL images BL2, BL31, and BL33 are loaded one after another, where for each BL its integrity is verified by its preceding BL. A chain of trust for the software loaded by the ARM chip is done as described in the section "TTB Sequence" at https://github.com/ARM-software/arm-trusted-firmware/blob/master/docs/design/trusted-board-boot.rst.</p>	<p>By establishing a consistent chain of trust, the complete software image including the OS kernel is protected, so that both integrity and authenticity are ensured. The software image is protected against manipulation before booting up.</p>	<p>If an arbitrary part of the BL chain including the software image cannot be verified, the DUT's verification of its BLs will fail because the signature check fails. In this case the DUT panics and stops its boot process completely.</p>	<p>The user will be notified through a red blinking LED at the left side of the DUT when an unauthorised change appears.</p>	<p>There are no network functionalities involved.</p>

MCMC MTSFB TC G050:2025

Table E.21: Sample CTIF 21-PersData (Personal Data)

ID	Description	Processing Activities	Communication Mechanisms	Sensitive	Obtaining Consent	Withdrawing Consent
PersData-1	Full name of the user	The user's name is entered on the app or the web interface and is used for displaying an individualized welcome message. Also the user's name will be used for sending failure reports solely to the Example Vendor Inc.	ComMech-2, ComMech-1. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw their consent by resetting the DUT to factory defaults.
PersData-2	Email address of the user	The user's email address is entered on the app and the DUT and used for identifying a user against the backend servers. Also the user's email address will be used for sending failure reports solely to the Example Vendor Inc. and for advertisement emails regarding products of the Example Vendor Inc.	ComMech-2, ComMech-1. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw his/her consent for receiving advertisement emails by sending an email to privacy@example.net to opting out.
PersData-3	Global Positioning System (GPS) data of the DUT's location	The GPS data is transmitted to the associated services (cloud infrastructure) of Example Vendor Inc. for a statistical evaluation to find out where its products are being used.	ComMech-2. The communication partner is an associated service.	Yes	The user needs to confirm the general terms and conditions prior to installing the DUT and the app.	The user can withdraw his/her consent by disabling the checkbox "Help improving this product" on the configuration page on the web interface or in the app.

Table E.22: Sample CTIF 22-ExtSens (External Sensors)

ID	Description
ExtSens-1	Microphone to record the sound of the DUT's environment located on the front of the DUT.
ExtSens-2	Camera (visible spectrum) to record the DUT's environment located on the front of the DUT.
ExtSens-3	Camera (infrared spectrum) for the DUT's motion sensor functionality located on the front of the DUT.

Table E.23: Sample CTIF 23-ResMech (Resilience Mechanisms)

ID	Description	Type	Security Guarantees
ResMech-1	The DUT uses a built-in battery that can supply the DUT with power for 15 minutes. After 12 minutes of power outage the DUT initiates a graceful shutdown. However, to increase system stability the DUT also uses the UBIFS file system that was designed with tolerance against hard power-cuts.	Power outage	The DUT's main functions, the video and audio stream, completely remain operational during a power outage of max. 12 minutes. In case there is a hard power-cut, the DUT remains operational after booting up again and is not affected negatively by a corrupted file system.
ResMech-2	The DUT buffers its video and audio data for 5 minutes to provide resilience against network failures. After reconnection the video and audio data can be received by external devices normally.	Network connectivity	The DUT's main functions, the video and audio stream, completely remain operational during a network failures of max. 5 minutes.

Table E.24: Sample CTIF 24-TelData (Telemetry Data)

ID	Description	Purpose	Security Examination	Personal Data
TelData-1	Crash data in case of a service failure. In case of a crashed process the DUT writes a core dump file containing the state of a process when the process receives certain signals, e.g. segmentation fault or illegal instruction. The core dump contains a snapshot of the allocated memory and registers.	The data will be analysed by the Example Vendor Inc. to improve especially the system stability of its products.	The telemetry data is uploaded after a crash (caused by a security violation) without any user interaction to the associated services (cloud infrastructure) of Example Vendor Inc. so that it can be analysed what caused the crash and what code improvements are possible. The core dump is analysed with GNU Debugger (GDB) and similar tools by the staff of Example Vendor Inc. to gain the necessary information.	PersData-3, PersData-4, PersData-5
TelData-2	Crash data in case of a kernel failure. In case of a crashed kernel the DUT automatically boots into a second kernel using kexec and writes a crash dump file containing the whole volatile RAM. The DUT then automatically boots into the original kernel.	The data will be analysed by the Example Vendor Inc. to improve especially the system stability of its products.	The telemetry data is uploaded without any user interaction to the associated services (cloud infrastructure) of Example Vendor Inc. so that it can be analysed what caused the crash (caused by a security violation) and what code improvements are possible. The crash dump is analysed with GDB and similar tools by the staff of Example Vendor Inc. to gain the necessary information.	PersData-1, PersData-2, PersData-3, PersData-4, PersData-5, PersData-6

MCMC MTSFB TC G050:2025

Table E.24: Sample CTIF 24-TelData (Telemetry Data) (continued)

ID	Description	Purpose	Security Examination	Personal Data
TelData-3	Meta data of the video stream. The video stream is continuously monitored for the following meta data: Compression rate, bitrate, framerate, and usage of Central Processing Unit (CPU) capacities. The data will be collected while the stream is played by a user.	The data is analysed by the Example Vendor Inc. to improve especially the performance of its products.	N/A <i>(The data is not used for security examination)</i>	None
TelData-4	Meta data of the audio stream: Compression rate, bitrate, and usage of CPU capacities.	The audio stream is continuously monitored for various meta data like compression rate, bitrate, and usage of CPU capacities. The data will be collected while the stream is played by a user. The data is analysed by the Example Vendor Inc. to improve especially the performance of its products.	N/A <i>(The data is not used for security examination)</i>	None

Table E.25: Sample CTIF 25-DelFunc (Deletion Functionalities)

ID	Description	Target Type	Initiation and Interaction	Confirmation
DelFunc-1	The user can choose to reset the DUT to factory defaults. In this case all configuration data created by the user or created by consequence of user-provided input is erased from the flash memory. All configuration data that is created in defined configuration files (SQLite databases) is deleted from the file system in the flash memory. Then new configuration files are created with empty content.	User data on the device	The user needs to select "Maintenance" -> "Reset" on the web interface or "Maintenance" -> "Reset" in the app.	Before starting the erasing the app or the web interface presents a notification about the erasing process and informs the user about a subsequent restart. After deletion the DUT is restarted and is in the factory default state after delivery then. The user can verify this by noticing that the DUT is no longer connected to the Wireless network and the user cannot login by its configured username/passwords combination on the web interface.
DelFunc-2	The user can choose to remove the user's online profile. In this case the user's account on the associated services (cloud infrastructure) and on the app is deleted. All data that is stored on the servers of Example Vendor Inc. connected with the user's account is removed.	Personal data on associated services	The user needs to select "Maintenance" -> "Delete account" on the web interface or "Maintenance" -> "Delete account" on the app.	Before starting the removal the app or the web interface presents a notification about the removal process and informs the user about a subsequent logout. After removing the account the user is automatically logged out in the app. Also, the web interface shows an account error. The user cannot use the remote services anymore.

Table E.26: Sample CTIF 26-UserDec (User Decisions)

ID	Description	Options	Triggered By
UserDec-1	The user needs to set a new password for the admin user. This is the first action the user has to make to setup the DUT.	The user needs to choose a password that complies with the password rules (no default). The strength of the chosen password is displayed to the user.	The user wants to access the DUT via the app or the web interface for the first time. The decision cannot be triggered by the user.
UserDec-2	The user can add additional user accounts for the web interface. This is the second action the user has to make to setup the DUT. After initialization the user can still add or remove user accounts for the web interface independently from any other configuration workflow.	The user needs to choose a username/password combination that complies with the password rules (no default). The strength of the chosen password is displayed to the user.	The user wants to access the DUT via the app or the web interface for the first time. In this case the decision is triggered automatically. Additionally the decision can be triggered by the user after initialization.
UserDec-3	The user needs to enter his/her full name and email address. This is the third action the user has to make to setup the DUT. After initialization the user can still edit his/her full name and email address independently from any other configuration workflow.	The user needs to choose a valid name and email format (no default).	The user wants to access the DUT via the app or the web interface for the first time. In this case the decision is triggered automatically. Additionally the decision can be triggered by the user after initialization.

Table E.27: Sample CTIF 27-UserIntf (User Interfaces)

ID	Description
UserIntf-1	The user can enter configuration data on the web interface accessible on remote port 443.
UserIntf-2	The user can enter configuration data on the app which is then transferred over the associated services (cloud infrastructure) to the DUT.

Table E.28: Sample CTIF 28-ExtAPI (External APIs)

ID	Description
ExtAPI-1	The DUT offers a SOAP interface that can be used by other devices to control the movement of the DUT's camera and receive audio and video streams via a direct connection on remote port 8085.

Table E.29: Sample CTIF 29-InpVal (Data Input Validation)

ID	Description
InpVal-1	For each user data transferred to the DUT over one of its APIs a defined validation rule is applied. A validation rule consists of at least one regular expression which receives the input data and gives back whether the input matches the expression. In case the input is more complex, the input can be matched against not just one but a set of regular expressions so that only valid values are processed by the DUT. Invalid values are rejected. The regular expressions are applied on any data received from the web interface, the SOAP interface, and the app.

Annex F
(normative)

Key secure by design principles of Internet of Things

Table F.1 below outlines the key secure by design principles of the Internet of Things, providing essential security considerations for the entire IoT lifecycle.

Table F.1. Essential Security Considerations - Secure by Design Principles for IoT

No.	Principles	Description	Implementation
1.	Proactive security integration	Security considerations must be integrated from the beginning of the development lifecycle rather than being added as an afterthought.	Conduct security assessments during the initial design phase and continue them throughout development, deployment, and maintenance. System development should incorporate the Secure Software Development Lifecycle (S-SDLC).
2.	Threat modelling	Identifying potential threats and vulnerabilities early in the design phase helps anticipate and mitigate security risks.	Develop threat models to understand how an attacker might exploit the system. Use these models to guide the design of security measures.
3.	Principle of Least Privilege	Each component, device, and user should have the minimum level of access necessary to perform its functions, reducing the attack surface.	Implement role-based access control (RBAC) and ensure that permissions are restricted to the least privilege necessary for operation.
4.	Defence in Depth	Multiple layers of security controls provide redundancy, ensuring that if one layer is compromised, others still provide protection.	Use a combination of network security, application security, and physical security measures to protect IoT devices and data.
5.	Secure defaults	Devices should be configured with secure settings by default, minimising the risk of vulnerabilities due to misconfiguration.	Ensure default configurations prioritise security, such as disabling unnecessary services and enforcing strong authentication out of the box.
6.	Fail-safe defaults	In the event of a failure, systems should default to a secure state, preventing unintended exposure of vulnerabilities.	Design systems to fail securely, such as locking down access or reverting to a known good state when an error occurs.
7.	Secure update mechanisms	The ability to securely update firmware and software is crucial for maintaining the security of IoT devices over their lifecycle.	Implement signed updates and secure boot processes to apply only authenticated and trusted updates.
8.	Data protection	Sensitive data, both at rest and in transit, should be protected from unauthorised access and tampering.	Use strong encryption for data storage and communication. Implement secure key management practices.
9.	Identity and Access Management	Strong authentication and authorisation mechanisms are essential to ensure that only authorised users and devices can access the system.	Implement multifactor authentication (MFA) and secure credential storage. Use certificates or other secure methods for device authentication.
10.	Monitoring and Logging	Continuous monitoring and logging of device activity are essential for detecting and responding to security incidents.	Implement comprehensive logging and monitoring solutions and support remote system log functions to track access, usage, and anomalies. Ensure that logs are securely stored and regularly reviewed.

MCMC MTSFB TC G050:2025

Table F.1. Essential security considerations - secure by design principles for IoT *(continued)*

No.	Principles	Description	Implementation
11.	Privacy by Design	Protecting user privacy should be a fundamental consideration in the design of IoT devices and systems.	Minimize data collection to what is strictly necessary, anonymise data where possible, and ensure compliance with privacy regulations (e.g., PDPA, GDPR).
12.	Secure decommissioning	When IoT devices reach the end of their lifecycle, they should be decommissioned in a way that securely erases all sensitive data.	Provide clear guidelines and tools for securely wiping data and decommissioning devices, preventing data leaks from retired devices.

Bibliography

- [1] ETSI TS 103 701, *CYBER; Cyber Security for Consumer Internet of Things: Conformance Assessment of Baseline Requirements*

MCMC MTSFB TC G050:2025

Acknowledgements

Internet of Things (IoT) and Smart Sustainable Cities Working Group

Working Group Leaders

Dr Gopinath Rao Sinniah (Chair)	Favoriot Sdn Bhd
Mr Mohd Amin Mohd Din (Vice Chair)	Maxis Broadband Sdn Bhd
Asst Prof Dr Teng Kah Hou (Secretary)	UCSI Education Sdn Bhd

Drafting Committee Members

Assoc Prof Ir Dr Yusnani Mohd Yussoff (Draft Lead)	Universiti Teknologi MARA
Mr Mohamad Norzamir Mat Taib (Secretariat)	Malaysian Technical Standards Forum Bhd
Ms Alisa Rafiqah Adenan (Secretariat)	Malaysian Technical Standards Forum Bhd
Mr Muhammad Arman Selamat	CyberSecurity Malaysia
Ts Mohd Zulfadzli Abu Seman	SIRIM Berhad
Ts Norhanisah Mohd Basri	SIRIM Berhad
Asst Prof Dr Teng Kah Hou	UCSI Education Sdn Bhd
Prof Dr Mohd Yamani Idna Idris	Universiti Malaya
Assoc Prof Dr Nor Muzlifah Mahyuddin	Universiti Sains Malaysia
Ms Norhaflyza Marbukhari	Universiti Teknologi MARA
Ts Dr Lucyantie Mazalan	Universiti Teknologi MARA

Contributors

Mr Ang Kah Heng	Cyberview Sdn Bhd
Dr Gopinath Rao Sinniah	Favoriot Sdn Bhd
Prof Lau Sian Lun	Sunway University College Sdn Bhd
Mr Mohd Zakir Hussin Baharuddin	TM Technology Services Sdn Bhd
<i>Mr Syahrudin A Ghani</i>	<i>Pertubuhan Smart Industri</i>
<i>Mr Mohamed Shajahan Mohamed Iqbal</i>	<i>Three-OPP (M) Sdn Bhd</i>