|  |  |  |  |
| --- | --- | --- | --- |
|  | | TSG Doc xx\_xx  **Draft Compliance Test Specification for AI Mobile Device** | |
| Meeting Information | | | |
| Meeting Name and Number | | TSG#xx | |
| Date | | xxxx | |
| Location | | e-meeting | |
| Document Information | | | |
| Document Author(s) | | China Telecom. | |
| Document Creation Date | | 16th Mar 2021 | |
|  | | Approval |  |
| This document is for: *(mark X as appropriate)* | | Discussion | X |
|  | | Information only |  |
| Security Classification | | | |
| Confidential | | GSMA Full, Associate & Rapporteur members | X |
| Document Summary | | | |
| Draft KPI test for AI mobile device hardware requirements | | | |
| Document History | | | |
| Date | Version | Author / Comments | |
|  |  |  | |
|  |  |  | |

© GSMA 2017. The GSM Association (“Association”) makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice. This document has been classified according to the GSMA [Document Confidentiality Policy](https://infocentre.gsm.org/cgi-bin/prddets.cgi?274175). GSMA meetings are conducted in full compliance with the GSMA [Antitrust Policy](https://infocentre.gsm.org/cgi-bin/docdisp.cgi?275305).

Table of Contents

[1 Introduction 4](#_Toc85612507)

[1.1 Overview 4](#_Toc85612508)

[1.2 Scope 4](#_Toc85612509)

[1.3 Definition 4](#_Toc85612510)

[1.4 Abbreviations 4](#_Toc85612511)

[1.5 References 4](#_Toc85612512)

[1.6 Modal verbs terminology 5](#_Toc85612513)

[2 Test Methodology 5](#_Toc85612514)

[2.1 Testing of optional requirements 5](#_Toc85612515)

[2.2 Implicit testing 5](#_Toc85612516)

[2.3 Repetition of tests 5](#_Toc85612517)

[2.4 Testing of cases that can leverage the existing certification scheme 5](#_Toc85612518)

[3 Hardware Performance 5](#_Toc85612519)

[3.1 Test purpose 5](#_Toc85612520)

[3.2 Referenced requirements 6](#_Toc85612521)

[3.3 Preconditions 6](#_Toc85612522)

[3.4 Initial configuration 6](#_Toc85612523)

[3.5 Test procedure 6](#_Toc85612524)

[4 Software Functions 7](#_Toc85612525)

[4.1 Deep learning model update 7](#_Toc85612526)

[4.1.1 Test purpose 7](#_Toc85612527)

[4.1.2 Referenced Requirements 7](#_Toc85612528)

[4.1.3 Preconditions 7](#_Toc85612529)

[4.1.4 Initial configuration 7](#_Toc85612530)

[4.1.5 Test procedure 7](#_Toc85612531)

[4.2 Native API requirements 8](#_Toc85612532)

[4.2.1 Test purpose 8](#_Toc85612533)

[4.2.2 Referenced Requirements 8](#_Toc85612534)

[4.2.3 Preconditions 8](#_Toc85612535)

[4.2.4 Initial configuration 8](#_Toc85612536)

[4.2.5 Test procedure 8](#_Toc85612537)

[4.3 Application APIs requirements 8](#_Toc85612538)

[4.3.1 Test purpose 8](#_Toc85612539)

[4.3.2 Referenced Requirements 9](#_Toc85612540)

[4.3.3 Preconditions 9](#_Toc85612541)

[4.3.4 Initial configuration 9](#_Toc85612542)

[4.3.5 Test procedure 9](#_Toc85612543)

[4.4 Model Format conversion 9](#_Toc85612544)

[4.4.1 Test purpose 9](#_Toc85612545)

[4.4.2 Referenced Requirements 10](#_Toc85612546)

[4.4.3 Preconditions 10](#_Toc85612547)

[4.4.4 Initial configuration 10](#_Toc85612548)

[4.4.5 Test procedure 10](#_Toc85612549)

[4.5 Customized Operator 10](#_Toc85612550)

[4.5.1 Test purpose 10](#_Toc85612551)

[4.5.2 Referenced Requirements 10](#_Toc85612552)

[4.5.3 Preconditions 10](#_Toc85612553)

[4.5.4 Initial configuration 11](#_Toc85612554)

[4.5.5 Test procedure 11](#_Toc85612555)

[5 Inference Performance 11](#_Toc85612556)

[5.1 Test purpose 11](#_Toc85612557)

[5.2 Referenced Requirements 11](#_Toc85612558)

[5.3 Preconditions 11](#_Toc85612559)

[5.4 Initial Configuration 11](#_Toc85612560)

[5.5 Test Procedure 11](#_Toc85612561)

[6 AI Application Requirements 11](#_Toc85612562)

[6.1 Biometric Performance 11](#_Toc85612563)

[6.1.1 2D facial biometric system performance 11](#_Toc85612564)

[6.1.2 3D facial biometric system performance 12](#_Toc85612565)

[6.1.3 Fingerprint biometric system performance 13](#_Toc85612566)

[6.2 On-device Image Processing 13](#_Toc85612567)

[6.2.1 Photo scene detection and recognition 13](#_Toc85612568)

[6.2.2 Text detection and recognition 14](#_Toc85612569)

[6.2.3 Facial photo enhancement (FPE) 15](#_Toc85612570)

[6.3 Voice Processing 16](#_Toc85612571)

[6.3.1 Speech 16](#_Toc85612572)

[6.3.2 Voice Assistant 17](#_Toc85612573)

[6.4 Augmented Reality (AR) 20](#_Toc85612574)

[6.4.1 AI capabilities for AR applications 20](#_Toc85612575)

[6.4.2 AR application 21](#_Toc85612576)

[7 Privacy and Security 22](#_Toc85612577)

[7.1.1 Compliance with privacy laws 22](#_Toc85612578)

[7.1.2 Personal data protection by default 23](#_Toc85612579)

[7.1.3 AI Applications on-off 23](#_Toc85612580)

[7.1.4 Responsibility of a Data Processor related to AI applications 24](#_Toc85612581)

[Annex A Applicability Table 25](#_Toc85612582)

[Annex B Letter of commitment template 34](#_Toc85612583)

[Annex C Document Management 35](#_Toc85612584)

[C.1 Document History 35](#_Toc85612585)

[C.2 Other Information 35](#_Toc85612586)

# Introduction

## Overview

While more and more device manufacturers declare their products support AI, unfortunately there are obvious difference in the functionality and performance, which greatly impact the user’s experience and perception of AI. In order to guide the industry and align the performance of AI mobile device, GSMA has published TS.47 to set up the standard for AI mobile device. The purpose of this document is to define test cases to verify the compliance of a device to the requirements defined in GSMA PRD TS.47.

## Scope

This document defines the test cases to verify whether a device comply to GSMA PRD TS.47, including test set-up, test method, test procedure and expected results.

The devices covered by this document are mobile devices and tablets.

## Definition

| **Term** | **Description** |
| --- | --- |
| AI Mobile Device | Refer to the definition of AI Mobile Device in TS.47 AI Mobile Device Specification [1]. |
| Power Meter | Equipment that used for power measurement and can fulfil the following functions:  1. Provide power for DUT.  2. Display the current value in diagram. |
| VGG16\_notop | VGG16 without last three fully connected layers, in float32 format. |

## Abbreviations

| **Term** | **Description** |
| --- | --- |
| AI | Artificial Intelligence |
| OEM | Original Equipment Manufacturer |
| DUT | Device Under Test |
| SDO | Standard Developing Organisations |
| TOPS | Tera Operations Per Second |
| TOPS/w | Tera Operations Per Second / Per Watt |

## References

Requirements shall be based on the exact versions as indicated below. However if the manufacturers use a later release and/or version this should be indicated. The GSMA will continually align with other SDOs as appropriate.

| Ref | Doc Number | Title |
| --- | --- | --- |
|  | GSMA PRD TS.47 | AI Mobile Device Specification, Version 1.0, September 2019 |
| [2] | ISO-IEC-19795-1 | Information technology — Biometric performance testing and reporting —Part 1: Principles and framework |
| [3] |  | FIDO Biometrics Requirements (2020) |
| [4] | GSMA PRD TS.29 | Smartphone Performance Test Case Guideline Version 6.0 or later |
| [5] | RFC 2119 | “Key words for use in RFCs to Indicate Requirement Levels”, S. Bradner, March 1997. Available at <http://www.ietf.org/rfc/rfc2119.txt> |
| [6] | RFC8174 | Ambiguity of Uppercase vs Lowercase in RFC 2119 Key Words  <https://www.rfc-editor.org/info/rfc8174> |

## Modal verbs terminology

The key words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, and “OPTIONAL” in this document are to be interpreted as described in RFC 2119 [5] (RFC8174) [6] when, and only when, they appear in all capitals, as shown here.

# Test Methodology

## Testing of optional requirements

Any requirement which is optional may be subject to a conformance test if it is supported by the DUT.

A declaration by the device manufacturer based on Applicability Table (Annex A), is used to determine whether an optional requirement is supported.

## Implicit testing

The conformance of some requirements may not verified explicitly in the present document. This does not imply that these requirements are not essential, but these are implicitly tested to a sufficient degree in other tests. For clarity these are marked out correspondingly below:

XX

## Repetition of tests

As a general rule, the test cases specified in the present document are highly reproducible and don't need to be repeated unless otherwise stated.

## Testing of cases that can leverage the existing certification scheme

For those test cases that can leverage the existing certification scheme, the corresponding conformance test here to will directly accept the results from the certification scheme.

# Hardware Performance

## Option 1 – VGG Network - Test purpose

To verify that the DUT can meet the minimum requirements of TOPS and TOPS/w.

## Option 1 – VGG Network - Referenced requirements

|  |  |
| --- | --- |
| Requirement for the modified VGG 16 network | |
| TS47\_3.1\_REQ\_001 | An AI Mobile Device SHOULD have a minimum of (1) int8 TOPS. |
| TS47\_3.1\_REQ\_002 | An AI Mobile Device SHOULD have a minimum of (0.5) float16 TOPS. |
| TS47\_3.1\_REQ\_003 | An AI Mobile Device SHOULD have a minimum of (0.5) int8 TOPS/Watt. |
| TS47\_3.1\_REQ\_004 | An AI Mobile Device SHOULD have a minimum of (0.3) float16 TOPS/Watt. |

## Option 1: Using VGG16 Network - Preconditions

* **Test Model preparation**

1. Take VGG16\_notop as the Reference Model.

2. Use the Model Conversion tool provided by the chipset vendor to convert the Reference Model to an int8 or/and a float16 model that can be run on the DUT, take this converted model as Model\_t.

3. Validate Model\_t can be used as the Test Model. (TBD)

* **Test Scripts preparation**

Scripts to pre-process the test dataset, run the test model and measure TOPS.

* **Test Dataset**

1000 images of size 224\*224\*3.

## Option 1 - Initial configuration

DUT is loaded with test scripts and test model for int8 or/and float16 TOPS, TOPS/watt measurement.

DUT is Switched OFF.

Power meter is Switched OFF.

## Option 1 - Test procedure

|  |  |  |
| --- | --- | --- |
| Step | Test procedure | Expected result |
| 1 | Switch the power meter on and connect it to DUT for power measurement. | The power meter is on. |
| 2 | Switch DUT on and adjust the screen brightness to the lowest level, turn off the Bluetooth, mute the DUT and turn on the flight mode. | DUT is on and is in flight mode. |
| 3 | Record the current and voltage. | The current curve and the voltage are displayed. |
| 4 | Wait until the current is stable, i.e. the current curve is stable [+/-5%]. | The current is stable. |
| 5 | Record the background current and the voltage for 60 seconds, compute the average value. | The value of average background current and average voltage are obtained. |
| 6 | Run the test scripts for int8 Test Model, record the inference time and compute the average inference current. | The inference time and the average inference current value are obtained. |
| 7 | Compute int8 TOPS and compare the result with the value specified in the requirement TS.47\_3.1\_REQ\_001. | The int8 TOPS result meets requirement TS.47\_3.1\_REQ\_001. |
| 8 | Compute int8 TOPS/Watt and compare the result with the value specified in the requirement TS.47\_3.1\_REQ\_003. | The int8 TOPS/Watt result meets requirement TS.47\_3.1\_REQ\_003. |
| 9 | Stop recording the current. | The current curve stops recording. |
| 10 | Change the test model to float16 Test Model, repeat step 3 to 9 for float16 TOPS and float 16 TOPS/Watt measurement. | The float16 TOPS result meets requirement TS.47\_3.1\_REQ\_002.  The float16 TOPS/Watt result meets requirement TS.47\_3.1\_REQ\_004. |

# Option 2: Using MLCommons Mobile Application

## Hardware Performance Referenced Requirements

Alternatively, a better network may be used.

|  |  |
| --- | --- |
| Requirement for better networks | |
| TS47\_3.1\_REQ\_001 | An AI Mobile Device SHOULD have a minimum of [1] int8 TOPS. |
| TS47\_3.1\_REQ\_002 | An AI Mobile Device SHOULD have a minimum of [0.5] float16 TOPS |
| TS47\_3.1\_REQ\_003 | An AI Mobile Device SHOULD have a minimum of [0.5] int8 TOPS/Watt. |
| TS47\_3.1\_REQ\_004 | An AI Mobile Device SHOULD have a minimum of [0.3] float16 TOPS/Watt. |

### Software Requirements

|  |  |
| --- | --- |
| TS47\_3.2\_REQ\_001 | An AI Mobile Device SHALL support on-device model updates of an existing deep learning network. |
| TS47\_3.2\_REQ\_002 | An AI Mobile Device SHALL support native APIs to expose the AI hardware functions. |
| TS47\_3.2\_REQ\_003 | An AI Mobile Device SHALL support application APIs (See Appendix A) for native and third-party applications to access Computer Vision (CV), Automatic Speech Recognition (ASR), Natural Language Understanding (NLU) models. |
| TS47\_3.2\_REQ\_004 | An AI Mobile Device SHOULD provide an SDK to convert DNN models from an existing format to the native format of the AI mobile device. Non exhaustive examples of DNN model file format are: \*.ckpt or \*.pb, \*.tflite, \*.prototxt, \*.pb or \*.pth or \*.pt, \*.json and \*.onnx. |
| TS47\_3.2\_REQ\_005 | An AI Mobile Device SHOULD provide an SDK to support definition of new customized Deep Learning operators. |
| TS47\_3.2\_REQ\_001 | An AI Mobile Device SHALL support on-device model updates of an existing deep learning network. |

### Biometric Performance Requirements

|  |  |
| --- | --- |
| TS47\_3.4.1\_REQ\_001 | An AI Mobile Device SHOULD support a 2D facial biometric system. |
| TS47\_3.4.1\_REQ\_002 | An AI Mobile Device SHOULD support a 3D facial biometric system. |
| TS47\_3.4.1\_REQ\_003 | An AI Mobile Device SHOULD support a fingerprint biometric system. |
| TS47\_3.4.1\_REQ\_004 | An AI Mobile Device supporting 2D facial biometric system SHALL support the biometric KPI requirement TS47\_3.4.1\_REQ\_004.1 for each of the use cases: Device Unlock, Application Login and Payment Authorization. |
| TS47\_3.4.1\_REQ\_004.1 | 2D Facial FAR <= [0.002]% and FRR <= [3]% simultaneously |
| TS47\_3.4.1\_REQ\_005 | An AI Mobile Device supporting 3D facial biometric system SHALL support the biometric KPI requirement TS47\_3.4.1\_REQ\_005.1 for each of the use cases: Device Unlock, Application Login and Payment Authorization. |
| TS47\_3.4.1\_REQ\_005.1 | 3D Facial FAR <= [0.001]% and FRR <= [3]% simultaneously |
| TS47\_3.4.1\_REQ\_006 | An AI Mobile Device supporting fingerprint biometric system SHALL support the biometric KPI requirement TS47\_3.4.1\_REQ\_006.1 for each of the use cases: Device Unlock, Application Login and Payment Authorization. |
| TS47\_3.4.1\_REQ\_006.1 | Fingerprint FAR <= [0.002]% and FRR <= [3]% simultaneously |
| TS47\_3.4.1\_REQ\_007 | The biometric key performance indicators (KPIs) for the supported biometric system SHOULD be certified by one or more of the following programs:   * Fast IDentity Online (FIDO) Alliance Biometric Component Certification Program * Internet Finance Authentication Alliance (IFAA) biometric Certification Program |

### On-Device Image Processing Requirements

|  |  |
| --- | --- |
| TS47\_3.4.2\_REQ\_001 | An AI Mobile Device SHOULD have optical character recognition (OCR) capability on the device. |
| TS47\_3.4.2\_REQ\_002 | An AI Mobile Device SHOULD have image detection, image classification and image segmentation capabilities on the device. |
| TS47\_3.4.2\_REQ\_003 | An AI Mobile Device SHOULD have face detection and face clustering capabilities within a group of photos on the device. |
| TS47\_3.4.2\_REQ\_004 | An AI Mobile Device SHOULD have video super-resolution capabilities on the device. |
| TS47\_3.4.2\_REQ\_005 | An AI Mobile Device SHOULD have video classification capabilities on the device. |

#### On-Device Image Processing Applications

|  |  |
| --- | --- |
| TS47\_3.4.2.1\_REQ\_001 | * The AI Mobile Device SHOULD support photo scene detection and recognition where the User has the ability to consent to their use: |
| TS47\_3.4.2.1\_REQ\_001.1 | If REQ\_001 is supported then the AI Mobile Device SHALL support  Identification of one or more objects in different scenes such as portraits, landscapes, foods, night scenes and texts, etc. |
| TS47\_3.4.2.1\_REQ\_001.2 | If REQ\_001 is supported then the AI Mobile Device SHALL support  Scene detection capabilities to optimize camera settings for image capture based on scene content. |
| TS47\_3.4.2.1\_REQ\_002 | The AI Mobile Device SHOULD support text detection and recognition of installed language packages, where the User has the ability to consent to the text detection and recognition use. |
| TS47\_3.4.2.1\_REQ\_003 | The AI Mobile Device SHOULD support automatic language detection. |
| TS47\_3.4.2.1\_REQ\_004 | The AI Mobile Device SHOULD provide personalized FPE for users based on gender, age, and skin tone. |
| TS47\_3.4.2.1\_REQ\_005 | The AI Mobile Device SHOULD support FPE of multiple people in a single photo. |
| TS47\_3.4.2.1\_REQ\_006 | The FPE functionality SHOULD be switched off by default and the AI Mobile Device SHOULD support user adjustment of the FPE level from no enhancement to the max FPE. |
| TS47\_3.4.2.1\_REQ\_007 | The AI Mobile Device SHOULD support automatic classification of photos in an album by different categories. |

### Speech

|  |  |
| --- | --- |
| TS47\_3.4.3\_REQ\_001 | The AI Mobile Device SHOULD have speech ability.. |
| TS47\_3.4.3\_REQ\_002 | The AI Mobile Device SHOULD support Automatic speech recognition (ASR) capabilities where the User has the ability to consent to ASR |
| TS47\_3.4.3\_REQ\_003 | The AI Mobile Device SHOULD support Natural Language Understanding (NLU) capabilities where the User has the ability to consent to NLU |
| TS47\_3.4.3\_REQ\_004 | The AI Mobile Device SHOULD support Synthesized Voice (Text-To-Speech (TTS) capabilities where the User has the ability to consent to TTS |
| TS47\_3.4.3\_REQ\_005 | If the AI Mobile Device supports Voice Assistant then the requirements in section 3.4.3.1 SHALL apply. |

#### Voice assistant

|  |  |
| --- | --- |
| TS47\_3.4.3.1\_REQ\_001 | AI Mobile Device SHALL support functions.   1. Automatic speech recognition (ASR) capabilities 2. Natural Language Understanding (NLU) capabilities 3. Synthesized Voice (Text-To-Speech (TTS)) capabilities |
| TS47\_3.4.3.1\_REQ\_002 | The AI Mobile Device SHALL support voice trigger, and its specific requirements are listed in the following sub requirements: TS47\_3.4.3.1\_REQ\_002.1, 002.2 and\_002.3 |
| TS47\_3.4.3.1\_REQ\_002.1 | It SHOULD support voiceprint recognition for preventing people other than the device’s owner from triggering voice assistant. |
| TS47\_3.4.3.1\_REQ\_002.2 | In a quiet environment, the following SHALL be required:  The true acceptance rate (TAR) >= [90]%, and the false acceptance rate (FAR) of voiceprint recognition <= [20]%. |
| TS47\_3.4.3.1\_REQ\_002.3 | In a noisy environment, the following SHALL be required:  TAR >=[80]%, and FAR of voiceprint recognition <= [20]%. |
| TS47\_3.4.3.1\_REQ\_003 | The AI Mobile Device SHALL have on-device speech recognition library (i.e. with no access to the Internet) for changing the system setting (e.g. Turn Bluetooth on/off via voice assistant) and invoking the native applications (e.g. send SMS via voice assistant). |
| TS47\_3.4.3.1\_REQ\_004 | The AI Mobile Device SHOULD have access to different categories of applications and invoke these applications’ services and functions via voice assistant. |
| TS47\_3.4.3.1\_REQ\_005 | The AI Mobile Device SHALL support information search by on-device voice assistant. |
| TS47\_3.4.3.1\_REQ\_006 | The AI Mobile Device SHOULD support interaction with smart devices (e.g. home appliances) via voice assistant. |

### Augmented Reality (AR)

|  |  |
| --- | --- |
| TS47\_3.4.4\_REQ\_001 | The AI Mobile Device SHOULD provide the following AI capabilities for AR native and third-party applications:   1. Hand gesture recognition 2. Hand skeleton tracking 3. Human body pose recognition 4. Human body skeleton tracking |
| TS47\_3.4.4\_REQ\_002 | The AI Mobile Device SHOULD support the following applications:   1. AR Emoji    1. Creating customized AR-based Emoji.    2. Tracking user’s facial movement and expression and render these on the AR-based Emoji. 2. AR video    1. Compositing real objects with virtual objects and/or virtual background    2. Minimum [30] fps frame rate    3. AR shadow effect and occlusion handling.    4. AR enhanced information text labels should not deviate or disappear from the actual target scene when the AI Mobile Device moves. |

### System Optimization

|  |  |
| --- | --- |
| TS47\_3.4.5\_REQ\_001 | Only with the explicit permission of the User in order to respect the User’s right to privacy around their habits: The AI Mobile Device SHOULD support dynamic system resource allocation and optimization based on feedback provided by on-device sensors measuring environmental conditions combined with continuous learning of user habits and behaviours or device or network usage or performance indicators:  1. Dynamic application management (e.g. pre-loading, closing, put to sleep, control network access) based on user’s habits (e.g. usage duration, frequency).  2. Dynamic application management based on abnormal behaviour detection (e.g. increased memory usage, abnormal power consumption, self-starting in the background)  3. Dynamic system resource management based on continuous learning of system performance (e.g. memory and storage defragmentation, off-line storage during off-peak periods).  4. Dynamic system resource allocation for high performance applications (e.g., gaming and video). |

### Preconditions

1. MLCommons GSMA application has been properly compiled from Open and Closed source for each device.
2. All models have been agreed upon and integrated into the application to support all requirements above.
3. Proper report formatting has been agreement upon between MLC and GSMA.

### Test purpose

Using the MLCommons application to test all requirements above.

### Initial Conditions

1. MLCommons Mobile App has been loaded and initialized onto each device.
2. MLC app is responsible for clearing the memory and ensuring no other application is running at the same time.
3. MLC initialization testing procedures have been followed

### Test Procedure

1. Run MLCommons Mobile App to produce **GSMA Official Test Report**
2. Review test report to ensure all requirements have been met

# Privacy and Security

## Privacy

### Compliance with privacy laws

#### Test Purpose

To verify that DUT complies with the privacy laws.

#### Referenced Requirements

|  |  |
| --- | --- |
| TS47\_4.1\_REQ\_001 | AI on mobile device SHOULD comply with the privacy laws in the country where the device is commercially retailed. |

#### Preconditions

None.

#### Initial Configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check letter of commitment provided by OEM. | OEM provides a letter of commitment that declares AI on mobile device complies with the privacy laws in the country where the device is commercially retailed |

### Personal data protection by default

#### Test Purpose

To verify that DUT protects personal data by default.

#### Referenced Requirements

|  |  |
| --- | --- |
| TS47\_4.1\_REQ\_002 | Appropriate technical and organisational safeguards SHOULD be implemented to ensure that, by default, only the personal data reasonably necessary for a specific purpose are processed. |

#### Preconditions

None.

#### Initial Configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check letter of commitment provided by OEM. | OEM provides a letter of commitment that declares only the personal data reasonably necessary for a specific purpose are processed by default. |

### AI Applications on-off

#### Test Purpose

To verify that

1. AI Applications which process Personal Data are switched off by default unless processing exclusively takes place locally on the device
2. User can control the AI applications on-off

#### Referenced Requirements

|  |  |
| --- | --- |
| TS47\_4.1\_REQ\_003 | AI Applications that process Personal Data SHALL be off by default unless processing exclusively takes place locally on the device. |
| TS47\_4.1\_REQ\_003.1 | The User SHOULD be allowed to control whether individual AI applications are switched on. |
| TS47\_4.1\_REQ\_003.2 | The User SHOULD be allowed to control whether individual AI applications are switched off. |

#### Preconditions

None.

#### Initial Configuration

DUT is Switched ON.

OEM provides the AI applications list the DUT supports.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check letter of commitment provided by OEM. | OEM provides a letter of commitment that declares AI Applications are switched off by default unless Personal Data processing exclusively takes place locally on the device. |
| 2 | Check whether every individual AI application can be switched on/off. | All the individual AI applications can be switched on/off . |

### Responsibility of a Data Processor related to AI applications

#### Test Purpose

To verify that a Data Processor related to AI applications has the responsibility to

1) Be transparent with the User on the nature of the input data used in the AI processing (e.g. personal files, biometrics, …).

2)  Forbid transferring personal data processing off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law.

3)  Forbid transferring results of on-device AI processing containing personal data off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law.

#### Referenced Requirements

|  |  |
| --- | --- |
| TS47\_4.1\_REQ\_004 | The AI Application on the AI Mobile Device SHALL be designed in such a way that a Data Processor will have the responsibility to:  1) Be transparent with the User on the nature of the input data used in the AI processing (e.g. personal files, biometrics, …).  2) Forbid transferring personal data processing off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law.  3)  Forbid transferring results of on-device AI processing containing personal data off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law. |

#### Preconditions

None.

#### Initial Configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check letter of commitment provided by OEM. | OEM provides a letter of commitment that declares the AI Applications are designed in such a way that a Data Processor will have the responsibility to:  1) Be transparent with the User on the nature of the input data used in the AI processing (e.g. personal files, biometrics, …).  2) Forbid transferring personal data processing off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law.  3)  Forbid transferring results of on-device AI processing containing personal data off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law. |

## Security

### Requirement of information protection

#### Test purpose

To verify whether DUT has reasonable safeguards for information protection.

#### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2\_REQ\_001 | The AI Mobile Device SHALL use reasonable safeguards appropriate to the sensitivity, confidentiality and integrity of the information. |

#### Preconditions

None.

#### Initial configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares the AI Mobile Device use reasonable safeguards appropriate to protect the sensitivity, confidentiality and integrity of the information. |

### Requirement of personal data collection control

#### Test purpose

To verify that the user is in control of the collection of their personal data and its usage.

#### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2\_REQ\_002 | Except as required or permitted by applicable law, the User SHALL always remain in control of the collection of their personal data and its usage, in order to minimise the risk of malicious usage or data leakage. |

#### Preconditions

None.

#### Initial configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares the User always remains in control of the collection of their personal data and its usage, except as required or permitted by applicable law. |

### Requirement of Off toggle switches

#### Test purpose

To verify whether there are Off ‘toggle’ switches that can be used to turn off the functionality, except as permitted or required by applicable law.

#### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2\_REQ\_003 | Off ‘toggle’ switches SHALL turn off the functionality, except as permitted or required by applicable law. |

#### Preconditions

OEM provides Self declare FORM that list all the Off ‘toggle’ switches.

#### Initial configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares Off ‘toggle’ switches turn off the functionality, except as permitted or required by applicable law. |
| 2 | Check Off ‘toggle’ switches with Self declare FORM provided by OEM. | All the Off ‘toggle’ switches turn off the functionality, except as permitted or required by applicable law. |

### Requirement of manipulation techniques

#### Test purpose

To verify that the techniques (such as ‘Dark Pattern’) that manipulate the user’s choice are not used.

#### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2\_REQ\_004 | Techniques, such as ‘Dark Patterns’, that manipulate the User’s choice SHALL NOT be used. |

#### Preconditions

None.

#### Initial configuration

None.

#### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares Techniques (such as ‘Dark Patterns’) that manipulate the User’s choice are not used. |

### Security for AI applications

#### Requirement of AI models

##### Test purpose

To verify that the AI models used by an AI Mobile Device meet the secure requirements.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_001 | The AI models used by an AI Mobile Device SHOULD be secure and robust, and be protected with appropriate safeguards to prevent and to mitigate attacks. |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares the AI models used by an AI Mobile Device are secure and robust, and are protected with appropriate safeguards to prevent and to mitigate attacks. |

#### Requirement of training data protection

##### Test purpose

To verify that defence techniques are deployed to protect the training data for protecting models.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_002 | Defence techniques SHOULD be employed to protect the training data for protecting models. For example, in evasion attacks, data can be manipulated to mislead AI models |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares defence techniques are deployed to protect the training data for the AI models that being used natively on DUT. |

#### Requirement of autonomous AI Mobile Device operations

##### Test purpose

To verify that Autonomous AI Mobile Device operations meet the secure requirements.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_003 | Autonomous AI Mobile Device operations SHALL be controlled, and/or authorized by the authenticated User. |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment declares that Autonomous AI operations are controlled, and/or authorized by the authenticated User on DUT. |

#### Requirements of Secured Environment

##### Test purpose

To verify that AI mobile device operations are performed in the secured environment.

To verify that Data and metadata are stored with encryption, and keys are stored in the Secured Environment.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_004 | AI Mobile Device operations SHOULD be performed in the Secured Environment [4], e.g. a secure boot and upgrade is enforced, and the system integrity is protected. |
| TS47\_4.2.1\_REQ\_005 | Data and metadata for AI Mobile Device SHALL be stored with encryption with keys that are stored securely in a Secured Environment, e.g. Trusted Execution Environment (TEE). |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares AI Mobile Device operations are performed in the Secured Environment and data and metadata for AI Mobile Device are stored with encryption with keys that are stored securely in a Secured Environment. |

#### Requirement of Biometric Data for authentication

##### Test purpose

To verify that Biometric Data processed by an AI Application used for authentication within the AI Mobile Device are not transferred off the device.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_006 | Biometric Data, which are processed by an AI Application (e.g. templates) used for authentication within the AI Mobile Device, SHALL NOT be transferred off the device. |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares Biometric Data processed by an AI Application used for authentication within the AI Mobile Device are not transferred off the device. |

#### Requirements of Biometric Data

##### Test purpose

To verify that:

1. Users' Biometric Data are encrypted when at rest on the device.
2. Encryption/decryption of this data is performed in a Secured Environment.
3. Biometric Data are stored in the Secured Environment.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_007 | Users' Biometric Data (such as facial data, fingerprint data, etc.) SHALL be encrypted when at rest on the device. Encryption/decryption of this data SHALL be performed in a Secured Environment. |
| TS47\_4.2.1\_REQ\_007.1 | Biometric Data SHALL also be stored in the Secured Environment. |
| TS47\_4.2.1\_REQ\_011 | Voiceprint Data SHOULD be stored on the device with encryption. |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares:   1. Users' Biometric Data are encrypted when at rest on the device. 2. Encryption/decryption of Biometric Data is performed in a Secured Environment. 3. Biometric Data are stored in the Secured Environment. |

#### Requirement of biometric algorithms

##### Test purpose

To verify that biometric algorithms are run in a private and Secure Environment.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_008 | Biometric algorithms (such as face recognition algorithms, fingerprint algorithms, etc.) SHOULD run in a private and Secure Environment such as a Trusted Execution Environment (TEE). |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares biometric algorithms are run in a private and Secure Environment such as a Trusted Execution Environment (TEE). |

#### Requirement of Biometric Data replacement

##### Test purpose

To verify that Biometric Data replacement meets the secure requirements.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_009 | If Users' Biometric Data is replaced, the previous Biometric Data before the replacement SHALL be deleted completely and permanently and not be recoverable by data rollback. |
| TS47\_4.2.1\_REQ\_013 | When the Voiceprint Data is permanently and completely deleted, it SHALL NOT be recoverable by data rollback |

##### Preconditions

Prepare different Biometric Data 1 and Biometric Data 2 for testing.

Note: Biometric Data involve finger, face or voice, etc.

##### Initial configuration

DUT is Switched Off.

Biometric Data 1 is pre-stored on DUT with user’s consent.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Switch DUT on. | DUT is in idle mode. |
| 2 | Use Biometric Data 1 to login/unlock AI applications. | AI applications can execute with Biometric Data1. |
| 3 | Replace Biometric Data 1 with Biometric Data 2. | Users' Biometric Data is updated and Biometric Data 1 is deleted. |
| 4 | Use Biometric Data 1 to login/unlock AI applications | AI applications cannot be executed. |
| 5 | Use Biometric Data 2 to login/unlock AI applications | AI applications can be executed. |
| 6 | Execute data rollback operation. |  |
| 7 | Use Biometric Data 1 to login/unlock AI applications | AI applications cannot be executed. |
| 8 | Use Biometric Data 2 to login/unlock AI applications | AI applications can execute with Biometric Data 2. |
| 9 | Delete all the Biometric Data on DUT. | Users’ Biometric Data is wiped out and cannot be found on DUT. |
| 10 | Use Biometric Data 1 and Biometric Data 2 to Execute AI applications respectively. | AI applications cannot be executed. |

#### Requirement of device factory reset

##### Test purpose

To verify that the Biometric Data are wiped out and made unrecoverable by a device factory reset.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_010 | The Biometric Data SHALL be wiped and made unrecoverable by a device factory reset. |
| TS47\_4.2.1\_REQ\_014 | The Voiceprint Data SHALL be wiped and made unrecoverable by a device factory reset. |

##### Preconditions

Prepare User1’s biometric data as Biometric Data 1.

##### Initial configuration

DUT is Switched OFF.

Biometric Data 1 is pre-stored on DUT with user’s consent.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Switch DUT on. | DUT is in idle mode. |
| 2 | Execute AI applications with Biometric Data 1. | AI applications can be executed with Biometric Data 1. |
| 3 | Execute factory reset on DUT |  |
| 4 | Check the information of Biometric Data on DUT. | Biometric Data 1 is wiped out. |
| 5 | Execute AI applications with the Biometric Data 1. | AI applications cannot be executed. |

#### Requirement of temporary Voiceprint Data

##### Test purpose

To verify that the temporary Voiceprint Data do not remain in the memory after processing.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_012 | The temporary Voiceprint Data SHALL NOT remain in the memory after processing. |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares the temporary Voiceprint Data do not remain in the memory after processing. |

#### Requirement for Voice replay attack defense

##### Test purpose

To verify that the device can be resistant to voice replay attacks.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_015 | The device SHOULD be resistant to voice replay attacks. |

##### Preconditions

Prepare voice replay samples.

* **Test Environment preparation**

The background noise refer to TS.29 Smartphone Performance Test Case Guideline [4], section 6.1.2.1 - 6.1.2.3.

* **Test Dataset**

Voice replay test dataset should be prepared by recording the user’s wake-up words for the AI application that support voice recognition.

Look into the Self declare Form to see what AI applications support voiceprint recognition are preloaded on DUT (Self declare FORM).

Initial configurationDUT is Switched OFF.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Switch DUT on. | DUT is in idle mode. |
| 2 | Open the AI applications that support voice recognition and use voice replay test dataset to perform voice replay attacks under different background noise. | AI applications cannot execute with voice replay test dataset under all background noise. |

#### Requirement of AR applications

##### Test purpose

To verify that appropriate safeguards are used to protect AR applications from malicious application attacks.

##### Referenced requirements

|  |  |
| --- | --- |
| TS47\_4.2.1\_REQ\_016 | Appropriate safeguards SHOULD be used to protect AR applications from malicious application attacks, such as spoofing a User with information about the real and/or virtual world, sensory overload attacks, hijacking the User's clicks, etc. |

##### Preconditions

None.

##### Initial configuration

None.

##### Test procedure

| Step | Test procedure | Expected result |
| --- | --- | --- |
| 1 | Check the letter of commitment provided by OEM. | OEM provides a letter of commitment that declares appropriate safeguards are used to protect AR applications from malicious application attacks. |

1. Applicability Table

Applicability Table : A document, in the form of a questionnaire , which requires the device manufacturer to declare which requirement the device meets and to provide the necessary information for conducting tests.

| **TS.47 Requirement Number** | **Requirement** | **TS.53 Test Cases Number** | **Test Case Applicability**  **M = Mandatory**  **O = Optional**  **C = Conditional** | **Is this requirement supported?**  **Yes / No** | **Is this requirement tested?**  **Yes / No** | **If the requirement is supported, but not tested give reasons and confirm compliance.** | **Self-Declaration Requirement**  **(Questions)** | **Self-Declaration**  **(Answers)** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| TS47\_3.1\_REQ\_001 | An AI Mobile Device SHOULD have a minimum of (1) int8 TOPS. |  | **O** |  |  |  |  |  |
| TS47\_3.1\_REQ\_002 | An AI Mobile Device SHOULD have a minimum of (0.5) float16 TOPS. |  | **O** |  |  |  |  |  |
| TS47\_3.1\_REQ\_003 | An AI Mobile Device SHOULD have a minimum of (0.5) int8 TOPS/Watt. |  | **O** |  |  |  |  |  |
| TS47\_3.1\_REQ\_004 | An AI Mobile Device SHOULD have a minimum of (0.3) float16 TOPS/Watt. |  | **O** |  |  |  |  |  |
| TS47\_3.2\_REQ\_001 | An AI Mobile Device SHALL support on-device model updates of an existing deep learning network. |  | **M** |  |  |  | What are the AI models supported by the device?  At least provide one. |  |
| TS47\_3.2\_REQ\_002 | An AI Mobile Device SHALL support native APIs to expose the AI hardware functions. |  | **M** |  |  |  | Please list the native APIs |  |
| TS47\_3.2\_REQ\_003 | An AI Mobile Device SHALL support application APIs (See Appendix A in TS.47) for native and third-party applications to access Computer Vision (CV), Automatic Speech Recognition (ASR), Natural Language Understanding (NLU) models. |  | **M** |  |  |  | Please list the application APIs |  |
| TS47\_3.2\_REQ\_004 | An AI Mobile Device SHOULD provide an SDK to convert DNN models from an existing format to the native format of the AI mobile device. Non-exhaustive examples of DNN model file format are: \*.ckpt or \*.pb, \*.tflite, \*.prototxt, \*.pb or \*.pth or \*.pt, \*.json and \*.onnx. |  | **O** |  |  |  | Please list the file formats that can be converted to native one by the SDK |  |
| TS47\_3.2\_REQ\_005 | An AI Mobile Device SHOULD provide an SDK to support definition of new customized Deep Learning operators. |  | **O** |  |  |  | Please list all the operators that have been already supported. |  |
| TS47\_3.4.1\_REQ\_001 | An AI Mobile Device SHOULD support a 2D facial biometric system. |  | **O** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_002 | An AI Mobile Device SHOULD support a 3D facial biometric system. |  | **O** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_003 | An AI Mobile Device SHOULD support a fingerprint biometric system. |  | **O** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_004 | An AI Mobile Device supporting 2D facial biometric system SHALL support the biometric KPI requirement TS47\_3.4.1\_REQ\_004.1 for each of the use cases: Device Unlock, Application Login and Payment Authorization. |  | **M** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_004.1 | 2D Facial FAR <= (0.002)% and FRR <= (3)% simultaneously |  | **M** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_005 | An AI Mobile Device supporting 3D facial biometric system SHALL support the biometric KPI requirement TS47\_3.4.1\_REQ\_005.1 for each of the use cases: Device Unlock, Application Login and Payment Authorization. |  | **M** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_005.1 | 3D Facial FAR <= (0.001)% and FRR <= (3)% simultaneously. |  | **M** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_006 | An AI Mobile Device supporting fingerprint biometric system SHALL support the biometric KPI requirement TS47\_3.4.1\_REQ\_006.1 for each of the use cases: Device Unlock, Application Login and Payment Authorization. |  | **M** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_006.1 | Fingerprint FAR <= (0.002)% and FRR <= (3)% simultaneously. |  | **M** |  |  |  |  |  |
| TS47\_3.4.1\_REQ\_007 | The biometric key performance indicators (KPIs) for the supported biometric system SHOULD be certified by one or more of the following programs:  Fast IDentity Online (FIDO) Alliance Biometric Component Certification Program.  Internet Finance Authentication Alliance (IFAA) biometric Certification Program. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2\_REQ\_001 | An AI Mobile Device SHOULD have optical character recognition (OCR) capability on the device. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2\_REQ\_002 | An AI Mobile Device SHOULD have image detection, image classification and image segmentation capabilities on the device. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2\_REQ\_003 | An AI Mobile Device SHOULD have face detection and face clustering capabilities within a group of photos on the device. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2\_REQ\_004 | An AI Mobile Device SHOULD have video super-resolution capabilities on the device. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2\_REQ\_005 | An AI Mobile Device SHOULD have video classification capabilities on the device. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_001 | The AI Mobile Device SHOULD support photo scene detection and recognition where the User has the ability to consent to their use. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_001.1 | If REQ\_001 is supported then the AI Mobile Device SHALL support  Identification of one or more objects in different scenes such as portraits, landscapes, foods, night scenes and texts, etc. |  | **M** |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_001.2 | If REQ\_001 is supported then the AI Mobile Device SHALL support  Scene detection capabilities to optimize camera settings for image capture based on scene content. |  | **M** |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_002 | The AI Mobile Device SHOULD support text detection and recognition of installed language packages, where the User has the ability to consent to the text detection and recognition use. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_003 | The AI Mobile Device SHOULD support automatic language detection. |  | **O** |  |  |  | Please list all the languages that the device supports |  |
| TS47\_3.4.2.1\_REQ\_004 | The AI Mobile Device SHOULD provide personalized FPE for Users based on gender, age, and skin tone. |  | **O** |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_005 | The AI Mobile Device SHOULD support FPE of multiple people in a single photo. |  |  |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_006 | The FPE functionality SHOULD be switched off by default and the AI Mobile Device SHOULD support User adjustment of the FPE level from no enhancement to the max FPE. |  |  |  |  |  |  |  |
| TS47\_3.4.2.1\_REQ\_007 | The AI Mobile Device SHOULD support automatic classification of photos in an album by different categories. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3\_REQ\_001 | The AI Mobile Device SHOULD have speech ability. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3\_REQ\_002 | The AI Mobile Device SHOULD support Automatic speech recognition (ASR) capabilities where the User has the ability to consent to ASR. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3\_REQ\_003 | The AI Mobile Device SHOULD support Natural Language Understanding (NLU) capabilities where the User has the ability to consent to NLU. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3\_REQ\_004 | The AI Mobile Device SHOULD support Synthesized Voice (Text-To-Speech (TTS) capabilities where the User has the ability to consent to TTS. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3\_REQ\_005 | If the AI Mobile Device supports Voice Assistant then the requirements in section 3.4.3.1 SHALL apply. |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_001 | AI Mobile Device SHALL support the following functions.  Automatic speech recognition (ASR) capabilities.  Natural Language Understanding (NLU) capabilities.  Synthesized Voice (Text-To-Speech (TTS)) capabilities. |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_002 | The AI Mobile Device SHALL support voice trigger, and its specific requirements are listed in the following sub requirements: TS47\_3.4.3.1\_REQ\_002.1, 002.2 and\_002.3 |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_002.1 | The AI Mobile Device SHOULD support voiceprint recognition for preventing people other than the device’s owner from triggering voice assistant. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_002.2 | In a quiet environment, the following SHALL be required:  The true acceptance rate (TAR) >= (90)%, and the false acceptance rate (FAR) of voiceprint recognition <= (20)%. |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_002.3 | In a noisy environment, the following SHALL be required:  TAR >=(80)%, and FAR of voiceprint recognition <= (20)%. |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_003 | The AI Mobile Device SHALL have on-device speech recognition library (i.e. with no access to the Internet) for changing the system setting (e.g. Turn Bluetooth on/off via voice assistant) and invoking the native applications (e.g. send SMS via voice assistant). |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_004 | The AI Mobile Device SHOULD have access to different categories of applications and invoke these applications’ services and functions via voice assistant. |  | **O** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_005 | The AI Mobile Device SHALL support information search by on-device voice assistant. |  | **M** |  |  |  |  |  |
| TS47\_3.4.3.1\_REQ\_006 | The AI Mobile Device SHOULD support interaction with smart devices (e.g. home appliances) via voice assistant. |  | **O** |  |  |  |  |  |
| TS47\_3.4.4\_REQ\_001 | The AI Mobile Device SHOULD provide the following AI capabilities for AR native and third-party applications:   1. Hand gesture recognition. 2. Hand skeleton tracking. 3. Human body pose recognition. 4. Human body skeleton tracking. |  | **O** |  |  |  |  |  |
| TS47\_3.4.4\_REQ\_002 | The AI Mobile Device SHOULD support the following applications:   1. AR Emoji    1. Creating customized AR-based Emoji.    2. Tracking User’s facial movement and expression and render these on the AR-based Emoji. 2. AR video    1. Compositing real objects with virtual objects and/or virtual background.    2. Minimum (30) fps frame rate.    3. AR shadow effect and occlusion handling.    4. AR enhanced information text labels should not deviate or disappear from the actual target scene when the AI Mobile Device moves. |  | **O** |  |  |  |  |  |
| TS47\_3.4.5\_REQ\_001 | Only with the explicit permission of the User in order to respect the User’s right to privacy around their habits: the AI Mobile Device SHOULD support dynamic system resource allocation and optimization based on feedback provided by on-device sensors measuring environmental conditions combined with continuous learning of User habits and behaviours or device or network usage or performance indicators:  1. Dynamic application management (e.g. pre-loading, closing, put to sleep, control network access) based on User’s habits (e.g. usage duration, frequency).  2. Dynamic application management based on abnormal behaviour detection (e.g. increased memory usage, abnormal power consumption, self-starting in the background).  3. Dynamic system resource management based on continuous learning of system performance (e.g. memory and storage defragmentation, off-line storage during off-peak periods).  4. Dynamic system resource allocation for high performance applications (e.g., gaming and video). |  | **O** |  |  |  |  |  |
| TS47\_4.1\_REQ\_001 | AI on mobile device SHOULD comply with the privacy laws in the country where the device is commercially retailed. |  | **O** |  |  |  |  |  |
| TS47\_4.1\_REQ\_002 | Appropriate technical and organisational safeguards SHOULD be implemented to ensure that, by default, only the personal data reasonably necessary for a specific purpose are processed. |  | **O** |  |  |  |  |  |
| TS47\_4.1\_REQ\_003 | AI Applications that process Personal Data SHALL be off by default unless processing exclusively takes place locally on the device. |  | **M** |  |  |  |  |  |
| TS47\_4.1\_REQ\_003.1 | The User SHOULD be allowed to control whether individual AI applications are switched on. |  | **O** |  |  |  |  |  |
| TS47\_4.1\_REQ\_003.2 | The User SHOULD be allowed to control whether individual AI applications are switched off. |  | **O** |  |  |  |  |  |
| TS47\_4.1\_REQ\_004 | The AI Application on the AI Mobile Device SHALL be designed in such a way that a Data Processor will have the responsibility to:  1) Be transparent with the User on the nature of the input data used in the AI processing (e.g. personal files, biometrics, …).  2)     Forbid transferring personal data processing off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law.  3)     Forbid transferring results of on-device AI processing containing personal data off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law. |  | **M** |  |  |  |  |  |
| TS47\_4.2\_REQ\_001 | The AI Mobile Device SHALL use reasonable safeguards appropriate to the sensitivity, confidentiality and integrity of the information. |  | **M** |  |  |  |  |  |
| TS47\_4.2\_REQ\_002 | Except as required or permitted by applicable law, the User SHALL always remain in control of the collection of their personal data and its usage, in order to minimise the risk of malicious usage or data leakage. |  | **M** |  |  |  |  |  |
| TS47\_4.2\_REQ\_003 | Off ‘toggle’ switches SHALL turn off the functionality, except as permitted or required by applicable law. |  | **M** |  |  |  |  |  |
| TS47\_4.2\_REQ\_004 | Techniques, such as ‘Dark Patterns’, that manipulate the User’s choice SHALL NOT be used. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_001 | The AI models used by an AI Mobile Device SHOULD be secure and robust, and be protected with appropriate safeguards to prevent and to mitigate attacks. |  | **O** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_002 | Defence techniques SHOULD be employed to protect the training data for protecting models. For example, in evasion attacks, data can be manipulated to mislead AI models. |  | **O** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_003 | Autonomous AI Mobile Device operations SHALL be controlled, and/or authorized by the authenticated User. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_004 | AI Mobile Device operations SHOULD be performed in the Secured Environment [4], e.g. a secure boot and upgrade is enforced, and the system integrity is protected. |  | **O** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_005 | Data and metadata for AI Mobile Device SHALL be stored with encryption with keys that are stored securely in a Secured Environment, e.g. Trusted Execution Environment (TEE) [4]. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_006 | Biometric Data, which are processed by an AI Application (e.g. templates) used for authentication within the AI Mobile Device, SHALL NOT be transferred off the device. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_007 | Users' Biometric Data (such as facial data, fingerprint data, etc.) SHALL be encrypted when at rest on the device. Encryption/decryption of this data SHALL be performed in a Secured Environment [4]. |  | **M** |  |  |  |  |  |
| TS47\_3.2.1\_REQ\_007.1 | Biometric Data SHALL also be stored in the Secured Environment. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_008 | Biometric algorithms (such as face recognition algorithms, fingerprint algorithms, etc.) SHOULD run in a private and Secure Environment such as a Trusted Execution Environment (TEE) [4]. |  | **O** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_009 | If Users' Biometric Data is replaced, the previous Biometric Data before the replacement SHALL be deleted completely and permanently and not be recoverable by data rollback. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_010 | The Biometric Data SHALL be wiped and made unrecoverable by a device factory reset. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_011 | Voiceprint Data SHOULD be stored on the device with encryption. |  | **O** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_012 | The temporary Voiceprint Data SHALL NOT remain in the memory after processing. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_013 | When the Voiceprint Data is permanently and completely deleted, it SHALL NOT be recoverable by data rollback. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_014 | The Voiceprint Data SHALL be wiped and made unrecoverable by a device factory reset. |  | **M** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_015 | The device SHOULD be resistant to voice replay attacks. |  | **O** |  |  |  |  |  |
| TS47\_4.2.1\_REQ\_016 | Appropriate safeguards SHOULD be used to protect AR applications from malicious application attacks, such as spoofing a User with information about the real and/or virtual world, sensory overload attacks, hijacking the User's clicks, etc. |  | **O** |  |  |  |  |  |

1. Letter of commitment template

\_\_\_\_\_(Company name) \_\_\_\_\_\_\_\_(DUT model) complies with these privacy requirements

| **TS.47 Requirement Number** | **Requirement** | **Is this requirement supported?**  **Yes / No** |
| --- | --- | --- |
| TS47\_4.1\_REQ\_001 | AI on mobile device SHOULD comply with the privacy laws in the country where the device is commercially retailed. |  |
| TS47\_4.1\_REQ\_002 | Appropriate technical and organisational safeguards SHOULD be implemented to ensure that, by default, only the personal data reasonably necessary for a specific purpose are processed. |  |
| TS47\_4.1\_REQ\_003 | AI Applications that process Personal Data SHALL be off by default unless processing exclusively takes place locally on the device. |  |
| TS47\_4.1\_REQ\_004 | The AI Application on the AI Mobile Device SHALL be designed in such a way that a Data Processor will have the responsibility to:  1) Be transparent with the User on the nature of the input data used in the AI processing (e.g. personal files, biometrics, …).  2)     Forbid transferring personal data processing off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law.  3)     Forbid transferring results of on-device AI processing containing personal data off the device except if the User has explicitly agreed or other legal basis has been satisfied in accordance with the law. |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Company Signature & Stamp)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Data)

Note: Requirements for TS.47\_4.1\_REQ\_001 and TS.47\_4.1\_REQ\_002 are not mandatory.

1. Letter of commitment template

\_\_\_\_\_(Company name)\_\_\_\_\_\_\_\_(DUT model)complies with these privacy requirements

| **TS.47 Requirement Number** | **Requirement** | **Is this requirement supported?**  **Yes / No** |
| --- | --- | --- |
| TS47\_4.2\_REQ\_001 | The AI Mobile Device SHALL use reasonable safeguards appropriate to the sensitivity, confidentiality and integrity of the information. |  |
| TS47\_4.2\_REQ\_002 | Except as required or permitted by applicable law, the User SHALL always remain in control of the collection of their personal data and its usage, in order to minimise the risk of malicious usage or data leakage. |  |
| TS47\_4.2\_REQ\_003 | Off ‘toggle’ switches SHALL turn off the functionality, except as permitted or required by applicable law. |  |
| TS47\_4.2\_REQ\_004 | Techniques, such as ‘Dark Patterns’, that manipulate the User’s choice SHALL NOT be used. |  |
| TS47\_4.2.1\_REQ\_001 | The AI models used by an AI Mobile Device SHOULD be secure and robust, and be protected with appropriate safeguards to prevent and to mitigate attacks. |  |
| TS47\_4.2.1\_REQ\_002 | Defence techniques SHOULD be employed to protect the training data for protecting models. For example, in evasion attacks, data can be manipulated to mislead AI models. |  |
| TS47\_4.2.1\_REQ\_003 | Autonomous AI Mobile Device operations SHALL be controlled, and/or authorized by the authenticated User. |  |
| TS47\_4.2.1\_REQ\_004 | AI Mobile Device operations SHOULD be performed in the Secured Environment [4], e.g. a secure boot and upgrade is enforced, and the system integrity is protected. |  |
| TS47\_4.2.1\_REQ\_005 | Data and metadata for AI Mobile Device SHALL be stored with encryption with keys that are stored securely in a Secured Environment, e.g. Trusted Execution Environment (TEE). |  |
| TS47\_4.2.1\_REQ\_006 | Biometric Data, which are processed by an AI Application (e.g. templates) used for authentication within the AI Mobile Device, SHALL NOT be transferred off the device. |  |
| TS47\_4.2.1\_REQ\_007 | Users' Biometric Data (such as facial data, fingerprint data, etc.) SHALL be encrypted when at rest on the device. Encryption/decryption of this data SHALL be performed in a Secured Environment. |  |
| TS47\_4.2.1\_REQ\_007.1 | Biometric Data SHALL also be stored in the Secured Environment. |  |
| TS47\_4.2.1\_REQ\_008 | Biometric algorithms (such as face recognition algorithms, fingerprint algorithms, etc.) SHOULD run in a private and Secure Environment such as a Trusted Execution Environment (TEE). |  |
| TS47\_4.2.1\_REQ\_011 | Voiceprint Data SHOULD be stored on the device with encryption. |  |
| TS47\_4.2.1\_REQ\_012 | The temporary Voiceprint Data SHALL NOT remain in the memory after processing. |  |
| TS47\_4.2.1\_REQ\_016 | Appropriate safeguards SHOULD be used to protect AR applications from malicious application attacks, such as spoofing a User with information about the real and/or virtual world, sensory overload attacks, hijacking the User's clicks, etc. |  |

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Company Signature & Stamp)

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(Date)

1. Document Management
   1. Document History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
| 0.3 | Oct 2021 | The following CRs have been included:   * TSGAI#21 Doc 003 TS.53 CR Section 6 Biometric Performance test cases * TSGAI#21 Doc 004 TS.53 CR Section 6 Voice assistant test cases * TSGAI#21 Doc 005 TS.53 CR Section 7 privacy test cases * TSGAI#20 Doc 004 TS.53 AI Mobile Device Requirements Specification Test Book 0921 * TSGAI#19 Doc 004 - Draft CTS for AI mobile device V0.2-China Telecom 0816 (partly approved) * TSGAI#19 Doc 003 - Fido biometric requirements Introduction (For discussion) * TSGAI#19 Doc 005 - Dataset for TS.53 CTS (For discussion) * TSGAI#18 Doc 003 TS.53 Section 4 Updated FPE test case * TSGAI#18 Doc 004 TS.53 Section 6 Updated privacy requirements * TSGAI#16 Doc 003 TS53 CR001 v0.3 Section 2-3 China Telecom ( **updated one based on TSGAI#15 Doc 004**) * TSGAI#15 Doc 004 TS53 CR001 Section 2-3 Updated hardware and software test cases China Telecom * TSGAI#15 Doc 005 TS53 CR002 Section 6 Updated security requirements test cases China Telecom * TSGAI#13 Doc 001 TS.53 CTS for AI mobile device China Telecom CR0001 v1 (partly approved) | TSGAI | Di Zhang China Telecom |
| 0.4 |  | The following CRs have been included:   * TSGAI#22 Doc 005 - CR Section 6.4.1 AI capabilities for AR application test cases-CT * TSGAI#22 Doc 007 CR for Security test cases-CT(open) | TSGAI | Di Zhang China Telecom |
|  |  |  |  |  |

* 1. Other Information

|  |  |
| --- | --- |
| Type | Description |
| Document Owner | Terminal Steering Group AI |
| Editor / Company |  |

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at [prd@gsma.com](mailto:prd@gsma.com)

Your comments or suggestions & questions are always welcome.