Advanced Card Systems Ltd.
Card & Reader Technologies

ACS VAS Test Tool (USB/Serial)

ACS VAS Test Tool User Guide V0.03

info@acs.com.hk
www.acs.com.hk

Table of Contents

List of Figures

No table of figures entries found.

List of Tables

No table of figures entries found.

1.0. Preparation

This section provides instructions on how to install the following test passes on your mobile device.

1.1. Downloading the ACS Apple Test Pass in Apple Wallet

The following steps outline the procedure for downloading and storing the ACS Apple Test Pass in Apple Wallet:

1. Open the **Camera** application on your iPhone and scan the **Apple Demo Pass QR Code**.
2. Click on the corresponding bit.ly link.

3. If the **bit.ly** link fails to open, ensure that **Safari** is set as the default browser and attempt again.
4. Click **"Next"** to save the ACS Test Pass to Apple Wallet.

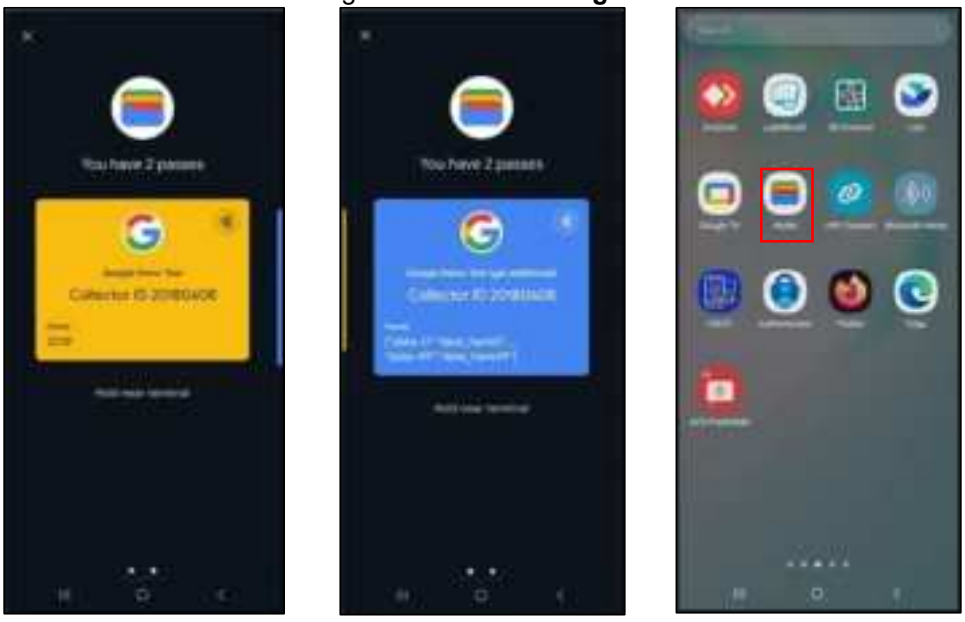
5. The pass can now be accessed via the **Wallet** application.

1.2. Downloading the Google Test Pass in Google Wallet

The following steps outline the procedure for downloading and storing the Google Test Pass in Google Wallet:

1. Open the **Camera** application on your Android device or use a QR code scanning application to scan one of the following QR codes:
   Google Demo Pass#1 QR Code (the Basic loyalty demo pass, expected payload 2018) or
   Google Demo Pass#2 QR Code (a Long loyalty demo pass which get additional data, expected payload {"data-0":"data_here0", ... "data-49":"data_here49"}).
2. Both demo passes may be saved if required.
3. Click on the displayed **web link** after scanning the QR code.

4. Click **"Add"** to store the Google Test Pass in **Google Wallet**.



1.3. Apple ECP 2.0 Test Pass Preparation

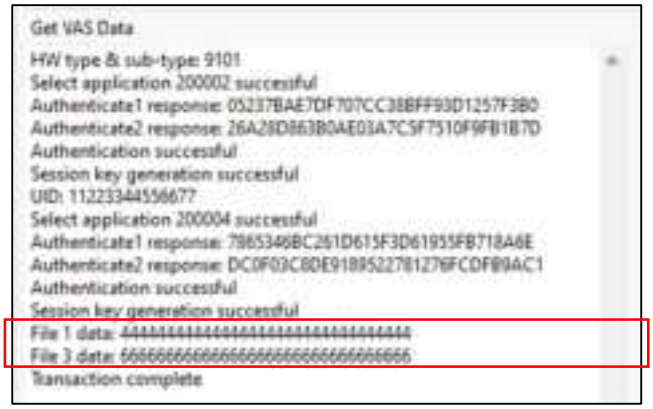
1.3.1. Downlaod the Test Pass to Apple Wallet

Follow Apple's instructions to add the ECP 2.0 Pass to the Apple Wallet.

Notes: Due to an NDA with Apple, we cannot provide the ECP 2.0 Apple Demo Pass to customers.

1.3.2. Adjust the code of VAS Test Tool (IMPORTANT)

The demo scenario involves Access Control. The goal is to read Desfire, File 1, and File 3. Access is granted if the files are read correctly.



The following steps outline the procedure for adjust the code of VAS Test Tool for your Apple ECP 2.0 Pass:

1. Get the DESFIRE Pass information from the Pass issuer:
    a. AID of the UID file
    b. Key of the UID file
    c. AID of the Data file
    d. Key of the Data file
    e. Terminal Info of the Pass
    f. Terminal type of the Pass
    g. TCI value of the Pass
    h. Data of the Pass (if have)
2. According to the information, modify the ProcessDesfireDemoPass function(line 661) in Worker.cs of the VAS Test Tool source code.
   Since the file structure may not be the same, please refer to line 709 for UID file and line 742 for Data file.

```
661     private void ProcessDesfireDemoPass()
662     {
663         ErrorCode res = ErrorCode.VasNoError;
664         bool isApple = false;
665         // Apple Desfire demo pass access
```

```
708         }
709         // Authenticate for AID 200002
710         byte[] aid0 = Utils.HexToBytes("200002");
711         byte[] key0 = Utils.HexToBytes("F202020202020202020202020202020202");
712         if (!AuthenticateDesFire(key0, 0, aid0))
713             break;
714         // Get UID
```

```
741                 }
742                 // Authenticate for AID 200004
743                 byte[] aid1 = Utils.HexToBytes("200004");
744                 byte[] key1 = Utils.HexToBytes("F606060606060606060606060606060606");
745                 if (!AuthenticateDesFire(key1, 0, aid1))
746                     break;
747                 // Read data file 01, 03
```

3. Rebuild the VAS Test Tool

2.0. ACS VAS Test Tool

The **ACS VAS Test Tool** is a proprietary software solution developed by **Advanced Card Systems Ltd. (ACS)**, designed to facilitate the testing of **NFC-enabled Google Pay passes** using the **WalletMate II** reader. Currently, the **ACS VAS Test Tool** is exclusively supported on **Windows operating systems**.

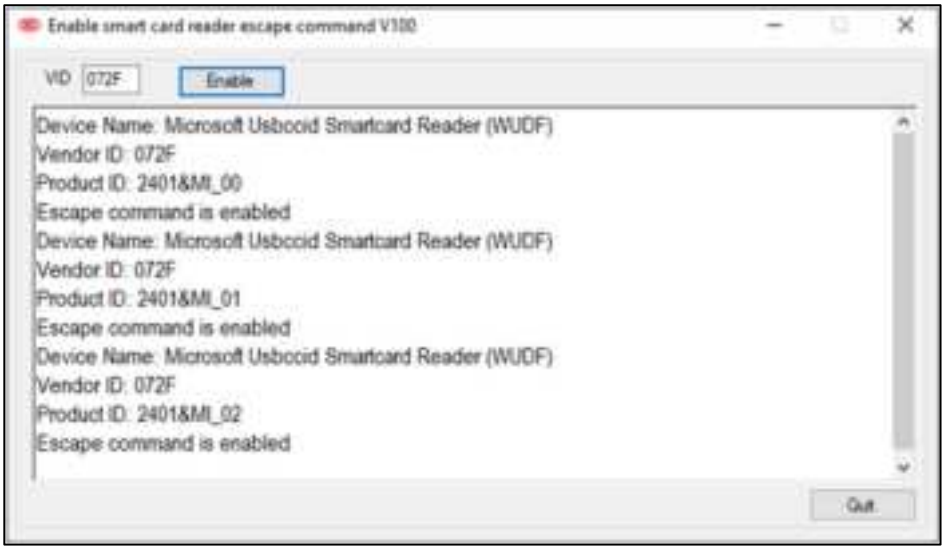
2.1.1. Activating the Escape Command

Due to ongoing driver development, it is necessary to manually activate the **Escape Command** by following the steps outlined below:

Notes: Each Reader needs to be enabled once per USB port.

1. Insert the **WalletMate II Reader** into the computer.

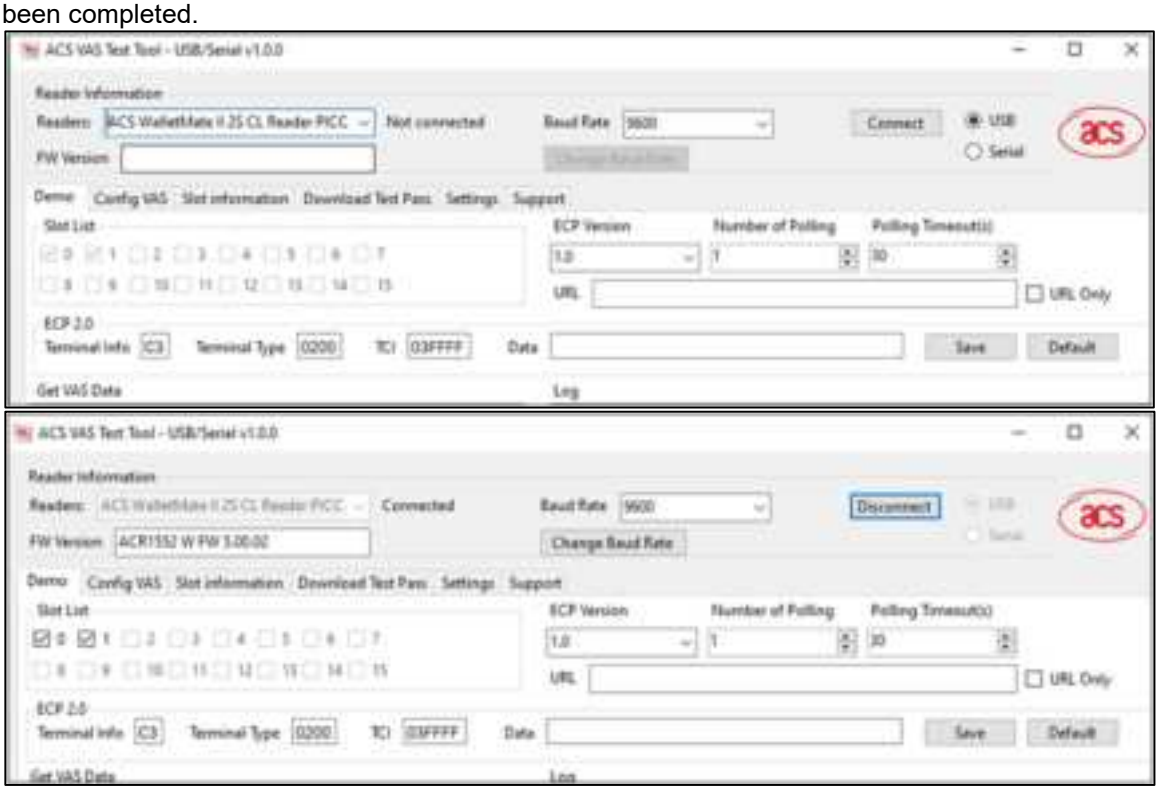
2. Launch the **Enable Smart Card Reader Escape Command V100.exe** application.
3. Click the **"Enable"** button.
4. After approximately **30 seconds**, a confirmation message will be displayed, indicating successful activation.



2.1.2. Launching the ACS VAS Test Tool

To initialize and configure the **ACS VAS Test Tool**, proceed with the following steps:

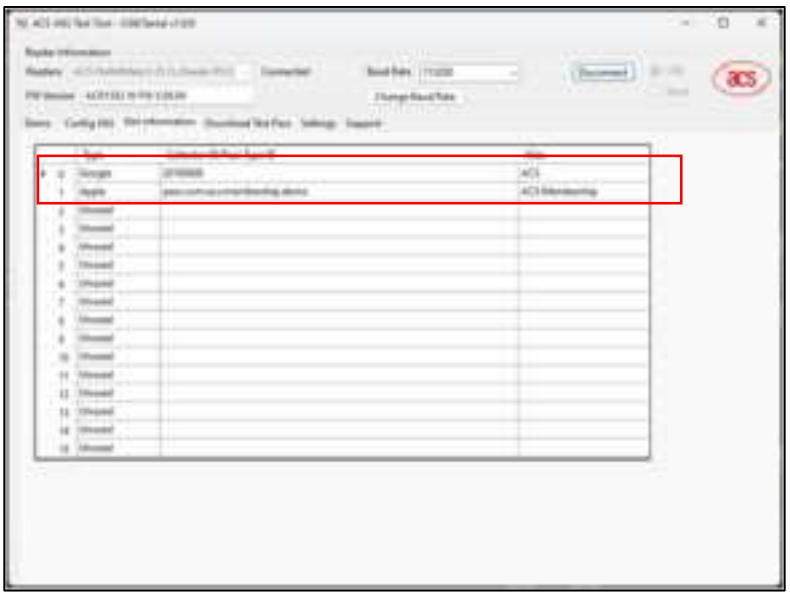
1. Extract the **VASTestToolSerial-XXXXXX.zip** file provided by ACS.Connect your WalletMate II Reader to your PC via USB cable.
2. Establish a **USB connection** between the **WalletMate II Reader** and the computer.
3. Navigate to the **\VASTestToolSerial-XXXXXX\VASTestToolSerial\bin\Debug** folder and double-click **VASTestToolSerial.exe** to launch the application.
4. If prompted with a dialog box requesting the installation of missing **Microsoft Windows Components**, follow the on-screen instructions to install them.
5. Upon successful connection and recognition of the **WalletMate II Reader**, its name will be displayed in the upper left corner of the application interface.
6. Click the **"Connect"** button. If the firmware version is displayed, the connection has been successfully established.
   If the firmware version is not displayed, ensure that **Activating the Escape Command has been completed.



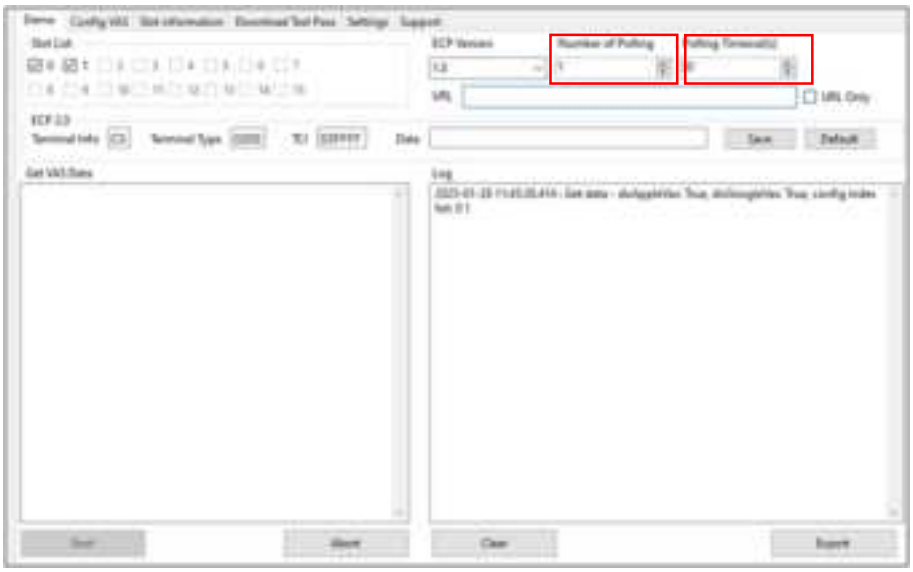
2.1.3. Testing ACS Apple and Google Passes

This section provides a step-by-step guide for testing **ACS Test Passes** stored in **Apple Wallet** and **Google Wallet** using the **ACS VAS Test Tool**:

1. Navigate to the **Slot Information** tab.
   - **Slot 0** is pre-configured for **Google Pass** parameters.
   - **Slot 1** is pre-configured for **ACS Apple Pass**.



2. Return to the **Demo Tap** section. Adjust the **Number of Polling** and **Polling Timeout (in seconds)** as needed.



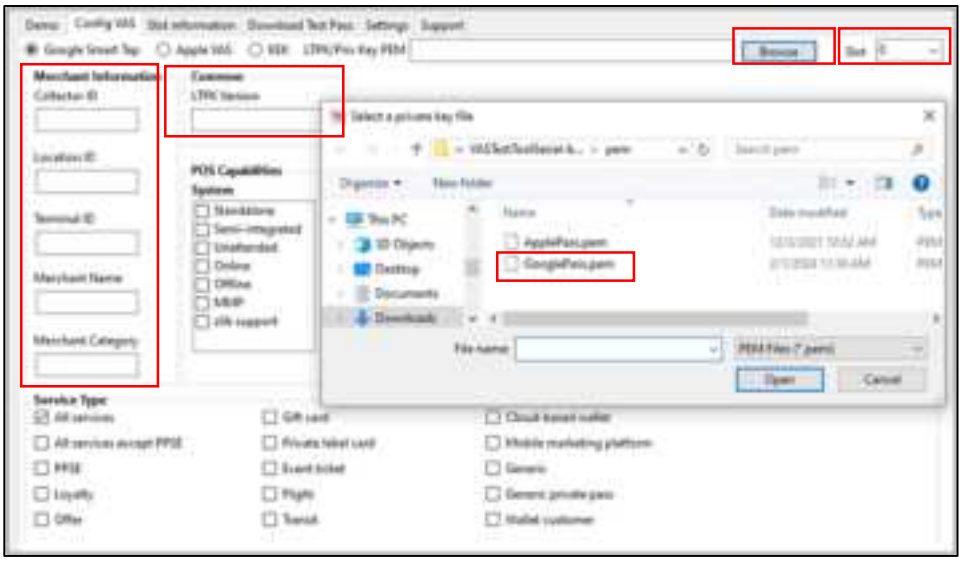
3. Click the **"Start"** button to commence testing.
4. Place the mobile device on top of the **WalletMate II Reader.**

5. If the test is successful:
    - The acquired data will be displayed under “Get VAS Data” box.
    - The mobile device screen will display a **blue tick mark**, signifying successful authentication.

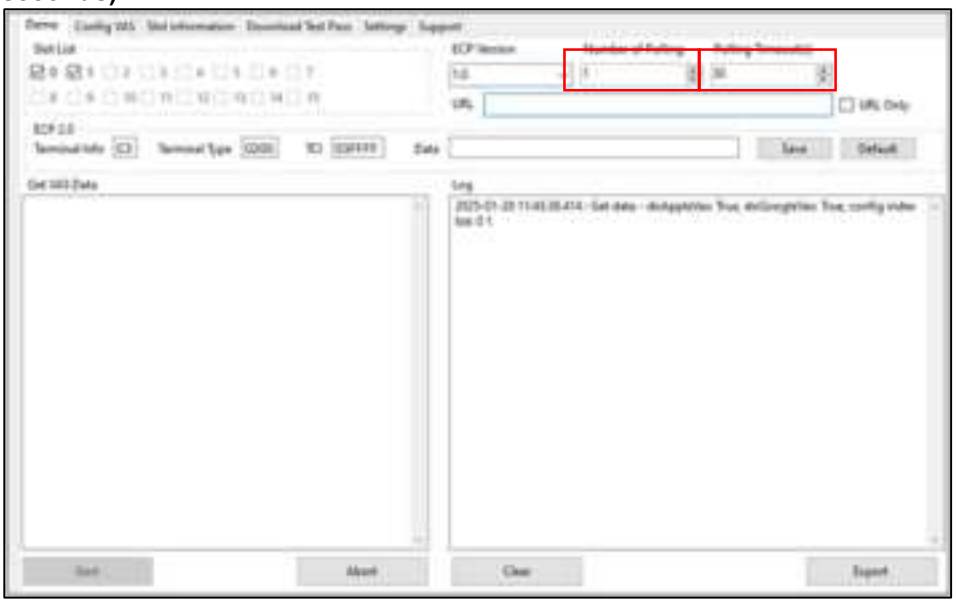
2.1.4. Testing Custom NFC-Enabled Google Passes

If a **custom NFC-enabled Google Pass** has been developed and the requisite **Public and Private Keys** have been generated (with the **Public Key uploaded to the Google Wallet API Issuer Account**), the following steps should be followed to conduct testing using the **ACS VAS Test Tool**:

1. Navigate to the **Config Google Smart Tap** tab and enter the **Collector ID, Location ID, Terminal ID, Merchant Name, Merchant Category, LTPK Version.**
2. Select the **Pass Type** to be received (*default: All Services*).
3. Click **Browse** and select the **.pem** file (private key) that was generated.
4. Prior to saving, ensure that the **correct slot number** is selected (e.g., Slot 2).
    - **Caution:** Selecting an occupied slot may result in **overwriting the slot data**



5. Return to the **Demo Tap** section and configure the **Polling Count** and **Polling Timeout (in seconds)**.



6. Click **"Start"** to initiate the custom Google Pass test.

2.1.5. Testing Custom NFC-Enabled Apple ECP 1.0 Passes

To authenticate a **custom NFC-enabled Apple ECP 1.0 Pass** using the **ACS VAS Test Tool**, follow the steps below:

1. Navigate to the Config VAS tab and select Apple VAS.

2. Click **Browse** and select the **.pem** file (private key) that was generated.
3. Enter the **Pass Type Identifier**.
4. Prior to saving, ensure that the **correct slot number** is selected (e.g., Slot 3).
    - **Caution:** Selecting an occupied slot may result in **overwriting the slot data**

5. Return to the **Demo Tab**, adjust the **Polling Count** and **Polling Timeout (in seconds)**, and then click **"Start"**.

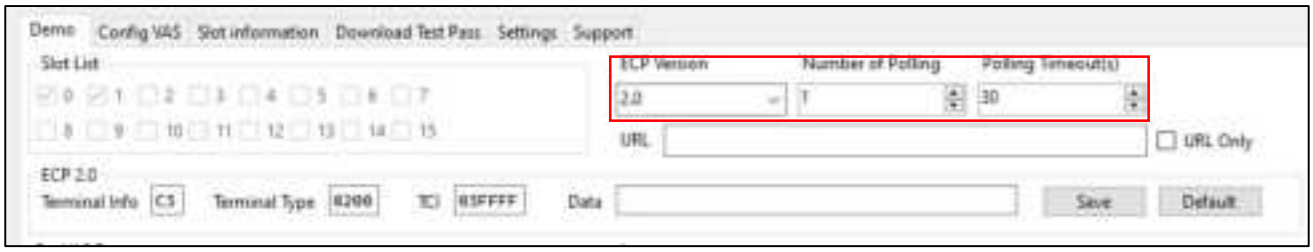
6. Tap the iPhone on top of the WalletMate II NFC Reader.
    - If the iPhone is locked (Face ID/Touch ID/Passcode), an authentication prompt will be displayed.

7. Tap the **iPhone or Apple Watch** once again on the **WalletMate II NFC Reader.**
    - If successful, a **tick mark** will be displayed on the screen, and the pass will automatically close.

2.1.6. Testing Custom Apple ECP 2.0 Passes

After Adjust the code of VAS Test Tool (IMPORTANT), to authenticate a **custom Apple ECP 2.0 Pass** using the **ACS VAS Test Tool**, follow the steps below:

1. Navigate to the Demo tab, change ECP Version to 2.0
2. Enter the following parameters (from Apple) in the ECP 2.0 section:
    a. Terminal Info of the Pass
    b. Terminal type of the Pass
    c. TCI value of the Pass
    d. Data of the Pass (if have)
3. Adjust the **Polling Count** and **Polling Timeout (in seconds)**, and then click **"Start"**.



4. Tap the **iPhone or Apple Watch** once again on the **WalletMate II NFC Reader.**
    - If successful, a **tick mark** will be displayed on the screen, and the pass will automatically close.

3.0. FCC Warning Statement

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

—Reorient or relocate the receiving antenna.

—Increase the separation between the equipment and receiver.

—Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

—Consult the dealer or an experienced radio/TV technician for help.

This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.