3GPP TSG CT WG6 Meeting #103-e C6-200837
Electronic meeting, 17-20 November 2020
Source: Qualcomm Incorporated
Title: Black Box Testing for 31.121 and 31.124 test cases
Agenda item : 7.10.9
Document for: Discussion
Comments: Revision of C6-200819 which is revision of C6-200758

Content

- Background
- Black Box testing
- Use of Standard UICC in ME for Black Box testing
- Black Box test setup examples
- Challenges to meet Acceptance Criteria
- Requirements for APDUs in SIM-ME interface
- List of EF Reads to be verified for 31.121 5G TCs
- Verification of EF read (1)
- Verification of EF read (2)
- Verification of EF read (3)
- Verification of GET IDENTITY command
- Verification of AUTHENTICATE command
- Changes for 31.124
- Summary

Background

- 3GPP 31.121 and 31.124 Test suites available today support only the removable SIM form factor.
- Black Box test systems can be used with any device irrespective of the form factor of SIM it has.
- For this test approch ME is cosidered as a Black Box. Test systems do not aware of the form factor of the card ME has and it can be removable, embedded or integrated.
- As per the GCF CC Annex H.2.10 removable eSIMs with starndard profile can also be used if Test system supports it.

  Case 1: *Device with SIM slot supporting the removable UICC:*
  All existing test cases are applicable.
  A removable UICC/eUICC/eSIM with TS.48 Generic Test Profile loaded can also be used if test system supports TS.48 Generic Test Profile as the default profile in the UICC.
- Some of the Test Cases in the current 31.121 and 31.124 specifications can't support Black Box testing.
- Test Cases in the following sections need new TC variants for Black Box testing.
  - 31.121 5.3, 5.5 and 15
  - 31.124
- Only some of the TCs in above sections need new TC variant. Some of TCs can be used as it is for Black Box testing.
- In case of 31.124, APDUs can be monitored if Test Applets are used in Black Box testing. Hence very minimum or no changes are required for the TCs in 31.124.
  - Minor change in initial conditions is sufficient for all most all the TCs and TC changes are needed only for Event Download TCs
- Having the test environment and the practical environment same is an advantage with Black Box testing.
  - Testing is performed with real cards and avoid using fixed data in EFs.
- Test System shall make sure to verify ***all*** the existing requirements in acceptance criteria even without monitoring the ADPUs.
- New TCs introduce new methods to verify all the existing requirements in acceptance criteria of the TC.

Black Box testing

- Black Box testing may be performed on an ME with UICC inserted or embedded or integrated where the physical interface between the ME and the UICC is not exposed to a SIM Simulator for monitoring the APDUs or for triggering any command.
- Test System shall update Elementery Files in the UICC to set up the Initial conditions for each Test Case.
- If Black Box testing is performed,
  - Acceptance Criterias of a test case related to Elementery Files read shall be verified without monitoring the structure and content of the APDUs send to the UICC.
  - Triggering of toolkit commands if needed shall be performed from the UICC itself.
  - UICC files shall be reset back to the orginal default contents for the test cases if needed.
- The solution provided in this discussion paper is mainly focused on,
  - proving the source of the data or functionality (SUCI calculation or Authentication) is UICC and
  - using standard UICC in the ME (eg: compliant with ETSI 102.221 and TCA eUICC PP IF v2.3 higher).

Use of Standard UICC in ME for Black Box testing

- Use of standard UICC to verify ME behaviour is not a new approach. SGP.23 Device/LPA testing in GCF has been using this approach for some time.

- Here is the 3.2.3 clause from SGP.23.

> ***3.2.3 Device/LPAd - Test Environment***
>
> *The following test environment is used for all LPAd Interfaces related test cases as defined in chapter 4.4 and 5.4 (unless it is specified differently in the specific test case). Following conditions apply:*
>
> - *The Device contains an eUICC configured with Test Certificates and Test Keys*
> - *The Test eUICC is either soldered or removable. In case the eUICC is removable, it SHALL NOT be removed during testing*
> - *The Test eUICC is only used for LPAd testing and SHALL not be considered as an IUT*
> - *The Test eUICC SHALL not support LPAe*
> - *The Test eUICC SHOULD be compliant with the GSMA RSP Technical Specification [2]*
> - ....

- As per GCF CC Annex H.2.10 removable eSIM with starndard profile can be used for case 1 if Test system supports it.
- Black Box testing introduces the same approach that is being used in GCF already.
- For Black Box testing a UICC compliant with ETSI 102.221 and TCA eUICC PP IF v2.3 higher can be used.

Black Box test setup examples

- Black Box testing may use AT interface or RFM interface for the Test System to update files or trigger commands from UICC.
- AT interface may not be supported in all the UEs.
- RFM can be used for such UEs but it shall be camped on to NW simulator for sending the RFM commands.
- It would be an advantage if Test Systems can support both interfaces and select the interface depend on the UE capabilities.
- Test Applets in the UICC can be used to trigger proactive commands from the card.
  - RFM (ETSI 102.226) or AT commands can be sent for Test System to trigger proactive commands.
  - Test Applet can be used for file updates as well. It can be loaded using RAM (ETSI 102.226) or any other tools.

Challenges to meet requirements in Acceptance Criteria

31.121

- Some of the TCs need to verify ME has read certain EFs from the UICC.
- SUCI calculation by USIM TCs need to verify if ME has sent correct GET IDENTITY command to the UICC.
- Authentication TCs need to verify that ME forwards the RAND and AUTN received in OTA NAS messages to the USIM.
- Some of the files in the USIM are not accessible in all the cards.
  - Eg: EFs under DF-SAIP, EF-SQN

31.124

- Need to trigger proactive commands from the UICC.
  - No TC changes are required for this and how to trigger the proactive commands is implementation specific.
  - Use of Test Applets is commonly used in commercial cards for carrier requirements and it can be used for test purpose as well.
- Need to verify TERMINAL RESPONSE and ENVELOP commands send by the ME
  - No TC changes are required for this and how to verify TERMINAL RESPONSE and ENVELOP commands is implementation specific.
- Since SET UP EVENT LIST proactive command is handled by the CAT Runtime Environment TERMINAL RESPONSE for this command can’t be accessed by Toolkit Applets.
  - Configuring EVENT LIST in SET UP EVENT LIST proactive command is required for verifying LOCATION STATUS EVENT or any other EVENT.
  - Configuring EVENT LIST in SET UP EVENT LIST is an initial condition and it is not in the Test Purpose. Hence it can be included as initial condition and test system to make sure EVENT LIST is configured with required EVENTs if it is needed for the TC.

Requirements for APDUs in SIM-ME interface

- Black Box implementation is vendor specific, but it shall make sure APDU structure and the contents in SIM-ME interface adhere to relavent specifications.
- Following specifications can be considered for Black Box implementation:
  - GSMA TS.48 Generic Test Profile (GTP) v3.0 or higher can be used as the default UICC profile and Test System shall update the EFs as needed for the Test Cases.
    - This profile can be pre-loaded on to a removable/embedded eSIM or integrated iSIM whatever available in the ME.
  - Removable/embedded eSIM or iSIM should be compliant with
    - ETSI 102.221 and 3GPP 31.122 (Test spec) with respect to EF referencing and APDU command structures.
    - Trusted Connectivity Alliance eUICC Profile Package Interoperable Format (TCA PP IF) Technical Specification v2.3 or higher.
  - Having compliance with TCA PP IF v2.3 or higher and with ETSI 102.221 (test spec 31.122) is important for SUCI calculation and processing of GET IDENTITY APDU or any other APDU (READ BINARY or READ RECORD).
    - Eg: If Test System guarantees only the data related to SUCI calculation by USIM is available and expected data for SUCI is received OTA by NG-SS, it implicitly proves ME has sent GET IDENTITY to the TCA PP IF v2.3 and ETSI 102.221 compliant eSIM/iSIM correctly.
    - The same logic applies for READ BINARY and READ RECORD if Test System guarantees data to be read is only available in the eSIM/iSIM.

List of EF Reads to be verified for 31.121 5G TCs

- 3GPP 31.121 5G TCs include verification of READ commands for the following EFs.
  - EF-IMSI,
  - EF-UST,
  - EF-SUCI_Cal_info,
  - EF-Routing_Indicator,
  - EF-5GS3GPPNSC,
  - EF-5GAUTHKEYs,
  - EF-5GS3GPPLOCI.
- Test case procedure and acceptance criteria shall make sure the source of file content read is from the relevant EF in USIM.
  - If the Test UICC used in the ME is a standard UICC (eg: compliant with ETSI 102.121 Rel 15 or higher and TCA PP IF v2.3 or higher) APDU structure and the content send by the ME shall be compliant with specifications.
- All the EFs above should be verified but not necessary to verify the same EF in all the TCs.
  - All those EFs are read at power up initialization and that procedure is same for all the TCs. It is not necessary to verify reading of the same file during power up initialization in all the TCs.
  - Hence new TC variants may not include verification of the same EF read in all the TCs.

Verification of EF read (1)

EF-IMSI, EF-SUCI_Calc_Info, EF-Routing_Indicator

- Test System shall update EF-IMSI, EF-Routing_Indicator and EF-SUCI_Calc_Info with different / random values as the last digit of the IMSI (x), RI (y) and HN Public Key Identifier (z) every time the TC is initialized.
- Also Test System shall delete the data required for SUCI calculation by USIM to avoid any possible SUCI calculation by USIM for SUCI calculation by ME.
- NG-SS shall compare x, y, z extracted from SUCI against what Test System updated in the USIM and confirm if matches.
- If for example, removable / embedded eSIM or iSIM is compliant with TCA-PP-IF and ETSI 102.221 specifications, APDU structure for the READ command should be correct.
- Considering all the above, Acceptance Criteria that ME read EF-IMSI, EF-Routing_Indicator and EF-SUCI_Calc_Info can be verified by comparing the random x, y and z values updated by the Test System and values received from SUCI.

Verification of EF read (2)

EF-5GS3GPPNSC, EF-5GAUTHKEYS

- TC shall use valid 5G NAS Security Context and valid 5G Keys instead of using no valid security context (ngKSI=7) as the initial context, for the TCs need verification of reading EF-5GS3GPPNSC and EF-5GAUTHKEYS.
  - The condition with no initial 5G NAS Security Context shall be verified with TCs do not need verification of reading of those EFs.
  - This will provide an additional verification compared to what we have in current 31.121.
- NG-SS generates Authentication vectors using the RAND send to the ME and the K used in the USIM and uses the CK/IK to derive the 5G Authentication Keys and the NAS security context .
- Test System shall update EF-5GS3GPPNSC file with the NAS Security Context and EF-5GAUTHKEYS with the K_{AMF}, K_{AUSF} and K_{SEAF} already generated.
  - Since RAND is a random number 5G Keys and NAS Security Context will be different each time the TC is initialized
  - If RFM is used for the file update NG-SS shall send AUTHENTICATION REJECT before powering down the ME at TC initialization to avoid the security EFs being overwritten by the ME.
- ME shall use protected NAS messages to send REGISTRATION REQUEST since card has valid NAS security context.
- If NS-SS can decode the REGISTRATION REQUEST that proves ME has read the files EF-5GS3GPPNSC and EF-5GAUTHKEYS.
- If for example, removable / embedded eSIM or iSIM is compliant with TCA-PP-IF and ETSI 102.221 specifications, APDU structure for the READ command send by the ME should be as per the specifications.
- Considering all the above, Acceptance Criteria for read EF-5GS3GPPNSC and EF-5GAUTHKEYS can be verified by using NAS protected messages and ability for decoding the REGISTRATION REQUEST correctly.

Verification of EF read (3)

EF-UST

- EF-UST verification can be done by using Service nº 124. Test System shall update service nº 124 randomly.
- NS-SS to verify that ME uses Null scheme or scheme B/A at power up correctly to confirm that ME read the UST file.
  - If Test system has chosen to make service nº 124 not available at powerup verify that ME uses NULL scheme. Otherwise, verify that ME uses protection scheme B/A.
  - For some TCs Test System can toggle the service nº 124 and verify the change in the Protection Scheme by resetting the device (Eg. 15.1.1)
- If for example, removable / embedded eSIM or iSIM is compliant with TCA-PP-IF and ETSI 102.221 specifications, APDU structure for the READ command should be correct.
- Considering all the above, Acceptance Criteria for read EF-UST can be verified by verifying the protection schemes used at power up REGISTRATION.

Verification of GET IDENTITY command

- Test System updates EF-IMSI, EF-Routing_Indicator and data for SUCI calculation by USIM with different / random values as the last digit of the IMSI (x), RI (y) and HN Public Key Identifier (z) every time the TC is initialized.
  - A Test Profile with access to files under DF-SAIP shall be loaded on to the UICC (eg: GSMA TS.48 Generic Test Profile).
- Also Test System shall delete the data required for SUCI calculation by ME (EF-SUCI_Calc_Info) to avoid any possible SUCI calculation by ME.
- NG-SS shall verify if x, y, z extracted from SUCI against what Test System updated in the USIM.
- If for example, removable / embedded eSIM or iSIM is compliant with TCA-PP-IF v2.3 or higher and ETSI 102.221, SUCI calculation should have been done by the USIM and the APDU structure for the GET IDENTITY command sent by the ME should be correct.
- Considering all the above, Acceptance Criteria if ME has sent the correct GET IDENTITY can be verified by comparing the random x, y and z values updated by the NS-SS and received from SUCI.

Verification of AUTHENTICATE command

- Some of the TCs need to verify ME forwards the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge message to the USIM.
- For such TCs, Test System shall choose a different / random SQN value (SQN_{HE}) every time the TC is initialized and update EF-SQN in the USIM with SQN_{MS} (highest received SQN, SEQ_{MS} -SEQ < L. Ref Annex C.2.2 in 3GPP 33.102).
  - Make sure SEQ received is accepted by the USIM and not generate a sequence numbers sync failure.
  - A Test Profile with access to EF-SQN file shall be loaded no to the UICC (eg: GSMA TS.48 Generic Test Profile).
- NG-SS to use same SQN when generating the AUTN.
- If Authentication procedure initiated by the NG-SS is successful, that implicitly verifies that ME forwards the RAND and AUTN received in OTA message to the USIM.
  - SQN received in AUTN is acceptable and does not generate a Sync Failure by the USIM.
  - Successful Authentication Response with RES* at NG-SS.
- If for example, removable / embedded eSIM or iSIM is compliant with ETSI 102.221 and 3GPP 31.122 the APDU structure for the AUTHENTICATE command with RAND and AUTN sent by the ME should be correct.
- Considering all the above, Acceptance Criteria that ME forwards the RAND and AUTN received in EAP message IE with EAP-request/AKA'-challenge message to the USIM can be verified by updating the EF-SQN in the USIM to match with the SQN used by NS-SS for computing AUTN.
  - TCs that do not verify this requirements can have the default SQNs (all zeros) without any change.

Changes for 31.124

Verify TERMINAL RESPONSE and ENVELOP commands send by the ME

- No TC changes in the specification are required except to allow using any type of SIM with a Test Profile loaded (eg: GSMA TS.48 eUICC Generic Test Profile).
- How Test System verify TERMINAL RESPONSE and ENVELOP commands is implementation specific.
- Using a Test Applet may be an option for that purpose.

TCs with LOCATION STATUS ENVELOP

- Since SET UP EVENT LIST proactive command is handled by the CAT Runtime Environment TERMINAL RESPONSE for this command can’t be accessed by Toolkit Applets.
- Configuring EVENT LIST in SET UP EVENT LIST proactive command is required for verifying LOCATION STATUS EVENT or any other EVENT.
- Though the required EVENT LIST configured in SET UP EVENT LIST is an initial condition and not in the Test Purpose current TCs consider it as a test step and not an initial condition.
- Therefore, TCs verifying LOCATION STATUS events shall be modified to include EVENTs to be registered as initial conditions
- If Test Applets are used it can call ***reg.setEvent()*** with required EVENTs during TC initialization to register for required EVENT LIST.

Summary

- As per reply LS C6-200618 for the GSMA LS (TSG eSIMTest meeting #29) a new version of TCs will be required for Black Box testing.
- For this test approch ME is cosidered as a Black Box. Test systems do not aware of the form factor of the card ME has.
- Black Box testing may be performed on an ME with UICC inserted or embedded or integrated where the physical interface between the ME and the UICC is not exposed to a SIM Simulator.
- TC modifications suggested shall be done so that the new variant of the TCs meet ***all*** the requirements in acceptance criteria to ensure black box testing can be used with both removable/non-removable eSIM and iSIMs.
- There are several challenges to handle all the test requirements in acceptance criteria of those TCs and each case shall be handled separately (eg: Read EFs, GET IDENTITY, AUTHENTICATE, SET UP EVENT LIST proactive command etc.) as described in this discussion paper.
  - EF read happens during power up initialization and it is common for all the TCs
  - Hence it is not necessary to verify reading of the same EF in all the TCs.
- Test systems shall update certain EFs with random data to mitigate the challenges.
  - Test Profile loaded on to the UICC shall provide access to all the needed EFs. Eg: EF under DF-SAIP for SUCI calculation by USIM, EF-SQN.

Thank you

Follow us on:

For more information, visit us at:

www.qualcomm.com & www.qualcomm.com/blog

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

©2016 Qualcomm Technologies, Inc. and/or its affiliated companies. All Rights Reserved.

Qualcomm is a trademark of Qualcomm Incorporated, registered in the United States and other countries. Other products and brand names may be trademarks or registered trademarks of their respective owners.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes Qualcomm’s licensing business, QTL, and the vast majority of its patent portfolio. Qualcomm Technologies, Inc., a wholly-owned subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of Qualcomm’s engineering, research and development functions, and substantially all of its product and services businesses, including its semiconductor business, QCT.

Back Up slides

Complete 5G TC list for each test methods

- Currently all the TCs available in test specifications are selected for the device certification.
- Additional Execution Rules AE0xx and AE0yy are introduced to enable Black Box based testing.

AER0xx	TC is optional if Test System supports Black Box testing as in Annex X
AER0yy	TC is mandatory if Test System supports Black Box testing as in Annex X

- Some of the TCs are applicable for both Black Box based and SIM Simulator based test methods.
- Hence the TC selection shall be done as below.
  - For Black Box TCs:

    <TC_list_BlackBox> = <All 5G TCs> != AER0xx

  - For SIM Simulator TCs:

    <TC_list_SimSimulator> = <All 5G TCs> != AER0yy

List of 5G 31.121 TCs need changes for Black Box testing

TC #	TC changes required?	Change required for verifying
5.3.1	Y	Read EF_{IMSI}, $EF_{Routing_Indicator}$ and $EF_{SUCI_Calc_Info}$
5.3.2	Y	Read EF_{IMSI}, $EF_{Routing_Indicator}$ and $EF_{SUCI_Calc_Info}$
5.3.3	Y	GET IDENTITY command
5.3.4	N	
5.3.5	N	
5.3.6	N	
5.3.7	Y	Read EF_{IMSI}, EF_{UST}, $EF_{SUCI_Calc_Info}$ and $EF_{Routing_Indicator}$
5.3.8	Y	Read EF_{IMSI} and $EF_{5GS3GPPLOCI}$
5.3.9	Y	Read EF_{IMSI}.
5.3.10	Y	Read EF_{IMSI}.
5.3.11	Y	Read EF_{IMSI}, EF_{UST}, $EF_{SUCI_Calc_Info}$ and $EF_{Routing_Indicator}$
5.3.12	Y	GET IDENTITY command
5.3.13	Y	Read EF_{IMSI}, $EF_{Routing_Indicator}$ and $EF_{SUCI_Calc_Info}$
5.3.14	Y	Read EF_{IMSI}, $EF_{Routing_Indicator}$ and $EF_{SUCI_Calc_Info}$
5.3.15	Y	Read EF_{IMSI}.
5.3.16	Y	Read EF_{IMSI}, EF_{UST}, $EF_{SUCI_Calc_Info}$ and $EF_{Routing_Indicator}$
5.3.17	Y	Read EF_{IMSI}, $EF_{Routing_Indicator}$ and $EF_{SUCI_Calc_Info}$
	.	
5.4.x	N	
	.	
5.5.x	N	
	.	
15.1.1	Y	Read EF_{UST}, $EF_{5GS3GPPNSC}$ and $EF_{5GAUTHKEYS,}$ AUTHENTICATE command
15.1.2	Y	Read EF_{UST}, $EF_{5GS3GPPNSC}$ and $EF_{5GAUTHKEYS,}$ AUTHENTICATE command
15.1.3	Y	AUTHENTICATE command (Response AUTS)
15.1.4	N	
15.2.1	Y	Read EF_{UST}, $EF_{5GS3GPPNSC}$ and $EF_{5GAUTHKEYS,}$ AUTHENTICATE command
15.2.2	Y	Read $EF_{UST,}$ AUTHENTICATE command
15.2.3	Y	AUTHENTICATE command (Response AUTS)
15.2.4	N	