Test methods for devices with NSR SIMs (eSIM / iSIM / eSSP / iSSP)

C6-210346

Nov 2021

Confidential and Proprietary – Qualcomm Technologies, Inc.

Restricted Distribution: Not to be distributed to anyone who is not an employee of either Qualcomm or its subsidiaries without the express approval of Qualcomm's Configuration Management.

Not to be used, copied, reproduced, or modified in whole or in part, nor its contents revealed in any manner to others without the express written permission of Qualcomm Technologies, Inc.

Qualcomm reserves the right to make changes to the product(s) or information contained herein without notice. No liability is assumed for any damages arising directly or indirectly by their use or application. The information provided in this document is provided on an "as is" basis.

This document contains confidential and proprietary information and must be shredded when discarded.

Qualcomm is a trademark of QUALCOMM Incorporated, registered in the United States and other countries. All QUALCOMM Incorporated trademarks are used with permission. Other product and brand names may be trademarks or registered trademarks of their respective owners.

This technical data may be subject to U.S. and international export, re-export, or transfer ("export") laws. Diversion contrary to U.S. and international law is strictly prohibited.

Qualcomm Technologies, Inc.
5775 Morehouse Drive
San Diego, CA 92121
U.S.A.

© 2016 Qualcomm Technologies, Inc.
All rights reserved.

Content

- Background
- Test Methods
- Requirements for Test Methods
- Verification of ME-iSIM interface
- What is not acceptable?
- Test Method Applicability table
- Comparison of Test methods
- Key advantages of the Test Event based solution
- Objections and answers for the Test Event based solution
- Summary

Background

- 3GPP 31.121 and 31.124 Test suites available today support only the removable SIM form factor and a SIM Simulator is used.
- Black Box test systems can be used for devices with NSR SIMs (eSIM/iSIM and eSSP/iSSP).
- There are 3 approaches for Black Box testing.
  - Implicit verification with test case modifications
  - Test Toolkit Events based verification with no or minimum test case modifications.
  - Seamless eUICC / iSIM testing using APDU verification through Baseband logging

Test Methods

Test Method	Test method details
Implicit APDU verification with test case modifications	- APDU Communication in SIM-ME interface is not verified - Test System updates certain EFs run time and verify functionality from the NW simulator. - Modification to the Test specification is high. - All the UICC Conformance requirements can't be verified. - Test toolkit Applet is required for STK Test Cases.
Test Toolkit Events based verification	- Test toolkit Applet registers for two new Test Events and verify APDUs at NSR SIM itself. - The same Test toolkit Applet used for STK Testing can verify all the APDU requirements. - Can be used for all the NSR SIM variants including iSIM/iSSP. - No change is required for the current 31.121 Test specifications. A minimum change is required for 31.124 (SETUP EVENT LIST and it is done already). - See backup slides for complete details
Seamless eUICC / iSIM testing using APDU verification through Baseband logging	- APDU Communication in SIM-ME interface is verified through Baseband logging - No standardized logging interface is available. - Test verdict depends on BB logging data and not on the true content of APDU commands/responses in the SIM-ME interface - Loss of log packets can lead to test failures even device meets the spec requirements. - Some OEMs are mandating certain logging data to be masked due to security reasons. - Does not verify complete SW path between Baseband and SIM for iSIM/iSSP. - Test toolkit Applet is required for STK Test Cases.

Requirements for Test Methods

- All test methods shall support the requirements below.
  1. A Test profile is installed or UICC Test configuration is programmed in NSR SIM
  2. A Test Toolkit Applet is installed if Toolkit testing is required
  3. A means to verify content and format of APDU communication in the SIM-ME interface
  4. An interface for sending commands to the NSR SIMs
  5. Extending APDU monitoring capability to the Test System for debugging purposes.

- All the above shall be supported in any Black Box solutions for devices with NSR SIMs.
- Standard procedures (AT commands, RFM, etc) shall be used for sending commands to the NSR SIM.
- If eSIM RSP procedures are supported TS.48 Test profile can be used. If not, a similar UICC Test configuration shall be programmed.
  - For device conformance tests, known Test Authentication Keys and IMSIs shall be used in NSR SIM and in the NW simulators to meet Test initial conditions.
- Each Test method uses a different approach to verify the content and format of APDUs. Depending on the NSR type being used and the level of verification needed carriers/OEMs can choose the test method.

Verification of ME-iSIM interface

- Unlike with eSIM or removable SIM solutions, integrated SIM solutions (iSIM / iSSP) includes additional Software layers and processors between the Baseband and iSIM / iSSP.
- Card specific conformance tests verify only the SW implementation at the iSIM end and it does not verify the ME-iSIM interface.
- If APDU contents and communication is verified at the device end only there will not be any test solution to verify SW implementation in the ME-iSIM interface.
- In that case devices will get commercialized without testing the complete ME-iSIM interface.
- 3GPP 31.121 and 3GPP 31.124 are the only test specifications that can verify the complete ME-iSIM or ME-iSSP interface.
- Hence it is important to choose a test solution that provides test capability to verify the complete ME-iSIM/iSSP interface.
- Test Toolkit Event based solution is the only Test method that fulfills this requirement.

What is not acceptable?

	What is not acceptable?	Why?
1	Baseband logging for APDU verification	• Test verdict depends on BB logging data and not on the true content of APDU commands/responses in the SIM-ME interface • No standardized logging interface is available. • Loss of log packets can lead to test failures even device meets the spec requirements. • Some OEMs and Carriers are mandating certain logging data to be masked due to security reasons.
2	Test verdicts depend on tools within the DUT	• Test verdict shall not be determined based on data provided from the tools (eg: Logging tools) within DUT. • Test system shall use its own applications (eg: Test Applets) to determine test verdicts. • Otherwise DUT vendors can update/manipulate their own tool to meet the test case requirements. • Without an entity owned by the test system loaded onto the NSR SIM, verification of the interface between Terminal and NSR SIM can't be trusted.
3	A test solution without supporting all NSR SIM variants	• Test solution shall include support for devices with iSIM and iSSP. • APDU verification at the SIM end is an important requirement for the iSIM/iSSP solutions since multiple SW layers and processors are involved in the interface between the device and iSIM/iSSP. • A Baseband logging based solution does not verify the complete APDU communication between the device and iSIM/iSSP. • 31.121 and 31.124 are the only test specifications that can provide complete ME-iSIM/iSSP interface verification and test solutions should include such test capability.
4	Test specification changes to include Test EF data required for STK test cases	• Number of Test EFs required and the content/format of data in those EFs depends on the Test Applet implementation. • As long as Test Applet can send command or response data as specified in the Test specification it should be sufficient. • Test Applet and Test EFs shall be implementation-specific.
5	Having Test Methodology open for implementation	• Availability of unacceptable test solutions. • All available and acceptable test solutions shall be standardized, and it is up to Carriers, OEMs, and Chipset vendors to choose the test solution depending on the type of NSR SIM being used in the device and the level of verification needed. • Test Environment/Method Applicability shall be defined in the new specification (see next slide for more details)

Test Method Applicability table

- Some of the Test Devices/Samples with eSIM have a physical adaptor to connect a SIM Simulator for Electrical verification of the eSIM-ME interface.
- Such Test Devices with eSIM can use the same interface adaptor for UICC Protocol testing as well.

- Test Environment/Method Applicability shall be defined in the test specification.
- All the test solutions accepted shall be included.
- It is up to Carriers, OEMs, and Chipset vendors to choose the test solution depending on the type of NSR SIM being used in the device and the level of verification needed.

NSR Type	Test requirement for the DUT	Examples of Test Packages or device types	Applicable Test Method		
			Test Event based verification	Implicit verification	SIM Simulator based verification using a physical adaptor (for some Test samples only)
eSIM/eSSP	UICC tests for a Consumer Device with eSIM/eSSP	3GPP 31.121 and 31.124	✓	✓	✓
	UICC Electrical testing for a Test sample with eSIM/eSSP	ETSI 102 230 for eSIM	NA	NA	✓
	UICC tests for a Device with eSIM without Toolkit capability	IoT devices (3GPP 31.121)	NA	✓	✓
iSIM/iSSP	UICC tests for a Consumer Device with iSIM/iSSP	3GPP 31.121 and 31.124	✓	✓	NA
	UICC tests for a Device with iSIM without Toolkit capability	IoT devices (3GPP 31.121)	NA	✓	NA
Any	Non-UICC tests for a Device with any NSR SIM	RAN5 test suites (eg: 3GPP 38.521)	NR	✓	NR
Legacy SIM is embedded (no eSIM capabilities)	UICC tests for a Consumer Device with legacy SIM / UICC embedded (Test UICC configuration should be programmed in the UICC within the DUT)	3GPP 31.121 and 31.124	✓	✓	✓
	UICC tests for a Device with iSIM without Toolkit capability (Test UICC configuration should be programmed in the UICC within the DUT)	IoT devices (3GPP 31.121)	NA	✓	✓

NA - Not Applicable

NR - Not Required

Comparison of Test methods

	Requirement description	Test Method		
		(3) Seamless eUICC/iSIM testing	(2) Implicit Verification	(1) Test Event based verification
1	APDU content verification	Using APDU logging from BB through ESIM command handler	None	Test Events with APDU content received at the e/iSIM
2	NW signaling verification	Check at NW end	Check at NW end	Check at NW end
3	SIM Toolkit command triggering	Test Applet	Test Applet	Test Applet
4	SIM Toolkit response and envelop verification	Using APDU logging from BB through ESIM command handler	Test Applet	Test Applet
5	TC verdict reliability	Not reliable (possible log packet drops)	Reliable but not sufficient	Reliable and sufficient
6	Is APDU logging the true representation of APDUs sent by the BB or received at NSR SIM?	May not be the True representation	Not Applicable	Not Applicable
7	Elementary File Update for TC initial conditions	ESIM Command Handler	Standard AT commands, RFM	Standard AT commands, RFM
8	TC modification in test spec	Needed	Needed	Not required.
9	Monitoring of APDU communication interface between Modem and iSIM	None (Need additional logging interface for iSIM/iSSP)	None	Test Events with APDU content received at the iSIM
10	APDU logging interface for debug issues	Using APDU logging from BB through ESIM command handler	Using APDU logging from BB	Using APDU logging from BB
11	Test Applet installation on commercial cards is protected (Data Encryption Key and Security Parameters (RC/CC/DS).	Protected	Protected	Protected
12	Test Events registration/trigger on Commercial cards with commercial Auth Keys, IMSIs and Algorithms.	Not applicable	Not applicable	Not possible
13	Different card OS is required for test samples?	Not required	Not required	Not required
14	Prove device is using iSIM/iSSP and not a different SW entity.	Not Possible	Not Possible	Possible
15	Logging standardization is required for TC verdicts	Required	Not Required	Not Required
16	GSMA TSG Recommended	Not discussed	Not recommended	Recommended

Key advantages of the Test Event based solution

- The only test method that can provide a solution for verifying the complete ME – NSR SIM interface necessary for both the device and the embedded SIM commercialization.
- Provides the same confidence on test results as what test solutions for removable SIMs gave the industry for decades.
- Verify real APDU communication in the interface rather than another representation of APDUs through DUT.
- Provides 100% assurance EF data is read from eSIM or iSIM and not from the device memory or from a different entity within the device.
- Scalable for future commands/features and technologies (eSSP/iSSP) in ME-SIM interface.
- Do not have impacts on the commercial environment, the same card OS with Test Toolkit Event support can be used in test and commercial environments.

Objections and answers for the Test Event based solution

	Objection	Answer
1	There are some issues related to using dedicated test UICCs	• Dedicated test UICC is not a requirement for Test Toolkit Events based solution. Since Test Events will work (event registration and event triggering) with Test IMSIs and Test Authentication Keys and Algorithms only such events will not be available in commercial or live environments.
2	You need to be able to load or activate an applet, which requires to have the necessary access rights. Isn't that a security issue?	• Loading a Test Applet is necessary for ANY test method if 31.124 testing is a requirement and it is not specific for Test Event based solutions. • All the conformance testing shall be executed with Test cards. Such test cards or profiles have known Data Encryption Key and other Security Parameters (RC/CC/DS) need for Applet installation. Such Test cards have even known IMSIs and Authentication Keys and Algorithms and there is no security issue when dealing with Test Cards or profiles.
3	If you follow the approach being discussed in GSMA of using a test profile, each and every UICC needs to support the eSIM functionality. At the end all this means additional efforts, more memory and thus more expensive chips.	• Having a test card or test profile is a fundamental requirement for device conformance. None of the GCF or PTCRB conformance tests use commercial cards or profiles. This is not a Test Event based solution specific requirement and it is required for all the proposals we have. This is a requirement even for non-UICC specific conformance testing. • Party responsible for the DUT shall make sure the required test UICC configuration is loaded in the eSIM or iSIM. If not, shall make sure necessary configuration is available for the test system to install a test UICC configuration. If GSMA eSIM functionality is not supported, it shall support a means to configure the UICC EFs, Authentication Algos, etc. That method shall be used to install or program the test UICC configuration onto the eSIM.
4	Every UICC needs to support the eSIM functionality??	• DUT owner shall make sure Test UICC configuration is programmed in the embedded Legacy SIM. Again, having a Test UICC configuration in any type of SIM / UICC (including removable SIM) is a fundamental requirement for GCF/PTCRB testing.
5	Having doubts that this solution will be acceptable for low cost IoT equipment.	• IoT devices shall still use Test UICC configuration (eg: similar to GSMA TS.48) for any GCF conformance tests. If memory is limited to one profile only then the DUT shall be configured with Test UICC configuration only for device conformance testing. • If any eSIM does not support Toolkit (may be due to memory limitation) the option for such devices is to use 'Test Solution based on Implicit verification'. Test Environment Applicability Table shall include this and let the user decide what test solution is necessary for the DUT.
6	This solution doesn't solve all the problems. There are other tests not executable in case of non-removable UICC solution.	• Electrical TCs in ETSI TS 102 230 requires a test interface capable of making electrical measurements. Hence it will need a physical adaptor for devices with eSIM to connect the test system and some rework to the device is required. For such devices (rework is done already) can be used for other testing as well (for eSIM, not iSIM). Any test suite that exists today can be executed on such reworked devices with eSIM. • Electrical testing (ETSI 102 230) in the SIM-ME interface is not applicable for iSIM. But devices with iSIM have an additional requirement to verify the complete SW path between Baseband and iSIM. That is why the Test Events were proposed and it is targeting the TCs in 31.121 and 31.124 since it includes all end-to-end requirements for any Access Technology.
7	A new dedicated task force is being created to define a specific tool and guarantee the testability of the new platform. Do we need Test Event based solution?	• We may have to look at the test solutions for eSSP/ iSSP as well when deciding on test solutions for eSIM / iSIM. • For SSP, HCI/SPI level testing can be supported using the SCL Router as mentioned in the draft test specification. That discussion may be out of scope here. But there is a similarity when end-to-end testing for 31.121 and 31.124 specifications are considered. Test Events can be used for eSSP/iSSP as well without any new requirements. Taskforce shall consider all the requirements (Electrical, HCI/SPI protocol, end-to-end verification). Only the end-to-end verification (31.121 / 31.124) can be same for eSIM/iSIM and eSSP/iSSP.
8	Adding complexity in the USIM exclusively to test some features of the terminals, and not solving the general issue, is not acceptable.	• Only two Test Events are required and out of two test events requested one event has a lot of similarities with one of the already existing events. New technologies can't be supported without making changes. • One test solution is not used for all the test packages even today with removable SIMs. There are some deltas. The same will be the case for eSIM/iSIM and eSSP/iSSP testing. Test Events solution is focusing on end-to-end testing for 31.121 and 31.124 only. • It is necessary to define a Test Environment Applicability table with acceptable test methods for users to choose depending on the NSR type and level of testing required.

Summary

- Verdicts for TCs from a Test system shall not depend on supporting tools in the Device Under Test.
- It is important to include the complete SW path between the BB and the iSIM or iSSP when verifying the requirements for APDU content for the devices with integrated SIMs.
- End-to-end Test solution (31.121 and 31.124) for devices with NSR SIMs shall support all NSR SIM variants.
- The Test Event based method is the only test method that can provide a solution for verifying the complete ME – NSR SIM interface necessary for both the device and embedded SIM commercialization.
- It provides the same confidence on test results as what test solutions for removable SIMs gave the industry for decades.
- Multiple solutions will be required to support all the possible NSR SIMs and test requirements.
- Test Environment/Method Applicability for different acceptable test methods shall be defined in the test specification.

Back up slides

Why do we need Test Events?

- The new CT6 WI will mainly focus on implicit verification of test requirements by modifying the TCs in the new specification. However,
  - All the GCF/PTCRB test requirements will not be able to verify even if TCs are modified.
    - > Some of the GCF/PTCRB test requirements will be removed when implicit verification is not possible for certain requirements.
  - Correctness of ADPUs sent by the Terminal is essential for UICC testing but it will never be verified in the test solution with implicit verification.
  - Unable to assure if data is read from the device memory (from a copy of the files in eSIM) or from the eSIM
- MNOs may face field issues on GCF/PTCRB certified devices due to lack of original test requirements in the new specifications.
- Without an entity owned by the test system loaded onto the eSIM, verification of the interface between Terminal and eSIM can't be trusted.
- Above points will raise concerns on the test methods available for the devices with eSIM.
- The alternative test method with proposed Test Toolkit Events can verify all the GCF/PTCRB USIM requirements without removing any existing Conformance Requirements.

Test Events details

EVENT_TEST_EXTERNAL_FILE_READ

Toolkit Applet shall use registerTestEventFileRead() method to register for this EVENT and shall use deregisterTestEventFileRead() method to deregister this EVENT.

```
void registerTestEventFileRead (
        short fileEvent, byte[] baFileList, short sOffset1, short sLength1, byte[] baADFAid, short sOffset2, byte
        bLength2)
```

The CAT Runtime Environment shall trigger all the Toolkit applets registered to this event with the associated read file,

- Upon successful execution of a READ BINARY or READ RECORD APDU command sent by the Terminal to the UICC (External File Read) as defined in 102.221 and
- if the READ command is executed for a file in the registered File List and
- if the active profile is a Test Profile.

An applet shall only be triggered once per command.

When an applet is triggered by the EVENT_TEST_FILE_READ event, the system EnvelopeHandler shall be made available, and shall contain the following COMPREHENSION TLVs (the order of the TLVs given in the system EnvelopeHandler is not specified):

- Device Identity with source set to terminal and destination set to UICC for External File Read as defined in TS 102 223;
- File List, as defined in TS 102 223. The number of files shall be set to one. If a SFI referencing is used in the APDU Command, it shall be converted to its File Identifier;
- C-APDU object as defined in TS 102 223.

Byte(s)	Description	Length
1	C-APDU Tag	1
2	Length	1 or 2
T	C-APDU	T

EVENT_TEST_RX_APDU

Toolkit Applet shall use registerTestEventRxApdu() method with the command specified in the Instruction Code INS to register for this EVENT and shall use deregisterTestEventRxApdu() to deregister this EVENT.

```
void registerTestEventRxApdu (
        short event,
        byte[] baInsCode,        # INS, Instruction Code as defined in ETSI 102.221
        short sOffset1,
        short sLength1)
```

Upon successful execution of the command specified in INS (sent by the Terminal and received by the UICC) as defined in TS 102 221 and if the active profile is a Test Profile, the CAT Runtime Environment shall trigger all the Toolkit applets registered to this event.

An applet shall only be triggered once per command. This event shall be triggered for at least INS=78 (GET IDENTITY) and INS='88' (AUTHENTICATION) and it shall not be triggered for File Management commands (eg: INS='B0, D6, B2, DC, etc') and Toolkit commands (INS='C2, 14, 12').

When an applet is triggered by the EVENT_TEST_RX_APDU event, the system EnvelopeHandler shall be made available, and shall contain the following COMPREHENSION TLVs (the order of the TLVs given in the system EnvelopeHandler is not specified):

- Device Identity with source set to terminal and destination set to UICC, as defined in TS 102 223;
- C-APDU object as defined in TS 102 223.

Byte(s)	Description	Length
1	C-APDU Tag	1
2	Length	1
T	C-APDU	T

Security aspects of Test Events

- As per Qualcomm proposal in **SCPREQ(21)000002r2**,
  - Event registration for both events will be successful only if the active profile is a test profile. JCRE shall block event registration if the active profile is a commercial profile.
  - Event triggering for both events will be successful only if the active profile is a test profile. JCRE shall block event triggering if the active profile is a commercial profile.
  - Determination of Test Profile is associated with Authentication Keys, Authentication algorithm, and IMSI being used.
  - Test Applet installation on commercial cards is protected with Data Encryption Key and other Security Parameters (RC/CC/DS). This is already available in commercial networks.
  - Specifications do not define any response method for applets to trigger a response to an Event it received. Events are for monitoring purposes only.

Note: A 'Profile' is a combination of a file structure, data, and applications on an eSIM. It is referred to the same meaning as the profile referred to in the REFRESH mode 'eUICC Profile State Change' in section 6.4.7 of ETSI TS 102.223.

- A malicious applet must be installed and then change the Authentication Key (to have a Test Key), Authentication algorithm to Test algorithm or change the IMSI (to have a test IMSI) to receive any of the test specific events.
- Installation of a malicious applet and modifying the authentication parameters are well protected in commercial cards today.
- If those actions are protected and JCRE strictly follows the rules to expose the Test events, new events should not have any impact on commercial cards or commercial applications.

Current status of Test Events verification

- Proof of Concept for Test Events was completed recently using a removable eSIM with TS.48 profile loaded.
- Proprietary event numbers were used by the card OS for implementing the proposed events.
- Triggering of EVENT_TEST_EXTERNAL_FILE_READ upon receiving READ BINARY command for EF-UST file read from the terminal was verified successfully.
- Triggering of EVENT_TEST_RX_APDU event upon receiving GET IDENTITY command and AUTHENTICATE command from the terminal were tested successfully as well.
- OS Update procedure was used to update an existing card OS to support the new Test Events.

- **Results from Test Applet during SUCI Calculation by USIM at power up and AUTHENTICATION during 5G REGISTRATION:**

```
01 51 ---------------------------------------- Offsets of TCin and TCout
   00 4D ------------------------------------- Total length of data

      02 02 81 82 ------------------------- Destination identity
      12 07 01 3F 00 7F FF 6F 38  ----- File List (EF-UST)
      22 05 00 B0 00 00 11 ------------- C-APDU (READ BINARY '00 B0 00 00 11')

      02 02 81 82 ------------------------- Destination identity
      22 05 80 78 00 01 00 ------------- C-APDU (GET IDENTITY '80 78 00 01 00)

      02 02 81 82 ------------------------- Destination identity
      22 28 00 88 08 81 22------------- C-APDU (AUTHENTICATE '00 88 08 81 22 <data> Le')
                           10 D5 77 0C 6D 36 3E 30 C3 64 A4 07 8F 1B F8 ED 3A
                           10 6E 32 24 D6 BF 7B D5 55 D5 76 11 8E 49 2C E3 91
                           3D
```

- **Above data verifies the READ BINARY command for EF-UST, GET IDENTITY command and AUTHENTICATE command sent by the Terminal.**

APDU Monitoring through Base Band

- Test Systems shall have a method to monitor APDUs sent by the BB or received at the NSR SIMs.
- However, logging mechanisms can't guarantee all the APDU related logs are captured all the time (logging is always a 'best effort' only).
- APDU logging may not be the true representation of APDUs sent by the BB or received at NSR SIM. APDU data manipulation within the logging interface is possible.
- Verdicts for TCs from a Test system shall not depend on supporting tools in the Device Under Test and such tools can be used for some other purposes.
- Test systems can display all the APDUs captured through the device logging, and it will be helpful for debugging failures if any.
- Due to lack of reliability and trust in the logging mechanisms Test Case verdicts shall not depend on device logging.
- Conformance TCs may fail unfairly due to missing log packets even if a device meets the TC requirements. This will create unreliable test results from Test Systems.
- This will require the logging interface to be standardized. Otherwise, Test systems shall be customized for different devices.
- As explained in the slide 'APDU Logging at iSIM/iSSP end' additional logging is required for integrated solutions.

APDU logging at iSIM / iSSP end

- Unlike with eSIM or removable SIM solutions, integrated SIM solutions (iSIM / iSSP) includes additional Software layers and processors between the Baseband and iSIM / iSSP.
- APDU logging at BB/Modem level only excludes monitoring of a critical SW interface in integrated solutions.
- If the logging method is acceptable for APDU verification, the logging tool shall collect iSIM/iSSP OS level APDU logging for conformance testing with integrated solutions.
- This will also prove the device is using iSIM/iSSP and not a different SW entity and that proof is necessary for integrated solutions.
- Test systems need to support two different logging interfaces, one for BB and the other for iSIM/iSSP logging.
- However, logging from iSIM/iSSP may lead to impacts on APDU processing.

Interface for sending commands to the eSIM / iSIM

- GSMA TS.48 listed possible methods for modifying the Test Profile for each TC if required.
  - RFM
  - AT Commands
  - Test Applet
  - Proprietary approach such as using CCID
- Standard approaches can be used without defining a new interface (eg: ESIM Command Handler) to send commands to eSIM / iSIM.

Handling of Toolkit scenarios using Test Applet

- In any Test method, a Test Applet will be necessary for SIM Toolkit test scenarios.
- How the Test Applet triggering proactive commands or sending responses to Envelop commands shall be test system implementation-specific.
- It can be implemented using several EFs or using a max of 1 or 2 EFs. Depending on the Test Applet code written can decide on how many Test EFs are needed and what format shall be used in Test EFs.
- Such details shall not be included in Test Specification, and it shall be implementation-specific.
- Test system shall make sure Proactive command data and Envelop response data are aligned with the Conformance TC.
- TERMINAL RESPONSE and ENVELOP command content can be verified using the Test Applet itself using standard ProactiveResponseHandler and EnvelopHandler.
- Extra logging is not required to verify the STK APDU content and format.

Test Specification update to include Test EF data for STK TCs

- As described in the previous slide what Test EFs shall be used, and the format of Test EF data shall depend on the Test Applet code. It shall be implementation-specific.
- As long as Test Applet can send command or response data as specified in the current specification it should be sufficient.
- Additional update to include Test EF data within the TC in 31.121 or 31.124 is not required and it is an unnecessary overhead.

What is not acceptable? w/ Apple and Qualcomm Responses

	What is not acceptable?	Why?	Apple Response	Qualcomm Response
1	Baseband logging for APDU verification	• Test verdict depends on BB logging data and not on the true content of APDU commands/responses in the SIM-ME interface • No standardized logging interface is available. • Loss of log packets can lead to test failures even device meets the spec requirements. • Some OEMs and Carriers are mandating certain logging data to be masked due to security reasons.	No security risk is there, since this is similar to the legacy case (using removable UICC/Test Equipment) - except that the logging is now done on the DUT side. Logging interface is to be handled by DUT, so implementation specific - and OEM shall ensure that required 'minimal' data is guaranteed without loss for testing purpose if this method of testing is supported.	For a removable SIM case, a monitoring system must be connected. But in a device logging case if an application is loaded onto the device it can easily monitor sensitive data. The logging interface can still have bugs and TE vendors have to depend on OEMs for the reliability of the verdict. A failure can be due to not meeting TC requirements or a bug in the logging interface. Other key issues are, logging may not be having a true representation of the APDUs and not have standardized logging as mentioned under 1st two bullets.
2	Test verdicts depend on tools within the DUT	• Test verdict shall not be determined based on data provided from the tools (eg: Logging tools) within DUT. • Test system shall use its own applications (eg: Test Applets) to determine test verdicts. • Otherwise DUT vendors can update/manipulate their own tool to meet the test case requirements. • Without an entity owned by the test system loaded onto the NSR SIM, verification of the interface between Terminal and NSR SIM can't be trusted.	Existing PTCRB/GCF test's already utilize DUT, Modem based solutions (example MMI, AT command), and this has never been a concern for PTCRB/GCF. Monitoring C-APDU, or R-APDU rely on the direct interface to NSR UICC or relevant software component. Similar concern of manipulation shall apply to even test methodology currently proposed by Qualcomm., including Test Events based solution.	MMI and AT commands are standard interfaces. Even any solution we discuss can use such standard commands. The logging interface is not a standard interface. Test events are triggered from card OS and it is not dependent on the device. Test Applet is also owned by the test system. Device SW can't manipulate card OS or Applet behavior.
3	A test solution without supporting all NSR SIM variants	• Test solution shall include support for devices with iSIM and iSSP. • APDU verification at the SIM end is an important requirement for the iSIM/iSSP solutions since multiple SW layers and processors are involved in the interface between the device and iSIM/iSSP. • A Baseband logging based solution does not verify the complete APDU communication between the device and iSIM/iSSP. • 31.121 and 31.124 are the only test specifications that can provide complete ME-iSIM/iSSP interface verification and test solutions should include such test capability.	This method can be adopted for other NSR type devices as well, as the monitoring the APDU traffic can be done at the required interface (relevant software component as per implementation).	Yes, APDU monitoring from Baseband can be available in any solution. But due to the reasons mentioned the verdict based on BB logging is not sufficient for integrated NSR solutions. In fact, ADPU monitoring from the device shall be available in any test solution to allow a user to monitor it at BB level and perform debugging if needed.
4	Test specification changes to include Test EF data required for STK test cases	• Number of Test EFs required and the content/format of data in those EFs depends on the Test Applet implementation. • As long as Test Applet can send command or response data as specified in the Test specification it should be sufficient. • Test Applet and Test EFs shall be implementation-specific.	Agree, this can be implementation specific. However, a standardized approach in the definition of test EF can be helpful to ensure a well defined test specification.	As mentioned in the 2nd bullet, as long as the Test applet can trigger proactive commands or envelop response data as specified in the Test Specification it should be sufficient. Test Applet and Test EF structure to be used shall be implementation-specific. It is an unnecessary effort to update the whole spec with test EF data.
5	Having Test Methodology open for implementation	• Availability of unacceptable test solutions. • All available and acceptable test solutions shall be standardized, and it is up to Carriers, OEMs, and Chipset vendors to choose the test solution depending on the type of NSR SIM being used in the device and the level of verification needed. • Test Environment/Method Applicability shall be defined in the new specification (see next slide for more details)		

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.