GSMA RCS IOT Self-Accreditation Handbook.
joyn Crane Priority Release.
Document version 8.0
17 November 2016

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

Table of Contents

1 Introduction

1.1 Scope

This document provides practical guidelines on performing the self-accreditation process for joyn Crane Priority Release which is defined in the Annex B of the RCC.62 joyn Crane Product Definition Document version 3.0.

The process is described step-by-step with respect to different types of accreditation applicants, which are RCS client providers, Operators, Hosted Solution Providers, API-based Products Providers and Test tool Providers. Detailed procedures are provided for the test cases matrix tool usage and network traces processing.

The document includes overview of the general GSMA Self-Accreditation Framework and provides answers to the frequently asked questions (FAQs). In the section 6 ‘Knowledge Base’ of the current document you can find useful information on the ‘Interoperability and Testing’ (IOT) related documents availability and location plus contact information for additional question on the Accreditation process.

1.2 Definition of Terms

Term	Description
API	Application Programming Interface
AR	Accreditation Ready, an accreditation state awarded by the GSMA to a Hosted Solution Provider, which reflects that the applicable part of the accreditation process has been successfully undertaken
ARHS	Accreditation Ready Hosted Solution, an RCS Hosted Solution that has achieved Accreditation Ready status, which is hosted and managed by a Hosting Solution Provider who is not an Operator
CS	Circuit-Switched
FAQs	Frequently asked questions
HO	Hosted Operator (Recipient), an Operator using a RCS Hosted Solution to provide services directly to their end users/subscribers through their access network
HS	Hosted Solution, A RCS service offering based on infrastructure components, typically an IMS core and RCS service nodes, independent of any Operator access network
HSP	Hosted Solution Provider, a Company providing services of the RCS Hosted Solution to Operators
HTTPS	Hypertext Transfer Protocol Secure

IM	Instant Messaging
IMS	IP Multimedia Subsystem
IOT	Interoperability testing
IP	Internet Protocol
MNO	Mobile Network Operator
NDA	Non-Disclosure Agreement
NNI	Network-to-Network Interface
OEM	Original Equipment Manufacturer
OMA	Open Mobile Alliance
OS	Operating system
P-CSCF	Proxy Call Session Control Function
PS	Packet Switched domain
RCS	Rich Communications Services, the set of functionality documented in the RCS releases 1 to 6 and Rich Communications Services – enhanced (RCS-e) specifications
REST	Representational State Transfer
RTP	Real-Time Transport Protocol
SBC	Session Border Controller
SIP	Session Initiation Protocol
TC	Test Case
TLSoWi-Fi	Transport Layer Security over Wi-Fi
TTM	Time-to-market
UE	User Equipment
UI	User Interface
UNI	User-to-Network Interface

1.3 Document Cross-References

Ref	Document Number	Title
[1]	RCS IOT 001	joyn Crane Priority Release IOT Test Cases Matrix
[2]	RCC.62	RCC.62 joyn Crane Product Definition Document version 3.0
[3]	RCS IOT 004	Self-accreditation declaration form provided by network providers_jCPR
[4]	RCS IOT 005	Self-accreditation declaration form submitted by RCS client's providers_jCPR
[5]	jIG	joyn Implementation Guidelines
[6]	-	joyn Crane Priority Release Quality Check Test Matrix
[7]	RCS IOT 007	Self-accreditation declaration form provided by hosted solution provider_jCPR

[8]	-	joyn Crane Priority Release UX Test Case Matrix
[9]	RCS5.1	Rich Communication Suite 5.1 Advanced Communications Services and Clients specification Version 2.0
[10]	-	Self-accreditation declaration form provided by API-based Products Providers_jCPR
[11]	TS.11	TSG TS.11 Device Field and Lab Test Guidelines
[12]	GCF-CP - "Client Procedures"	GLOBAL CERTIFICATION FORUM Client Application Certification Procedures and Criteria as stated in any current and valid GCF-CP version
[13]	-	Self-accreditation declaration form submitted by test tool providers_jCPR

2 Self-accreditation process overview

2.1 Accreditation Framework summary

The accreditation process is part of the GSMA Network 2020 programme's IOT activities.

The GSMA determined that the best way to ensure standardised RCS compliant services on the market was to establish the accreditation process which is a part of the IOT process. To maximize the synergies between providers and vendors and in order to accelerate time-to-market (TTM) the accreditation process was designed as a self-accreditation process.

There are five types of applicants defined as follows:

- Operators (networks), companies providing RCS services to users.
- RCS client providers (clients), companies producing independent software for the end-user devices or embedded solutions from Original Equipment Manufacturer (OEM) supporting provisioning of the RCS services in the operator's network.

  NOTE: *The downloadable clients and PC/Tablet produced by Application developers are deemed to be of 'RCS client providers' type.*

- Hosted Solution Providers (hosted solutions), companies supplying complete RCS solutions to Operators;
- API-based Products Providers (APIs), companies delivering the following types of Products:
  - RCS Web thin client, a Web-based application emulating RCS client and uses OMA RESTful Network APIs to connect to the RCS Service Network and provide users with the RCS service;
  - RCS API Gateway (API GW), an interworking functional entity which is simulating RCS client on the UNI interface side towards RCS Service Network and supporting OMA RESTful APIs on interface towards web-clients;
  - RCS Network APIs sets, API Application server or API Gateway solutions which provide network interface towards Web thin clients and supporting OMA RESTful APIs. **Such products shall be only accredited by Operators or Hosted Solution Providers**;
  - RCS Web Solutions (gateway+client), a product which contains both an API Gateway and a Web thin client used inseparable one from each other and supporting proprietary APIs.

    NOTE: *Web Solutions supporting standard OMA RESTful APIs shall fall into categories API Gateways and Web thin clients and therefore provide two accreditation submissions.*

- Test Tool Providers, companies supplying solutions to Operators for automated RCS end-to-end testing by emulation of RCS clients.

All the documents related to the accreditation framework can be found on the GSMA website and Infocentre2. Please refer to the links in the section 6 'Knowledge Base' of the current document.

2.2 Accreditation process steps

From an applicant perspective the GSMA Accreditation process contains 7 main steps:

- **Step 1** – applicant visits http://www.gsma.com/network2020/accreditation-and-certification/
- **Step 2** – webpage provides instructions, contact details and all relevant documents
- **Step 3** – The applicant is given the contact and information so that they can proceed to start IOT testing with accredited networks and accredited clients as required
- **Step 4** – Once applicant has successfully completed testing as stated in the minimum accreditation requirements they must provide back to GSMA all required results, traces and signed self-accreditation declaration form [7, 8]
- **Step 5** – If there are any relevant updates, e.g. amendments to the guidelines or minimum requirements, it is communicated via the website and an email sent to the applicant

Company is added to the central GSMA database. Companies are not added to the website or any other public area/document until they have confirmed that accreditation requirements are satisfied.

As feedback the applicant will be provided with the following information:

- IOT central contact (rcsiot@gsma.com) and access to the secure IOT resources
- IOT accreditation process guidelines (this will also be available at http://www.gsma.com/network2020/accreditation-and-certification/
- Test cases and the latest version of the technical specification
- Quality check test set only applicable for clients
- User Experience (UX) self-assessment matrix only applicable for native not downloadable clients
- Information on the relevant accredited test harness:
  - Operator representatives' contact details
  - Network configuration details (provided by Operators directly)
  - joyn Implementation Guidelines [9] based on the network traces provided by all applicants

The contacts on the central database (kept by the GSMA) will receive an update notification by email in the following cases:

- There is a new version of the RCS Technical Specification or any other related GSMA RCS IOT document available on the website
- There is a change to the minimum accreditation requirements

For more details on the self-accreditation procedures for different types of applicants please refer to the section 3 of this document.

2.3 Test harness

As mentioned in clause 2.1 of the current document, the accreditation process is a self-accreditation one.

This self-accreditation process is driven by a tool which is known as the test harness. The test harness represents a tool defining both the IOT criteria (e.g. test cases, pass criteria, etc.) and allowing an efficient way of verifying interoperability and thus avoids running endless test cycles for each client implementation against all the other available implementations and, in doing so, drives convergence of RCS compliant networks and clients.

There are 4 main components of test harness defined by GSMA in the accreditation process:

- **Test cases**: A configurable matrix of end-to-end (E2E) test cases which generates the set of tests required to be passed dependent upon the Mobile Network Operator (MNO), terminal profile or test environment setup. Each test case has its own status which can be Mandatory, Recommended or Optional. Additionally and in order to improve quality of the product or service, the UX verification self-assessment matrix and operator Quality Check sets are included as per minimum accreditation requirements
- **Results**: The results of the actual tests run, as determined by various test matrixes mentioned above, shall be provided to GSMA. GSMA agrees not to publish applicant's traces on the GSMA website and leave them only for purpose of challenges to the Accreditation Framework. In the meantime GSMA is going to publish joyn Implementation Guidelines [9] which shall be based on these network traces and clarification notes provided by applicant, but these Guidelines will be anonymised.
- **Accredited client**: Clients that have undertaken and passed the accreditation tests are documented and have been formally declared by the RCS IOT Programme Office as accredited (either provisionally or fully as appropriate). They may be used along with other clients to drive client and network accreditation, and be a tool to identify areas requiring work to drive convergence.

  Accredited network: Networks that have undertaken and passed the accreditation tests are documented and have been formally declared by the RCS IOT Programme Office as accredited (either provisionally or fully as appropriate). They may be used along with other networks to drive client verification for the purpose of formal accreditation, obviating the need to perform a full IOT for each MNO.

The RCS client provider 'Provisional' accreditation can be obtained in one single network implementing only the mandatory functionality. However, if that network has limitations for the optional features of the RCS specification, the RCS client provider SHALL complete the remaining test cases through several networks but with the same hardware and software version of the client (or an improved version but the Vendor must ensure it works in the other networks).

Nevertheless, each operator and supplier must establish their own independent testing process and fund it. Each operator/supplier must conduct their own IOT tests as part of their standard product acceptance procedures in accordance with the approved test harness. No operator or supplier is expected to provide a test harness for a competitor (Operator A cannot certify Operator B's clients) except where mutually agreed for full accreditation purposes as stated in the section 3 of the current document.

2.4 Accreditation applicability for RCS client providers

Accreditation is awarded to the RCS Client detailed in the Self-Accreditation Declaration that is delivered to the GSMA RCS IOT Programme Office as a formal part of the accreditation submission. The RCS Client Provider shall declare for which version of the OS platform the functionality is supported (e.g. version 4.3 of Android) along with the version of the client and, for OEMs, the hardware platform details.

It shall be noted that accreditation is not automatically applicable to other implementations of the same Client Provider. For example, accreditation awarded to an implementation accredited on OS Android 4.3 would not be applicable to the implementation on OS Android

4.4, or accreditation awarded to the hardware model X would not be automatically applicable to the hardware model Y of the same Client Provider even if the same client stack is being used.

For OEMs in the particular case of devices and due to the diversity of form factors, an additional category of applicability also applies:

- Tablets: Devices running a tablet version of the OS or mobile OS
- Smartphones: Devices running a smartphone version of the OS
- Feature phones
- Basic phones

2.5 Industry obligations

2.5.1 RCS client providers

For the case where at least Provisional accreditation has been achieved and Accreditation of the respective joyn release is not transferred to the GCF, the RCS Client Provider shall submit to the GSMA accreditation process for any variation in RCS Client version, Operating System version or hardware platform to that stated in the Self-Accreditation Declaration provided with the accreditation submission. In case of a major OS update the Client Provider shall perform the regression testing which is the Quality check step as described in the minimum requirements for the corresponding accreditation type in order to achieve the same accreditation level for the modified implementation. The results from an acceptance testing on accredited Operator networks can be also used to confirm the quality of the updated implementation. In all cases, the Client Provider needs to submit to GSMA the Self-Accreditation Declaration describing the change.

NOTE: *Major OS update as defined in GCF documentation and procedures [12].*

In addition, GSMA may recommend GCF certification if a decline in quality is reported by an Operator as a result of a Quality Check conducted with an updated client.

2.5.2 Operators

Once initial accreditation has been achieved, the RCS operator SHALL agree to:

- Maintain the accreditation by making sure those future modifications due to software/hardware upgrades do not affect the outcome of the initial accreditation in case it is re-run again.
- Inform GSMA of any changes in the accredited network configuration details.
- Share the result of the test cases with the GSMA for the purpose of Accreditation Framework verification and development.
- Verify the completing minimum accreditation requirements by RCS compliant devices supplied to the network in accordance with the procedures provided in the clause 3 of the current document.

2.5.3 Hosted Solution Providers

Once initial accreditation has been achieved, the RCS Hosted Solution Provider shall agree to:

- Maintain the accreditation by making sure those future modifications due to software/hardware upgrades do not affect the outcome of the initial accreditation in case it is re-run again.
- Inform GSMA of any changes in the accredited Hosted Solution configuration details.
- Share the result of the test cases with the GSMA for the purpose of Accreditation Framework verification and development.

2.5.4 API Products Providers

Once initial accreditation has been achieved, the API Products Provider shall agree to:

- Maintain the accreditation by making sure that future modifications required to pass IOTs in different networks (after the initial accreditation) do not invalidate the initial accreditation.
- Maintain the accreditation by making sure those future modifications due to hardware/software upgrades do not affect the outcome of the initial accreditation in case it is re-run again. As an example, if an API Gateway provider gets the accreditation on Linux version 2.6.1.2, the provider is responsible to make sure a platform upgrade, for example to Linux 2.7.3.1, does not affect the RCS accreditation.
- Provide the results of the test cases to the GSMA for the purpose of Accreditation Framework verification and development.
- Provide the network traces (plain text) captured on a network element (preferably SBC/P-CSCF) or by a client trace capture application to the GSMA. These traces will not be shared publically, instead they are required to verify the test cases pass and anonymously to develop the GSMA interoperability and implementation guidelines.

2.5.5 Test Tool Providers

Once initial accreditation has been achieved, the Test Tool Provider shall agree to:

- Maintain the accreditation by making sure that future modifications required to pass IOTs in different networks (after the initial accreditation) do not invalidate the initial accreditation.
- Maintain the accreditation by making sure those future modifications due to hardware/software upgrades do not affect the outcome of the initial accreditation in case it is re-run again. As an example, if an test tool provider gets the accreditation on Linux, the provider is responsible to make sure a platform upgrade or change, for instance to Windows Sever, does not affect the RCS accreditation.
- Provide the results of the test cases to the GSMA for the purpose of Accreditation Framework verification and development.
- Provide the network traces (plain text) captured on a network element (preferably SBC/P-CSCF) or by a test tool trace capture application to the GSMA. These traces will not be shared publically, instead they are required to verify the test cases pass and anonymously to develop the GSMA interoperability and implementation guidelines.

2.6 Network and client convergence issues

Accredited clients shall be used in different networks (ideally with different setups and network equipment providers) to identify potential interoperability issues. Conflicts can be resolved in two ways:

- If the issue is caused because the clients did not take into account a valid configuration (according to the relevant 3GPP, RCS and endorsed specifications), the clients need to be updated to support it and at the same time, to fulfil the accreditation terms (not breaking compatibility with the previous networks where they have been accredited) provide traces to GSMA proving that this particular issue has been resolved.
- If the issue is due to a non-standard network configuration, the MNO/testbed provider shall liaise with the relevant vendors to correct this anomaly.
- Key issues shall be reported to the RCS IOT central contact (rcsiot@gsma.com) to keep track of the progress

Once one previously accredited client passes a new IOT (Mandatory test cases) in a different network, the published information shall be updated to reflect the new network setup where the test are passed.

Accredited clients shall be used to validate new RCS client implementations:

- Conflicts are resolved based in terms of compliance to 3GPP, RCS and endorsed specifications. By default, an accredited client is deemed to be correct and in case a new client raises an interoperability issue, the default action is that the problem shall be solved in the new client.
- In the unlikely case that the issue is caused by the accredited client (i.e. that test refers to an optional functionality that was not tested in previous IOTs), this accredited client needs to be updated and at the same time, to fulfil the accreditation terms (not breaking compatibility with the previous networks where they have been accredited) provide traces to GSMA proving that this particular issue has been resolved.
- If the issue is due to a non-standard network configuration, the MNO/testbed provider shall liaise with the relevant vendors to correct this anomaly.
- Key issues shall be reported to the RCS IOT central contact (rcsiot@gsma.com) to keep track of the progress

A client passing the IOT in an accredited network against an accredited client becomes accredited. Please note that this process can be both driven by a MNO or by a client/OEM vendor itself:

- When a vendor declares that he has passed the IOT, details on the employed network, test results (pass/no pass) and the traces of the test against an accredited client must be provided. Implementation Guidelines [9] based on network traces and anonymised will be published so all MNOs and vendors can access them
- The vendor is then endorsing the RCS accreditation (i.e. needs to maintain compatibility and perform the necessary changes to support new setups in future versions)

2.7 Roles and Responsibilities

The GSMA is responsible for:

- Keeping the Accreditation Framework webpage up to date with documents, notification of changes, and list of companies accredited.
- Keeping a central database of contacts
- Providing applicants with the relevant documentation, test cases and contacts

The Applicant is responsible for:

- Ensuring they keep up to date with any changes and keep their device/platform compliant.
- Providing a central point of contact to the GSMA and keeping this up to date
- Establishing their own independent testing process and funding it. Each operator/supplier must conduct their own IOT tests as part of their standard product acceptance procedures in accordance with the approved test harness.
- Providing all the required information as advised in this document

3 Accreditation Process guidelines for the applicants

3.1 Operator (Network) accreditation and assurance

3.1.1 Non-hosting configuration

3.1.1.1 Clarification

A network deploying its own solution (non-hosting) becomes ***provisionally*** **accredited** by passing 100% of the Mandatory accreditation tests [1] with at least two different ***fully*** Accredited Clients (Case 1, one against another). Traces are taken at the UNI. Caveat conditions considering different types of limitations (section 3 Step 9) apply. The accredited network can be either of the following: production environment or pre-production-environment.

NOTE*:* *For the initial RCS launch in a first country it is possible to use provisionally accredited clients*

Provisional network accreditation can be also achieved by testing against an accredited test tool listed on the GSMA website. In all cases traces shall be provided for verification to the GSMA.

Provisional accreditation shall be valid until the required facilities for full accreditation are available, **plus three [3] months**. Provisional accreditation is granted for a **maximum of 12 months**, thereafter it will lapse and re-accreditation will subsequently be required. In case of re-accreditation event occurs applicant will only need to provide signed self-accreditation form. Traces are only requested if there are any updates in the declaration forms and only for those updates (e.g. new service available).

A network becomes ***fully*** **accredited** by

(1) Undertaking the Accreditation Process and passing 100% of the Mandatory **accreditation tests** [1] with at least two different **fully** Accredited Clients (Case 1, one against another). Traces are taken at the UNI, and additionally

(2) Undertaking the Accreditation Process and passing 100% of the **interworking accreditation tests** [1] with one fully accredited client on accredited network [A] against one **fully** accredited client (**can be the same**) on the **fully** accredited network [B] (Cases 2, 3 or 4). Traces are taken at the NNI or the UNI.

NOTE*: For the initial RSC launch in a country it is possible to use provisionally accredited network [B].*

The accredited network [B] shall be provided by different Operator than for accredited network [A] and can be located in the same or another country. The accredited network [B] of the same Operator could be provided ONLY in case if there are no Operators planned to launch RCS in this country.

Networks which provide RCS services from a Hosted Solution Provider or hosting Operator (i.e. they are ‘recipient networks’) shall not be used as accredited networks for the purpose of accrediting other networks (i.e. as network [B]).

All the Cases mentioned above are presented on the following Figure 1.

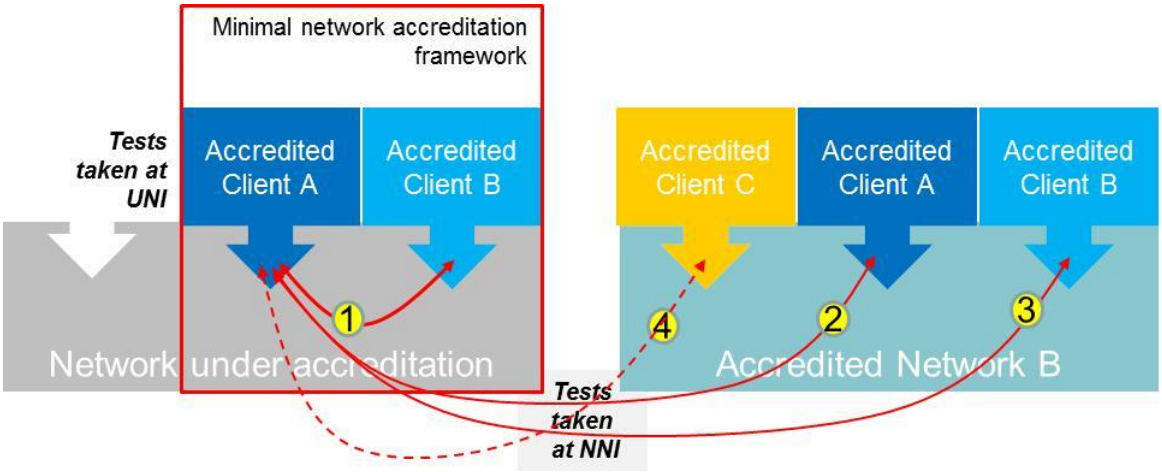

Figure 1. Test Cases for network accreditation

3.1.1.2 Procedure

The applicant of that type shall prepare for testing a candidate to the accredited network and at least two accredited clients or an accredited test tool (valid only for Provisional accreditation).

For the full accreditation applicant of that type shall test against another accredited network in order to perform testing on the NNI, using 'Interworking' list of test cases in the Test Cases Matrix tool [1].

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Use your candidate to accredited network configuration setup.

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the Step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 8 of the current document*

NOTE 3: *Please remember that you shall provide network traces for both accredited clients: one trace for each test case containing traffic from client 1 acting as originating party and traffic for client 2 acting as terminating party and ADDITIONALY provide one trace for each test case containing traffic from client 2 acting as originating party and traffic from client 1 acting as terminating party*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for both accredited clients

b. The excel files with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [3]

NOTE 4: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

3.1.2 Hosting configuration

3.1.2.1 Clarification

The Accreditation Framework allows Operators to be accredited with use of an 'Accreditation Ready' hosted solution from a vendor or an already accredited Hosting Operator. In both cases there is particular relief in the required procedures.

NOTE: *Use of non-hosted SBCs is not considered here*.

NOTE: Networks which provide RCS services from a Hosted Solution Provider or Hosting Operator (i.e. they are 'recipient networks') shall not be used as accredited networks for the purpose of accrediting other networks or clients.

To enable this hosted services facility and assure quality of the RCS networks the IOT Test Cases List [1] has been divided onto 3 following subsets.

- **Subset #1 – Access Operator Network related cases [1]:**
  - Mobile access, changing coverage during Capability Exchange
  - Configuration
- **Subset #2 – Tests applicable to the RCS Service Network [1]:**
  - Registration
  - User discovery
  - Capability exchange (except 3G coverage changes)
  - File transfer
  - RCS-e in-call services
  - IM/chat
  - Multidevice
  - End user confirmations
  - Social Presence
- **Subset #3 – Overall implementation [6]**
  - Quality Checks test set

As defined in section 2.2.3, Hosted Solution Providers are required to run only test subset #2 in order to get 'Accreditation Ready' status. Other subsets will be used depending on the hosting configuration as defined hereafter.

For all Hosting Configurations a formal Self-Accreditation Declaration form [3] shall be always provided by Operator seeking accreditation.

3.1.2.2 Procedures for Operators using 'Accreditation Ready' hosted solution

For the 1st Operator declaring use of an 'Accreditation Ready' hosted solution, Provisional Accreditation will be granted through successful execution of reduced test subset #1 [Access Operator Network related cases] [1] and subset #3 [Overall implementation] [3]. For all these test sets UNI traces shall be provided in accordance with procedure defined for Operators in section 2.2.1.1.2. Full Accreditation for the same Operator will be granted through use of pre-defined network interworking cases in accordance with standard procedures for Operators.

Subsequent Operators declaring use of an 'Accreditation Ready' hosted solution will achieve Provisional Accreditation through successful execution of test set #3 [Overall implementation] [3] without any traces, instead a formal declaration of successful execution is required. Full Accreditation for the subsequent Operator will be granted only through use of pre-defined network interworking cases as per standard procedures for Operators.

3.1.2.3 Procedures for Operators hosted by an accredited Operator

For the 1st Operator hosted by an already accredited Hosting Operator there will achieve the same level of accreditation as the Hosting Operator granted through testing using subset #3 [Overall implementation] [6]. Traces are not required.

Subsequent Operators hosted by an accredited Hosting Operator will achieve the same level of accreditation as Hosting Operator through test subset #3 [Overall implementation] [6] without any traces, instead formal declaration of successful execution is required.

3.2 RCS client provider (client) accreditation and assurance

3.2.1 Clarification

A client becomes ***provisionally*** **accredited** by undertaking the Accreditation Process and passing

A. 100% of the Mandatory accreditation tests [1] with a provisionally or fully Accredited Network [A] towards at least one Fully Accredited client (Case 1 or 2). Traces are taken at the UNI. Caveat conditions considering different types of limitations (section 3 Step 9) apply
B. verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and
C. pass 100% of the Quality Check testing [6] with an Operator's representative on an accredited network towards at least one Fully Accredited RCS Client.

   NOTE: *Downloadable client providers are not obligated to undertake UX testing (i.e. it is optional). If they choose to undertake testing, they are permitted to submit waivers and UX test cases remain mandatory for native implementations*

Networks which provide RCS services from a Hosted Solution Provider or Hosting Operator (i.e. they are 'recipient networks') shall not be used as accredited networks for the purpose of accrediting clients. An exception to this rule is made for Licensed Group Operating Companies who can guarantee that the UNI interface provided by a Network of Operation is identical to the UNI interface of the accredited Hosting Operator Network belonging to the same Group Company.

Please note that in order to get provisional accreditation and to achieve good quality of the RCS clients the sum of DESIGN LIMITATIONS and GO-TO-MARKET LIMITATIONS shall be not greater than 15%.

PENDING TESTBED LIMITATIONS & PRODUCTION ENVIRONMENT LIMITATIONS shall not hold back client provisional accreditation. However, Full accreditation shall be

dependent upon a formal statement from MNO received considering result of passing these test cases.

Provisional accreditation shall be valid until the required facilities for full accreditation are available, **plus three [3] months**. Provisional accreditation is granted for a **maximum of 12 months**, thereafter it will lapse and re-accreditation will subsequently be required. In case of re-accreditation event occurs applicant will only need to provide signed self-accreditation forms. Traces are only requested if there would be any updates in the declaration form and only for those updates (e.g. new service available).

A client becomes ***fully* accredited** by

A. Undertaking the Accreditation Process and passing
    A. 100% of the Mandatory **accreditation tests** [1] with a provisionally or fully Accredited Network towards at least one Fully Accredited client of this network (Case 1 or 2). Traces are taken at the UNI,
    B. verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and
    C. pass 100% of the Quality Check testing [6] with Operator's representative on an accredited network towards at least one Fully Accredited RCS Client, and additionally

       NOTE: *Downloadable client providers are not obligated to undertake UX testing (i.e. it is optional). If they choose to undertake testing, they are permitted to submit waivers and UX test cases remain mandatory for native implementations*

B. Undertaking the Accreditation Process and passing 100% of the **same accreditation tests** [1] with another provisionally or fully Accredited Network [B] towards the one **different** Accredited client than the client used in Accredited Network [A] (Case 3 or 4). Traces are taken at the UNI.

C. Pass 100% the **Quality check testing** [6] undertaken by Operator representatives in 2 rounds: first round on one provisionally or fully accredited network and second round on another provisionally or fully accredited network, each time against different Fully Accredited RCS Clients

NOTE: *If client can only be used in a single network [A] then it is allowed to perform testing against one different Fully Accredited client of another provisionally or fully Accredited Network [B] using the NNI (Case 5). Nevertheless traces shall be taken from UNI.*

All the Cases mentioned above are presented on the following Figure 2.

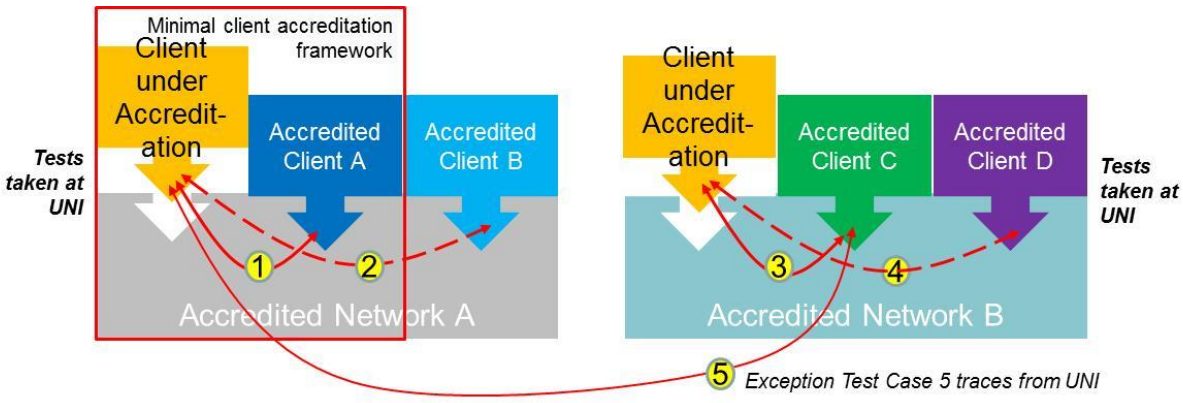

Figure 2. Test Cases for client accreditation

3.2.2 Procedure

The applicants of that type (client) shall test against an accredited network (pre-production or production environment) with one accredited client and use the simple steps provided below. If you are the first one to test, then you need to wait until another client provider or OEM is ready.

For the Accreditation Ready status the applicants of that type shall test in the environment provided by an Accreditation Ready Hosted Solution with one accredited client and use the simple steps provided below.

For the full accreditation applicant of that type shall test against another accredited network with one different accredited client on the UNI.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Take the accredited environment configuration setups which are available from particular MNO or the GSMA (please refer to the section 5 of the current document).

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 9 of the current document*

NOTE 3: *Please provide network traces for each test case containing traffic from candidate to accredited client acting as originating party and traffic for accredited client acting as terminating party.*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for candidate to the accredited client only

b. The excel file(s) with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [4]

NOTE 4: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

Step 5. In order to proceed with further UX verification [8] and Quality Check [6] steps applicant shall negotiate with GSMA and Operator representatives on dates for corresponding testing and consequently provide 4 devices or instances of the client for the express purpose of undertaking these activities, after which they shall be returned. Alternatively, the applicant may provide a representative with the devices or ready-installed clients to chaperone the devices/installed clients and support the activities in coordination with the GSMA Product team and Operator representatives.

Step 6. Pass through the UX validation process.

a. Download the latest UX Self-Assessment sheet [8] from the Accreditation page
b. Fulfill the matrix following the instructions provided inside the file.
c. Send the completed UX Self-Assessment sheet back and negotiate with GSMA Product team on dates and details of joint verification meeting via rcsiot@gsma.com.

Step 7. Pass through the Quality check process.

a. Operator's representative shall run all the test cases [6] without taking traces, except for failed cases
b. Indicate results of execution against each test case. The test case shall be marked as Passed only in case it was correctly performed without any crashes/software failures and functionality complaint to the RCS specifications, independently of repetition numbers.
c. Provide results back to *GSMA*

3.3 Hosted Solution Provider (hosted solutions) accreditation and assurance

3.3.1 Clarification

A Hosted Solution Provider achieves **'Accreditation Ready'** status by undertaking and passing 100% of the applicable Mandatory accreditation tests [1] with at least two different fully accredited clients with STANDARD profile.

'Accreditation Ready' status cab be also achieved by testing against an accredited test tool listed on the GSMA website. In all cases traces shall be provided for verification to the GSMA.

The 'Accreditation Ready' basic case above presumes that the RCS Hosted Solution provider has no connection with an RCS operator, there is no 3G/LTE access and there is no interconnect. Therefore the test configuration is simplified and User Equipment (UE, RCS client here) can be connected via (unencrypted) Wi-Fi. Nevertheless network traces shall be still provided unencrypted.

The case mentioned above is presented on the following Figure 3.

Connectivity aspect	Mechanism
to User Equipments	IP - WiFi
intra-operator network	n/a
inter operator network	n/a

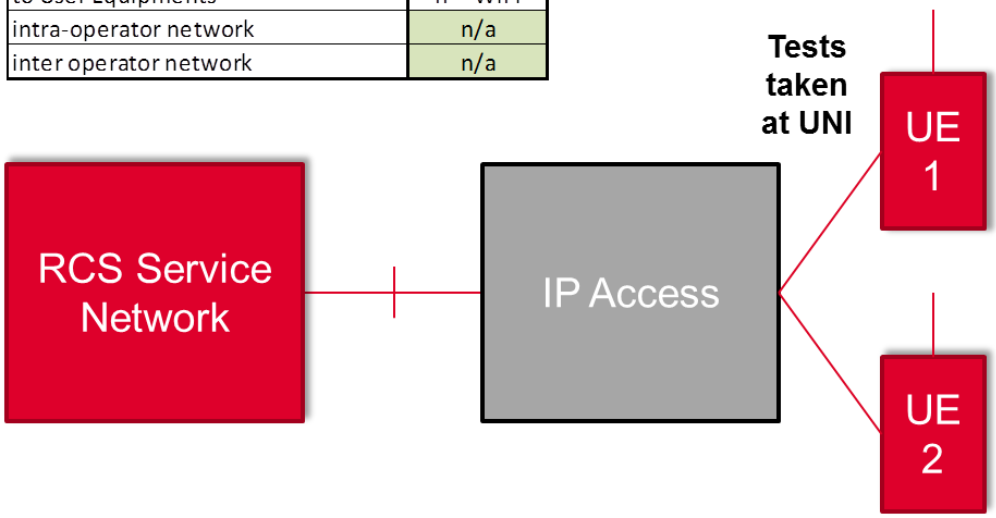

Figure 3. Basic Test Configuration for Hosted Solution accreditation

Alternatively '**Accreditation Ready'** status can be granted to the Applicant which complete RCS Hosted Solution has been used by accredited Operator during its accreditation (Standard case). In that case only a formal Declaration [7] from Hosted Solution Provider required though additionally countersigned by Operator representative.

The 'Accreditation Ready' standard case presumes that an RCS Hosted Solution Provider has connection with an RCS operator; there is 3G/LTE network connectivity, although there is no networks interconnect.

The case mentioned above is presented on the following Figure 4.

Connectivity aspect	Mechanism
to User Equipments	3G / 4G
intra-operator network	IP: LAN/WAN
inter operator network	n/a

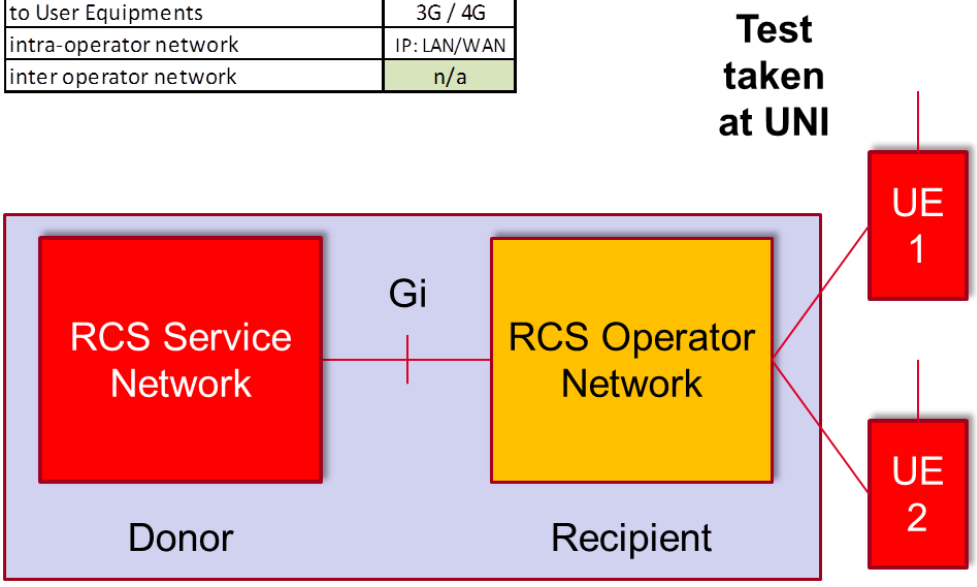

Figure 4. Standard Test Configuration for Hosted Solution accreditation

3.3.2 Procedure

In the basic case the applicant of that type shall prepare for testing an RCS Service Network based on Hosted Solution as per simplified diagram on the Figure 3 above and two fully

accredited clients with STANDARD profile. Clients shall be connected through unencrypted Wi-Fi access.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Use your network configuration setup.

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the Step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 8 of the current document*

NOTE 3: *Please remember that you shall provide network traces for both accredited clients: one trace for each test case containing traffic from client 1 acting as originating party and traffic for client 2 acting as terminating party and ADDITIONALY provide one trace for each test case containing traffic from client 2 acting as originating party and traffic from client 1 acting as terminating party*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for both accredited clients

b. The excel files with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [7]

3.4 API-based Products Providers (APIs) accreditation and assurance

The following four types of accreditations to joyn Crane Priority Release could be granted to API-based Products Providers:

- RCS Web thin client accreditation, targeting application vendors/OEMs to verify conformance to OMA RESTful API;
- RCS API Gateway accreditation, targeting RCS API gateway vendors to verify conformance to RCS UNI and OMA RESTful API;
- RCS Network APIs sets, targeting RCS Networks and Hosted Solution Providers to verify conformance to OMA RESTful API;
- RCS Web Solutions (gateway+client), targeting RCS API Gateway vendors who also produce RCS Web thin clients to verify conformance to RCS UNI. **Such solutions shall never be used inseparable one from each other, i.e. RCS Web thin client connected to another vendor's RCS API Gateway.**

Since at the very beginning there would be no reference web thin clients the following initial assumptions (ordered) apply to resolve the “what comes first” accreditation conflict:

- Provisional accreditation of the very first API Gateways is granted based on the RCS UNI accreditation (testing similar to secondary clients) and additional Declaration of Compliance to RESTful APIs [10];
- Provisional RCS Network APIs sets accreditation of the very first network is granted either by Declaration of accredited API Gateway use OR by a standalone Declaration of Compliance to RESTful APIs [10];
- Provisional accreditation of the very first Web thin clients is granted by testing against network with accredited APIs and one accredited main client on the UNI side;
- Once two different Web thin clients are accredited within the first Provisional accredited networks, networks and API Gateways could proceed with their Full accreditation;
- Provisionally accredited Web thin client is granted with Full accreditation by testing against another network with accredited APIs and another accredited main client on the UNI side;
- Web Solutions (gateway+client) are considered as ‘thick’ RCS clients and do not require APIs verification check therefore ordinary client accreditation approach is to be used with few modifications as specified in section 3.4.4 of the current document.

In the future development of the API accreditation framework there will be reference testing tool which would help to verify APIs both for Gateways and network’s Application Servers. This reference testing tool will replace requirement to provide Declaration of Compliance to APIs during Provisional accreditation of Gateways and RCS Network APIs sets.

All API-based Products categories defined above are considered as secondary clients implementations, which normally should not support CS voice calls. Due to the fact that joyn Crane Priority Release does not include RCS IP voice call feature the only applicable service profile for API-based Products is the BASIC one (IM/Chat, FTviaMSRP, FTviaHTTP). Partial support of BASIC profile services is not allowed for API-based Products.

Accreditation process and clarifications for each type of API-product are provided in the subsequent sections below.

3.4.1 API Gateway

3.4.1.1 Clarification

A RCS API Gateway becomes ***provisionally*** **accredited** by undertaking the Accreditation Process and:

A. 100% of the Mandatory accreditation tests [1] applicable to secondary clients with a provisionally or fully UNI (NNI) Accredited Network [A] towards at least one fully Accredited main client. Traces are taken at the UNI. Caveat conditions considering different types of limitations (section 3 Step 9) apply
B. two declarations: (a) Architectural declaration detailing compliance to OMA RCS architecture [10]; (b) Declaration of compliance to OMA RCS APIs [10]

To achieve **Accreditation Ready** status the RCS API Gateway must pass 100% of the Mandatory ‘RCS Service Network’ related accreditation tests [1] with an Accreditation Ready Hosted Solution towards at least one provisionally or fully accredited client AND provide two declarations: (a) Architectural declaration detailing compliance to OMA RCS architecture [10]; (b) Declaration of compliance to OMA RCS APIs [10]. Please note that RCS API Gateways with Accreditation Ready status cannot be used for accreditation of other networks, hosted solutions, API products or clients to any level or status.

An **Accreditation Ready** RCS API Gateway will be able to upgrade accreditation level to **Provisional** status by passing 100% of the Mandatory 'Access Operator Network' related accreditation tests [1] with a provisionally or fully accredited network[1] towards at least one provisionally or fully accredited client.

Please note that in order to get provisional accreditation and to achieve good quality of the RCS implementations the sum of DESIGN LIMITATIONS and GO-TO-MARKET LIMITATIONS shall be not greater than 15%. At the same time depending on the Self-Accreditation Declaration provided by the API Gateway Provider this limitation caveat may be changed upon review by the RCS IOT team.

PENDING TESTBED LIMITATIONS & PRODUCTION ENVIRONMENT LIMITATIONS shall not hold back client provisional accreditation. However, Full accreditation shall be dependent upon a formal statement from MNO received considering result of passing these test cases.

Provisional accreditation shall be valid until the required facilities for full accreditation are available, **plus three [3] months**. Provisional accreditation is granted for a **maximum of 12 months**, thereafter it will lapse and re-accreditation will subsequently be required. In case of re-accreditation event occurs applicant will only need to provide signed self-accreditation form. Traces are only requested if there are any updates in the declaration forms and only for those updates (e.g. new service available).

An API Gateway becomes ***fully* accredited** by

(1) Undertaking the Accreditation Process and:
   A. 100% of the Mandatory accreditation tests [1] applicable to secondary clients with a provisionally or fully UNI (NNI) Accredited Network [A] towards at least one fully Accredited main client (Case 1 or 2). Traces are taken at the UNI. Caveat conditions considering different types of limitations (section 3 Step 9) apply
   B. two declarations: (a) Architectural declaration detailing compliance to OMA RCS architecture [10]; (b) Declaration of compliance to OMA RCS APIs [10], ***and additionally***

(2) Undertaking the Accreditation Process and passing 100% of the same accreditation tests [1] applicable to secondary clients with another provisionally or fully API Accredited Network [B] towards the one different fully Accredited main client than the client used in Accredited Network [A] and against two different provisionally or fully accredited Web thin clients. Traces are taken at the UNI. Deep inspection criteria of [1] shall be ignored for Web thin clients.

Test configuration for Full accreditation mentioned above is presented on the following Figure 5.

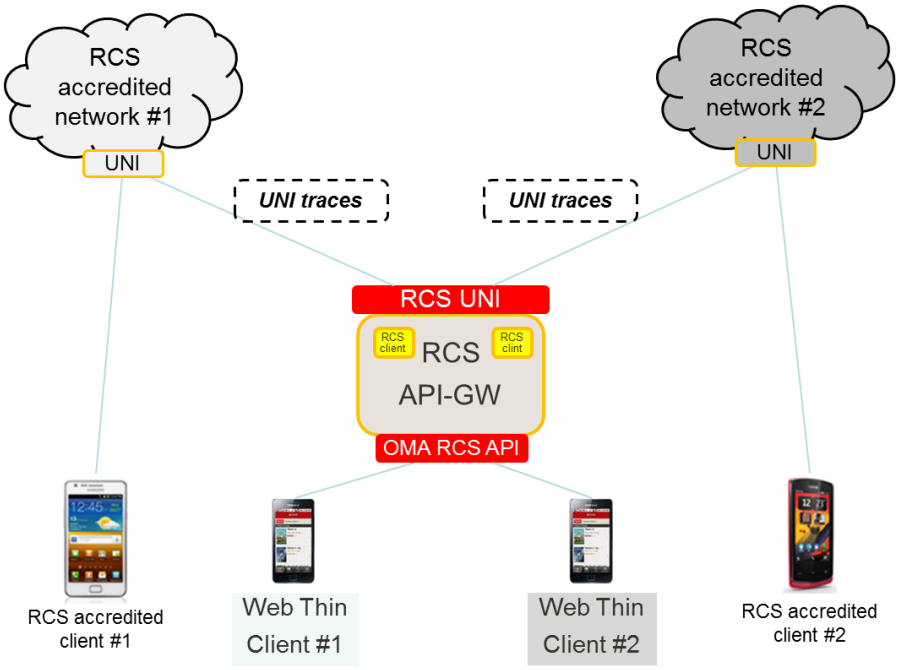

Figure 5. Test configuration for RCS API Gateway accreditation

3.4.1.2 Procedure

The applicants of that type (API Gateway) shall test against an UNI fully accredited network (pre-production or production environment) with one fully accredited main client and use the simple steps provided below.

For the Accreditation Ready status the applicants of that type shall test in the environment provided by an Accreditation Ready Hosted Solution with one accredited client and use the simple steps provided below.

For the full accreditation applicant of that type shall test against another UNI accredited network with one different fully accredited main client and two accredited Web thin clients. If you are the first one to test, then you need to wait until first two Web clients get accredited.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Take the UNI accredited environment configuration setups which are available from particular MNO or the GSMA (please refer to the section 5 of the current document).

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. For API-based implementations 'Secondary client' approach shall be used in Criteria sheet. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 9 of the current document*

NOTE 3: *Please provide network traces from UNI interface for each applicable test case containing traffic from candidate to accredited API Gateway acting as originating party and traffic from accredited main client acting as terminating party. Traces from clients are accepted.*

NOTE 4: *Deep inspection criteria of [1] shall be ignored for Web thin client*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for candidate to the accredited API Gateway as per note 3 above

b. The excel file(s) with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [10]

NOTE 5: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

3.4.2 RCS Network APIs sets

3.4.2.1 Clarification

RCS Network APIs sets of an Operator can be accredited only if its RCS Service Network (UNI and NNI) has been already granted with Full accreditation to joyn Crane Priority Release as a pre-requisite. The accredited network can be either of the following: production environment or pre-production-environment.

In case RCS Network APIs sets are deployed by Hosted Solution Provider then such Hosted Solution shall have 'Accreditation Ready' status to joyn Crane Priority Release in order to proceed with its RCS Network APIs sets accreditation.

RCS Network APIs sets deployed by the Operator become ***provisionally* accredited** by undertaking the Accreditation Process and:

A. by submitting two declarations: (a) Architectural declaration detailing compliance to OMA RCS architecture [10] to inherit accreditation in case using an accredited API-Gateway; (b) Declaration that accredited API Gateway is used by Operator and Gateway vendor

   OR

B. by submitting Declaration of compliance to OMA RCS APIs [10] in case not accredited API Gateway or own API Application Server is used.

Provisional accreditation shall be valid until the required facilities for full accreditation are available, **plus three [3] months**. Provisional accreditation is granted for a **maximum of 12 months**, thereafter it will lapse and re-accreditation will subsequently be required. In case of re-accreditation event occurs applicant will only need to provide signed self-accreditation form. Traces are only requested if there are any updates in the declaration forms and only for those updates (e.g. new service available).

RCS Network APIs sets deployed by the **Operator** become ***fully* accredited** by

(1) Undertaking the Accreditation Process and:

A. by submitting two declarations: (a) Architectural declaration detailing compliance to OMA RCS architecture [10] to inherit accreditation in case using an accredited API-Gateway; (b) Declaration that accredited API Gateway is used by Operator and Gateway vendor

OR

B. by submitting Declaration of compliance to OMA RCS APIs [10] in case not accredited API Gateway or own API Application Server is used, ***and additionally***

(2) Undertaking the Accreditation Process and passing 100% of the accreditation tests [1] applicable to secondary clients against two provisionally or fully accredited Web thin clients both testing against two different fully accredited main clients, with traces only from UNI-side.

RCS Network APIs sets deployed by the **Hosted Solution Provider** become **accredited** by

(1) Undertaking the Accreditation Process and by submitting Declaration of compliance to OMA RCS APIs [10] in case not accredited API Gateway or own API Application Server is used, and additionally

(2) Undertaking the Accreditation Process and passing 100% of the accreditation tests [1] applicable to secondary clients against two provisionally or fully accredited Web thin clients both testing against two different fully accredited main clients, with traces only from UNI-side.

NOTE: RCS Network APIs sets *exposed by Hosted Solution Providers cannot be used for Web Thin clients' accreditation purposes.*

Test configuration for Full accreditation of RCS Network APIs sets mentioned above is presented on the following Figure 6.

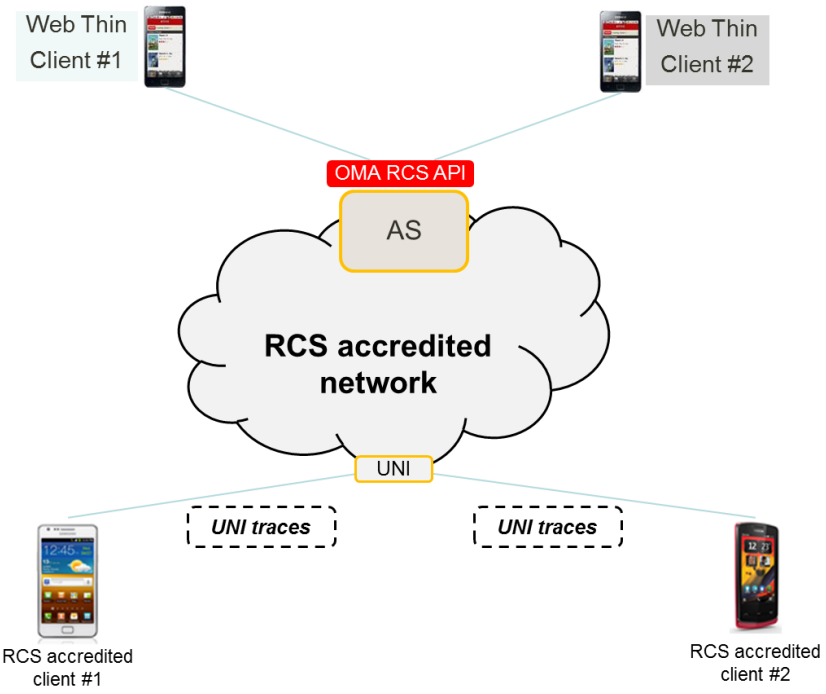

Figure 6. Test configuration for RCS Network APIs sets accreditation

3.4.2.2 Procedure

The applicant of that type (RCS Network APIs sets) shall ensure that its network is UNI fully accredited or granted with Accreditation Ready status in case of Hosted Solutions.

Provisional accreditation of Operator's RCS Network APIs sets can be granted based on declaration approach [10] described in section 2.2.4.2.1 above.

For the full accreditation Operator could either provide Declaration [10] in case Fully accredited API Gateway is used **OR** shall test against two accredited Web Thin clients and two fully accredited main clients.

Hosted Solutions Providers could accredit their RCS Network APIs sets only following Full API accreditation process meaning testing against two accredited Web Thin clients and two fully accredited main clients.

The applicant of that type shall prepare for testing a candidate to the accredited network, at least two fully accredited main clients and at least two accredited Web thin clients.

If you are the first one to test, then you need to wait until first two Web clients get accredited.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Use your candidate to accredited network configuration setup.

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. For API-based implementations 'Secondary client' approach shall be used in Criteria sheet. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the Step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 8 of the current document*

NOTE 3: *Please remember that you shall provide network traces for both accredited main clients: one trace for each test case containing traffic from Web thin client 1 acting as originating party and traffic for main client 2 acting as terminating party and ADDITIONALY provide one trace for each test case containing traffic from Web thin client 3 acting as originating party and traffic from main client 2 acting as terminating party*

NOTE 4: *Deep inspection criteria of [1] shall be ignored for Web thin client*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for both accredited main clients

b. The excel files with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [3]

NOTE 5: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

3.4.3 Web thin client

3.4.3.1 Clarification

A Web thin client becomes ***provisionally*** **accredited** by undertaking the Accreditation Process and passing

A. 100% of the Mandatory accreditation tests [1] applicable to secondary clients with a provisionally or fully API Accredited Network [A] towards at least one fully accredited main client. Traces are taken at the UNI. Deep inspection criteria of [1] shall be ignored for Web thin client. Caveat conditions considering different types of limitations (section 3 Step 9) apply
B. ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and
C. ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN 100% of the Quality Check testing [6] with an Operator's representative on an API accredited network towards the instances of the same client (back-to-back testing).

Network APIs exposed by Hosted Solution Providers cannot be used for Web Thin clients' accreditation purposes.

Please note that in order to get provisional accreditation and to achieve good quality of the RCS implementations the sum of DESIGN LIMITATIONS and GO-TO-MARKET LIMITATIONS shall be not greater than 15%. At the same time depending on the Self-Accreditation Declaration provided by the Web thin client Provider this limitation caveat may be changed upon review by the RCS IOT team.

PENDING TESTBED LIMITATIONS & PRODUCTION ENVIRONMENT LIMITATIONS shall not hold back client provisional accreditation. However, Full accreditation shall be dependent upon a formal statement from MNO received considering result of passing these test cases.

Provisional accreditation shall be valid until the required facilities for full accreditation are available, **plus three [3] months**. Provisional accreditation is granted for a **maximum of 12 months**, thereafter it will lapse and re-accreditation will subsequently be required. In case of re-accreditation event occurs applicant will only need to provide signed self-accreditation forms. Traces are only requested if there would be any updates in the declaration form and only for those updates (e.g. new service available).

A Web thin client becomes ***fully*** **accredited** by

(1) Undertaking the Accreditation Process and passing

A. 100% of the Mandatory accreditation tests [1] applicable to secondary clients with a provisionally or fully API Accredited Network [A] towards at least one fully accredited main client. Traces are taken at the UNI. Deep inspection criteria of [1] shall be ignored for Web thin client. Caveat conditions considering different types of limitations (section 3 Step 9) apply
B. ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and

C. ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN 100% of the Quality Check testing [6] with an Operator's representative on an API accredited network towards the instances of the same client (back-to-back testing) ***and additionally***

(2) Undertaking the Accreditation Process and passing 100% of the **same accreditation tests** [1] applicable to secondary clients with another provisionally or fully API Accredited Network [B] towards the one **different** fully Accredited main client than the client used in Accredited Network [A]. Traces are taken at the UNI. Deep inspection criteria of [1] shall be ignored for Web thin client.

Test configuration for Full accreditation of the Web thin client mentioned above is presented on the following Figure 7.

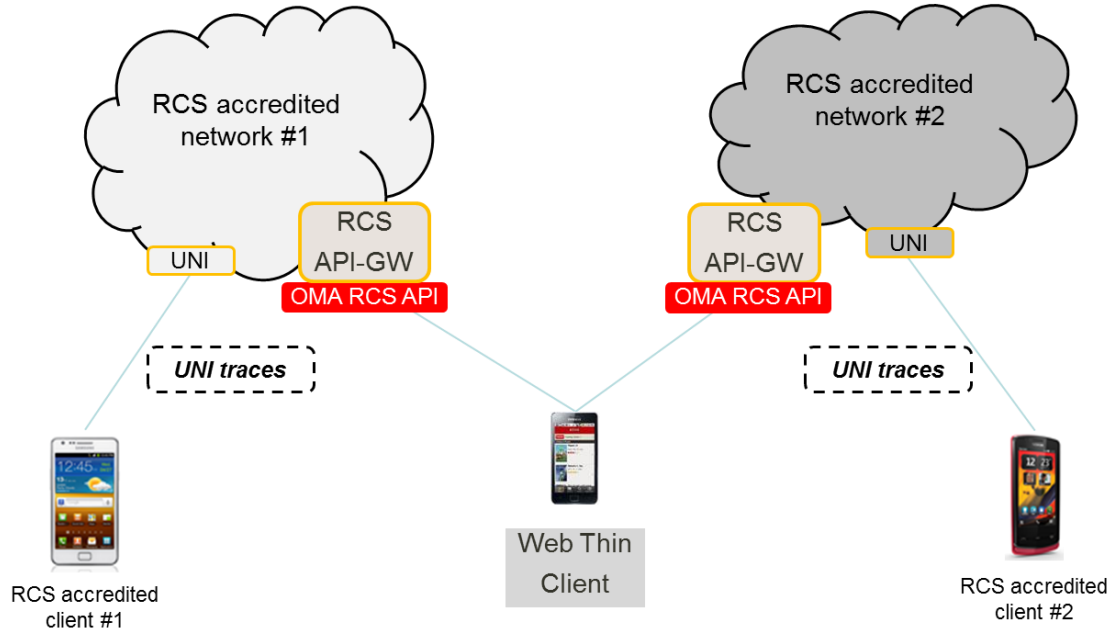

Figure 7. Test configuration for RCS Web thin client accreditation

3.4.3.2 Procedure

The applicants of that type (web thin client) shall test against an API accredited network (pre-production or production environment) with one fully accredited main client and use the simple steps provided below.

For the full accreditation applicant of that type shall test against another API accredited network with one different fully accredited main client on the UNI.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Take the API accredited network configuration setups which are available from particular MNO or the GSMA (please refer to the section 5 of the current document).

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. For API-based implementations 'Secondary client' approach shall be used in Criteria sheet. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 9 of the current document*

NOTE 3: *Please provide network traces from UNI interface for each applicable test case containing traffic from candidate to accredited Web thin client acting as originating party and traffic from accredited main client acting as terminating party. Traces from clients are accepted.*

NOTE 4: *Deep inspection criteria of [1] shall be ignored for Web thin client*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for candidate to the accredited Web thin client as per note 3 above

b. The excel file(s) with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [10]

NOTE 5: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

Step 5 (conditional). ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN in order to proceed with further UX verification [8] and Quality Check [6] steps applicant shall negotiate with GSMA and Operator representatives on dates for corresponding testing and consequently provide 4 instances of the Web thin client with devices if necessary for the express purpose of undertaking these activities, after which they shall be returned. Alternatively, the applicant may provide a representative with the devices or ready-installed clients to chaperone the devices/installed clients and support the activities in coordination with the GSMA Product team and Operator representatives.

Step 6 (conditional). ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN pass through the UX validation process.

a. Download the latest UX Self-Assessment sheet [8] from the Accreditation page

b. Fulfill the matrix following the instructions provided inside the file.

c. Send the completed UX Self-Assessment sheet back and negotiate with GSMA Product team on dates and details of joint verification meeting via rcsiot@gsma.com.

Step 7 (conditional). ONLY IF a Web thin client can be used on mobile devices (e.g. smartphone) THEN pass through the Quality check process.

a. Operator's representative shall run all the test cases [6] in the back-to-back configuration, i.e. Web thin client tested against the instances of itself on the same accredited network without taking traces, except for failed cases

b. Indicate results of execution against each test case. The test case shall be marked as Passed only in case it was correctly performed without any crashes/software failures and functionality complaint to the RCS specifications, independently of repetition numbers.

c. Provide results back to *rcsiot@gsma.com*

3.4.4 Web Solutions (gateway+client)

3.4.4.1 Clarification

A Web Solution (gateway+client) becomes ***provisionally*** **accredited** by undertaking the Accreditation Process and passing

A. 100% of the Mandatory accreditation tests [1] applicable to secondary clients with a provisionally or fully Accredited Network [A] towards at least one fully accredited main client. Traces are taken at the UNI. Caveat conditions considering different types of limitations (section 3 Step 9) apply

B. ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and

C. ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN 100% of the Quality Check testing [6] with an Operator's representative on an accredited network towards the instances of the same client (back-to-back testing).

To achieve **Accreditation Ready** status the Web Solution must pass 100% of the Mandatory 'RCS Service Network' related accreditation tests [1] with an Accreditation Ready Hosted Solution towards at least one provisionally or fully accredited client. Please note that Web Solutions with Accreditation Ready status cannot be used for accreditation of other networks, hosted solutions, API products or clients to any level or status.

An **Accreditation Ready** Web Solution will be able to upgrade accreditation level to **Provisional** status by:

A. passing 100% of the Mandatory 'Access Operator Network' related accreditation tests [1] with an accredited network[1] towards at least one accredited client,

B. ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and

C. ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN 100% of the Quality Check testing [6] with an Operator's representative on an accredited network towards the instances of the same client (back-to-back testing).

Please note that in order to get provisional accreditation and to achieve good quality of the RCS implementations the sum of DESIGN LIMITATIONS and GO-TO-MARKET LIMITATIONS shall be not greater than 15%. At the same time depending on the Self-Accreditation Declaration provided by the Web Solution (gateway+client) Provider this limitation caveat may be changed upon review by the RCS IOT team.

PENDING TESTBED LIMITATIONS & PRODUCTION ENVIRONMENT LIMITATIONS shall not hold back client provisional accreditation. However, Full accreditation shall be

dependent upon a formal statement from MNO received considering result of passing these test cases.

Provisional accreditation shall be valid until the required facilities for full accreditation are available, **plus three [3] months**. Provisional accreditation is granted for a **maximum of 12 months**, thereafter it will lapse and re-accreditation will subsequently be required. In case of re-accreditation event occurs applicant will only need to provide signed self-accreditation forms. Traces are only requested if there would be any updates in the declaration form and only for those updates (e.g. new service available).

A Web Solution (gateway+client) becomes ***fully* accredited** by

(1) Undertaking the Accreditation Process and passing

A. 100% of the Mandatory **accreditation tests** [1] applicable to secondary clients with a provisionally or fully Accredited Network towards at least one fully accredited main client. Traces are taken at the UNI. Caveat conditions considering different types of limitations (section 3 Step 9) apply,

B. ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN verification of all agreed applicable mandatory UX aspects [8] and with no launch blocking points to the satisfaction of the GSMA RCS Product team, and

C. ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN 100% of the Quality Check testing [6] with Operator's representative on an accredited network towards the instances of the same client (back-to-back testing)***, and additionally***

(2) Undertaking the Accreditation Process and passing 100% of the **same accreditation tests** [1] applicable to secondary clients with another provisionally or fully Accredited Network [B] towards the one **different** accredited main client than the client used in Accredited Network [A]. Traces are taken at the UNI.

Test configuration for Full accreditation of the Web Solution (gateway+client) mentioned above is presented on the following Figure 7.

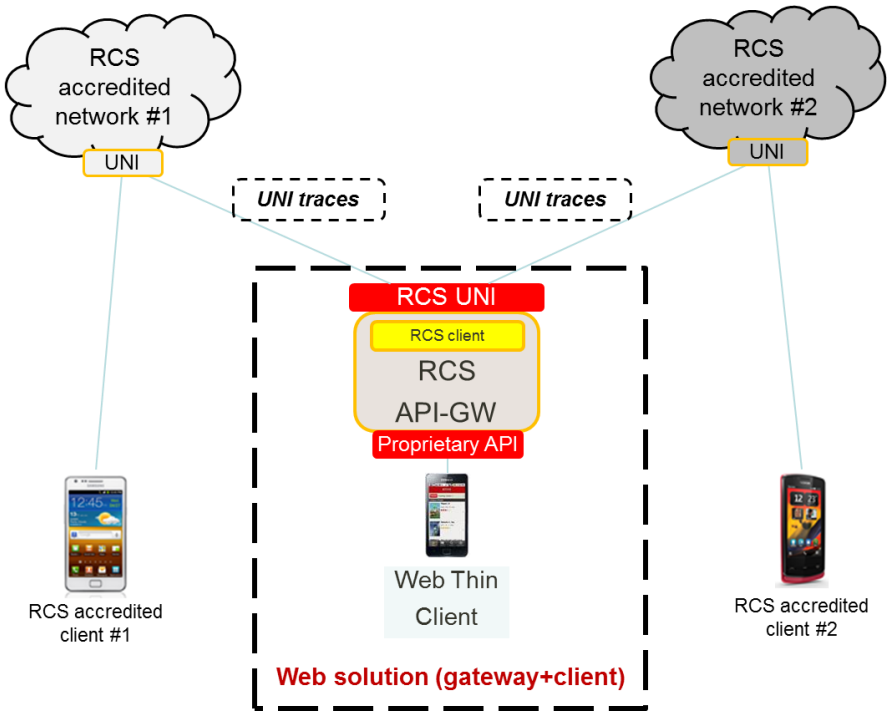

Figure 8. Test configuration for RCS Web Solution accreditation

3.4.4.2 Procedure

The applicants of that type (web solution) shall test against an accredited network (pre-production or production environment) with one fully accredited main client and use the simple steps provided below. If you are the first one to test, then you need to wait until another client provider or OEM is ready.

For the Accreditation Ready status the applicants of that type shall test in the environment provided by an Accreditation Ready Hosted Solution with one accredited client and use the simple steps provided below.

For the full accreditation applicant of that type shall test against another accredited network with one different fully accredited main client on the UNI.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 5 of the current document).

Step 2. Take the UNI accredited environment configuration setups which are available from particular MNO or the GSMA (please refer to the section 5 of the current document).

Step 3. Follow the instructions in the section 3 and section 4 of the current document in order to properly use the test cases matrix tool and network traces processing. For API-based implementations 'Secondary client' approach shall be used in Criteria sheet. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please follow the step 9 of the section 3.*

NOTE 2: *Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 Step 9 of the current document*

NOTE 3: *Please provide network traces for each test case containing traffic from candidate to accredited web solution acting as originating party and traffic for accredited main client acting as terminating party.*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces for candidate to the accredited Web Solution as per note 3 above

b. The excel file(s) with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [10]

NOTE 4: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

Step 5 (conditional). ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN in order to proceed with further UX verification [8] and Quality Check [6] steps applicant shall negotiate with GSMA and Operator representatives on dates for corresponding testing and consequently provide 4 instances of the Web thin client component with devices if necessary for the express purpose of undertaking these activities, after which they shall be returned. Alternatively, the applicant may provide a representative with the devices or ready-installed clients to chaperone the devices/installed clients and support the activities in coordination with the GSMA Product team and Operator representatives.

Step 6 (conditional). ONLY IF a Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN pass through the UX validation process.

a. Download the latest UX Self-Assessment sheet [8] from the Accreditation page
b. Fulfill the matrix following the instructions provided inside the file.
c. Send the completed UX Self-Assessment sheet back and negotiate with GSMA Product team on dates and details of joint verification meeting via rcsiot@gsma.com.

Step 7. ONLY IF Web thin client component of Web Solution can be used on mobile devices (e.g. smartphone) THEN pass through the Quality check process.

a. Operator's representative shall run all the test cases [6] in the back-to-back configuration, i.e. Web thin client tested against the instances of itself on the same accredited network without taking traces, except for failed cases
b. Indicate results of execution against each test case. The test case shall be marked as Passed only in case it was correctly performed without any crashes/software failures and functionality complaint to the RCS specifications, independently of repetition numbers.
c. Provide results back to *rcsiot@gsma.com*

3.5 Test Tool Provider accreditation and assurance

3.5.1 Clarification

A test tool becomes **accredited** by

A. Undertaking the Accreditation Process and passing 100% of the Mandatory accreditation tests [1] with a provisionally or fully Accredited Network towards clients emulated by a test tool. Traces are taken at the UNI,
B. Undertaking the Accreditation Process and passing 100% of the **same accreditation tests** [1] with another provisionally or fully Accredited Network [B] towards clients emulated by a test tool. Traces are taken at the UNI.

Test configuration for accreditation of the test tool mentioned above is presented on the following Figure 9.

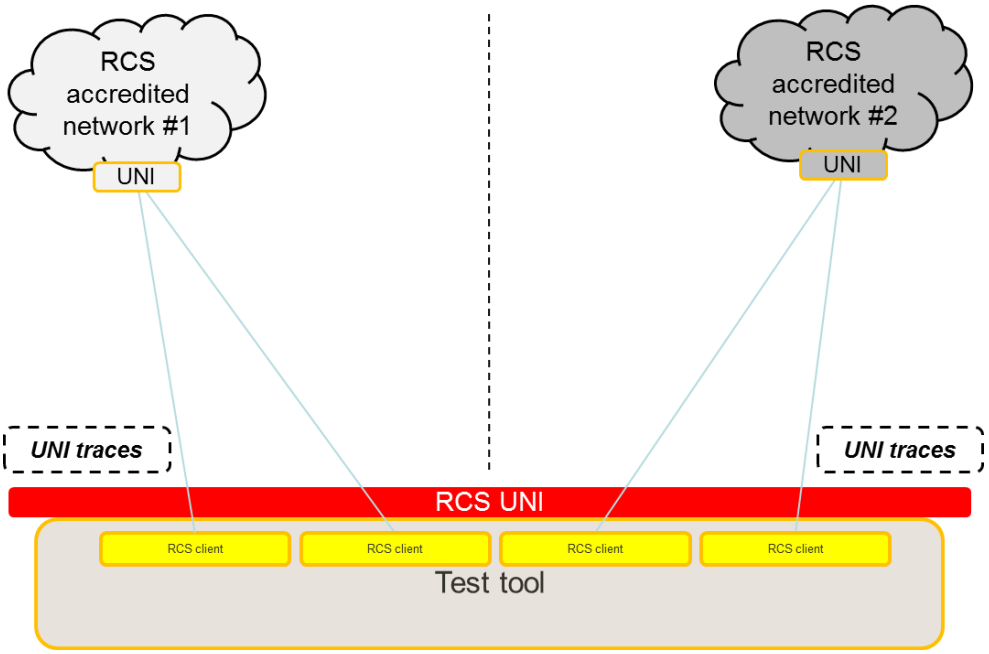

Figure 9. Test configuration for a test tool accreditation

Networks which provide RCS services from a Hosted Solution Provider or Hosting Operator (i.e. they are 'recipient networks') shall not be used as accredited networks for the purpose of accrediting test tools. An exception to this rule is made for Licensed Group Operating Companies who can guarantee that the UNI interface provided by a Network of Operation is identical to the UNI interface of the accredited Hosting Operator Network belonging to the same Group Company.

Please note that in order to get accreditation and to achieve good quality of the test tool the sum of DESIGN LIMITATIONS and GO-TO-MARKET LIMITATIONS shall be not greater than 20% indicated in the Statistics sheet of the IOT Test Cases Matrix tool [1].

3.5.2 Procedure

The applicants of that type (test tool provider) shall test against two different accredited networks (pre-production or production environment) and use the simple steps provided below.

Step 1. Take the latest test cases matrix tool which is available from the GSMA (please refer to the section 6 of the current document).

Step 2. Take the accredited environment configuration setups which are available from particular MNO or the GSMA (please refer to the section 4 of the current document).

Step 3. Follow the instructions in the section 4 and section 5 of the current document in order to properly use the test cases matrix tool and network traces processing. And report for each test case:

a. PASS

b. FAILED

c. LIMITATION:

NOTE 1: *Please configure test case matrix tool in the same way as for Client accreditation.*

NOTE 2: *Please provide network trace(s) for each test case containing traffic from originating and terminating clients.*

Step 4. Properly prepare and submit test results according to the instruction in the section 4.4 of the current document, including:

a. The network traces

b. The excel file(s) with the test cases matrix results [1]

c. The excel file with the self-accreditation declaration form [13]

NOTE 3: *If the accredited network resides in the Production environment additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

4 Test cases matrix tool usage guide

Please follow the simple steps below in order to properly use the Test case matrix tool:

4.1 Before use

Step 0. Before using this tool please answer the questions below:

Step 0a. To which type of applicant do you belong to?

Operator/Hosted Solution/Network APIs **OR** RCS-client/Test Tool/API-product (Thin client, Gateway, Web Solution)

Step 0b. Do you have accredited environment configuration details (*for clients only*)?

If NO, please contact GSMA (rcsiot@gsma.com) for further information or visit the GSMA Infocentre corner. Detailed information can be found in the section 6 of the current document.

Step 0c. Is that a Hosting Configuration (Operators and Hosting Solution Providers only)?

Yes (Hosting Solution Provider or hosted by an accredited Operator) **OR** No (Non-hosting configuration)

NOTE: For the Accreditation Ready status Client Providers and API-based Products Providers will be treated by the Test Matrix tool's macro as per **Hosting Configuration**

Step 0d. Which Hosting Configuration test subset do you need for accreditation?

RCS Service Network related cases (Subset #2 to be used by Hosting Solution Provider to get 'Accreditation Ready' status) **OR** Access Operator Network related cases (Subset #1 to be performed by Operator using Accreditation Ready solution in combination with subset #3 [3])

NOTE: For the Accreditation Ready status Client Providers and API-based Products Providers will need to test only RCS Service Network related cases and, once ready to go for Provisional accreditation, the remaining Access Operator Network set will have to be tested.

Step 0e. Which terminal profile do you use for accreditation?

Basic (not applicable for joyn Crane Priority Release) **OR** Standard (1-to-1 Chat, Group Chat, FTviaHTTP, Geolocation Push outside the call, Image Share, Video Share, Enriched Calling including Call Composer, Post Call and Audio Messaging, Share any file and Location Push during a call, Live Video, Shared Sketch, Shared Map).

Step 0f. Which RCS client type do you use for accreditation?

RCS client App (standalone downloadable software for devices, reduced list of test cases) **OR** Native/embedded client (Integrated OEM solution)

NOTE: *Please use Native setting in case you are accrediting a Test Tool*

Step 0g. Did you review the joyn Implementation Guidelines [5]?

If NO, we strongly recommend to do it before starting self-accreditation processes. This document provides the highlights of the issues discovered during IOT on the pre-production and production environments of the Operators and contains the guidelines for the RCS related protocols implementation in order to achieve seamless interoperability of RCS products.

Step 0h. Is that a secondary client?

Yes (PC/Tablet/API as described below) **OR** No (Native or App as described above)

Step 0i. Which Secondary client type do you use for accreditation?

Broadband Access (PC and Tablet clients) **OR** API-based implementation

4.2 Criteria and macro of the Technical Test Cases Matrix

Step 1. Save the Test cases Matrix tool on your PC/laptop

Step 2. Enable content (macro) in the document to provide proper functioning of the tool

Step 3. Switch to ‘Criteria’ sheet and set all the criteria based on your answers on step 0.

Step 4a. Run the macro (filter test cases)

Step 4b. Optionally run the macro (Interwoking_stats_count) for statistics table auto calculation in Interworking case, usually during network full accreditation process

IMPORTANT NOTE: *If you observe problems with macro calculation please check Options of the Workbook. Go to File->Options->Formulas->Calculation options-> Workbook Calculation and check whether 'Manual-Recalculate workbook before saving' option is checked. Otherwise please contact rcsiot@gsma.com.*

Step 5. As the result of macro work - in the ‘Result’ and ‘Interworking’ sheets you will find only those test cases which are applicable for the specific criteria.

Step 6. Switch to the ‘Result’ and/or ‘Interworking’ sheet(s). To see only the Mandatory test cases please apply the appropriate filter on the 'Status for networks' or Status for clients' columns depending on you applicant type.

Step 7. Carry on testing in a single network and/or interworking testing using test cases information presented in the 'Pre-condition', 'Description' and 'Expected results' columns of the 'Result' and/or 'Interworking' sheets. User A is expected to be always an implementation under test (IUT).

NOTE: *The capability exchange test cases (ID_RCS_4_3_1 - 4_4_1) for fully integrated and converged messaging format deviates from the general test case format due to the different type of inspection needed for UX-affected client behaviour.*

Step 8. Please pay your attention to 'IOT deep inspection required (traces)' columns of the 'Result' and/or 'Interworking' sheets. This parameter informs you for which test cases there is a need to collect traces. The following values are applicable:

YES - network traces required

NO - network traces NOT required

Step 9. Fulfil the ‘Result’ and/or ‘Interworking’ sheets with test cases execution statuses. Please choose the following values from the drop down list (brief definition provided below):

PASSED – *test case successfully passed in line with test case procedure*

FAILED – *test case was completed with the failure according to the test cases procedure*

NOT RUN – *test case was not run, this value is **NOT** applicable for the Mandatory test cases*

GO-TO-MARKET LIMITATIONS - test case was not run due to availability of the new features in the new spec and/or urgent go-to-market requirements

DESIGN LIMITATIONS - test case was not run due to UI, software or hardware limitation on the RCS client

PENDING - TESTBED LIMITATIONS – *test case was not run due to the part of the mandatory network functionality is not available on the test harness, statistics for these test cases would be automatically calculated based on the availability of servers as configured in the ‘Criteria’ sheet.*

PASS - MODIFIED TC - *test case successfully passed but with the modification to the test case procedure*

PRODUCTION ENVIRONMENT LIMITATION – *test case was not run due to the absence of physical possibility, this value is **ONLY** applicable for the error conditions test cases on the production environment*

4.3 Saving the results

Step 10. Press the Save button. It will lead to formula auto calculation in the 'Stats' and Stats inter' sheets.

NOTE: *You can change the criteria and run the macro again, but please note that at the end of the macro work it would delete all your previous results and save the file automatically.* ***So if you need to collect different statistics please RENAME the file before running the macro again.***

Step 11. Save the test cases matrix tool excel file with the unique name containing your company name and follow the instructions in the clause 4.4 of the current document.

5 Test results processing guide

5.1 Test results list

The list of test results contains the following items:

a. Completed and signed self-accreditation declaration form(s) [3, 4]

b. Completed Test Cases Matrix tool file(s) [1] with test results, network configuration in the 'Criteria' sheet and statistics

c. Network traces zip file(s) in the proper format

5.2 Test results processing

Please follow the simple steps below in order to process network traces:

5.2.1 Network traces collection

Step 1. Collect the traces from the accredited network (pre-production or production environment) in front of the SBC. Traces on the clients could be also used where it's not possible to take them from SBC or for complex test cases procedures, including NNI testing.

Not all of the test cases require collection of traces. Please always check the status in the column '**IOT deep inspection required (traces)**' (Yes/No/Option). For details please refer to the clause 3.2 of the current document.

Some test cases require support from the accredited network provider (i.e. Operator). In order to execute the maximum number of test cases it is recommended before starting the self-accreditation testing to directly approach any operator of an accredited network as you wish to determine whether each of them could provide you maximum support for testing.

Please note that all traces if possible shall NOT be encrypted by any means. In case there are no physical abilities to provide non-encrypted traces (e.g. HTTPS) please provide these encrypted traces and additionally if possible provide clarifications for issues discovered during these tests on the PS domain side. Furthermore these anonymised clarifications would be used in the joyn Implementation Guidelines' [5].

For the TLSoWi-Fi case please follow the rule: in some cases the encrypted end shall be the candidate to the accredited client and in others it shall be the reference accredited client. For instance for the test case 'A' candidate to the accredited client would be on Wi-Fi and the reference accredited client in PS domain and for the test case 'B' would be the opposite. This rule is only applicable to test cases that mention TLSoWi-Fi, in the rest of test cases, candidates to the accredited clients shall use PS domain (non-encrypted).

For the Group Chat test cases during the full network accreditation process using NNI alternate the initiator of the IM session in order to check interworking of IM servers of different networks.

NOTE: *If the accredited network resides in the Production environment, additional limitation becomes available, such as PRODUCTION LIMITATION. This value is **ONLY** applicable for the error conditions test cases on the Production environment.*

5.2.2 Network traces preparation

Step 2. Use the filters for traces preparation. As an example in Wireshark filters look like:

a) dns || sip || msrp || rtp - *for normal test cases*

b) dns || sip || http || https || xml - *for autoconfiguration test cases*

Step 3 (optional). Anonymise all the network traces or sign the additional multi-NDA between Applicant, GSMA and a third-party if it's strongly requested by this third-party which private information is presented in these network traces.

NOTE 1: *Traces will NOT be published by GSMA or disclosed by other means, so you DO NOT need to anonymise them and remember that relations between GSMA and Full Members, Associated Members and Rapporteur Members are supported by the NDA or Participation Agreement (for the Non-Members).*

NOTE 2: In any case if you intend to anonymise the traces, please consider the following sensitive data:

- Public IP addresses
- Port numbers
- SIP Message headers:
  - User Agent
  - IMS Server name
  - SIP authentication data (Proxy-Authenticate and Proxy-Authorization headers)
  - Via header contains public IP addresses and port numbers
  - Route header contains public IP addresses and port numbers
  - Record Route header contains public IP addresses and port numbers
  - Path header (in REGISTER SIP request)
  - P-Charging-Vector
- Time stamps
- Contact header field and transport parameters
- Test phone numbers

Step 4. Please prepare all the collected traces for submission to the GSMA in the **PCAP** format. The filename of the trace should contain the test case ID and a part for the originating party during the test case (e.g. OriginatingClient_ID_RCSE_6_1_1.pcap).

5.2.3 Test results submission

Step 5. Zip the files with test results (you can use password to achieve enhanced confidentiality).

Step 6. GSMA offers Dropbox services to all Applicants for test results and traces upload. Please send the signed declaration form to *GSMA* and in return you will get the details of the private Dropbox folder where to upload all your files.

5.2.4 Test results analysis

Step 7. Following revision of the test results and declaration form (*shall be not more than 1 week after submission*) you will be informed of the accreditation status and related information shall become available on the following GSMA webpage.

NOTE: *If you will not be able to meet all minimum requirements for the requested type of accreditation within 6 months after submission it would be automatically terminated and a complete new submission would be required.*

6 Knowledge Base

In order to find the interesting information considering IOT and accreditation process please refer to the table below (Table 1).

#	Document name	Location	Link
1.	Rich Communication Suite 5.1 Advanced Communications Services and Clients specification	GSMA Website	http://www.gsma.com/network2020/specs-and-product-docs/
2.	joyn Crane Priority Release IOT Test Cases Matrix	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
3.	Self-accreditation handbook_jCPR	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
4.	Self-accreditation declaration form provided by network providers_jCPR	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
5.	Self-accreditation declaration form submitted by RCS client providers_jCPR	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
6.	Self-accreditation declaration form provided by hosted solution provider_jCPR	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
7.	joyn Implementation Guidelines	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
8.	Accredited networks contact details	GSMA Website	https://infocentre2.gsma.com/gp/pr/V2020/N2020/RCSIOT/WorkingDocuments/Forms/AllItems.aspx?RootFolder=%2fgp%2fpr%2fV2020%2fN2020%2fRCSIOT%2fWorkingDocuments%2fAccreditation%20data&FolderCTID=0x0120008E48720242DA48419AB84D521EEF09D1
9.	List of current accreditations for clients and networks	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
10.	joyn Crane Priority Release UX Test Case Matrix	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/
11.	joyn Crane Priority Release Quality Check Test Matrix	GSMA Website	http://www.gsma.com/network2020/accreditation-and-certification/

Table 1. IOT and accreditation Knowledge Base

If you have any questions please refer to the FAQs clause of the current document or contact the following addresses (Table 2):

#	Name	Role	Contact
1.	Oscar Gallego (Vodafone Group)	RCS IOT Chair	Oscar.Gallego@vodafone.com
2.	Ian Crawford (GSMA)	IOT Consultant	ICrawford@gsma.com
3.	Konstantin Savin (GSMA)	RCS IOT Technical Consultant	ksavin@gsma.com
4.	Alex Martinez (GSMA)	RCS IOT Technical Consultant	amartinez@gsma.com
5.	Distribution list	Whole RCS IOT Group	rcsiot@lists.gsma.com
6.	Distribution list	RCS IOT MNOs	rcsiotmno@lists.gsma.com
7.	Distribution list	RCS IOT Working Team only	rcsiot@gsma.com

Table 2. RCS IOT contact table

Frequently asked questions (FAQs)

Q1. Where can I find the latest version of the RCS Test cases matrix tool?

You can always find the latest version of the Test Cases matrix tool on the GSMA website and in the General documents of the RCS IOT Group on the GSMA Infocentre. Please refer to the section 5 of the current document for further details.

Q2. Could a client be accredited on the pre-production environment?

The goal is to undertake and pass the accreditation tests for the client against the accredited production network. We recognise this is not always possible, nor indeed can all accreditation tests or tracing be undertaken. Therefore if MNO will accredit the pre-production environment, then a client can be accredited on the MNO pre-production environment.

Q3. Could we provide network traces taken from the client?

The proposed rule for traces collections is to collect the traces from the accredited network in front of the SBC. However, traces on the clients could be also provided where it's not possible to take them from SBC or for complex test cases procedures. It is also possible to take traces from the client while testing over NNI for network full accreditation.

Q4. Does GSMA break any Anti-Trust rules by publishing accredited networks configuration details?

No. Accredited network configuration details will be uploaded to the GSMA Infocentre sub-group which is restricted to OEMs only for the purposes of their self-accreditation process. MNOs in this case will have no possibilities to see other MNOs network details. Also please note that here accredited network configuration details means only availability of different servers, location and network type. Confidential information considering core network devices manufacturers or other sensitive data is NOT disclosed by GSMA.

Q5. Do I need to sign any additional NDAs before submitting the network traces to GSMA?

Please note that all traces will NOT be published by GSMA or disclosed by any other means. Nevertheless, relations between GSMA and Full Members, Associated Members, Rapporteur Members and non-members are supported by the NDA or Participation Agreement (for the Non-Members) which covers the confidentiality of information provided by parties. In the meantime a third-party (e.g. core network vendor) whose private information can be identified from the network traces could request you not to disclose this information. In order to avoid time spent for traces anonymization in this case GSMA provides an additional multi-NDA which would be signed by Applicant, GSMA and third-party. Please refer to the section 5 of the current document for further details.

Q6. How many declarations would we need to provide if our Company has 7 networks of operation?

The answer is 7. The Operators and Group Companies will have to complete IOT and self-accreditation for each network and country of operation although they will not be obligated

to produce the network traces each time. Where additional features are in the new operator network, then they will need to provide the network traces for only for the new feature(s).

Q7. Can we use for network accreditation an accredited client with Android OS v4 if it was previously accredited with Android OS v2?

Yes you can. In the Accreditation applicability section 2.4 it is defined that a vendor gets an accreditation for an OS platform and the vendor SHALL take the responsibility that the client is backward compatible with previous versions of the OS. Nevertheless remember that for instance getting the accreditation for Android 2.3 smartphone version does not mean that it is also applicable to Android 3.1 tablet version.

ANNEX A Lessons Learned in self-accreditation process

This annex contains descriptions of lessons learned so far in the self-accreditation process and is based on the submissions from RCS client providers and Operators.

A.1 Before starting self-accreditation process

- Accreditation testing may be performed on any accredited Operator network, either Production or pre-production
- Time may be required for investigation of possible issues
- Consequently it is important for the accrediting party to ensure support from the selected Operator in advance.
- Before starting testing it is recommended to approach different Operators from the list providing accredited networks and find the most appropriate resource for the particular timeframe.
- Accreditation testing can be performed either in Roaming or with local access to the network. Therefore it is recommended to verify remote connection to the network and in case of issue consider local testing in order to save time for fixing issues related to connectivity.
- It was observed that testing typically requires 10 days, though could last from 3 days up to 3 months
- SIMs from the selected operator are required for testing
  - In case of access to the Production networks they can be purchased in shops and there must be appropriate balance plus data traffic enabled.
  - For Pre-production networks access you would need again to purchase SIMs and contact Operator for provisioning those in network environment.
- According to the accreditation rules it is necessary to test against an accredited client. The easiest way is to find these in the Google Play and Pasture. In some particular cases the selected Operator may help to approach Vendor in order to assure availability of such a client

A.2 Use of the test cases matrix tool

The latest version of the RCS test cases matrix can be found on the following page of the GSMA website: RCS Specifications.

This test cases matrix is not only a list of test cases which you shall use for RCS implementation testing, it is also a tool which is driven by a powerful macro and facilitates the self-accreditation process according to latest ‘joyn’ accreditation policies.

There are currently 200 test cases in the matrix, although not all of them are necessary to be executed in order to get accredited. Some of them are even dependent on the accrediting network used, client type and RCS services available on your device. For instance, RCS downloadable clients need to pass only 100 Mandatory test cases in the typical network configuration to get provisionally accredited.

Improper use of Criteria in the test cases matrix tool in most cases will lead to an unacceptable number of test cases with status FAILED or DESIGN LIMITATION.

Please refer to clause 3 of this Handbook for instructions on correct test cases matrix tool usage.

NB:

- Please do NOT make any changes to formulas or other configuration parameters in the tool while submitting test results to GSMA for analysis
- Please do NOT make any filtering in the sheets of the tool before running the macro
- Please select presence of only those Network elements provided by the Accredited network

If you have any proposals to the test cases matrix tool updates, send them to rcsiot@gsma.com.

A.3 Test cases execution

A.3.1 RCS client testing against itself

In order to provisionally accredit an embedded RCS client it must be tested against an accredited RCS client. This accredited RCS client could be either a downloadable one or an embedded OEM solution. Use of the RCS downloadable client (software) obviously requires there shall be a device (hardware) available.

During analysis of network traces we have discovered that in case both candidate (embedded solution) and accredited (downloadable) RCS clients reside on the same device (hardware), at least in some results in the candidate client is testing against itself. From a protocol perspective it usually results in abnormal network behaviour and unsuccessful responses to requests.

Since it obviously would not lead to RCS industry interoperability, those traces will not be acceptable for accreditation and must be retested correctly.

In order to prevent such cases, please choose an accredited RCS client with different hardware platform. If this is not possible, use special mechanisms to distinguish downloadable and native RCS clients residing on the same device. Such mechanisms are outside the scope of this document.

A.3.2 Incorrect test case procedure

While analysing first test results submissions we have identified many traces in which the test case procedure was not correctly executed. Typical problems were as follows:

- wrong state of RCS client (offline/online)
- testing against the same client in back-to-back mode
- simulation of those cases which are NOT allowed to be simulated
- only one file sent within multiple transfers
- wrong behaviour of remote party – accepting of a session instead of rejection.

As a result those traces were requested to be redone which leads to additional unnecessary time and resources being expended.

In some traces there were obvious mistakes of testing engineers. In other cases some traces were executed incorrectly because of unclear test case descriptions. The latest version of the Test Cases Matrix tool has resolved many unclear areas. However, if you have any proposals to the test cases matrix tool update, please send them to rcsiot@gsma.com.

If while testing you are faced with an unclear test case description, provide a comment in the ‘OEM vendor test result prior to IOT’ column in front of the test case and execute this

test with modification to the procedure. Do not forget to set a status for this test as 'PASS – MODIFIED TC'.

A.4 Preparation of network traces

A.4.1 No messages in trace

During preparation of traces please spend the time to check whether there is any SIP inside or you will have to spend more time for retesting. The only exception could be cases with Wi-Fi coverage and private MSISDN.

We have also discovered that some traces do not have those significant messages requested by test cases procedure. So, please pay attention to trace capturing start and stop time, this should facilitate analysis of your submission by GSMA IOT team.

A.4.2 Fragmented packets

In most cases, especially when CPIM and XML bodies are used, SIP messages would exceed typical MTU limit of maximum 1500 bytes. This will obviously lead to fragmentation of packets. For RCS services implementations it could mean 40% of traces with fragmented messages.

The fragmentation itself though not a major problem is a challenge for the GSMA RCS IOT team during processing of traces since some of the messages could be removed from the trace while applying filters.

Please save unfiltered traces since they could be requested by GSMA in case of facing issue with fragmented messages.

A.4.3 TXT versus PCAP

In the first version of the Self-accreditation Handbook we requested all applicants to provide traces in TXT format. Our initial intention was to reduce the volume of zip archive with traces which should be sent by applicant to GSMA over Dropbox (see section 5.2.3).

After receiving first traces in TXT format we have realised that sometimes it is not so easy to import TXT file into sniffer (e.g. Wireshark) since we need to know original encapsulation type which could be Ethernet, Linux-cooked, IEEE 802.11 or any other.

Also our second lesson learned in trace formatting was that in most cases the size of PCAP file with traces is less than size of the same trace in TXT format.

Consequently, in this version of the Self-accreditation Handbook we request all applicants to provide only PCAP files with traces. Please refer to clause 4.2.2 of the current document.

A.5 Test results submission

A.5.1 Official test results submission

In order to formalise self-accreditation process we have defined procedure for official submission of test results.

After you have prepared all the test results and self-accreditation declaration form according to clause 4.2.3 of the current documents please use GSMA corporate Dropbox (see section 5.2.3) for submission of these materials to the GSMA.

Only those submissions received via Dropbox will be published on the GSMA Accreditation webpage. Other submissions of test results sent via email or by other means to GSMA will not be considered as official and consequently will not be published on the GSMA website.

A.5.2 Passwords for zip file

According to clause 4.2.3 you need to send files with test results using GSMA corporate Dropbox (see section 5.2.3) and it optionally it is allowed to zip files with password in order to provide enhanced security and confidentiality of information.

However, we have faced with a problem when it is not possible to open archive with provided password. So, please perform a double check of password provided to GSMA.

A.5.3 Caveats

Please note that in order to get provisional accreditation and to achieve good quality of the RCS-e clients the sum of DESIGN LIMITATIONS and GO-TO-MARKET LIMITATIONS shall be not greater than 15%.

At the same time PENDING TESTBED LIMITATIONS and PRODUCTION ENVIRONMENT LIMITATIONS shall not hold back client provisional accreditation.

In particular cases, especially if the sum of PENDING TESTBED LIMITATIONS and PRODUCTION ENVIRONMENT LIMITATIONS exceeds 30% GSMA would request MNO to provide formal confirmation of acceptance for those network-dependant limitations.

NB: Full accreditation shall be dependent upon a formal statement from MNO received considering result of passing these test cases.

A.6 Typical implementation issues

A.6.1 Potential network issues

Most of the issues discovered during analysis of the first test results submissions were caused by problems on the client side. In the mean time we have met several issues for which it was difficult to identify source of failure, i.e. client or network. Usually those issues were related to receiving abnormal 4xx responses to SIP requests.

And after some workaround with those issues we were informed that the source was on the network side, temporary problems. However, applicants could spend a lot of time resources for retesting these network issues.

So, please while capturing traces pay attention to abnormal behaviour of the network and retest these tests before submission to GSMA since this could cause additional time resources spent for identifying the source of failure.

A.6.2 Ambiguous areas in the RCS specification

We understand that it is not easy to create 100% unambiguous RCS specification for a couple of years and always trying to make it more clear. However, there are still unclear areas available in the Specification [9] which could lead to differences in RCS implementation and subsequently IOT issues.

In order to achieve seamless interoperability of RCS products and accelerate their time-to-market we have developed special clarification document which is called joyn Implementation Guidelines [5]. This document compliments RCS Specification [9] and also contains clarifications which would be incorporated in future versions of the spec.

ANNEX B Typical issues checklist

This annex contains examples of typical issues which could be validated by applicant before submitting test results to GSMA for review within self-accreditation process.

More issues available via Network 2020 IP Communications Issues Registry.

#	Issue for validation	YES
1	Have all test cases been executed according to the description?	☐
2	Are SIP messages present in all traces, except those made on Wi-Fi access?	☐
3	In case fragmentation occurred, are all fragments included in the traces allowing re-assembly?	☐
4	Do the REGISTER requests include all the required IARI tags, including the Image Share IARI?	☐
5	Does the accredited client reside on another device than the accredited client against which the tests are performed?	☐
6	Is the SIP URI only included in the P-Preferred-Identity header when no tel URI is available?	☐
7	Is the OPTIONS response sent without SDP in the body in test cases where no call is ongoing?	☐
8	Is a SIP 404 Not Found response or a 200 OK response without feature tags received in test cases where a SIP OPTIONS request is sent to a non-RCS user?	☐
9	Is the OPTIONS request during a call sent without SDP in the body?	☐

#	Issue for validation	YES
10	Does the SDP in the SIP OPTIONS request during a call indicate H.264 baseline profile level 1b when in 3G/HSPA coverage even if higher levels like 1.3 can be supported on other access networks? Note: It is not an issue to use H.264 level 1.3 in Wi-Fi or on LTE. In 3G/HSPA though this may lead to a media negotiation result where both ends support 1.3 and, consequently, encoding would initially require more than the available bandwidth.	☐
11	Is MSRP media omitted from the SDP in the OPTIONS response during a call in test cases where Image Share is not supported?	☐
12	Are Image Share tags included in the Contact header of INVITE and 200 OK for Image Share Sessions? Please note that IM tag shall not be present in the INVITE for Video and Image Sharing sessions.	☐
13	Is profile-level-id 42900B used to indicate the support for H.264 baseline profile level 1b in the SDP included in the OPTIONS response during a call?	☐
14	Does the SDP in the SIP INVITE request for Chat and the associated 200 OK response include an accept-wrapped-types attribute indicating support for plain text and IMDN at least? Note: inclusion of other parameters into accept-wrapped-types attribute (e.g. application/vnd.gsma.rcs-ft-http+xml) depends on RCS services use cases as per RCS5.1 specification	☐
15	Does the accept-types attribute in the SDP in the SIP INVITE request for Chat and the associated 200 OK response not include plain text?	☐
16	Does the Disposition-Notification header for chat messages not request negative delivery notifications?	☐
17	Is the IM feature tag present in the contact header in the SIP INVITE/SUBSCRIBE/REFER requests for Chat and the associated 200 OK response? Note: inclusion of other feature tags depends on RCS services use cases as per RCS5.1 specification	☐
18	Does client include only joyn feature tags into Contact of SIP REGISTER, INVITE, OPTIONS requests while provisioned in the joyn network?	☐
19	Is the SIP INVITE for a Group Chat sent without a first message in a CPIM body?	☐

#	Issue for validation	YES
20	Is payload type 20 used when sending an empty RTP packet?	☐
21	Does in the MSRP SEND messages the CPIM parameter Failure-Reports set to Yes and parameter Success-Report set to No or not present?	☐
22	Does the Disposition-Notification header for Group chat messages request positive-delivery notifications only?	☐

Table 3. Typical issues checklist

Document Management

Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
0.1	03.02.2012	First draft version based on available RCS IOT documents and overall proposals on the accreditation process.		Konstantin Savin / GSMA
0.2	13.02.2012	Updates made on the basis of the GSMA RCS IOT Team comments and the output from the RCS IOT MNO meeting (10.02.12) in order to make the accreditation guidelines more explicit.		Konstantin Savin / GSMA
0.3	17.02.2012	Clarification notes added to the clauses 2.2.1.1, 2.2.2.1, 4.2.1 considering accreditation process for clients and networks and traces collection process		Konstantin Savin / GSMA
1.0	20.02.2012	Version approved by MNOs within the IOT Group		Konstantin Savin / GSMA
1.1	07.03.2012	Changes made based on submitted CR# RCSIOTMNO_Doc_07_002		Konstantin Savin / GSMA
2.0	16.05.2012	Latest modifications to the test cases matrix and accreditation process added based on issues discovered during IOT on MNO's networks. All changes were approved by RCS IOT MNO Group and presented in the CR# RCSIOTMNO Doc 15_002	RCS IOT MNO	Konstantin Savin / GSMA
2.1	30.07.2013	Latest clarifications to the accreditation process added based on lessons learned during IOT on MNO's networks. All changes were approved by RCS IOT MNO Group and presented in the CR# RCSIOTMNO Doc 21_001rev2	RCS IOT MNO	Konstantin Savin / GSMA
3.0	14.12.2012	Latest improvements to the accreditation process added based on lessons learned during IOT on MNO's networks. All changes have been approved by RCS IOT MNO Group	RCS IOT MNO	Konstantin Savin / GSMA
3.1	15.02.2013	Document was updated with introduction of an Accreditation Framework for RCS Hosted Solutions. All changes have been approved by RCS IOT&TSG MNO Group	RCS TSG&IOT MNO	Konstantin Savin / GSMA
3.2	02.05.2013	Document has been updated with changes in traces collection	RCS TSG&IOT MNO	Konstantin Savin / GSMA

		procedures (4.2.1) in order to remove inconsistency allowing not having SBC in the RCS Service Network. All changes have been approved by RCS IOT&TSG MNO Group		
3.2.1	04.07.2013	Document has been updated with changes to the content of the BASIC service profile (3.1, Step 0e) in order to remove inconsistency allowing no support of FileTransfer service for BASIC profile. All changes have been approved by RCS IOT&TSG MNO Group	RCS TSG&IOT MNO	Konstantin Savin / GSMA
4.0	22.11.2013	All references and links to joyn Hot Fixes documents removed, Yousendit Dropbox service renamed to Hightail with update of the link. Accreditation guidelines for API-based products have been incorporated. Annex B has been updated to comply with joyn Blackbird release. All changes have been approved by RCS IOT MNO Group	RCS IOT MNO	Konstantin Savin / GSMA
4.0.1	06.12.2013	Editorial change of the document - all links have been updated to reflect changes on the GSMA website.		Konstantin Savin / GSMA
4.0.2	07.03.2014	Editorial change of the document - all links have been updated to reflect change of the future communications program to network2020 on the GSMA website.		Konstantin Savin / GSMA
5.0	22.05.2014	It is now focused on joyn Blackbird profile and therefore 'Drop 1' part has been removed. All changes have been approved by RCS IOT MNO Group.		Konstantin Savin / GSMA
5.1	14.08.2014	There has been introduced the option for client providers and API Products Providers those delivering API Gateways and Web Solutions to get Accreditation Ready status by testing against Accreditation Ready Hosted Solutions, All changes have been approved by RCS IOT MNO Group.		Konstantin Savin / GSMA
6.0	21.11.2014	On November 1st 2014 the joyn Blackbird accreditation framework for Client Providers has been transferred to the GCF. From that date all new accreditation submission from Client Providers need to be sent to the GCF Certification process. The corresponding changes have been		Konstantin Savin / GSMA

		introduced in the section 2.2.2 of the current document.		
6.1	16.04.2015	The section 4.2.3 Test results submission has been updated with the new procedure for Dropbox services.		Konstantin Savin / GSMA
7.0	20.05.2016	The document has been updated to refer to joyn Crane Priority Release. Licensing information has been removed from the document. Key aspects of the accreditation framework have been moved to this document from the former Guidelines for Licensing Framework, such as details on Test Harness, accreditation applicability and industry obligations, convergence principles, roles and responsibilities.		Konstantin Savin / GSMA
8.0	17.11.2016	The document has been updated with accreditation procedures for the new applicant type – test tool provider (section 3.5). The procedure for networks accreditation has been updated allowing to test against an accredited test tool (3.1.1.1).		Konstantin Savin / GSMA

Other Information

Type	Description
Document owner	RCS IOT
Editor / Company	Vodafone Group – IOT Group Lead Oscar Gallego