# GSMA Urgent Clarifications on RCS 5.3 Implementation

## Version 1.0

## 30 July 2015

.

Security Classification – NON CONFIDENTIAL GSMA MATERIAL

## Copyright Notice

## Antitrust Notice

**The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.**

# Table of Contents

**1 Introduction 3**
**1.1** Scope 3
**1.2** Definition of Terms 3
**1.3** Document Cross-References 3
**2 RCS implementation clarifications 4**
**2.1** IMAP Implementation 4
ID_1_1 Removal of STARTTLS 4
ID_1_2 Correction of CMS Authentication Procedure 4

**Document Management 7**
Document History 7
Other Information 7

# 1 Introduction

## 1.1 Scope

This document provides the highlights of the issues discovered during the development, Interoperability testing (IOT) and deployment of RCS services that have been resolved and agreed in GSMA GSG meetings but are not yet included in the current published RCS technical specs due to the planned RCS release dates. It is advice to the OEM community and infrastructure providers to take these clarifications in the document into considerations when they are developing relevant RCS products to avoid any interoperability and service migration issues in the deployment.

All clarifications in the current document are related to the latest version of the RCS specification [2] available on the GSMA website and all update recommendations of the current document would be incorporated in the new versions of the RCS specification.

## 1.2 Definition of Terms

| Term | Description |
|---|---|
| 3GPP | 3rd Generation Partnership Project |
| CPM | Converged IP Messaging |
| ICSI | IMS Communication Service Identifier |
| IMS | IP Multimedia Subsystem |
| MSRP | Message Session Relay Protocol |
| OEM | Original Equipment Manufacturer |
| OMA | Open Mobile Alliance |
| RCS | Rich Communications Suite |
| SIP | Session Initiation Protocol |
| URN | Uniform Resource Name |

## 1.3 Document Cross-References

| Ref | Document | Title |
|---|---|---|
| [1] | OMA CPM 2.0 | OMA-TS-CPM_Conversation_Function-V2_0 |
| [2] | RCC.07 | Rich Communication Suite 5.3 Advanced Communications Services and Client Specification version 6.0<br>http://www.gsma.com/ |
| [3] | RCC.15 | IMS Device Configuration and Supporting Services Version 1.0<br>http://www.gsma.com/ |

# 2 RCS implementation clarifications

## 2.1 IMAP Implementation

### ID_1_1 Removal of STARTTLS

| | |
|---|---|
| **Key Word** | Removal of STARTTLS |
| **Agreed and targeted RCS Release** | RCS 6.0 |
| **Date modified** | 10.04.2015 |
| **Other Information** | GSG RCS-Q12016_CR002R01 |

**Description**

Section 3.2.6.2.1 of [2] mandates the client to set-up the TLS connection before sending any IMAP command. RCS client implementations shall follow this requirement. This obsoletes a requirement in section 2.13.1.5 of [2] to apply the STARTTLS command.

### ID_1_2 Correction of CMS Authentication Procedure

| | |
|---|---|
| **Key Word** | Correction of CMS Authentication Procedure |
| **Agreed and targeted RCS Release** | RCS 6.0 |
| **Date modified** | 10.04.2015 |
| **Other Information** | GSG RCS-Q12016_CR004R01 |

**Description**

The current version of [2] contains contradicting requirements for the case where the CMS user name and password are not supplied by the configuration server via the parameters MESSAGE STORE USER / PASSWORD. It is clarified that the client shall

- use the values of "Realm User Name" and "Realm User Password" defined in Table 2 of [3] for authentication if the MESSAGE STORE AUTH parameter defined in Table 77 of [2] is set to "1"
- derive user name and password from the GBA bootstrapped security association as defined in section 3.2.4.7.7. of [2] if the MESSAGE STORE AUTH parameter defined in Table 77 of [2] is set to "2"

This correction requires the following new definitions in [2].

The GBA authentication procedure description in section 3.2.4.7.7 of [2] is newly defined as follows.

The client shall use the bootstrapped security association for the authentication with the Common Message Store if the client configuration parameter MESSAGE STORE AUTH value is set to "2" as defined in Table 77, section A.1.4.3.

In this case the client shall use the key material received from the Service Provider's BSF, the user's private identity (IMPI) and the FQDN of the Common Message Store derived from the value of the configuration parameter MESSAGE STORE URL (see Table 77 section A.1.4.3) to calculate the Ks_NAF as defined in [3GPP TS 33.220]. If no bootstrapped security association exists the client shall first create one as defined in [3GPP TS 33.220].

The client shall login to the Common Message Store either via IMAP AUTHENTICATE command (with PLAIN argument) or IMAP LOGIN command using the B-TID as username and the Ks_NAF as password. The Common Message Store authenticates the request in co-operation with the service Provider's BSF. It returns an OK response to the client if the authentication is successful. If the Common Message Store returns a NO response indicating that the authentication failed then the client shall renegotiate the bootstrapped security association as defined in [3GPP TS 33.220] and [3GPP TS 24.109]. It shall re-attempt the login to the Common Message Store with username and password derived from the B-TID and key material resulting from the re-negotiation.

Table 77 in section A.1.4.3 of [2] the configuration parameters MESSAGE STORE USER / PASSWORD and MESSAGE STORE AUTH are newly defined as follows.

| | | |
|---|---|---|
| MESSAGE STORE USER / PASSWORD | The plain text user name and password for authentication with the Message Store Server.<br>If the parameters are absent but the MESSAGE STORE URL is present the following applies:<br>• If the MESSAGE STORE AUTH parameter is set to "1" then the client shall use the values of "Realm User Name" and "Realm User Password" defined in Table 2 of [RCC.15] for authentication instead.<br>• If the MESSAGE STORE AUTH parameter is set to "2" then the client shall derive user name and password from the GBA bootstrapped security association as defined in section 3.2.4.7.7. | Optional parameter.<br>It is mandatory if the MESSAGE STORE AUTH parameter is absent or set to “0”. |
| MESSAGE STORE AUTH | This parameter controls the authentication mechanism used to access the Message Store Server.<br>**0**: Plain User Name password via LOGIN command with user name and password from MESSAGE STORE USER / PASSWORD<br>**1**: PLAIN SASL authentication with user name and password from MESSAGE STORE USER / PASSWORD if present, otherwise with "Realm User Name" and "Realm User Password" defined in Table 2 of [RCC.15]<br>**2**: Authentication with B-TID and Ks_NAF derived from the GBA bootstrapped security association as defined in section 3.2.4.7.7. The client shall select the appropriate IMAP authentication mechanism from the server's IMAP CAPABILITY command response (i.e. LOGIN or AUTHENTICATE command).<br>If not provided, the authentication mechanism defaults to the same as if 0 were selected: Plain User Name password. | Optional parameter |

In section A.2.7 of [2] the definition of the configuration parameter "AuthProt" is newly defined as follows:

Node: /<x>/CPM/MessageStore/AuthProt

Optional leaf node that can be used to force the Message Store Client to use one of the authentication methods defined in section 2.13.1.5. If not instantiated, but the /URL node in Table 202 is instantiated or present, the Message Store Client SHALL assume the same method as if value 0 had been specified.

| Status | Occurrence | Format | Min. Access Types |
|---|---|---|---|
| Required | ZeroOrOne | int | Get |

**Table 203: CPM MO sub tree addition parameters (AuthProt)**

- Values: 0, 1, 2
  0- Indicates that the user name / password method must be used by the Message Store Client (default)
  1- Indicates that the PLAIN SASL methods must be used by the Message Store Client
  2- Indicates that the authentication with the Common Message Store shall be based on the GBA security association.

- Post-reconfiguration actions: As the client remains unregistered during configuration, there are no additional actions apart from de-registering using the old configuration and registering back (see section 2.4) using the new parameter.
- Associated HTTP XML parameter ID: “AuthProt”

# Document Management

## Document History

| Version | Date | Brief Description of Change | Approval Authority | Editor / Company |
|---|---|---|---|---|
| 1.0 |  | First version with initial guidelines for RCS5.3 | GSG |  |

## Other Information