**3GPP TSG-SA WG1 Meeting #111 S1-253083r1-01**

**Goteborg, Sweden, 25-29 August, 2025**

Title: 22.870 pCR Update of Use case on Enhancement of short message service (SMS)

Agenda Item: 8.1.2 (6G study - System and Operation Aspects)

Source: Samsung, Verizon

Contact: Erik Guttman <erik.guttman@samsung.com>

*Abstract: This paper proposes to revise an existing use case to revise a human interface requirement that is out of scope of 3GPP standardization, so that the intent is captured by a requirement that is in 3GPP scope.*

**Discussion**

Requirements that involve display of information to a user are out of scope of 3GPP. Please see S1-252257.

The use case below needs to concentrate on exposing information to the Terminal Equipment. How this is used will depend on the implementation of the Terminal Equipment, which is out of scope of 3GPP. An RCS client, could for example, use this information to provide a rich human interface. Another Terminal Equipment, such as an IoT device or a router, etc. with no human interface, could use this information in a different way.

Modifications of S1-253083 in r1

- expose SMS provenance information to UEs not Terminal Equipment [Qualcomm]

- use the term SMS **sender** information instead of **provenance** information [Huawei]

- explicitly mention RCS and link this to existing features enabling 'display' of information to users [Huawei]

- add that additional information is integrity protected. [Verizon]

further modifications to r1 in r1-01

- change 'expose information' to 'provide information' in requirement -1 [Qualcomm]

**Proposal**

It is proposed to make the change listed below to TR 22.870 v031.

Begin changes

### 5.7.3 Enhancement of short message service (SMS)

#### 5.7.3.1 Description

Short Message Service (SMS) is one of the most traditional telecom services offered by operators. A growing number of enterprise customers and applications (i.e. Application-to-Point, A2P SMS senders) are using A2P SMS to send notifications, verification codes, and other messages to end users. In the 6G era, SMS is expected to remain favoured by A2P SMS senders due to its unmatched reliability and universal device compatibility.

The growing number and evolving forms of A2P SMS senders present both opportunities and challenges. On one hand, they create new business prospects for operators and enhance the value of carrier messaging channels. On the other hand, they raise end user concerns—such as identifying potential scams from fraudulent A2P SMS senders and ensuring secure interactions with legitimate A2P services via SMS, etc.

In Rich Communication Services (RCS) as specified in GSMA RCC.71 [209], Chatbots are introduced as enterprise users/applications to provide A2P and Point-to-Application messaging services. Within the RCS framework, Chatbots needs to be verified by the operator. Users can view the associated enterprise information and verification status of these Chatbots. For verified A2P sender end users can interact with them with greater confidence. For unverified A2P sender, end users can make more informed decisions about whether to reply or engage, while exercising greater caution to avoid potential scams.

However, this verification mechanism is exclusive to RCS Chatbot services and does not apply when enterprise users/applications utilize SMS. Therefore, in the 6G era, traditional SMS is expected to evolve delivering more secure and trusted interactions between end users and A2P SMS senders by introducing the similar capabilities.

There is a related feature, in 22.173 [59], Connected Name and Number Display. This provides information from the network concerning an incoming call, which "allows the device to display the name and/or telephone number of both current parties on a 2-party call."

#### 5.7.3.2 Potential New Requirements

[PR 5.7.3.2-1] The 6G SMS service shall enable a network operator to verify the identity of the SMS sender.

[PR 5.7.3.2-2] The 6G SMS service shall support a means to provide information concerning operator verified SMS sender information to UEs.

NOTE 1: Operator verified SMS sender information can be used, e.g. by client application software such as RCS, to inform the recipient of a SMS that the identity of the SMS sender is operator-verified and support displaying additional information (e.g. brand name, logo, etc.) of the SMS sender. Human interface aspects are out of scope of this requirement.

NOTE 2: Indication that the identity of the SMS sender is operator-verified, any additional information about the SMS sender and the message itself is assumed to be integrity protected.

NOTE 3: Based on interworking agreements and trust relationships, the requirements above apply also when the SMS recipient is roaming or receives a SMS from a sender served by other operators.

NOTE 4: The requirements above apply to A2P SMS and may apply to Person-to-Person SMS.End of changes