**SA WG2 Meeting S2#162 S2-2405053**

**April 15 – 19, 2024, Changsha, PR China revision of S2-2404593**

**Source: Nokia**

**Title: KI#4: Conclusion on solution principles**

**Document for: Approval**

**Agenda Item: 19.2**

**Work Item / Release: FS\_NG\_RTC\_Ph2**

*Abstract of the contribution: This contribution proposes to conclude on solution principles.*

# Introduction

KI#4 is mainly about support of third party IDs in IMS which was intensively discussed in TR 23.700-87 (Rel-18).

# 2 Proposal

It is proposed to add following text to TR 23.700-77.

\* \* \* \* First change\* \* \* \*

# 7 Overall Evaluation

Editor's note: This clause will provide evaluation of different solutions.

# 8 Conclusions

Editor's note: This clause will list conclusions that have been agreed during the course of the study item activities.

## 8.x KI#4 Principles for normative work

Editor's note: Current main discussed points are A) IMS AS versus S-CSCF C) multiple RCD .the operator can directly

For KI#4 on "Extensible IMS framework to support authorization and authentication of third-party identities in IMS sessions" the following solution principles are agreed:

1. Support authorization check in IMS AS whether the calling party (PBX/user) is authorized to use Third Party specific identity information based the user profile retrieved from the HSS.
2. The definition of Third Party specific user identity information used in IMS follows the definitions in draft-ietf-sipcore-callinfo-rcd-09 [19].

3. Signing and verification of Third Party specific user identity information follows draft-ietf-stir-passport-rcd-26 [18].

4a. Support configuration of an RCD address or optionally RCD information in the HSS per IMPU including wildcard IMPU.

4b. For some users (i.e. that have individual subscriptions in HSS), the operator can directly store per IMPU trusted RCD information from the Third Party network like caller name, job title, organization, and location information in the HSS.

4c For some users behind a PBX (i.e. managed via a wildcarded IMPU in HSS), the operator can store per wildcarded IMPU RCD information in the HSS.

4d For some users, the operator can store in HSS per IMPU an RCD address where Third Party specific user identity information can be fetched from.

Editor’s note: The nature of RCD information storage is FFS.

5. Based on operator policy, either the fetched RCD address or the fetched RCD information is signed and provided in SIP messages (SIP INVITE) towards the terminating party network.

6 The RCD address or optional RCD Information is fetched by the IMS AS from the HSS during IMS session setup.

7. The IBCF, or IMS AS invoke signing and verification of Rich Call Data information based on local policies and trust relationship with the Third Party network.

8. The fetched RCD address or RCD information is used by the Signing AS for signing the RCD PASSporT and by the Verification AS in terminating network to verify the signed RCD PASSporT.

9) Some third-party may support returning multiple RCD records per user, and where one RCD record is configured as default. In this case user input criteria in the incoming SIP INVITE is required to enable IMS AS to include the proper RCD record in the outgoing SIP INVITE,

In this Release, there is no user support to provide any user input selection criteria in the incoming SIP INVITE. The user must set the default RCD record in third party server by offline means (e.g portal) for proper RCD record selection and inclusion by IMS AS.

NOTE: This bullet 10 principle has no normative work, but will be described in the spec.

Editor’s note: ?

\* \* \* \* End of changes \* \* \* \*