**3GPP TSG-SA3 Meeting #115 *draft\_S3-240945-r2***

Athens, Greece, 26th February - 1st March 2024 merger of S3-240347, S3-240554, S3-240763

**Source: Ericsson, Philips International B.V., Huawei, HiSilicon**

**Title: New Key issue on the security of IMS Avatar Communication using Data Channel**

**Document for: Approval**

**Agenda Item: 5.2**

# 1 Decision/action requested

It is requested to agree to the proposed key issue for TR 33.790 on the security of IMS Avatar Communication using Data Channel.

# 2 References

[1] 3GPP TR 23.700-77: "Study on system architecture for next generation real time communication services; Phase 2".

# 3 Rationale

This contribution is the proposal of the key issue of security of IMS Avatar Communication using Data Channel.

# 4 Detailed proposal

**\*\*\*\*** START of 1st CHANGE **\*\*\*\***

## 5.X Key issue #X: Security of IMS based Avatar Communication using Data Channel

### 5.X.1 Key issue details

According to TR 23.700-77 [X1], there are scenarios that a UE uses an Avatar-ID to initiate an IMS based Avatar Communication using a data channel. Then the Avatar-ID is used to fetch objects such as an Avatar representation which may include Avatar metadata and Avatar media.

The IMS network can present the Avatar to the callee during the subsequent calling process. The UE can access the IMS network directly or via a SIP trunk as well.

From a security point of view, the enhanced IMS network needs to be able to support the Avatar-ID authentication and authorization during an IMS Avatar call. Also, Avatar objects such as Avatar representations could be used by malicious users to impersonate other users. Therefore, it is essential to ensure that the Avatar objects are secure and cannot be tampered with or accessed by unauthorized entities.

### 5.X.2 Threats

A malicious UE can use Avatar-IDs belonging to other UEs or forged Avatar-IDs to initiate IMS avatar communication in the IMS network and therefore impersonate other UEs.

The potential transfer of the Avatar-IDs between IMS networks can potentially be manipulated by intermediary network entities.

The potential transfer of the Avatar metadata between IMS networks can potentially be manipulated by intermediary network entities.

The potential transfer of the Avatar media between IMS networks can potentially be manipulated by intermediary network entities.

Avatar objects could be used for impersonating a IMS caller.

### 5.X.3 Potential security requirements

The 3GPP system shall support means to ensure that stored Avatar objects and Avatar-IDs are accessed only by authenticated and authorized users, UEs, and IMS network nodes.The IMS network shall support coordination with the repository which stores the Avatar objects to authenticate and authorize the Avatar-ID.

The IMS network shall support the integrity protection of the Avatar-ID on the originating side and terminating side.

The IMS network shall support the integrity protection of the Avatar objects such as the Avatar representation on the originating network and terminating network.

**\*\*\*\*** END of 1st CHANGE **\*\*\*\***

**\*\*\*\*** START of 2nd CHANGE **\*\*\*\***

# 2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non‑specific.

- For a specific reference, subsequent revisions do not apply.

- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[X1] 3GPP TR 23.700-77: "Study on system architecture for next generation real time communication services; Phase 2".

**\*\*\*\*** END of 2nd CHANGE **\*\*\*\***