**3GPP TSG-SA3 Meeting #109AdHoc-e *S3-230412-r1***

**Electronic meeting, 16 - 20 January 2023**

**Source: Ericsson**

**Title: Resolve EN for Solution#5**

**Document for: Approval**

**Agenda Item: 5.15**

1 Decision/action requested

***Approve the pCR to TR 33.890.***

2 References

[1] 3GPP TR 23.700-87: " Study on system architecture enhancement for next generation real time communication; phase 2".

[2] 3GPP TR 33.890 v 0.4.0: "Study on security support for Next Generation Real Time Communication services".

3 Rationale

This contribution addresses the following EN in Solution#5 in 3GPP TR 33.890 [2] by clarifying the different types of data channel and which scenario the e2ae or e2e security applies to.

Editor's Note: Alignment with SA2 is needed, e.g., the types of data channel and the scope of interfaces;

4 Detailed proposal

Approve the following changes to TR 33.890 [2].

\*\*\* Start of 1st 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".

[2] 3GPP TR 23.700-87: "Study on system architecture enhancement for next generation real time communication".

[3] 3GPP TS 33.328: "IP Multimedia Subsystem (IMS) media plane security".

[4] 3GPP TS 24.229: IP Multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3".

[5] ATIS-1000074: Signature-based Handling of Asserted information using Tokens (SHAKEN)

[6] IETF draft-ietf-stir-passport-rcd-18, "PASSporT Extension for Rich Call Data"

[7] draft-ietf-sipcore-callinfo-rcd-03: "SIP Call-Info Parameters for Rich Call Data".

[8] IETF RFC 8224: "Authenticated Identity Management in the Session Initiation Protocol (SIP)".

[9] IETF RFC 8831: “WebRTC Data Channels”

[10] 3GPP TS 23.334: “IP Multimedia Subsystem (IMS) Application Level Gateway (IMS-ALG) - IMS Access Gateway (IMS-AGW) interface: Procedures descriptions”

[11] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[12] 3GPP TS 23.228: “IP Multimedia Subsystem (IMS); Stage 2”

[13] IETF RFC 8827: “WebRTC Security Architecture”

[XX] 3GPP TS 32.274: "Telecommunication management; Charging management; Short Message Service (SMS) charging"

[YY] GSMA NG.129: "IMS Data Channel White Paper"

…

[x] <doctype> <#>[ ([up to and including]{yyyy[-mm]|V<a[.b[.c]]>}[onwards])]: "<Title>".

 \*\*\* End of 1st Change \*\*\*

\*\*\* Start of 2nd Change \*\*\*

## 6.5 Solution #5: How to avoid e2ae limitation and achieve e2e security for IMS Data Channel

### 6.5.1 Introduction

This solution addresses the key issue #2 (Security aspects of Data Channel usage in IMS network). As stated in the key issue details, clause N.3 of TS 33.328 [3] describes media security of the WebRTC data channel, but only e2ae (end-to-access edge) security is specified now. It means that an SCTP over DTLS connection is established between the DCMTSI client and the IMS-AGW (see section 5.20.2 of 3GPP TS 23.334 [10]). The text is void of any references to e2e security mode for the IMS data channels. However, there exist use cases in TS 23.700-87 [2] (Solutions #3, #6, #9, #16, and #20) where Data Channel Server (DCS) or related data channel application functionality can be deployed in an external data server outside the operator’s administrative domain. According to IETF RFC 8831 [9] (clause 6.2), SCTP over DTLS connection needs to be established between two endpoints supporting WebRTC data channel protocol (e.g., the DCMTSI client and the external data channel server or data channel application server).

This solution proposes to allow the DTLS connection from the data channel endpoints to pass transparently through the IMS network by allowing e2e security mode for IMS (and thus WebRTC) data channel media if the external Data Server supports both HTTP and IETF RFC 8831 WebRTC data channel protocols. In the model when the external Data Server supports only HTTP protocol and responds to DCMTSI service requests for the data channel content, end-to-access edge (e2ae) encryption is used, therefore all data channel traffic is anchored in IMS network and is transported unencrypted from IMS-AGW towards the external entities.

### 6.5.2 Solution details

#### 6.5.2.1 Solution Description

The MDC2 reference point as described in TS 23.700-87 [2] Solution#20(and similar reference points in other solutions in that document) is used for transport of data channel media between DC Media Function (either DCMF or enhanced MRF) and DC Application Server, see Figure 6.5.2.1-1 as one example of such solution. If the external DC application server supports both HTTP and IETF RFC 8831 WebRTC data channel protocols, the server responds to UE(DCMTSI client)service requests for the data channel content and the content driving the interaction with the server is delivered over the data channel. In order to establish the WebRTC data channel between the UE and the DC Application Server a signaling channel is required e.g. to exchange fingerprints binding the certificates. The end-to-end (e2e) encryption for the data channel should be used as specified in IETF RFC 8831 [9] and IETF RFC 8827 [13].



Figure 6.5.2.1-1: Use of IMS-external data channel media (see TS 23.700-87 [2], clause 6.20.1)

There are two types of Data Channels: Bootstrap Data Channel and Application Data Channel. According to GSMA NG.129 [YY], the application Data Channel supports the P2P, P2A and A2P use cases. The data channel related P2P/P2A/A2P definitions follow from 3GPP TS 32.274 [XX] and are applied accordingly to this document with the following meaning:

1. Person-to-Person (P2P): The session is originated by a UE and terminated on another UE.

2. Person-to-Application (P2A): The session is originated by a UE and terminated on a third-party application.

3. Application-to-Person (A2P): The session is originated by a third-party application and terminates on a UE.For the P2P use case, DC media resources are not required. So, the application data channel can either involve DCMF (enhanced MRF) or not.

For the P2A/A2P use cases, DC media resources are required. So, the application data channel should involve DCMF (enhanced MRF).

The IMS Data Channel user plane (not depicted in Figure 6.5.2.1-1) from UE (DCMTSI client in terminal) to the IMS-AGW is secured with DTLS regardless of e2ae or e2e security being used. The DC Application server can be deployed outside the operator’s administrative domain and provides service logic and/or media content for the data channel application.

If the DC Application server supports only the HTTP protocol, the data channel is established between the DCMTSI and the IMS. An SCTP connection over DTLS over UDP is established between the DCMTSI client (UE) and the IMS-AGW which is applied to P2P use case without DC media resources. An SCTP connection over DTLS over UDP is established between the DCMTSI client (UE) and DCMF (enhanced MRF) which is applied to the A2P/P2A use cases, the P2P use case with DC media resources and the bootstrap data channel. The data channel transport layer is terminated at IMS-AGW or DCMF (enhanced MRF) and e2ae security is achieved. The data channel is encrypted over the Mb interface but it is unencrypted over other interfaces.

If the DC Application server supports both HTTP and IETF RFC 8831 [9] WebRTC data channel protocols, the application data channel is established between the DCMTSI client (UE) and the External DC Application Server. An SCTP connection over DTLS over UDP is established directly between the DCMTSI client (UE) and the external DC Application server, which is applied to the A2P, and P2A use cases. In order to establish the WebRTC data channel, a signaling channel is required e.g., to exchange fingerprints binding the certificates. IMS-AGW does not terminate DTLS and thus only anchors IP and UDP protocol layers towards DCMF/enhanced MRF, and DCMF/enhanced MRF is also transparent to DTLS traffic between Mb and MDC2 reference points, e2e security is achieved between the UE and the DC Application Server, without security risks even if the DC Application Server is placed outside of the operator’s domain.

### 6.5.3 Evaluation

The solution addresses the KI#2 Security aspects of Data Channel usage in IMS network. The following changes are suggested:

* TS 33.328 [3] needs to be enhanced to allow e2e security for IMS (and WebRTC) Data Channel media and should (recommend or) mandate using e2e security whenever IMS Data Channel media is used towards an entity deployed outside the operator’s administrative domain.
* TS 23.334 [10] needs to be enhanced to describe use of e2e security for IMS (and WebRTC) Data Channel media.
* TS 24.229 [4] needs to be enhanced to describe use of e2e security for IMS (and WebRTC) Data Channel media.

\*\*\* End of 2nd Change \*\*\*