**SA WG3 Meeting S3#116 Draft\_S3-242437r1**

**Jeju, Korea 20 - 24 May 2024** revision of S3-242347

**Source: Nokia, Nokia Shanghai Bell, CableLabs**

**Title: new solution for secure IMS DC capability exposure**

**Document for: Approval**

**Agenda Item: 5.2**

**Work Item / Release: FS\_NG\_RTC\_Ph2/Rel19**

# 1 Decision/action requested

***Approve the solution added to TR 33.790***

# 2 References

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

[2] 3GPP TR 33.790 Study on the security support for the Next Generation Real Time Communication services phase 2

# 3 Rationale

The contribution proposes a new solution for secure IMS DC capability exposure.

# 4 Detailed proposal

All content in the change part is new.

\* \* \* \* First 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*.

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

\* \* \* \* Next change \* \* \* \*

## 6.x Solution #x: Secure IMS DC capability exposure

### 6.X.1 Introduction

The solution addressed KI#X security and privacy aspects of IMS DC capability exposure.

Solutions to support IMS event and capability exposure in the context of data channel (DC) communication/session are developed in TR 23.700-77. Without proper security control, the IMS DC services may be illegally used by malicious application function/server (AF/AS), e.g. the malicious AF may eavesdrop or manipulate IMS DCs, the malicious AF may launch DoS attack with updating/terminating an ongoing DC, and cause interruption on the IMS communication of an end user, privacy of IMS user may also be compromised.

This solution proposes security procedures to authenticate and authorize DC AS before grant permission to the DC AS on IMS DC event or IMS DC session control.

### 6.X.2 Solution detail

Basically, the DC AS/AF is authenticated based on the description in clause 13 or clause 12 of TS 33.501. The AF authorization is based on clause 13 or clause 12 or local configuration at the NEF. In addition, the solution describes detail procedure to authorize an DC AS/AF to subscribe to DC event or control DC session in IMS network. The solution assumes the DC specific authorization policies are preconfigured in HSS/UDM or NEF, and the authorization decision will be made by NEF/DCSF based on DC AS properties, DC related services and other conditions.

Editor's Note: Alignment with SA2 is FFS

#### 6.x.2.1 Procedure of DC AS authorization for DC event subscription

Precondition:

* Authorization policies are provisioned in NEF/HSS/UDM.



Figure 6.X-1 DC AS authorization for DC event subscription

Procedures:

1. NEF receives DC event subscription request from DC AF/AS.

2. After authenticating the AF/AS (TLS based mutual authentication), NEF retrieves authorization policies locally or from HSS/UDM.

3. NEF makes authorization decision and grants permission for the request based on the policies and user consent.

4. NEF sends DC event subscription request to DCSF.

5. NEF receives response from DCSF.

6. NEF sends response to the DC AF/AS

7. NEF receives event notification from DCSF.

8. NEF sends the notification to the DC AF/AS. The notification may be anonymized based on privacy policies or regulations.

#### 6.x.2.2 Procedure of DC AS authorization for data channel session control

DC session control includes bootstrap and application DC establishment, update and termination, as well as DC application download.



Figure 6.X-2 DC AS authorization for data channel session control

Procedures:

1. NEF receives bootstrap data channel (BDC)/application DC (ADC) establishment/termination/update or application download request from DC AF/AS.

2. After authenticating the DC AF/AS (TLS based mutual authentication), NEF retrieves authorization policies locally or from HSS/UDM.

3. If the session control is targeted an ADC, according to authorization policies, NEF may further check if the DC AF/AS is matched to the DC application associated to the target ADC.

NOTE 1: NEF may check locally or check with DCSF, or this check can be done by DCSF.

4. If the DC AF/AS is allowed to perform the required session control on the DC based on the authorization policies, NEF grants permission for the request.

5. NEF sends DC session control request to DCSF. DCSF triggers IMS AS to re-invite the IMS call to include DC offer with UEs, and reserve DC resource with MF if needed.

6. NEF receives response from DCSF.

7. NEF sends response to the DC AF/AS.

 Editor's Notes: The procedure of IMS DC capability exposure depends on SA2's conclusion.

### 6.X.3 Evaluation

TBD

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