**SA WG2 Meeting #115 S2-162752**

**23 - 27 May 2016, Nanjing, P.R. China (revision of S2-162430)**

**Source: NTT DOCOMO**

**Title: Updates to Solution 5**

**Document for: Approval**

**Agenda Item: 6.6**

**Work Item / Release: FS\_V8 / 14**

*Abstract of the contribution:*

*This contribution updates Solution #5 based on LS response from SA5 in S3-160775.*

# Discussion

SA5 has reviewed Solution #5 and provided their response in S3-160775. The key aspects that they want Solution #5 to support are given below and we also consider how these have been captured in the solution documentation.

1. **All PGWs supporting emergency PDN connection to the emergency P-CSCFs used by inbound roaming UEs shall implement measures to prevent source IP address spoofing.**

 Analysis: This has already been stated in the impacts of the solution. However, we add further clarification to the specific step of the solution where action by PGW is required and also to the impacts section of the solution. This is added in text before Step 9 -12.

2. **Only one contact IP address for the UE shall be used for the emergency call.**

TS 33.302, Annex T for GIBA it states the following for the P-CSCF and S-CSCF

:

The P-CSCF checks the source IP address against the IP address in the Via header of the REGISTER message. If the source IP address differs from the IP address in the Via header, the P-CSCF adds the source IP address to a received parameter in the Via header. The P-CSCF then forwards the REGISTER to the I-CSCF in the home network.

NOTE:    The source IP address differs from the IP address in the Via header only in case the UE is malicious or the UE is misbehaving for some reason.

..

The S-CSCF contacts the HSS and indicates that GIBA is used to authenticate the UE. The HSS returns the stored IP address to the S-CSCF. The S-CSCF then checks the IP address returned by the HSS against the IP address obtained in the REGISTER message ((if present, the received by parameter shall be used).

So at Stage 2 we can state that the P-CSCF checks the source IP address against IP address in the REGISTER messge. Which field of the REGISTER message that P-CSCF check (eg Via or the contact field) is for Stage 3 to determine

 This has been added to Step 6 as a check for the P-CSCF to perform in SIP REGISTER

3. **A one-to-one relation between IMSI and IMPI for the emergency call shall be ensured.**

The context for this from TS 33.203, annex T:

In GIBA the IMS user authentication is performed by linking the IMS registration (based on an IMPI) to a PDP context (based on an authenticated IMSI). The mechanism here assumes that there is a one-to-one relationship between the IMSI for bearer access and the IMPI for IMS access.

In solution 5, since the linking is based on only the IP address provided by the UE and not by any IMPI, or IMPU. In the solution, the IMPI that the UE provides has to be based on IMSI according to 24.229, and then by definition there is a one-to-one mapping and the requirement is met.

9. UE according to TS 24.229 [10], performs a new initial registration by sending a SIP REGISTER (UserID-2, IMEI) message and without inclusion of the Authorization header field. UserID-2 is an IMPI derived from IMSI. P-CSCF may verify the IMSI/IMEI provided by the PCRF in step 7b against the IMSI/IMEI derived from the IMPI provided by the UE, prior to accepting the SIP REGISTER message.

4. **The UE shall use only one IMS emergency APN for emergency calls and use the same IP address for the emergency call.**

 The first part of this requirement, i.e. “The UE shall use only one IMS emergency APN for emergency calls” is already implemented in the access-network by the MME only allowing one IMS emergency PDN Connectivity for the UE. The second part of the requirement “…and use the same IP address for the emergency call”, is covered as part of the source IP address spoofing prevention requirement for all PGWs supporting Emergency PDN Connectivity for inbound roamers with S8HR roaming agreement.

 Hence, no update to the solution is required.

Also added text to the conclusion section: The part of Solution #5 which deals with the optimization where the network (P-CSCF) provides a new indication to the UE to perform anonymous IMS emergency session and impacted UE behaviour is applicable to all IMS emergency sessions, both LBO and S8HR scenario. Hence, normative changes for this part will be captured as part of TEI14

# Proposal

\*\*\*\*\* Start of Change # 1 \*\*\*\*\*

## 6.5 Solution #5: IMS emergency session with or without IMS registration failure

### 6.5.1 Description

6.5.1.1 General

This solution addresses key issue 1 ("How to make UE-detected IMS emergency session successful").

In this solution the network is able to skip the IMS-level authentication with sufficient confidence based on the fact that the UE has been successfully authenticated at EPS level, the identities number retrieved via the PCRF serving as a "soft" proof. This is similar to GIBA (GPRS-IMS Bundled Authentication; see TS 33.203 [12]) where the IP address assigned at GPRS level (and retrieved by the IMS from the HSS) is used as a "soft" proof that the UE has been successfully authenticated at GPRS level, allowing the IMS to proceed without authenticating the UE at IMS-level.

This solution proposes to provision a PSAP callback number via the PCRF in the VPLMN (located between the P-CSCF in the VPLMN and the PGW in the VPLMN).

NOTE 1: The PSAP call back functionality is not changed. Only the retrieval of PSAP callback number is different.

In this solution the IMS network accepts the SIP REGISTER message without attempting to authenticate the UE, without creating a UE registration state in the VPLMN IMS, and without impacting the UE registration state that the UE may have on a parallel non-emergency IMS PDN connection (i.e. the one with HPLMN IMS from S8HR).

NOTE 2: SA WG3 needs to review the security aspects of this solution.

6.5.1.2 Solution description

The call flow for the case where IMS registration failure is avoided is described in Figure 6.5.1.2-1.

Figure 6.5.1.2-1: IMS Emergency Session Establishment

1. UE establishes a PDN connection for IMS emergency services.

2. IMSI, IMSI-unauthenticated indicator (if available) and IMEI(SV) are retrieved from the UE. The MSISDN (if available) is provided by the HSS.

3. MME sends a [S11] [S5] Create Session Request towards the PGW including the IMSI, the IMSI-unauthenticated indicator (if available), the IMEI(SV) and the MSISDN (if available).

4. PGW establishes an IP-CAN session with the PCRF as described in TS 23.401 [7] and TS 23.203 [11]. The IP-CAN session is identified with UE's IPv4 address of IPv6 prefix associated with the PDN connection for IMS emergency services. The IMSI, the IMSI-unauthenticated indicator (if available), the IMEI(SV) and the MSISDN (if available) are passed to the PCRF as part of the IP-CAN session establishment.

5. UE completes the Attach or UE requested PDN connection procedure.

 Up to here the procedure is identical with the existing PS domain emergency PDN and Attach handling, except that the IMSI-unauthenticated indicator is not available on Gx. Also the PCC may need some clarification in specifications as it seems that the sending of MSISDN over Gx is not mandatory.

Steps 6-12 apply in case the UE performs IMS Emergency Registration, based on conditions specified in TS 23.167 [9], e.g. UE is aware that it has sufficient IMS authentication material.

6. UE initiates IMS emergency registration by sending a SIP REGISTER (UserID-1) message. The UserID-1 parameter is an IMPI and optionally an IMPU.

7a. Upon reception of the SIP REGISTER message the P-CSCF contacts the PCRF for establishment of an Rx session. Based on configuration (e.g. only when serving emergency calls from S8HR inbound roamers that have no NNI for emergency registration, which is determined by analysing the UserID-1 parameter in the SIP REGISTER message) the P-CSCF decides to accept the SIP REGISTER message without attempting to authenticate the UE with HPLMN IMS. The P-CSCF includes an explicit request for EPS-level identities (e.g. IMSI, IMEI(SV), MSISDN) in the Rx request.

7b. The PCRF is able to perform session binding based on the UE's IP address/prefix (see TS 23.203 [11] clause 6.1.1.2) and provides the information that it has received upon IP-CAN session establishment in step 4. I.e. as part of the Rx session establishment the one or more EPS-level identities and the MSISDN (if available) are returned to the P-CSCF.

NOTE 1: A UE equipped with a UICC without any IMS credentials (but with valid PS credentials), initiates emergency IMS registration deriving IMS parameters from USIM (refer to TS 24.229 [10] annex C.2).

8. Based on operator configuration and if the network supports the GIBA procedure over Gm as defined in TS 24.229 [10], the P-CSCF responds with a 420 response with sec-agree value listed in the unsupported header field. Otherwise it rejects the IMS registration request with SIP 403 (Forbidden) as defined in TS 24.229 [10]. If the network supports anonymous IMS emergency sessions, P-CSCF adds an indication whether it supports anonymous IMS emergency sessions to the 403 or 420 response.

Steps 9-12 apply in case the P-CSCF has responded with a 420 response in step 8 and if the UE supports fallback to GIBA as part of emergency IMS registration. A requirement for Steps 9-12 to be supported is: All PGWs supporting emergency PDN connection for inbound roamers with S8HR roaming agreement shall implement measures to prevent source IP address spoofing as specified in Annex T.6 of TS 33.203 [x]:

 Specifically, a UE attached to the PGW shall not be able to successfully transmit an IP packet with a source IP address (or the prefix in the case of IPv6 stateless autoconfiguration) that is different to the one assigned by the PGW during PDN Connectivity Setup. If IP address spoofing is detected the PGW shall drop the packet. It shall be possible for the PGW to log the event in its security log against the subscriber information (IMSI/MSISDN), e.g. based on operator configuration.

9. UE according to TS 24.229 [10], performs a new initial registration by sending a SIP REGISTER (UserID-2, IMEI) message and without inclusion of the Authorization header field. UserID-2 is an IMPI derived from IMSI. P-CSCF may verify the IMSI/IMEI provided by the PCRF in step 7b against the IMSI/IMEI derived from the IMPI provided by the UE, prior to accepting the SIP REGISTER message.

 The UE and the network must support GIBA to be able to perform the next step.

10. P-CSCF accepts the registration with 200 OK and provides a tel-URI based on the MSISDN (if available) received from PCRF in step 7b to the UE in P-associated-URI header. From the UE point of view, the procedure is the same as specified for GIBA (GPRS-IMS bundled authentication) procedures in TS 24.229 [10].

11. UE then attempts an IMS emergency session by sending a SIP INVITE (UserID-3) message. UserID-3 is set to UE's public identity (i.e. MSISDN as Tel-URI received in step 10).

12. The P-CSCF verifies whether the UserID-3 indicated in the SIP INVITE message complies with the tel-URI that was provided to the UE. If compliant, P-CSCF forwards the SIP INVITE towards the PSAP including a callback parameter (CallBackPar) in the form of TEL-URI derived from the MSISDN received in step 7. The procedure stops here.

If the network has indicated that it supports anonymous IMS emergency sessions in either the 403 or 420 response in step 8 and if the UE is able to interpret the indication it shall attempt an anonymous IMS emergency session (steps 13-15 in Figure 6.5.1.2-1). If the UE cannot interpret the indication, the UE may attempt an anonymous IMS emergency sessions as specified in existing specifications.

NOTE 2: In reference to TS 23.167 Annex H.5, the anonymous IMS emergency session occurs between the “First EMC Attempt” (if it is performed in the PS domain) and the “Second EMC Attempt”. If the anonymous IMS emergency session fails, the UE proceeds with the “Second EMC Attempt” as indicated in TS 23.167 Annex H.5.

13. Subsequent to the IMS registration failure the UE may attempt an unauthenticated IMS emergency session including an "anonymous user" parameter in the SIP INVITE message.

14. Upon reception of the SIP INVITE the P-CSCF either internally retrieves the one or more EPS-level identities and the MSISDN (if available) that were received in step 7b, or performs step 7 again.

NOTE 3: Netloc procedure can be triggered at this point. It shall be possible for stage 3 to combine the Netloc procedure with the procedure for retrieving the identities in step 14 altogether.

15. The P-CSCF forwards the SIP INVITE (UserID-4, CallBackPar) towards the PSAP. UserID-4 is derived from one of the EPS-level identities received in step 7b. CallBackPar in the form of TEL-URI is derived from the MSISDN received in step 7b. The procedure stops here.

When the IMS registration fails, if the UE does not attempt an anonymous IMS emergency session, or if the anonymous IMS emergency session fails, the UE attempts an emergency call in the CS domain as specified in TS 23.167 clause 4.1 (step 16 in Figure 6.5.1.2-1).

16. Subsequent to the IMS registration failure in step 8 or subsequent to an anonymous SIP INVITE attempt the UE may attempt an emergency call in the CS domain.

### 6.5.2 Impacts on existing nodes and functionality

The impacted 3GPP nodes are the following:

P-CSCF:

- If the same P-CSCF handles emergency calls for both LBO and S8HR roaming architecture, the P-CSCF needs to be configured to know with which VPLMNs S8HR roaming agreement is used.

- P-CSCF needs to retrieve the IMSI/IMSI-unauthenticated indicator (if available)/IMEI and the MSISDN (if available) for an inbound roamer from the PCRF.

- For supporting Steps 9-12, P-CSCF accepts the SIP REGISTER message without authenticating the user. with the HPLMN IMS, i.e. the P-CSCF needs to support the GIBA procedure over Gm as defined in TS 24.229 [10].

- The P-CSCF may include an indication whether emergency IMS sessions are supported in the 403 or 420 response.

- The P-CSCF may verify IMSI/IMEI in SIP register against the IMSI/IMEI provided by the PCRF.

- The P-CSCF verifies the source IP address against the IP address used in specific headers in the REGISTER message.

PCRF:

- PCRF needs to provide IMSI/IMSI-unauthenticated/IMEI over Rx to the P-CSCF.

- PCRF needs to receive the IMSI-unauthenticated indicator (if available) over Gx.

PGW:

- For supporting Steps 9-12, all PGWs supporting emergency PDN connection for inbound roamers with S8HR roaming agreement shall implement measures to prevent source IP address spoofing as specified in Annex T.6 of TS 33.203 [x]. as required for GIBA authentication in TS 33.203 [12].

UE:

- To enable deterministic behaviour from UE to perform anonymous emergency call under the control of the serving network, UEs are required to interpret the indication whether anonymous IMS emergency sessions are supported in the serving network.

- Steps enclosed in block A in Figure 6.5.1.2-1 are possible only for UEs supporting the GIBA procedure defined in TS 24.229 [10] as part of the emergency IMS registration procedure.

HSS:

- The EPS user profile needs to contain exactly one MSISDN, which needs to be the same as in the IMS profile, in order to obtain the same result as current IMS Emergency sessions procedures.

### 6.5.3 Solution Evaluation

This solution applies when the user is allocated exactly one MSISDN for voice service. Other forms of Public User Identities cannot be used.

\*\*\*\*\* End of Change # 1 \*\*\*\*\*

\*\*\*\*\* Start of Change # 2 \*\*\*\*\*

# 8 Conclusions

For Key Issue 1a (How to handle UE's IMS emergency registration) and Key Issue 1b (How to support PSAP callback):

- Solution #5 captured in clause 6.5 is the selected solution.

 The part of Solution #5 which deals with the optimization where the network (P-CSCF) provides a new indication to the UE to perform anonymous IMS emergency session and impacted UE behaviour is applicable to IMS emergency sessions for both LBO and S8HR scenarios. Hence, normative changes for this part will be captured as part of TEI14.

For Key Issue 2 - Handling of non UE detectable Emergency Session:

- Solution #1 with option c) (possibly as described in Solution #1a: How P-CSCF can detect emergency numbers in a VPLMN”) for inter-operator database query is selected. This can be complemented with local configuration as in option a), with a limited number of roaming partners (e.g. bordering countries) and where option c is not used for these cases.

NOTE: When a serving network activates an S8HR roaming agreement it is recommended that all local emergency call numbers (including those for non-standardized emergency services) are downloaded during the EPS Attach procedure to the UEs camping on E-UTRAN, in order to ensure that local emergency call numbers are known to the UEs. This helps to reduce the number of non-UE detected emergency call numbers even for those PLMNs where only a subset of the local emergency call numbers can be downloaded to the UEs.

For Key Issue 3 - Determination of the ID of the visited PLMN at IMS Entities in HPLMN:

- Solution #6 as captured in Section 6.6 is the selected solution.

For Key Issue 4 - Local Number Translation and Routing:

- Solution #2 Local Number Translation captured in Section 6.2 is the selected solution.

 With regard to the aspect of key issue #4 regarding numbers not routable from international sources, how the HPLMN translates these numbers to international routable numbers is not specified by 3GPP. If translation of such numbers to international routable numbers is needed, then the HPLMN shall deploy an implementation specific NNI to the VPLMN (or other 3rd party in the visited country) so that these calls can be routed to the correct destination.

The solutions selected above provide the architecture enhancements required to support S8 home routed roaming architecture for VoLTE. Normative specification based on above selected solutions should proceed. Potential impacted stage 2 specifications are as follows (list is not exhaustive)

- TS 23.401 [7]

- TS 23.228 [8]

- TS 23.167 [9]

- TS 23.203[11] (if needed)

\*\*\*\*\* End of Change # 2 \*\*\*\*\*