**3GPP TSG-SA3 Meeting #104-e *S3-212478-r2***

**e-meeting, 16 - 27 August 2021** Revision of S3-21xxxx

**Source: InterDigital**

**Title: TR 33.847 Update for solution #10**

**Document for: Approval**

**Agenda Item: 5.9**

# 1 Decision/action requested

***It is proposed to approve this pCR for inclusion in TR 33.847.***

# 2 References

# 3 Rationale

The contribution proposes to address the following ENs in clause 6.10.2.2 and adds text to the evaluation:

Editor's note: When there is a KAMF (option 2), how to deal with desynchronization of K\_AMF is FFS.

Editor's note: How 5G-GUTI reallocation and Registration Update is performed when Remote UE is transferred to Relay’s AMF (option 2) is FFS.

# 4 Detailed proposal

It is proposed to approve the following changes for inclusion in TR 33.847.

\*\*\* BEGIN OF CHANGES \*\*\*

## 6.10 Solution #10: Authorization and security with UE-to-Network relay using Remote UE network primary authentication

### 6.10.1 Introduction

The contribution proposes a solution to address the following Key Issues:

- KI #3: Security of UE-to-Network Relay

- KI #4: Authorization in the UE-to-Network relay scenario

- KI #5: Privacy protection over the UE-to-Network Relay

- KI #9: Key management in 5G Proximity Services for UE-to-Network relay communication

- KI #12: Security of one-to-one communication over PC5

This solution builds on top of common high-level principles from existing solution #46 and solution #47 specified in TR 23.752 [2]. These solutions address Remote UE and UE-to-Network authorization aspects in the case of L3 relay. This solution leverages a Remote UE primary authentication run to establish keys used to secure the PC5 link between the Remote UE and the UE-to-Network relay. If the Remote UE has already successfully performed a primary authentication with the network prior to connecting with the relay, the solution enables the Remote UE to reuse its 5G native security context to be authorized and establish a secure connection via the UE-to-Network relay.

This solution assumes that the Remote UE selects a relay based on the connectivity service (e.g., S-NSSAI, DNN) that the relay can provide. The Remote UE learns about the connectivity service as part of the discovery procedure. It is assumed that the relay's Allowed NSSAI includes the S-NSSAIs needed to provide the connectivity service. The UE-to-Network relay either has a PDU session or is able to establish a new one without having to request a S-NSSAI (same assumption as solution #6 in TR 23.752 [2]). Therefore, in the context of the connectivity service provided by the relay, the AMF serving the relay is always able to serve the Remote UE.

### 6.10.2 Solution details

#### 6.10.2.1 Connection with UE-to-Network relay using Remote UE network primary authentication via the UE-to-Network relay

The procedure for Authorization and security with UE-to-Network relay using Remote UE network primary authentication is depicted in Figure 6.10.2.1-1.



Figure 6.10.2.1-1: Procedure for Authorization and security with UE-to-Network relay using Remote UE network primary authentication

0. The Relay UE is registered and authorized to operate as a UE-to-Network relay.

1. The Remote UE sends a Direct Communication request message to the Relay UE. The Remote UE includes its SUCI in the message to request the UE-to-Network relay service. The Remote UE also provides its security capabilities and security policy as in TS 33.536[8]. If the Remote UE is reconnecting to the same Relay UE and is already authenticated and authorized for relay communication via that Relay UE, it includes the Krelay ID (instead of SUCI) established during the previous connection using this procedure. If the Relay UE has the Krelay and Krelay ID it skips steps 2 to 12, otherwise the Relay UE rejects the connection request.

NOTE 1:Krelay and Krelay ID are reused during reconnection the same way as KRNP and KRNP ID in TS 33.536[8]. In case of reconnection with the relay, privacy protection of Krelay ID procedure reuses the same mechanism used for KNRP ID as described in TS 33.536 [8], clause 5.3.3.2.

2. The Relay UE sends a NAS Relay Authorization request message to its serving AMF. The Relay UE includes the Remote UE's SUCI in the message.

3. The Relay UE's AMF checks that the Relay UE is authorized to act as a Relay based on subscription information obtained during Relay UE's registration

4-8. The Relay UE's AMF initiates Remote UE authentication with Remote UE's AUSF according to existing primary authentication procedures. The authentication messages are exchanged transparently via the Relay UE. Authentication messages between AMF and AUSF and AMF and Relay UE include an indication that it is for a relayed authentication i.e. to authenticate Remote UE via Relay UE. The UDM does not need to be aware that the authentication is for a Remote UE as the AMF verifies (in subsequent step 10) with UDM that Remote UE is authorized to use UE-to-Network relaying.

9. Upon successful authentication of the network, the Remote UE derives a PC5 link root key Krelay and its Krelay ID from KAMF

NOTE 2:Krelay and its Krelay ID can be considered as equivalent to KRNP and KRNP ID in TS 33.536[8].

10. Upon successful authentication of the Remote UE, Relay UE's AMF checks with Remote UE's UDM that Remote UE is authorized to use UE-to-Network relaying. Upon successful authorization check, Relay UE's AMF registers with Remote UE's UDM as its Relay's AMF, providing the Relay UE identity (SUPI or GPSI).

11. Relay UE's AMF derives a PC5 link root key Krelay and its Krelay ID from KAMF asperformed by Remote UE in step 9.

12. Relay UE's AMF sends a NAS Relay Authorization response message to the Relay UE. The Relay UE's AMF includes the PC5 link root key Krelay and its Krelay ID in the message. The AMF may include the Remote UE identity (e.g., GPSI). The Relay UE stores the key and its id, Remote UE identity and associates them with the PC5 link with Remote UE.

13. The Relay UE initiates PC5 link security establishment with Remote UE based on PC5 link root key Krelay. The Relay UE derives PC5 session key Krelay-sess from Krelay, and confidentiality and integrity keys from Krelay-sess the same way KNRP-sess is derived from KNRP, and confidentiality and integrity keys from KNRP-sess in TS 33.536[8]. The Relay UE integrity protects the Direct Security Mode Command and includes parameters as in TS 33.536[8]. The Relay UE includes the Krelay ID to indicate that the PC5 security establishment should be based on Remote UE's primary authentication run.

14. The Remote UE checks that the received Krelay ID matches the one derived in step 9. If the provided key id matches, then the Remote UE proceeds with PC5 session, confidentiality, and integrity keys derivation using Krelay as the PC5 link root key as performed by the Relay UE. The Remote UE performs security checks of the Direct Security Mode Command message as in TS 33.536[8].

15. The Remote UE sends integrity and confidentiality protected Direct Security Mode Complete message to Relay UE as in TS 33.536[8].

16. Procedure continues as per L3 relay setup procedure as defined in TR 23.752 [2] (e.g., in step 3-4 in solution#6, and if N3IWF is used with solution#23 subsequent steps 5-6).

#### 6.10.2.2 Connection with UE-to-Network relay using the 5G native security context of the Remote UE

The procedure for Authorization and security with UE-to-Network relay using the 5G native security context of the Remote UE is depicted in Figure 6.10.2.2-1.

Figure 6.10.2.2-1: Procedure for Authorization and security with UE-to-Network relay using 5G native security context of Remote UE

0. The Remote UE has registered with the network and established a 5G native security context with a source AMF. The Relay UE is registered and authorized to operate as a relay.

1. The Remote UE performs a discovery procedure with a Relay UE and decides to connect with the Relay UE using its 5G native security context.

2. If the Remote UE is aware of the PLMN ID of the Relay UE's serving PLMN, the Remote UE verifies that its 5G native security context was established with the Relay UE's serving PLMN before sending its 5G-GUTI to the Relay UE. If the PLMN ID of the Relay UE's serving PLMN and the PLMN ID part in its 5G-GUTI are different, the Remote UE sends its SUCI instead (as described in clause 6.10.2.1, step 1). If the Remote UE is not aware of the PLMN ID of the Relay UE's serving PLMN, the Remote UE may choose to send no identifier (i.e. neither SUCI nor 5G-GUTI). If a 5G-GUTI is sent, the Remote UE sends a DCR message to the Relay UE including Remote UE's core network identity (e.g., 5G-GUTI), ngKSI identifying the KAMF being used, the Remote UE's NAS security capabilities, and current UL NAS COUNT. These parameters may be included in a message integrity protected using Remote UE's 5G native security context.

NOTE 1: Remote UE has the option to use the knowledge of Relay PLMN ID to select a Relay (e.g., select Relay 1 with same PLMN over Relay 2 with different PLMN). This option of PLMN ID based selection of Relay is to be confirmed with SA2.

3. If the request includes a 5G-GUTI, the Relay UE checks whether the PLMN ID of its serving PLMN and in Remote UE's 5G-GUTI are equal. If they are not equal, the Relay UE sends an Identity Request message to the Remote UE including Relay UE's serving PLMN ID, to obtain the Remote UE's identifier (SUCI or 5G-GUTI). If the Remote UE provides a SUCI in the Identity Response, Relay UE proceeds with the procedure as described in clause 6.10.2.1, from step 2. Otherwise, the Relay UE sends the Remote UE's 5G-GUTI and integrity protected message from Remote UE to its serving AMF (target AMF) in a NAS request message.

4. The target AMF checks that Relay UE is authorized to act as a relay.

5. The target AMF identifies the source AMF serving the Remote UE using the provided 5G-GUTI. If the source and target AMFs are different, the target AMF sends a request message to the source AMF to obtain security parameters for the Remote UE. The target AMF includes the integrity protected message from Remote UE and Remote UE's identity received from the Relay UE. The target AMF indicates that the access type and reason for the request are for relay access. If the source and target AMFs are the same (i.e., Remote UE has registered with target AMF), the target AMF retrieves the Remote UE’s context directly from its local storage instead.

6. [option 1] The source AMF locates the Remote UE's security context using the received Remote UE's 5G-GUTI. The source AMF checks the integrity protection of the message from the Remote UE using the Remote UE's security context. If the security checks are successful, the source AMF derives a Krelay and Krelay ID from KAMF identified by the ngKSI. [option 2] Alternatively, the source AMF may generate a new 5G security context. The derivation of the new KAMF is specified in TS 33.501 [14] (Annex A.13). The source AMF sends a response message to the target AMF that includes the Remote UE SUPI. The message may include a Krelay and Krelay ID, a new 5G security context to be used for Remote UE with a KAMF change indication or current Remote UE's 5G security context, and Remote UE's context.

NOTE 2: In the first option, the Remote UE's registration remains with Remote UE's (source) AMF which provides Relay UE's (target) AMF with Krelay and Krelay ID (and SUPI). In the second option, the Remote UE context is transferred to the Relay UE's AMF, with a KAMF change (using the same mechanisms as in TS 33.501[14], clause 6.9.2.3.3). In that case, the target AMF derives Krelay and Krelay ID. Source AMF uses its local policy to determine whether to transfer the Remote UE context and perform horizontal key derivation. If the Remote UE’s 5G security context is moved from the source AMF to the target AMF, then if the Remote UE has simultaneously access to the 3GPP network then this connection with the source AMF (of Remote UE) will be dropped. Following the context transfer, source and target AMF registration update with UDM is handled according to existing AMF change mechanisms (see TS 23.502, clause 4.2.2.2.2).

NOTE 3: Whether Option 2 (with Remote UE context transfer to Relay's AMF) can be used is to be confirmed with SA2.

7. The target AMF checks from Remote UE's context (e.g., obtained from source AMF or locally) or with Remote UE's UDM (e.g., using SUPI provided by source AMF) for authorization to use the Relay UE. If not provided by the source AMF, the target AMF derives a Krelay and Krelay ID using Remote UE's security context.

8. The target AMF sends a NAS response message to the Relay UE that includes the Remote UE id (e.g., GPSI), Krelay and Krelay ID. [Option 2] The message may include a KAMF change flag and new ngKSI if a new security context was generated by source AMF in previous step.

9. The Relay UE sends a Direct Security Mode Command message to the Remote UE that includes Krelay ID and, if provided by the target AMF, KAMF change flag and new ngKSI. The message is integrity protected using security key derived based on Krelay.

10. If the KAMF change flag is set, the Remote UE derives a new KAMF from the KAMF indicated by the value of ngKSI. The Remote UE derives a Krelay and Krelay ID from the existing KAMF or the newly derived KAMF. The Remote UE verifies the DSMC message security using security derived based on Krelay. A successful security verification indicates to the Remote UE that the Relay UE is authorized to provide the relay service for Remote UE. The new KAMF is derived the same way as described for NAS SMC procedure when KAMF change flag is set as described in TS 33.501 [14] clause 6.7.2 step 2a and Annex A.13. If the verification of the DSMC message is unsuccessful, the Remote UE replies with a Direct Security Mode Reject message. In that case, Remote UE discards the new security context if it was derived, continues the use of the existing security context, and the Relay UE aborts the link establishment procedure.

Editor's note: When there is a KAMF change (option 2), how to deal with desynchronization of K\_AMF is FFS.

11. If the security verification is successful, the Remote UE sends a Direct Security Mode Complete message to the Relay UE with security protection (integrity, confidentiality) using security keys derived based on Krelay. The Relay UE verifies the Direct Security Mode Complete message security using security derived based on Krelay. A successful security verification indicates to the Relay UE that the Remote UE is authorized to use the relay service provided by Relay UE.

12. [Option 2] If a new KAMF derivation was indicated (in step 9), the Relay UE sends a NAS complete message to inform the AMF of the key establishment result. If the Relay indicates a successful KAMF derivation then AMF registers with Remote UE's UDM causing UDM to deregister source AMF and removal or Remote UE context (as per TS 23.502, clause 4.2.2.2.2). If the KAMF derivation fails (e.g., verification of DSMC fails) then the PC5 link setup is aborted and the Remote UE discards the new security context if it was derived and continues the use the existing security context.

13. The Remote UE receives a DCA message completing the successful PC5 link establishment.

NOTE 4: The purpose of 5G GUTI reallocation is to preserve the privacy of the subscription temporary identifier. In the above procedure using first option (i.e., Remote UE context remains with source AMF), the Remote UE transmits its 5G-GUTI only once (in the DCR). In that case, 5G-GUTI re-allocation by source AMF over Uu is performed as per TS 33.501 [14], clause 6.12.3. If the Remote UE has already a prior connection with the Relay it can send the Krelay ID (see 6.10.2.1 step 1) instead of 5G-GUTI. An attacker cannot track the Remote UE using the 5G-GUTI during communication with the Relay UE. Therefore, 5G-GUTI re-assignment is not necessary for this procedure for these scenarios. For 5G-GUTI reallocation when option 2 is used, the Remote UE triggering a connection via a Relay using DCR is considered to be similar to the case of "Service Request message triggered from the UE not triggered by the network" in TS 33.501 [14] clause 6.12.3. In that case, it is left to implementation (i.e., not required) to re-assign a 5G-GUTI. For Registration Update (option 2), the Remote UE is considered to be in a "connected" state and Relay UE's AMF is aware of Remote UE whereabouts as long as a PC5 link between the Remote UE and the Relay UE is up. Therefore, it is not necessary for the Remote UE to perform either mobility or periodic Registration Update procedures for the Relay UE's AMF to keep track of the Remote UE.

Editor's note: How 5G-GUTI reallocation and Registration Update is performed when Remote UE is transferred to Relay’s AMF (option 2) is FFS.

#### 6.10.2.3 Key hierarchy, key derivation, and distribution

The Key Hierarchy for PC5 unicast link with UE-to-Network relay is shown in Figure 6.10.2.3-1. Details for Krelay andKrelay ID derivation are described next.

Overall, the keys Krelay, Krelay-sess, Krelay-enc, Krelay-int serve a similar function respectively asKNRP, KNRP-sess, NRPEK, and NRPIK in TS 33.536 [8] clause 5.3.3.1.2.1.

The key derived for access via UE-to-Network relay is Krelay, which is used by UE-to-Network relay and Remote UE to derive Krelay-sess.

Krelay-sess is derived from Krelay using noncesexchanged during the PC5 link establishment similarly to how KNRP-sess is derived fromKNRP in Annex A.3 of TS 33.536 [8].



Figure 6.10.2.3-1: Key Hierarchy for PC5 unicast link with UE to Network relay

When deriving the key Krelay from KAMF and the uplink NAS COUNT in the UE and the AMF the following parameters are used to form the input S to the KDF.

- FC = 0xXX

- P0 = Uplink NAS COUNT

- L0 = length of uplink NAS COUNT (i.e. 0x00 0x04)

- P1 = Access type distinguisher

- L1 = length of Access type distiguisher (i.e. 0x00 0x01)

The access type distinguisher is set to the value for non-3GPP (0x02) (see Annex A.9 in TS 33.501 [14]).

The input key KEY is KAMF.

When deriving the Krelay ID from KAMF, the following parameters are used to form the input S to the KDF:

- FC = 0xYY;

- P0 = "R-KID";

- L0 = length of "R-KID"; (i.e. 0x00 0x05)

- P1 = SUPI;

- L1 = length of SUPI.

The input key KEY is KAMF.

SUPI has the same value as parameter P0 in Annex A.7.0 of TS 33.501 [14].

#### 6.10.2.4 Remote UE authorization revocation/re-authentication

After a successful authorization of Remote UE to use the relay, the Relay UE's AMF may initiate a re-authentication/authorization of the Remote UE at any time. For example, during Relay UE mobility with a change of AMF, the new Relay UE's AMF obtains from the old Relay's AMF the Relay UE context that includes Remote UE information (Krelay, Krelay ID, etc) as described in clause 6.10.2.1. The new AMF may decide to initiate a re-authentication/authorization of Remote UE and derive new Krelay, Krelay ID as described in clause 6.10.2.1 steps 4-8 and 11. When a re-authentication/authorization is performed, the Remote UE generates a new Krelay, Krelay ID and the relay obtains the same from its serving AMF in a NAS message. The Relay UE replaces the old Krelay, Krelay ID with the new ones and initiates a re-key procedure over the PC5 link with the Remote UE to generate fresh new Krelay-session, Krelay-enc, Krelay-int similar to the procedure described in TS 33.536 [8] clause 5.3.3.1.4.4 for generating a fresh KNRP-sess, etc.

After a successful authorization of Remote UE to use the relay, the Relay UE's AMF may initiate revocation of authorization of the Remote UE at any time. For example, the AMF may receive an update message from the Remote UE's UDM to revoke authorization for the Remote UE to use the relay (e.g., due to Remote UE subscription change). The message includes the identity of the Relay UE serving the Remote UE as registered by the AMF in clause 6.10.2.1 step 10. The AMF sends a NAS message to the Relay UE to revoke authorization for the Remote UE to use the relay. The AMF may include the associated Krelay ID and the Remote UE identity (e.g., GPSI). The Relay UE locates the PC5 link context based on Krelay ID (or Remote UE's GPSI) and initiates a link release procedure for the PC5 link with the Remote UE.

### 6.10.3 Evaluation

The solution fulfils requirements of KI#3 (secure means to establish a PC5 link) using keys from the primary authentication to derive PC5 related keys. This solution can be combined with a solution using N3IWF (e.g., sol#19) to fulfil the second requirement of KI#3 (end to end security).

NOTE: The third requirement of KI#3 (i.e., security for path switch) is not considered within Rel-17 timeframe in line with TR 23.752 [2] conclusion ( clause 8.6).

The solution fulfils the requirements of KI#4 (authorization of Remote UE/ UE-to-Network relay) using a network-controlled authorization procedure based on primary authentication of Remote UE (building on TR 23.752 [2] sol#47 principles).

The solution fulfils the requirements of KI#9 (PC5 key management for relay communication) by supporting derivation /distribution of PC5 related keys based on keys from the primary authentication, using existing 5GC entities (AMF, AUSF).

The solution fulfils the requirements of KI#12 (Security of one-to-one communication over PC5) including support of the Remote UE out of coverage scenario by reusing PC5 link communication security procedure as defined in TS 33.536 [8].

Editor's note: Whether all or part of KI#12 requirements are fulfilled is FFS.

This solution requires a new relayed primary authentication procedure (aka "network controlled authorization" based on TR 23.752 [2] sol#47) to enable Remote UE to perform primary authentication with the AUSF of Remote UE via the AMF of Relay UE.

In this solution, the UE-to-Network relay 's AMF, is responsible for PC5 link root key Krelay and its Krelay ID derivation from KAMF, as the Remote UE. The AMF stores Remote UE information (Remote UE id, PC5 link root key) in the Relay UE context. The Relay UE uses the PC5 root key and associated id to establish the security of the PC5 link with the Remote UE.

Other impact on 5GC and existing procedure is documented in TR 23.752 [2] sol#47, clause 6.47.3. In addition and as an optimization to skip primary authentication, the Remote UE may optionally provide its 5G-GUTI when connecting for relayed communication authorization.

Editor’s Note: Further evaluation is FFS.

\*\*\* END OF CHANGES \*\*\*