**3GPP TSG-SA3 Meeting #105e *draft\_S3-214211-r3***

**e-meeting, 08 – 19 November 2021**

**Source: Ericsson**

**Title: ProSe: New solution PC5 anchor key generation via GBA Push**

**Document for: Approval**

**Agenda Item: 5.7**

# 1 Decision/action requested

***This paper proposes a new solution regarding PC5 anchor key generation via GBA Push.***

# 2 References

[1] 3GPP TR 33.847 "Study on security aspects of enhancement for proximity based services in the 5G System (5GS)"

[2] 3GPP TR 23.752 "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)"

# 3 Rationale

This paper proposes a new solution that enable 5G PKMF to generate PC5 anchor keys via GBA Push.

This solution reuses the solution from LTE Prose. According to TS 33.303, there could be two deployment options: standalone BSF deployed by HPLMN of Remote UE or BSF co-located with 5GPKMF (of Remote UE).

Similar deployment can be used in 5GC as well. Two alternative solutions are proposed:

* standalone BSF deployed by HPLMN of Remote UE:
	+ If the 5G PKMF supports the Zpn interface to the BSF of the Remote UE, the 5G PKMF shall request a GBA Push Info (GPI – see TS 33.223) for the Remote UE from the BSF. When requesting the GPI, it includes a KPC5 key ID in the P-TID field. On reception of the GPI, the 5G PKMF uses Ks(\_ext)\_NAF as the KPC5 key. ‘Get GPI request’ in the solution flow refers to GBA Push as described in TS 33.223.

Note: If the 5G PKMF support the SBI interface to the BSF of the Remote UE, the 5G PKMF can also request the GPI via SBI interface.

* BSF co-located with 5GPKMF (of Remote UE) or BSF functionality is integrated with 5GPKMF:
	+ If the 5G PKMF support the PC4a interface to the HSS of the Remote UE, then the 5G PKMF shall request an GBA Authentication Vector (AV) for the Remote UE. On receiving the AV, the 5G PKMF locally forms the GPI including a KPC5 key ID in the P-TID field and sets KPC5 key as above. ‘Get GBA AV request’ in the solution flow refers to AV retrieval in PC4a interface as described in TS 33.303.

Note: If the 5G PKMF support the SBI interface to the HSS/UDM of the Remote UE, the 5G PKMF can also request the GBA AV via SBI interface as described in TS 33.220.

# 4 Detailed proposal

It is proposed to add the new solution in the study in [1].

**\*\*\*\*** START OF CHANGES **\*\*\*\***

# 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 23.752: "Study on system enhancement for Proximity based Services (ProSe) in the 5G System (5GS)".

[3] 3GPP TS 22.278: "Service requirements for the Evolved Packet System (EPS)".

[4] 3GPP TS 22.261: "Service requirements for the 5G system; Stage 1".

[5] 3GPP TS 23.303: "Proximity-based services (ProSe); Stage 2".

[6] 3GPP TS 33.303: "Proximity-based Services (ProSe); Security aspects".

[7] 3GPP TS 33.535: "Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS)".

[8] 3GPP TS 33.536: "Security aspects of 3GPP support for advanced Vehicle-to-Everything (V2X) services".

[9] 3GPP TS 23.287: "Architecture enhancements for 5G System (5GS) to support Vehicle-to-Everything (V2X) services".

[10] 3GPP TS 23.502: "Procedures for the 5G System (5GS); Stage 2".

[11] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[12] 3GPP TS 33.220: "Generic Authentication Architecture (GAA), Generic Bootstrapping Architecture (GBA)".

[13] 3GPP TS 33.222: "Generic Authentication Architecture (GAA); Access to network application functions using Hypertext Transfer Protocol over Transport Layer Security (HTTPS)".

[14] 3GPP TS 33.501: "Security architecture and procedures for 5G system".

[15] 3GPP TS 23.501: "System Architecture for the 5G System".

[16] 3GPP TS 23.304: "Proximity based Services (ProSe) in the 5G System (5GS)".

[17] 3GPP TS 23.503: " Policy and charging control framework for the 5G System (5GS); Stage 2".

[xx] 3GPP TS 33.223: "Generic Bootstrapping Architecture (GBA) Push function".

**\*\*\*\*** NEXT CHANGE **\*\*\*\***

## 6.Y Solution #Y: PC5 anchor key generation via GBA Push

### 6.Y.1 Introduction

This solution addresses key issue#4, and key issue #9.

This solution is to provide means for Remote UE to establish PC5 keys while out of 3GPP coverage.

The 5G PKMF in this solution can be a NF (network function) which resides in Remote UE’s HPLMN for commercial service or managed by a public safety operator and located outside of the 3GPP network for public safety use case.

The solution is based on the procedures of solution #21 and GBA push solutions of EPC Prose as specficed in TS 33.303.

There are two deployment options:

* standalone BSF deployed by HPLMN of Remote UE:
	+ If the 5G PKMF supports the Zpn interface to the BSF of the Remote UE, the 5G PKMF shall request a GBA Push Info (GPI – see TS 33.223) for the Remote UE from the BSF. When requesting the GPI, it includes a KPC5 key ID in the P-TID field. On reception of the GPI, the 5G PKMF uses Ks(\_ext)\_NAF as the KPC5 key. ‘Get GPI request’ in the solution flow refers to GBA Push as described in TS 33.223.

NOTE: If the 5G PKMF support the SBI interface to the BSF of the Remote UE, the 5G PKMF can also request the GPI via SBI interface.

* BSF co-located with 5GPKMF (of Remote UE) or BSF functionality is integrated with 5GPKMF:
	+ If the 5G PKMF support the PC4a interface to the HSS of the Remote UE, then the 5G PKMF shall request an GBA Authentication Vector (AV) for the Remote UE. On receiving the AV, the 5G PKMF locally forms the GPI including a KPC5 key ID in the P-TID field and sets KPC5 key as above. ‘Get GBA AV request’ in the solution flow refers to AV retrieval in PC4a interface as described in TS 33.303.

NOTE: If the 5G PKMF support the SBI interface to the HSS/UDM of the Remote UE, the 5G PKMF can also request the GBA AV via SBI interface as described in TS 33.220.

### 6.Y.2 Solution details



Figure 6.Y.2.1-1: PC5 anchor key generation via GBA Push

The remote UE is provisioned with 5G PKMF address and the discovery security materials when it is in coverage. If the UE does not have valid discovery security materials, the Remote UE needs to connect to the PKMF and obtain fresh ones to use the UE-to-Network relay services.

NOTE: The procedure is described for a scenario that the 5G PKMF of the remote UE and the 5G PKMF of the UE-to-network relay are deployed in their HPLMN accordingly for commercial use case.

If there is only one 5G PKMF deployed and managed by a public safety operator and located outside of the 3GPP network for public safety use case, the remote UE and the UE-to-network relay can use pre-configured information and are served by a single 5G PKMF which takes the role of the 5G PKMF of the remote UE and the 5G PKMF of the UE-to-network relay, and the inter-5G PKMF message exchanges are not needed. In the procedure flow, it is assumed that 5G PKMF-1 takes this role.

Step 0a) The Remote UE gets the 5G PKMF-1 address from its 5G DDNMF and gets the discovery security material from the 5G PKMF-1.

Step 0b) The Relay UE gets the 5G PKMF-2 address from its 5G DDNMF and gets the discovery security material from the 5G PKMF-2.

Step 0c) The Remote UE gets the PC5 anchor key (KPC5 key, KPC5 key ID) from 5G PKMF-1 from its HPLMN when it is in coverage.

NOTE: Check more details of step 0 from UP based solutions addressing KI#3 in this document.

Step 1) The UE-to-network relay discovery is taken place on PC5 interface using either model A or model B discovery.

Step 2) The Remote UE sends a Direct Communication Request on PC5 interface. The Remote UE includes its HPLMN ID, the Nonce\_1 and the KPC5 key ID together with the Relay Service Code. The Remote UE’s HPLMN ID is used by the UE-to-network relay’s 5G PKMF-2 to find the 5G PKMF-1 in the Remote UE’s HPLMN.

Editor’s Note: Whether the DCR requires protection for using GBA Push functionality via relay is FFS.

Step 3) The UE-to-network Relay request PC5 communication keys from the 5G PKMF-2 (UE-to-network Relay) and includes the HPLMN ID of Remote UE, the KPC5 key ID, the Relay Service Code and Nonce\_1 in the Key Request message for PC5 communication.

Step 4) The 5G PKMF-2(UE-to-network Relay) forwards the Key Request message including the KPC5 key ID, the Relay Service Code and Nonce\_1 to the 5G PKMF-1(Remote UE).

Step 5-6) In case the Remote UE is authorized for PC5 communication, the 5G PKMF-1 (Remote UE) decides if it requires a new KPC5 key for this Remote UE. If so, the 5G PKMF-1 (Remote UE) proceeds one of the followings:

* Step 5a-5b: If the 5G PKMF-1 (Remote UE) supports the Zpn interface to the BSF of the Remote UE, the 5G PKMF-1 (Remote UE) requests a GBA Push Info (GPI – see TS 33.223[xx]) for the Remote UE from the BSF. When requesting the GPI, it includes a locally generated KPC5 key ID in the P-TID field.

If the 5G PKMF support the SBI interface to the BSF of the Remote UE, the 5G PKMF can also request the GPI via SBI interface as described in TS 33.223[xx].

On reception of the GPI, the 5G PKMF uses Ks(\_ext)\_NAF as the KPC5 key.

NOTE: 5G PKMF-1 can be deployed in the remote UE's HPLMN for commercial service or managed by a public safety operator and located outside of the 3GPP network for public safety use case.

* Step 6a-6c: If the 5G PKMF-1 (Remote UE) supports the PC4a interface to the HSS of the UE, then the 5G PKMF-1 (Remote UE) requests a GBA Authentication Vector (AV) for the Remote UE from the HSS (Remote UE).

If the 5G PKMF is co-located or integrated with BSF functionality (Remote UE) and supports the SBI interface to the HSS/UDM of the Remote UE, the 5G PKMF can also request the GBA AV via SBI interface as described in TS 33.220 [12].

On receiving the AV, the 5G PKMF locally forms the GPI including a KPC5 key ID in the P-TID field. The 5G PKMF uses Ks(\_ext)\_NAF as the KPC5 key.

NOTE: To support PC4a interface or collocate with BSF, 5G PKMF-1 can only be deployed in the remote UE's HPLMN.

Step 7) The 5G PKMF-1 generates a new KPC5-COM freshness parameter and a new key KPC5-COM key from at least the KPC5 key, Nonce\_1, Relay Service Code and the KPC5-COM freshness parameter.

Step 8) The 5G PKMF-1 includes the KPC5-COM freshness parameter, the KPC5-COM key and GPI (if available) in the Key Response message to the 5G PKMF-2.

Step 9) The 5G PKMF-2 forwards the Key Response message including the GPI (if available) to the UE-to-network Relay.

Step 10) The UE-to-network Relay generates a Nonce\_2 and KSESS key from the KPC5-COM key and Nonce\_2. The UE-to-network Relay initiates a Direct Security Mode Command integrity protected with KSESS-IK key generated from the KSESS key. The UE-to-network Relay includes the KPC5-COM freshness parameter together with calculated MAC and the Nonce\_2 and GPI (if available) in the Direct Security Mode Command message.

Handling of synchronisation failure (for details of synchronisation failures – see TS 33.102[42]) when UE processes the authentication challenge in the GPI is performed similarly to  clause 6.7.3.2.1.2 in TS 33.303

Step 11) If the Remote UE receives the message containing the GPI, it processes the GPI as described in TS 33.223[xx]. The Remote UE derives the KPC5 key and obtains the KPC5 key ID using the information in GPI. The Remote UE generates the KPC5-COM key in the same way as the 5G PKMF-1 in step 7 using the KPC5-COM freshness parameter. The Remote UE then generates the KSESS key from the KPC5-COM key and Nonce\_2.

Step 12) The UE-to-network Relay responds with a Direct Communication Accept on the PC5 interface.

### 6.Y.3 Evaluation

This solution resolves key issue #4 and key issue #9 for user plane based U2N relay security solution to enable 5G PKMF to generate PC5 anchor keys via GBA Push.

This solution is proposed both for commercial services and for public safety use case.

In this solution, which is similar to the ProSe solution in 4G, the 5G PKMF-1 (Remote UE) decides if it requires a new KPC5 key for this Remote UE, then the 5G PKMF-1 (Remote UE) can request either:

* a GBA Push Info (GPI – see TS 33.223[xx]) for the Remote UE from the BSF or
* a GBA Authentication Vector (AV) for the Remote UE from the HSS/UDM (Remote UE) and the 5G PKMF locally forms the GPI from the AV.

Based on GBA Push Info the 5G PKMF generates PC5 keys, as well does the Remote UE.

This solution needs support for GBA Push functionality in UE, PKMF, BSF.

Editor’s Note: Further Evaluation is FFS

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