|  |  |
| --- | --- |
| 3GPP TR 33.847 V0.1.0 (2020-08) | |
| Technical Report | |
| 3rd Generation Partnership Project;  Technical Specification Group Services and System Aspects;  Study on Security Aspects of Enhancement for Proximity Based Services in 5GS  (Release 17) | |
|  | |
|  |  |
|  | |
| The present document has been developed within the 3rd Generation Partnership Project (3GPP TM) and may be further elaborated for the purposes of 3GPP. The present document has not been subject to any approval process by the 3GPPOrganizational Partners and shall not be implemented. This Specification is provided for future development work within 3GPPonly. The Organizational Partners accept no liability for any use of this Specification. Specifications and Reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organizational Partners' Publications Offices. | |

|  |
| --- |
|  |
| ***3GPP***  Postal address  3GPP support office address  650 Route des Lucioles - Sophia Antipolis  Valbonne - FRANCE  Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16  Internet  http://www.3gpp.org |
| ***Copyright Notification***  No part may be reproduced except as authorized by written permission. The copyright and the foregoing restriction extend to reproduction in all media.  © 2020, 3GPP Organizational Partners (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC).  All rights reserved.  UMTS™ is a Trade Mark of ETSI registered for the benefit of its members  3GPP™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners LTE™ is a Trade Mark of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners  GSM® and the GSM logo are registered and owned by the GSM Association |

Contents

Foreword 5

Introduction 6

1 Scope 7

2 References 7

3 Definitions of terms, symbols and abbreviations 7

3.1 Definitions 7

3.2 Abbreviations 8

4 Security Aspects of 5G ProSe 8

4.1 Architecture assumption 8

4.1.1 Control Plane based architecture 8

4.2.1 User Plane based architecture 9

5 Key issues 9

5.1 Key Issue #1: Discovery message protection 9

5.1.1 Key issue details 9

5.1.2 Security threats 10

5.1.3 Potential security requirements 10

5.2 Key Issue #2: Key issue Keys in ProSe discovery scenario 10

5.2.1 Key issue details 10

5.2.2 Security threats 11

5.2.3 Potential security requirements 11

5.3 Key Issue #3: Security of UE-to-Network Relay 11

5.3.1 Key issue details 11

5.3.2 Security threats 12

5.3.3 Potential security requirements 12

5.4 Key issue #4: Authorization in the UE-to-Network relay scenario 12

5.4.1 Key issue details 12

5.4.2 Security threats 12

5.4.3 Potential security requirements 13

5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay 13

5.5.1 Key issue details 13

5.5.2 Security threats 13

5.5.3 Potential security requirements 13

5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay 13

5.6.1 Key issue details 13

5.6.2 Security threats 13

5.6.3 Potential security requirements 14

5.7 Key issue #7: Authorization in the UE-to-UE relay scenario 14

5.7.1 Key issue details 14

5.7.2 Security threats 14

5.7.3 Potential security requirements 14

5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay 14

5.8.1 Key issue details 14

5.8.2 Security threats 15

5.8.3 Potential security requirements 15

5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication 15

5.9.1 Key issue details 15

5.9.2 Security threats 16

5.9.3 Potential security requirements 16

5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF 16

5.10.1 Key issue details 16

5.10.2 Security threats 17

5.10.3 Potential requirements 17

5.X Key Issue #X: <Key Issue Name> 17

5.X.1 Key issue details 17

5.X.2 Security threats 17

5.X.3 Potential security requirements 17

6 Solutions 17

6.0 Mapping of Solutions to Key Issues 17

6.1 Solution #1: Solution for key management in 5G Proximity Services relay communication 18

6.1.1 Introduction 18

6.1.2 Solution details 18

6.1.3 Evaluation 20

6.2 Solution #2: Secure data transfer between UE and 5GDDNMF 20

6.2.1 Introduction 20

6.2.2 Solution details 20

6.2.3 Evaluation 21

6.Y Solution #Y: <Solution Name> 21

6.Y.1 Introduction 21

6.Y.2 Solution details 21

6.Y.3 Evaluation 21

7 Conclusions 21

Annex <X> (informative): Change history 21

For definitive guidance on drafting 3GPP TSs and TRs, see [3GPP TS 21.801](http://www.3gpp.org/DynaReport/21801.htm) supplemented by the 3GPP web page <http://www.3gpp.org/specifications-groups/delegates-corner/writing-a-new-spec>.

Ensure all blue guidance text is removed before submitting the TS/TR to the TSG for approval.

# Foreword

This clause is mandatory; do not alter the text in any way other than to choose between "Specification" and "Report".

This Technical Report has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

x the first digit:

1 presented to TSG for information;

2 presented to TSG for approval;

3 or greater indicates TSG approved document under change control.

y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

z the third digit is incremented when editorial only changes have been incorporated in the document.

In drafting the TS/TR, pay particular attention to the use of modal auxiliary verbs! TRs shall not contain any normative provisions.

In the present document, modal verbs have the following meanings:

**shall** indicates a mandatory requirement to do something

**shall not** indicates an interdiction (prohibition) to do something

The constructions "shall" and "shall not" are confined to the context of normative provisions, and do not appear in Technical Reports.

The constructions "must" and "must not" are not used as substitutes for "shall" and "shall not". Their use is avoided insofar as possible, and they are not used in a normative context except in a direct citation from an external, referenced, non-3GPP document, or so as to maintain continuity of style when extending or modifying the provisions of such a referenced document.

**should** indicates a recommendation to do something

**should not** indicates a recommendation not to do something

**may** indicates permission to do something

**need not** indicates permission not to do something

The construction "may not" is ambiguous and is not used in normative elements. The unambiguous constructions "might not" or "shall not" are used instead, depending upon the meaning intended.

**can** indicates that something is possible

**cannot** indicates that something is impossible

The constructions "can" and "cannot" are not substitutes for "may" and "need not".

**will** indicates that something is certain or expected to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**will not** indicates that something is certain or expected not to happen as a result of action taken by an agency the behaviour of which is outside the scope of the present document

**might** indicates a likelihood that something will happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

**might not** indicates a likelihood that something will not happen as a result of action taken by some agency the behaviour of which is outside the scope of the present document

In addition:

**is** (or any other verb in the indicative mood) indicates a statement of fact

**is not** (or any other negative verb in the indicative mood) indicates a statement of fact

The constructions "is" and "is not" do not indicate requirements.

# Introduction

This clause is optional. If it exists, it shall be the second unnumbered clause.

# 1 Scope

The technical report to study the security and privacy aspects of proximity based services (including public safety and commercial proximity services) in 5G system and ensure the security solutions are aligned with the work in SA2 (i.e. in TR 23.752 [2]) and SA1 (i.e. in TS 22.278 [3] and TS 22.261 [4]). The work is comprised of the following parts:

* Study the security and privacy key issues, threats and requirements of proximity based services in 5G system.
* Elaborate on the potential security solutions to cover these requirements.

Both non-roaming and roaming scenarios will be considered.

# 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".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in 3GPP TR 21.905 [1] and the following apply. A term defined in the present document takes precedence over the definition of the same term, if any, in 3GPP TR 21.905 [1].

**5G ProSe UE-to-Network Relay:** A UE that provides functionality to support connectivity to the network for Remote UE(s).

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in 3GPP TR 21.905 [1] and the following apply. An abbreviation defined in the present document takes precedence over the definition of the same abbreviation, if any, in 3GPP TR 21.905 [1].

5GC 5G Core

ProSe Proximity-based Services

5G DDNMF 5G Direct Discovery Name Management Function

AF Application Function

AMF Access and Mobility management Function

AS layer Access Stratum layer

NG Next Generation

NG-RAN Next Generation RAN

NGAP NG Application Protocol

NR New Radio (5G)

PCF Policy Control Function

RAN Radio Access Network

RAT Radio Access Technology

UDM Unified Data Management

# 4 Security Aspects of 5G ProSe

Editor’s Note: This clause contains a high-level overview of the 5G ProSe features, the security aspects and the potential impacts on the current Rel-17 security mechanisms.

## 4.1 Architecture assumption

### 4.1.1 Control Plane based architecture

The Control Plane based architecture has been captured in TR 23.752[2] Annex B.



Figure 4.1.1-1: Control Plane based architecture

In Figure 4.1.1-1, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from architecture point of view to the DDNMF part of ProSe Function as defined in TS 23.303[5].

Control Plane based 5G Prose architecture only reuses the PC5 interface comparing to the Prose Architecture defined in TS 23.303[5]. This means the UE will use NAS message to get discovery parameters for open discovery or restricted discovery.

### 4.2.1 User Plane based architecture

The User Plane based architecture has been captured in TR 23.752[2] Annex B.



Figure 4.2.1-1: User Plane based architecture

In Figure 4.2.1-1, 5G DDNMF is introduced into 5GC as a new network function. 5G DDNMF has similar functions from architecture point of view to the DDNMF part of ProSe Function as defined in TS 23.303[5].

User Plane based 5G Prose architecture tries to reuse Prose reference points defined in TS 23.303[5], especially for PC2 and PC3 reference points.

# 5 Key issues

Editor’s Note: This clause contains all the key issues identified during the study.

## 5.1 Key Issue #1: Discovery message protection

### 5.1.1 Key issue details

The Open ProSe direct discovery procedure is used for a UE to discover or be discovered by other UE(s) in proximity over the PC5 interface. The UE can discover other UE(s) with interested application(s) and/or interested group(s) using the ProSe direct discovery procedure. In Open Discovery, a UE which wants to discover other UE’s does not require any explicit permission from the other UE’s in order to be allowed to discover them.

The Restricted ProSe direct discovery procedure is used for a UE to discover or be discovered by other UE(s) in proximity over the PC5 interface. In Restricted Discovery, a UE which wants to discover other UE’s requires an explicit permission from the other UE’s in order to be allowed to discover them.

There could be a case where a discoverer UE intends to discover two different discoveree UEs (called discoveree UE A and discoveree UE B) at a time. With the existing ProSe architecture, the three UEs have to have the same security keys to support the case.

There is a vulnerability with the model B architecture in this use case. Despite discoveree UE A allowing to be discovered by only the discoverer UE, discoveree UE B is also capable of detecting and decoding the discovery response message from discoveree UE A because it has the same keys, and thus discoverying discoveree UE A.

Hence it needs to be studied how to protect the discovery response message of a UE in a restricted direct discovery model B architecture mode from being discovered by other discoveree UE(s).

Editor’s Note: Whether there is a case where a discoverer UE wants to discover more than one different discoveree UEs using same ProSe service at a time is FFS.

### 5.1.2 Security threats

If the discovery message cannot be confidentiality protected, integrity protected, and replay protected, the Prose APP Code can be intercepted, modified, or replayed by an attacker. The announcing UE or discoveree UE may connect with a UE that is not interested in the that particular Prose service.

An attacker may impersonate the discoveree or the discovered UE.

A malicious application running on a discoveree UE can detect the response message from other discoveree UE(s) that uses the same security keys in restricted direct discovery model B architecture and may discover other discoveree UE(s), that are not supposed to be discoverable to it. This puts the privacy of other discoveree UE(s) at risk.

Editor’s Note: Whether this threat is valid is FFS.

### 5.1.3 Potential security requirements

The discovery message in restricted discovery shall support confidentiality protection, integrity protection, and replay protection.

The entity which receives a restricted discovery message on the PC5 interface shall be able to verify the source authenticity.

Editor note: It is FFS in SA2 whether ProSe code or similar parameter will be used in discovery messages sent on PC5 interface. Any related privacy issues with the use of ProSe code or similar parameter needs to be further studied in restricted discovery.

The 5G System shall provide means to protect the discovery response message of a discoveree UE in the restricted direct discovery model B architecture from other discoveree UE(s).

Editor’s Note: In case that a discoverer UE wants to discover more than one different discoveree UEs using same ProSe service at a time, if security protection between different discoveree UEs is needed is FFS

## 5.2 Key Issue #2: Key issue Keys in ProSe discovery scenario

### 5.2.1 Key issue details

In TS 33.303[6], Prose Function sends discovery key to announce UE for calculating MIC in open discovery. In Restricted discovery, Prose Function also may send DUCK, DUIK, and DUSK to UEs.

In 5G, The functions of Prose Function is spitted into different network functions along with different network architecture approach. Meanwhile, AKMA has been defined in TS 33.535[7], and 5G GBA is working in the group. Above all are the elements to consider how to calculate discovery key(s) to UEs in 5G Prose.

Following issues need to be addressed in this key issue:

- Which network function derives the discover key.

- How to send the keys to the UEs.

### 5.2.2 Security threats

Not applicable

### 5.2.3 Potential security requirements

Not applicable

## 5.3 Key Issue #3: Security of UE-to-Network Relay

### 5.3.1 Key issue details

In KI#3 of TR 23.752[2], the UE maybe be able to access the network via the direct network communication or the indirect network communication as showing in figure 5.3.1-1. The path#1 is direct network communication path and the path#2 and path#3 are indirect network communication paths via different UE-to-network Relays.



Figure 5.3.1-1

The UE-to-Network relay is registered to the 5GS as a UE. In order to provide service to the remote UE, the UE-to-Network relay needs to establish an NR PC5 link with the Remote UE. Security for PC5 link establishment is documented for LTE Prose in TS 33.303 [6] and for eV2X in TS 33.536 [8]. However, it should be studied how to accommodate such procedures to 5G Prose.

For UE-to-Network relay, two options (Layer-2 UE-to-Network relay and Layer-3 UE-to-Network relay) are under consideration in TR 23.752 [2]. Both options commonly provide network access service to remote UE with the following differences.

* Layer 2 relay: remote UE is registered to the 5GC and has an AS security context established with the gNB in the connected mode.
* Layer 3 relay: remote UE may be registered to the 5GC, but does not have an AS security context.

Both options described above require PC5 unicast link between the remote UE and UE-to-Network relay. Therefore, it should be studied how to establish PC5 link securely (e.g., authentication and security context establishment) for both options.

TR 23.752 [2] in Clause 5.3, Key Issue #3: Support of UE-to-Network Relay has the following key issue:

*- How to transfer data between the Remote UE and the network over the UE-to-Network Relay.*

*NOTE 1: Security and privacy aspects will be handled by SA WG3.*

The UE-to-Network Relay in 5G is enhanced compared to LTE ProSe, to support commercial case. This may bring new security requirements compared to LTE Prose where the UE-to-Network Relay is only used in public safety scenario as defined in clause 4.4.3 of TS 23.303[5]. Public safety enabled UEs can be considered under control by police or government. When a UE-to-Network Relay is used in commercial case, the UE-to-network Relay may be a commercial UE that could belong to any person. In this case, the trust relationship between remote UE and relay UE is not as strong as the trust relationship between public safety enabled UEs.

### 5.3.2 Security threats

Lack of security during PC5 link establishment for UE-to-Network relay may cause to DoS attacks against the remote UE.

Lack of security during PC5 link establishment for UE-to-Network relay may allow MitM attack where the attacker can eavesdrop, modify, or inject messages into the remote UE data.

Failure to protect integrity and confidentiality of information exchanged between the Remote UE and the network over the UE-to-Network Relay will open vulnerability in 5GS and allow various attacks such as unauthorised access..If the UE-to-Network Relay is compromised, the security (i.e., the integrity and confidentiality) of information between the Remote UE and the network may be compromised.

### 5.3.3 Potential security requirements

The system shall support a secure means to establish a PC5 link between the remote UE and the UE-to-Network relay.

Confidentiality protection, Integrity protection and replay-protection shall be supported between the remote UE and the 3GPP network.

## 5.4 Key issue #4: Authorization in the UE-to-Network relay scenario

### 5.4.1 Key issue details

3GPP system has to be able to authorise a UE to access 5GC via a 5G UE-to-Network Relay and to authorise a UE to perform as a UE-to-Network Relay. Without a proper authorisation, unauthorised entities will be able to access 5GC via UE-to-Network Relay or act as UE-to-Network Relays creating a vulnerability and causing possible (D)DOS attacks or leading to unauthorised service usage on both 5GS and UE-to-Network Relay.

TR 23.752 [2], key issue #3 describes the issue on the support of UE-to-Network Relay, i.e.

*“-How to authorize a UE to be a 5G UE-to-Network Relay and how to authorize a UE to access 5GC via a 5G UE-to-Network Relay.*

*…*

*NOTE 1: Security and privacy aspects will be handled by SA WG3”*

From the security point of view, whether the UE can play the UE-to-Network Relay role shall be assured by the Remote UE. On the contrary, whether the UE can play the remote UE rule shall be assured by the UE-to-Network relay.

This key issue is to study the authorization issue in the UE-to-Network relay scenario.

### 5.4.2 Security threats

An attacker may impersonate the UE-to-Network Relay. If the authorization of the UE-to-Network relay role is not supported, the attacker UE could play the UE-to-Network relay role, and force a UE to camp on to it by passing all the message on between the UE and the network. It may then deny the UE services between the two UEs, such as drop the message.

An attacker may impersonate the Remote UE. If the authorization of the remote UE is not supported, the attacker UE could play the remote UE role, and arbitrarily consume the services provided by the UE-to-Network relay. The charging of the attacker UE as a remote UE may not be supported.

### 5.4.3 Potential security requirements

The 5GS shall support to authorize the UE as a UE-to-Network relay in the UE-to- Network relay scenario.

The 5GS shall support to authorize the UE as a Remote UE in the UE-to-Network relay scenario.

## 5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay

### 5.5.1 Key issue details

3GPP system has to be able to protect privacy of the Remote UE that is using the UE-to-Network Relay. Failure to protect privacy of the Remote UE that is using the UE-to-Network Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

TR 23.752 [2] in Clause 5.3, Key Issue #3: Support of UE-to-Network Relay has the following key issue:

*- How to transfer data between the Remote UE and the network over the UE-to-Network Relay.*

*NOTE 1: Security and privacy aspects will be handled by SA WG3.*

### 5.5.2 Security threats

Failure to protect privacy of the Remote UE that is using the UE-to-Network Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

### 5.5.3 Potential security requirements

The 5G System should provide means for mitigating trackability attacks on the Remote UE during communications over a UE-to-Network Relay.

The 5G System should provide means for mitigating linkability attacks on the Remote UE during communications over a UE-to-Network Relay.

## 5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay

### 5.6.1 Key issue details

3GPP system has to be able to protect security (i.e, the integrity and confidentiality) of information between the peer UEs over the UE-to-UE Relay. Failure to protect integrity and confidentiality of information exchanged between the peer UEs over the UE-to-UE Relay will open vulnerability in 5GS and allow various attacks such as unauthorised disclosure and modification of information. Protection of communications between the peer UEs shall take into consideration that the UE-to-UE Relay is an untrusted node.

TR 23.752 [2] in Clause 5.4, Key Issue #4: Support of UE-to-UE Relay, has the following key issue:

*- How to enhance the system architecture to provide the security protection for relayed connection?*

### 5.6.2 Security threats

Failure to protect integrity and confidentiality of information exchanged between the peer UEs over the UE-to-UE Relay will open vulnerability in 5GS and allow various attacks such as unauthorised disclosure and modification of information.

The UE-to-UE Relay being an untrusted node may be compromised, allowing the security (i.e., the integrity and confidentiality) of information between the peer UEs to be compromised. Therefore, end-to-end security between the peer UEs communicating over the UE-to-UE Relay is needed.

A malicious Relay UE that can establish unicast link with the source UE as well as the target UE may conduct MITM attack.

### 5.6.3 Potential security requirements

3GPP system shall provide means to confidentially and integrity protect security end-to-end between the peer UEs during communications over the UE-to-UE Relay.

## 5.7 Key issue #7: Authorization in the UE-to-UE relay scenario

### 5.7.1 Key issue details

TR 23.752 [2], key issue #4 describes its Key Issue regarding support of UE-to-UE Relay:

*“- Whether and how for the network can control the UE-to-UE Relay operation, at least including how to:*

*- Authorize the UE-to-UE Relay, e.g. authorize a UE as UE-to-UE Relay?*

*- Authorize the Remote UE to access a UE-to-UE Relay?*

*…*

*NOTE 2: For security aspects, coordination with SA3 is needed.”*

From a security point of view, whether the UE can act as a UE-to-UE Relay is be assured by the Remote UE. On the contrary, whether the UE can act as a remote UE should be assured by the UE-to-UE relay.

3GPP system has to be able to autorise a UE to perform as UE-to-UE Relay and a UE to communicate with another UE via a UE-to-UE Relay. This key issue directs SA3 to study the authorization aspects in the UE-to-UE relay scenario.

### 5.7.2 Security threats

An attacker may impersonate the UE-to-UE Relay. If the authorization of the UE acting as UE-to-UE relay is not supported, the attacker UE may impersonate the UE-to-UE relay, and force a remote UE to camp on it by passing messages between two UEs. The attacker may then deny the UE services between the two UEs (e.g., arbitrary discard messages).

An attacker may impersonate the source UE or the target UE.

### 5.7.3 Potential security requirements

The 5GS shall support authorisation of the UE as a UE-to-UE relay in the UE-to-UE relay scenario.

Authorisation of a UE that requests to be a source UE or a target UE discovering a UE-to-UE Relay, should be provided.

3GPP system shall provide means to authorise a UE to communicate with another UE via a UE-to-UE Relay.

## 5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay

### 5.8.1 Key issue details

3GPP system has to be able to protect the privacy of identities exchanged in the communications between peer UEs over a UE-to-UE Relay. Failure to protect privacy of identities of peer UEs communicating over the UE-to-UE Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

TR 23.752 [2] in Clause 5.4, Key Issue #4: Support of UE-to-UE Relay, has the following key issue:

*- How to enhance the system architecture to provide the security protection for relayed connection?*

### 5.8.2 Security threats

Failure to protect privacy of identities exchanged in the communications between the peer UEs over the UE-to-UE Relay will open vulnerability in 5GS and allow various privacy attacks including tracing and tracking of identities.

Existing Link identifier update procedure specified in TS 33.536 [8] provides privacy of the identities on a per unicast link basis (e.g., the link between a UE and the UE-to-UE Relay). Therefore an attacker may be able to link identities exchanged over the link between a UE and the UE-to-UE Relay to those exchanged over the corresponding link between the peer UE and the UE-to-UE Relay

### 5.8.3 Potential security requirements

The 5G System should provide means for mitigating trackability attacks on peer UEs during communications over a UE-to-UE Relay.

The 5G System should provide means for mitigating linkability attacks on peer UEs during communications over a UE-to-UE Relay.

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

### 5.9.1 Key issue details

This key issue covers both Layer-2 and Layer-3 relays in 5G Proximity Services.

SA2 TR 23.752 [2] has candidate solution for both layer 2 and layer 3 UE-to-network relay. There are security solutions which will be adapted for PC5 unicast communication for ProSe from 5G V2X.

Currently, Rel-16 V2X does not support relay communication (both UE-to-network or UE-to-UE relay).

Based on V2X security TS 33.536 [8], the Direct Provisioning Function (DPF) defined in TS 23.303 [5] is replaced by PCF, based on the V2X architecture as defined in TS 23.287 [9], and is not supported by the DDNMF. The architecture reference model as described in clause 2 User Plane based architecture, with the following additional considerations:

* each PLMN deploys one logical 5G DDNMF
* the 5G DDNMF interacts with PCF for the authorization of the ProSe discovery service



Figure 5.9.1-1: User Plane architecture for ProSe

In LTE ProSe, the ProSe Key Management Function supports the key derivation required to support the UE-to-network relay communication.

Whereas in 5G the existing entity can support the key derivation, authentication and authorization of the remote UE and UE-to-Network relay.

In order to attach to the network via a UE-to-network relay, a remote UE may have to authenticate to the network and vice versa. Because the UE-to-network relay sits in between the remote UE and the network, it may have the possibility to perform MitM, DoS, and replay attacks in between.

### 5.9.2 Security threats

Following are the possible threats

- A man-in-the-middle attack by the relay UE;

- A denial of service attack by the relay UE on the remote UE;

- Impersonation of the remote UE by the relay UE.

### 5.9.3 Potential security requirements

- 5GS shall support secure communication between the remote UE and the network via UE-to-Network relays.

- 5GS shall support generation of separate security contexts for remote UEs for ProSe relay communication.

## 5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF

### 5.10.1 Key issue details

This key issue describes about the issue in secure communication between UE and ProSe function (5GDDNMF).

The ProSe-enabled UEs have many interactions with the 5GDDNMFin the 5G ProSe solution currently described in SA2 study TR 23.752 [2]. For example, to retrieve ProSe Discovery parameters and provision of ProSe discovery related security parameters.

If not secured an attacker may manipulate or modify the data being transmitted between UE and 5GDDNMF, thus adversely affecting the ProSe communication.

### 5.10.2 Security threats

- An attacker may manipulate thedata being transmitted between the UE and 5GDDNMF, thus adversely affecting the ProSe communication.;

- An attacker may eavesdrop on transmitted data and further utilize it for improper use.;

- An attacker may replay an intercepted data thus affecting an expected state of action at the ProSe-enabled UE. .

### 5.10.3 Potential requirements

The ProSe-enabled UE and 5GDDNMF shall mutually authenticate each other for secure ProSe communication.

The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be integrity protected.

The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be confidentiality protected

The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be protected from replay attacks.

## 5.X Key Issue #X: <Key Issue Name>

### 5.X.1 Key issue details

### 5.X.2 Security threats

### 5.X.3 Potential security requirements

# 6 Solutions

Editor’s Note: This clause contains the proposed solutions addressing the identified key issues.

## 6.0 Mapping of Solutions to Key Issues

Table 6.0-1: Mapping of Solutions to Key Issues

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Key Issues | | | | | | | | | |
| Solutions | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
| 1 |  |  |  |  |  |  |  |  | X |  |
| 2 |  |  |  |  |  |  |  |  |  | X |
| 3 |  |  |  |  |  |  |  |  |  |  |
| 4 |  |  |  |  |  |  |  |  |  |  |
| 5 |  |  |  |  |  |  |  |  |  |  |
|  |  |  |  |  |  |  |  |  |  |  |

## 6.1 Solution #1: Solution for key management in 5G Proximity Services relay communication

### 6.1.1 Introduction

This solution describes how the existing network function Authentication Server Function performs the key management instead of PKMF (ProSe Key Management Function) as done in TS 33.303 [6] in LTE ProSe. This solution addresses key issue #9.

### 6.1.2 Solution details

In this solution it is assumed that the 5GDDNMF is a functionality of PCF and not a separate entity. Proposed solution reuses the PCF discovery procedure as defined in 23.502[10] for provisioning or configuration of the relay discovery material and the required security material.



Figure 6.1.2-1: Procedural call flow for key management in 5G ProSe

Step 0a-0e: The remote UE seeking access via UE-to-Network relay, REAR (Remote Access via Relay) sends a UE policy provisioning request to the AMF. The request may include the Remote UE capability i.e., ProSe UE capability, PC5 capability.

AMF sends N5gddnmf\_UEpolicycontrol\_update or Npcf\_UEpolicycontrol\_update request over Service based interface to discover the corresponding PCF or 5GDDNMF and requests for the policy required for ProSe UE Discovery and security material.

5GDDNMF or PCF responds back with the N5gddnmf\_UEpolicycontrol\_update response with the required ProSe relay discovery and security material. AMF delivers the ProSe relay discovery and security material to the Remote UE.

The UE-to-Network relay gets authenticated and authorized by the network to support as a relay for ProSe communication.

Editor's Note: Whether the security keys can be provided in step 0d is FFS.

Editor's Note: The definition of 5GDDNMF shall be aligned with SA2.

Step 1: The Remote UE sends a key request message to the AMF, where the message includes the ProSe Remote access indication and 5G-GUTI if already assigned or the SUCI. This solution based on single hop relay i.e., one UE-to-Network relay between Remote UE and the core network. The proposed solution also works for multiple hop relay communication.

The ProSe Remote access indication is set to 1, which indicates that there is only single hop UE-to-Network relay in between.

The AMF forwards the Key request to the AUSF instance which is capable of authentication, authorization and key derivation for the ProSe UE-to-Network relay communication.

Step 2: In order to authorize the UE requesting for keys for remote access, the AUSF sends Nudm\_UEAuthentication request to UDM and retrieves the UE details or subscription data. In this message the AUSF includes ProSe Remote access indication and 5G-GUTI or SUCI.

Step 3: On receiving the Nudm\_UEAuthentication request, the UDM verifies the 5G-GUTI or SUCI and sends the corresponding SUPI to the AUSF in Nudm\_UEAuthentication response message.

Step 4: On receiving the SUPI from UDM, the AUSF generates the REAR Key for Remote UE communication via UE-to-Network relay. REAR key will be used for deriving the ProSe key KNR\_ProSe.

Input to the Key Derivation Function for deriving the REAR key is as follows:

REAR Key = KDF (Latest KAUSF, SUPI of the Remote UE, Relay UE ID bound to SUPI of relay/TempID of relay, other possible parameters)

The generated key is 256 bits in which, the 128 bits MSB of key is the REAR Key and the other 128 bits is the REAR Key ID. The purpose of REAR Key ID is to identify the REAR key.

Editor's Note: The key name and input parameters are FFS.

Step 5: AUSF sends the generated REAR key and Relay UE ID/TempID of Relay which is bound to UE-to-Network relays SUPI in the key response message to the Remote UE.

Step 6: Remote UE discovers the relay UE using any of Model A or Model B method. The discovery message must include the relay UE ID provided by the AUSF.

Step 7: After the discovery of the UE-to-Network relay, the Remote UE sends the Direct communication request to the discovered relay for establishing secure PC5 unicast link. The message should include Relay Service Code or ServiceID, 5G-GUTI of the Remote UE and Message Authentication Code MACREAR.

Step 8: On receiving the Direct Communication request, the UE-to-Network relay sends a key request message Relay Service Code or ServiceID, 5G-GUTI of the Remote UE and Message Authentication Code MACREAR received from the remote UE.

Step 9: AUSF authorizes the remote UE requesting for remote access by checking the MACREAR using the REAR key, and 5G-GUTI.

Step 10: After authorization the AUSF generates the ProSe key to be used for Remote access via Relay.

The input to the KDF for generating ProSe key is as follows:

KNR\_ProSe = KDF (REAR key, 5G-GUTI, Relay Service Code or ServiceID, KNR\_ProSe freshness parameter, other possible parameters). KNR\_ProSe freshness parameter can be any nonce or counter or random number.

Editor's Note: The purpose of KNR\_ProSe is FFS.

Step 11: AUSF sends the KNR\_ProSe freshness parameter in the key response message to the UE-to-Network relay.

Step 12: The UE-to-Network relay sends the received KNR\_ProSe freshness parameter to the Remote UE in Direct Security mode command message.

Step 13: The remote UE generates the ProSe key to be used for Remote access via Relay same as defined in step 10.

Step 14: Remote UE sends the Direct Security mode complete message to the UE-to-Network relay. Further communication between Remote UE and Network takes place securely via the UE-to-Network relay.

Editor's Note: This solution assumes and require network connectivity for both remote UE and relay UE.

Editor's Note: This solution may impact more than one key issue.

### 6.1.3 Evaluation

TBD

## 6.2 Solution #2: Secure data transfer between UE and 5GDDNMF

### 6.2.1 Introduction

This solution addresses key issue#10.

### 6.2.2 Solution details

In LTE ProSe, the protection of traffic between UE and ProSe Function is as specified in clause 5.3.3.2 in TS 33.303 [6]. For 5G ProSe the security can be established using Authentication and Key Management for Applications. Where AF is the ProSe Application Function (5GDDNMF) and AF should be authenticated and authorized by the operator network before providing the AKMA Application Key (KAF) to the AF.

Editor's Note: Whether 5GDDNMF is a functionality of PCF or an AF is based on conclusion from SA2.

It is proposed to use the AKMA network model and security procedure to have a secure data transfer between UE and the 5GDDNMF.



Figure 6.2.2-1: User plane architecture

Figure 6.2.2-1 is reference model for AKMA modified for supporting Proximity based services. The Application function in AKMA is 5GDDNMF in ProSe having a service-based interface N5gddnmf with other Network Functions, to consume or provide services from or to other NFs.

Editor's Note: Whether AKMA user plane architecture is used shall be based on conclusion from SA2.The PC3 interface between UE and 5GDDNMF is considered as Ua\* interface and depends on Ua\* protocol.

However, the security requirement of PC3 interface should be aligned to satisfy the Ua\* interface. Also, the interface Ua\* needs to have new functionalities in addition to specified in clause 4.4.1 of TS 33.535 [7] for Ua\*.

Editor’s note: The need of new functionalities is FFS and whether the new functionalities can be used in Ua\* is FFS.

Editor’s note: The impact on Ua\* interface and PC3 interface are FFS.

### 6.2.3 Evaluation

TBD

## 6.Y Solution #Y: <Solution Name>

### 6.Y.1 Introduction

Editor’s Note: Each solution should list the key issues being addressed.

### 6.Y.2 Solution details

### 6.Y.3 Evaluation

Editor’s Note: Each solution should motivate how the potential security requirements of the key issues being addressed are fulfilled.

# 7 Conclusions

Editor’s Note: This clause contains the agreed conclusions.

Annex <X> (informative):  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2020-08 | SA3#100e | S3-202145 |  |  |  | S3-201804, S3-202144, S3-201826, S3-201756, S3-202129, S3-201757, S3-202130, S3-202147, S3-201616, S3-202157, S3-202146, S3-201618, S3-202064, S3-202066, S3-202065, S3-202067implemented | 0.1.0 |
|  |  |  |  |  |  |  |  |