3GPP TR 33.814 V16.0.1 (2019-10)

Technical Report

3rd Generation Partnership Project;

Technical Specification Group Services and System Aspects;

Study on the security of the enhancement to the 5G Core (5GC) location services

(Release 16)

** 

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 Report 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.

Keywords

5G, eLCS, security

***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.

© 2019, 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

Bluetooth® is a Trade Mark of the Bluetooth SIG registered for the benefit of its members

Contents

Foreword [5](#__RefHeading___Toc22559850)

Introduction [6](#__RefHeading___Toc22559851)

1 Scope [7](#__RefHeading___Toc22559852)

2 References [7](#__RefHeading___Toc22559853)

3 Definitions of terms, symbols and abbreviations [7](#__RefHeading___Toc22559854)

3.1 Terms [7](#__RefHeading___Toc22559855)

3.2 Symbols [8](#__RefHeading___Toc22559856)

3.3 Abbreviations [8](#__RefHeading___Toc22559857)

4 Security aspects of eLCS in the 5G System [8](#__RefHeading___Toc22559858)

4.1 Introduction [8](#__RefHeading___Toc22559859)

5 Key issues [9](#__RefHeading___Toc22559860)

5.1 Key Issue #1: Security and privacy in Bluetooth positioning [9](#__RefHeading___Toc22559861)

5.1.1 Key issue details [9](#__RefHeading___Toc22559862)

5.1.2 Security threats [9](#__RefHeading___Toc22559863)

5.1.3 Potential security requirements [9](#__RefHeading___Toc22559864)

5.2 Key Issue #2: Security and privacy in TBS positioning [9](#__RefHeading___Toc22559865)

5.2.1 Key issue details [9](#__RefHeading___Toc22559866)

5.2.2 Security threats [10](#__RefHeading___Toc22559867)

5.2.3 Potential security requirements [10](#__RefHeading___Toc22559868)

5.3 Key Issue #3: Security and privacy in WLAN positioning [10](#__RefHeading___Toc22559869)

5.3.1 Key issue details [10](#__RefHeading___Toc22559870)

5.3.2 Security threats [10](#__RefHeading___Toc22559871)

5.3.3 Potential security requirements [10](#__RefHeading___Toc22559872)

5.4 Key Issue #4: Privacy control in LCS [10](#__RefHeading___Toc22559873)

5.4.1 Key issue details [10](#__RefHeading___Toc22559874)

5.4.2 Security threats [11](#__RefHeading___Toc22559875)

5.4.3 Potential security requirements [11](#__RefHeading___Toc22559876)

5.5 Key Issue #5: UE faking/altering location estimate or measurements [11](#__RefHeading___Toc22559877)

5.5.1 Key issue details [11](#__RefHeading___Toc22559878)

5.5.2 Security threats [12](#__RefHeading___Toc22559879)

5.5.3 Potential security requirements [12](#__RefHeading___Toc22559880)

5.6 Key Issue #6: Positioning data confidentiality between UE and network [12](#__RefHeading___Toc22559881)

5.6.1 Key issue details [12](#__RefHeading___Toc22559882)

5.6.2 Security threats [12](#__RefHeading___Toc22559883)

5.6.3 Potential security requirements [12](#__RefHeading___Toc22559884)

5.X Key Issue #X: <Key Issue Name> [13](#__RefHeading___Toc22559885)

5.X.1 Key issue details [13](#__RefHeading___Toc22559886)

5.X.2 Security threats [13](#__RefHeading___Toc22559887)

5.X.3 Potential security requirements [13](#__RefHeading___Toc22559888)

6 Solutions [13](#__RefHeading___Toc22559889)

6.1 Solution #1: Supervised Bluetooth measurements from UEs [13](#__RefHeading___Toc22559890)

6.1.1 Introduction [13](#__RefHeading___Toc22559891)

6.1.2 Solution details [13](#__RefHeading___Toc22559892)

6.1.3 Evaluation [14](#__RefHeading___Toc22559893)

6.2 Solution #2: Solution for TBS measurements from UEs [14](#__RefHeading___Toc22559894)

6.2.1 Introduction [14](#__RefHeading___Toc22559895)

6.2.2 Solution details [14](#__RefHeading___Toc22559896)

6.2.3 Evaluation [14](#__RefHeading___Toc22559897)

6.3 Solution #3: Supervised WLAN measurements from UEs [15](#__RefHeading___Toc22559898)

6.3.1 Introduction [15](#__RefHeading___Toc22559899)

6.3.2 Solution details [15](#__RefHeading___Toc22559900)

6.3.3 Evaluation [16](#__RefHeading___Toc22559901)

6.4 Solution #4: Enhanced privacy control in LCS [16](#__RefHeading___Toc22559902)

6.4.1 Introduction [16](#__RefHeading___Toc22559903)

6.4.2 Solution details [16](#__RefHeading___Toc22559904)

6.4.3 Evaluation [18](#__RefHeading___Toc22559905)

7 Conclusions [18](#__RefHeading___Toc22559906)

7.1 General conclusions [18](#__RefHeading___Toc22559907)

7.2 Conclusions on Key Issue #1 [18](#__RefHeading___Toc22559908)

7.3 Conclusions on Key Issue #2 [18](#__RefHeading___Toc22559909)

7.4 Conclusions on Key Issue #3 [18](#__RefHeading___Toc22559910)

7.5 Conclusions on Key Issue #4 [18](#__RefHeading___Toc22559911)

Annex A: Change history [19](#__RefHeading___Toc22559912)

# Foreword

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 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

3GPP TS 23.273 [6] specifies enhanced Location Services (eLCS) in the 5G System. The enhanced location services may bring new security issues such as authorization, privacy protection. The present document studies the security aspects of the eLCS and provides potential solutions.

# 1 Scope

The scope of the present document is to analyse the security aspects of location service in 5G system and ensure the security solutions are aligned with the work in SA1 (i.e. in TS 22.261 [2] and TR 22.872 [3]) and SA2 (i.e. in TR 23.731 [4]). The work is comprised of the following parts:

- Study the security key issues, threats and requirements of location service 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 TS 22.261: "Service requirements for next generation new services and markets; Stage 1".

[3] 3GPP TR 22.872: "Study on positioning use cases".

[4] 3GPP TR 23.731: "Study on Enhancement to the 5GC LoCation Services".

[5] 3GPP TS 38.305: "NG Radio Access Network (NG-RAN); Stage 2 functional specification of User Equipment (UE) positioning in NG-RAN".

[6] 3GPP TS 23.273: "5G System Location Services".

[7] 3GPP TS 36.331: "Evolved Universal Terrestrial Radio Access (E-UTRA); Radio Resource Control (RRC); Protocol specification".

# 3 Definitions of terms, symbols and abbreviations

## 3.1 Terms

For the purposes of the present document, the terms 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].

**LCS Client:** Defined in 3GPP TS 23.271 [2].

**LCS (LoCation Services):** Defined in 3GPP TS 23.271 [2].

**Target UE:** Defined in 3GPP TS 23.271 [2].

**Location Estimate:** Defined in 3GPP TS 23.271 [2].

## 3.2 Symbols

Void.

## 3.3 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 Network

5GS 5G System

CID Cell-ID (positioning method)

E-CID Enhanced Cell-ID (positioning method)

GMLC Gateway Mobile Location Centre

LCS LoCation Services

LMF Location Management Function

LPP LTE Positioning Protocol

MAC Master Auxiliary Concept

OTDOA Observed Time Difference Of Arrival

RSSI Received Signal Strength Indicator

SSID Service Set Identifier

TBS Terrestrial Beacon System

VGMLC Visited GMLC

WLAN Wireless Local Area Network

# 4 Security aspects of eLCS in the 5G System

## 4.1 Introduction

TR 23.731 [4] describes an enhanced Location Service (eLCS) architecture. The normative work of eLCS is specified in TS 23.273 [6].

The eLCS proposes to use NAS signalling to transmit positioning messages between UE and 5GC. The location services may be exposed to the third parties through the Le and N33 interfaces.

In 5G Rel-15, location services provided by the home operator are restricted to location services required by regulation. In 5G Rel-16, location services will support the commercial use of location by third parties via the home operator. It is assumed that the requests from regulatory agencies are always authorized to use location services. However, in commercial use cases, the user is able to choose and change their privacy settings for location. In order to support commercial services, the location service architecture is extended to support roaming scenario, the location service exposure and Mobile Originating Location Request scenario.

The LCS subscription information, LCS privacy profile and routing information are proposed to be stored in the UDM. The UDM is accessible from an AMF, GMLC or NEF via the Nudm interface.

eLCS may raise a series of security issues, such as positioning data eavesdropping, UE location tracking, privacy information leak. The present document studies the security aspects of LCS in the 5G System.

# 5 Key issues

## 5.1 Key Issue #1: Security and privacy in Bluetooth positioning

### 5.1.1 Key issue details

Location services in 3GPP include the Bluetooth positioning method in which the UE position is estimated with the knowledge of geographical coordinate of "reference" Bluetooth beacons.

The Bluetooth positioning mode could be: (a) "standalone" where the UE performs Bluetooth position measurements and location computation; or (b) "UE-assisted" where the UE provides Bluetooth position measurements without assistance from the network to the location management function for computation of a location estimate by the network. The 3GPP TS 38.305 [5] and the 3GPP TR 23.731 [4] are referred for further details.

In Bluetooth positioning, information that may be transferred over-the-air include Bluetooth location information (such as media address control (MAC) address, received signal strength (RSSI), and time stamp) as well as UE location information (such as UE position estimate and position time stamp).

This key issue is about investigating if and how any new security and privacy mechanism need to be added in Bluetooth positioning, in addition to currently existing mechanisms.

### 5.1.2 Security threats

Lack of secure and privacy preserving mechanism to transfer location-related information over-the-air could potentially have undesirable effects like position poisoning or subscriber traceability.

### 5.1.3 Potential security requirements

The system shall support secure and privacy preserving mechanism for Bluetooth positioning.

## 5.2 Key Issue #2: Security and privacy in TBS positioning

### 5.2.1 Key issue details

Location services in 3GPP include the TBS (terrestrial beacon systems) positioning method in which the UE position is estimated with the knowledge of geographical coordinate of "reference" ground-based transmitters broadcasting signals for geo-spatial positioning with wide-area or regional coverage.

The TBS positioning mode could be: (a) "standalone" where the UE performs TBS measurements and calculates its own location, possibly using additional measurements from other (non-TBS) sources, without network assistance; or (b) "UE-assisted" where the UE performs TBS measurements with or without assistance from the network, and sends these measurements to the location management function where the position calculation takes place, possibly using additional measurements from other (non-TBS) sources; or (c) "UE-based" where the UE performs TBS measurements and calculates its own location, possibly using additional measurements from other (non-TBS) sources. The 3GPP TS 38.305 [5] and the 3GPP TR 23.731 [4] are referred for further details.

In TBS positioning, information that may be transferred over-the-air include UE location information such as UE position estimate (which could be latitude, longitude, and altitude) and timestamp.

The TBS positioning method consists of a network of ground-based transmitters that broadcast signals only for positioning purposes. A difference in TBS positioning method from WLAN and Bluetooth positioning methods is that these ground-based transmitters are not supposed to represent a human user. Nevertheless, it is prudent to investigate if and how any new security and privacy mechanism need to be added in TBS positioning, in addition to currently existing mechanisms.

### 5.2.2 Security threats

Lack of secure and privacy preserving mechanism to transfer location-related information over-the-air could potentially have undesirable effects like position poisoning or subscriber traceability.

### 5.2.3 Potential security requirements

The system shall support secure and privacy preserving mechanism for TBS positioning.

## 5.3 Key Issue #3: Security and privacy in WLAN positioning

### 5.3.1 Key issue details

Location services in 3GPP include the WLAN positioning method in which the UE position is estimated with the knowledge of geographical coordinates of "reference" WLAN access points.

The WLAN positioning mode could be: (a) "standalone" where the UE performs WLAN position measurements and location computation without network assistance; or (b) "UE-assisted" where the UE provides WLAN position measurements with or without assistance from the network to the location management function for computation of a location estimate by the network; or (c) "UE-based" where the UE performs WLAN position measurements and computation of a location estimate with network assistance. The 3GPP TS 38.305 [5] and the 3GPP TR 23.731 [4] are referred for further details.

In WLAN positioning, information that may be transferred over-the-air includes WLAN location information (such as basic service set identifier (BSSID), service set identifier (SSID), received signal strength (RSSI), and time stamp) as well as UE location information (such as UE position estimate and position time stamp).

This key issue is about investigating if and how any new security and privacy mechanism need to be added in WLAN positioning, in addition to currently existing mechanisms.

### 5.3.2 Security threats

Lack of secure and privacy preserving mechanism to transfer location-related information over-the-air could potentially have undesirable effects like position poisoning or subscriber traceability.

### 5.3.3 Potential security requirements

The system shall support secure and privacy preserving mechanism for WLAN positioning.

## 5.4 Key Issue #4: Privacy control in LCS

### 5.4.1 Key issue details

In relation to 5G and service-based architecture, the LCS architecture in roaming scenario is shown in Figure 5.4.1-1.

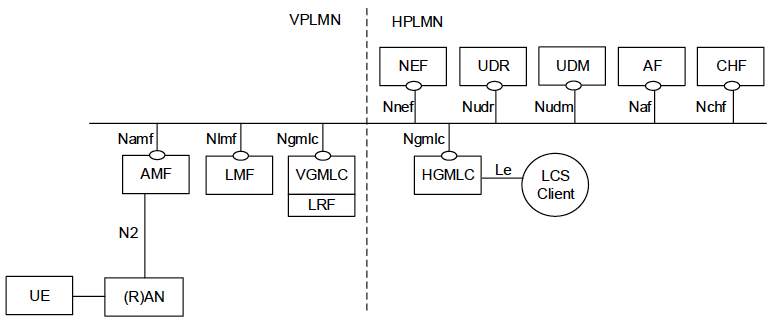


Figure 5.4.1-1: LCS architecture in roaming scenario (Figure 4.2.2-2 in TS 23.273 [6])

Location services (LCS) in the 3GPP system already address privacy control of UE's user by providing mechanisms for the user's consent processing, and privacy settings update procedure. In the existing mechanisms, the UE's privacy settings are primarily distributed by the UDM, however, the UDM itself cannot enforce its use in other entities like the AMF in the VPLMN.

Hence, it is important to analyse if the privacy controls are effective, especially taking into consideration that multiple entities are involved and trust relations between them vary.

### 5.4.2 Security threats

Lack of effective privacy control could potentially lead to undermining privacy preferences of UE's users.

### 5.4.3 Potential security requirements

The 5G system shall support privacy control in LCS.

Editor's Note: Who is enforcing the privacy control is FFS.

## 5.5 Key Issue #5: UE faking/altering location estimate or measurements

### 5.5.1 Key issue details

For UE based positioning procedure, the UE performs positioning measurement and computation. The location estimate will be reported to network from UE.

For UE assisted positioning procedure, the UE of which the location is to be determined performs measurements itself and sends these measurements to the network so the network can determine its location. Examples are

- OTDOA (Observed Time Difference Of Arrival),

- Enhanced cell ID - measurement of arrival times of specific messages, and

- Enhanced cell ID - measurement of received signal strength of specific messages.

It may be advantageous for a UE to appear to be located somewhere else than it actually is. This can be done by the UE by faking/altering the above measurements or location estimate before sending these to the network.

This key issue is about investigating how the network can detect that a UE has faked/altered location estimate or the measurements that are used for determining its location estimate. For this key issue it is assumed that the reports provided by the UE are not trusted.

### 5.5.2 Security threats

Not being able by the network to detect a UE faking/altering location estimate or the measurements that are used for determining the location of that UE may lead to

- granting a UE a service that is based on the UE having to be in a particular location when the UE is actually not in that location, which may allow the user to defraud a monetized service, such as cheap calls when being close to one's home,

- a UE being able to provide a fake alibi for its user.

### 5.5.3 Potential security requirements

Editor's Note: The potential security requirements are FFS.

## 5.6 Key Issue #6: Positioning data confidentiality between UE and network

### 5.6.1 Key issue details

The positioning messages exchanged between UE and 5GC is via NAS signalling.

In TS 22.261 [2] there is following description:

Subject to regional or national regulatory requirements, the 5G system shall be able to provide the 5G positioning services while ensuring the protection of the privacy of the UE's user or owner, including the respect of his consent to the positioning services.

NOTE 1: This includes the ability for the 5G system to provide the positioning services on demand without having to track continuously the position of the involved UE.

NOTE 2: The respect of the user's consent to some positioning services could abide by different rules in case of emergency (for example, rules that would also receive consent from the user, but well before the emergency occurs).

This requirement requires that UE's positioning information shall not be eavesdropped or exposed to unauthorized parities.

This key issue will study:

- Confidentiality protection for the positioning information exchanged via NAS signalling.

### 5.6.2 Security threats

The positioning information exchanged via NAS signalling between the UE and the 5GC may be used by attackers to track the location of UE.

### 5.6.3 Potential security requirements

- It shall be possible to support confidentiality protection of positioning data exchanged between UE and network.

NOTE 1: In case NAS confidentiality protection is disabled, positioning data carried in NAS cannot be protected.

NOTE 2: The serving network is trusted with the location of the UE.

## 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

## 6.1 Solution #1: Supervised Bluetooth measurements from UEs

### 6.1.1 Introduction

This solution addresses following key issues:

1) Key issue #1: Security and privacy in Bluetooth positioning.

Location services (LCS) in 3GPP system include the Bluetooth positioning method in which the UE position is estimated with the knowledge of geographical coordinate of "reference" Bluetooth beacons in serving network. The 3GPP TS 38.305 [5] is referred for further details. They sufficiently address privacy of UE's user by providing mechanisms for the user's consent processing, and confidentiality/integrity protection of messages. However, there is no way instruct the UE to "not" report everything they see in the neighbourhood. Doing so is necessary to respect the privacy of neighbouring UE's users, and to avoid potential issues like "mass surveillance". Nevertheless, it should also be considered that one of the main use cases of LCS is locating UE during emergency and failure to locate the UE could prove fatal to the health or life of the UE's user. Depending upon regulations, privacy of neighbouring Bluetooth devices may be considered comparatively less important than saving life of the user. Depending upon regulations, it might even be the obligation of neighbouring Bluetooth devices to assist in locating the concerned UE. It could also be the case that there are some users who have opted-in so that their Bluetooth devices could be reported to the network.

To strike a balance between "collect everything" and "collect nothing", this solution proposes a supervision mechanism so that the network can carefully limit the information reported by the UE and tweak the limit according to regulation or network policy. Mind that in MDT (minimization of drive tests) the network can configure the UE with a "whitelist" so that UE only measures the neighbouring Bluetooth devices whose "names" are included in the whitelist. See "BT-NameList" in 3GPP TS 36.331 [7].

There are 2 positioning modes that are supported in Bluetooth positioning method, namely (a) standalone, (b) UE-assisted. Among those, it is only in the UE-assisted positioning mode (b) that the UE sends measurements to the network and therefore it is the only mode that needs a supervision mechanism. A short summary follows:

- in the standalone positioning mode (a), the UE itself does the computation of location estimate. Bluetooth measurements around the UE are not sent from UE to the network.

- in the UE-assisted positioning mode (b), the UE does not get assistance data from network and the network does the computation of location estimate. Bluetooth measurements around the UE are sent from UE to the network.

### 6.1.2 Solution details

For the positioning modes requiring the UE to send Bluetooth measurements to the network (i.e., UE-assisted), the following applies:

(1) The network should provide "Bluetooth supervision data" to UE. This Bluetooth supervision data shall contain a list of Bluetooth AP data that are to be measured by UE. Each Bluetooth AP data shall contain the Bluetooth public-address information and/or the Bluetooth device-name information. See details below for the values of Bluetooth public-address/device-name.

(2) If the UE gets the Bluetooth supervision data from the network, the UE shall send only those Bluetooth measurements to the network whose Bluetooth public-addresses and/or Bluetooth device-names match the ones indicated in the provided Bluetooth supervision data.

(3) If the UE does not get the Bluetooth supervision data from the network, the UE shall send only those Bluetooth measurements to the network whose Bluetooth public-addresses and/or Bluetooth device-names match the ones in "reference Bluetooth supervision data". This reference Bluetooth supervision data shall contain "reference Bluetooth public-address" information and "reference Bluetooth device-name" information. See details below for their values.

The Bluetooth public-address/device-name information may be values, e.g., defined by 3GPP, or based on MCC, MNC, realm, or any PLMN specific identifiers. They could also be patterns instead of exact values, e.g., MCC\*. They could also be values, e.g., provided by network dynamically to UE as broadcast information or in other protocol messages like RRC, NAS, or LPP. It also means that the reference Bluetooth supervision data could be static or dynamic.

### 6.1.3 Evaluation

This solution enables the network to control the collection of Bluetooth measurements from UE. When used, the solution makes it possible for the network to avoid collecting unintended Bluetooth measurements around the UE.

It should be noted that whilst it is easy to broadcast spoofed Bluetooth identifiers, it is relatively difficult to block Bluetooth identifiers being transmitted in the same location. Therefore, any solution that only listens for specific Bluetooth identifiers may be easier to get spoofed than solutions that listen to all Bluetooth identifiers in a specific location.

For Bluetooth based positioning in general, it should be noted that because Bluetooth identifiers can be spoofed, there is low confidence in collected data.

## 6.2 Solution #2: Solution for TBS measurements from UEs

### 6.2.1 Introduction

This solution addresses following key issues:

(1) Key issue #2: Security and privacy in TBS positioning.

Location services (LCS) in 3GPP system sufficiently address privacy of the user of a UE by providing mechanisms for the user's consent processing, and confidentiality/integrity protection of messages. Further, there are two types of broadcasted signals in the TBS positioning, i.e., MBS (Metropolitan Beacon System) signals and Positioning Reference Signals (PRS). These signals are broadcasted by a network of ground-based transmitters "only" for positioning purposes, see TS 38.305 [5]. Thus, the neighbouring devices, whose measurements are collected by the UE, are not supposed to represent a human user.

Therefore, no new security and privacy solution specific to TBS positioning method is deemed necessary for both regulatory and commercial positioning.

### 6.2.2 Solution details

Existing mechanisms in the LCS system sufficiently address security and privacy aspects for TBS positioning method and shall be re-used for both regulatory and commercial positioning.

### 6.2.3 Evaluation

Existing security and privacy solution sufficiently address TBS measurements from UE.

It should be noted that whilst it easy to broadcast spoofed TBS signals, it is relatively difficult to block TBS signals being transmitted in the same location. Therefore, any solution that only listens for specific TBS signals may be easier to get spoofed than solutions that listen to all TBS signals in a specific location.

## 6.3 Solution #3: Supervised WLAN measurements from UEs

### 6.3.1 Introduction

This solution addresses following key issues:

(1) Key issue #3: Security and privacy in WLAN positioning.

Location services (LCS) in 3GPP system include the WLAN positioning method in which the UE position is estimated with the knowledge of geographical coordinates of "reference" WLAN access points in serving network. The 3GPP TS 38.305 [5] is referred for further details. They sufficiently address privacy of UE's user by providing mechanisms for the user's consent processing, and confidentiality/integrity protection of messages. However, there is no way instruct the UE to "not" report everything they see in the neighbourhood. Doing so is necessary to respect the privacy of neighbouring UE's users, and to avoid potential issues like "mass surveillance". Nevertheless, it should also be considered that one of the main use cases of LCS is locating UE during emergency and failure to locate the UE could prove fatal to the health or life of the UE's user. Depending upon regulations, privacy of neighbouring WLAN devices may be considered comparatively less important than saving life of the user. Depending upon regulations, it might even be the obligation of neighbouring WLAN devices to assist in locating the concerned UE. It could also be the case that there are some users who have opted-in so that their WLAN devices could be reported to the network.

To strike a balance between "collect everything" and "collect nothing", this solution proposes a supervision mechanism so that the network can carefully limit the information reported by the UE and tweak the limit according to regulation or network policy. Mind that in MDT (minimization of drive tests) the network can configure the UE with a "whitelist" so that UE only measures the neighbouring WLAN devices whose "names" are included in the whitelist. See "WLAN-NameList" in 3GPP TS 36.331 [7].

There are 3 positioning modes that are supported in WLAN positioning method, namely (a) standalone, (b) UE-based, and (c) UE-assisted. Among those, it is only in the UE-assisted positioning mode (c) that the UE sends measurements to the network and therefore it is the only mode that needs a supervision mechanism. A short summary follows:

- in the standalone positioning mode (a), the UE itself does the computation of location estimate. WLAN measurements around the UE are not sent from UE to the network.

- in the UE-based positioning mode (b), it is again the UE that itself does the computation of location estimate. Difference from the standalone positioning mode being that the UE uses assistance data from the network. Nevertheless, WLAN measurements around the UE are not sent from UE to the network.

- in the UE-assisted positioning mode (c), the UE optionally gets assistance data from network and the network does the computation of location estimate. WLAN measurements around the UE are sent from UE to the network.

### 6.3.2 Solution details

For the positioning modes requiring the UE to send WLAN measurements to the network (i.e., UE-assisted), the following applies:

(1) The network should provide "WLAN supervision data" to UE. This WLAN supervision data shall contain a list of WLAN AP data that are to be measured by UE. Each WLAN AP data shall contain the basic service set identifier (BSSID) information and/or the service set identifier (SSID) information. See details below for the values of BSSID and SSID.

(2) If the UE gets the WLAN supervision data from the network, the UE shall send only those WLAN measurements to the network whose BSSIDs and/or SSIDs match the ones indicated in the provided WLAN supervision data.

(3) If the UE does not get the WLAN supervision data from the network, the UE shall send only those WLAN measurements to the network whose BSSIDs and/or SSIDs match the ones in "reference WLAN supervision data". This reference WLAN supervision data shall contain "reference BSSID" information and "reference SSID" information. See details below for their values.

The BSSID/SSID information and the reference BSSID/SSID information may be values, e.g., defined by 3GPP, or based on MCC, MNC, realm, or any PLMN specific identifiers. They could also be patterns instead of exact values, e.g., MCC\*. They could also be values, e.g., provided by network dynamically to UE as broadcast information or in other protocol messages like RRC, NAS, or LPP. It also means that the reference WLAN supervision data could be static or dynamic.

### 6.3.3 Evaluation

This solution enables the network to control the collection of WLAN measurements from UE. When used, the solution makes it possible for the network to avoid collecting unintended WLAN measurements around the UE.

It should be noted that whilst it is easy to broadcast spoofed WLAN identifiers, it is relatively difficult to block WLAN identifiers being transmitted in the same location. Therefore, any solution that only listens for specific WLAN identifiers may be easier to get spoofed than solutions that listen to all WLAN identifiers in a specific location.

For WLAN based positioning in general, it should be noted that because WLAN identifiers can be spoofed, there is low confidence in collected data.

## 6.4 Solution #4: Enhanced privacy control in LCS

### 6.4.1 Introduction

This solution addresses following key issues:

1) Key issue #4: Privacy control in LCS.

In LCS, the UDM provides the UE privacy setting to GMLC and NEF.

The H-GMLC checks UE privacy profile settings prior to delivering a location estimate. The H-GMLC also checks UE privacy profile settings to verify if an LCS client is authorized for 5GC\_MT\_LR.

Further, the NEF uses the UE privacy settings to verify if AF is authorized for 5GC\_MT\_LR.

It is also allowed that an authorized AF provisions the UE privacy setting for specific UE(s) via NEF. If the privacy setting provided by the UE and the AF conflict, NEF gives precedence to the one provided by UE.

Most of these existing mechanisms of privacy control in LCS work well when the entities are in same trust domain and are behaving as expected. What is missing is that there is no assurance that the privacy control is effective when trust domain between the entities vary, and when all the entities might not be behaving as expected.

The current solution caters that missing aspect. Further details are given below.

### 6.4.2 Solution details

The Figure 6.4.2-1 below shows an example of procedures and messages involved in LCS. In Step 7, if an indicator of privacy check related action indicates that the UE needs to either be notified or notified with privacy verification, a notification invoke message is sent to the target UE. In Step 8, the target UE notifies the UE user of the location request and, if privacy verification was requested, waits for the user to grant or withhold permission. The UE then returns a notification result to the AMF indicating whether permission is granted or denied for the current LCS request. See 3GPP TS 23.273 [6] for details.



Figure 6.4.2-1: 5GC-MT-LR Procedure for the commercial location services  
 (Figure 6.1.2-1 in TS 23.273 [6])

Steps 1-15 are in Figure 6.4.2-1 are described in TS 23.273 [6].

As described above, Figure 6.4.2-1's Step 7 and Step 8 are important procedure messages that enable the network to acquire verification from the UE's user, when required. However, there is no protocol level mechanism to ensure that those steps not simply skipped. In other words, Step 12 could happen without Step 7 and Step 8, meaning that the privacy control at Step 7 and Step 8 could be ineffective. To avoid such situation, this solution requires the following.

When the UE is transferring measurements related to LCS positioning to the network, the UE shall verify the privacy settings before transferring those measurements to the network.

In relation to Figure 6.4.2-1, it means that the UE shall perform privacy settings check during Step 12. The privacy settings check could for example be the following: whether positioning is allowed or disallowed by the UE (at that time), does the user of the UE need to be informed and asked for permission, whether other conditions are met, e.g., what type of positioning is being performed, etc.

If steps 7 and 8 are skipped and privacy settings check is performed during Step 12, for synchronization of the privacy settings between the UE and the network, the UE needs to notify the AMF whether positioning is permitted or denied for the current LCS request or other privacy settings (e.g. time for disallowing the subsequent LCS requests) if updated. Then the AMF needs to invoke the Nudm\_SDM\_Update service operation, in the same way as Step 9, to store the updated UE privacy settings into the UDM, which then stores the updated UE privacy settings into the UDR.

### 6.4.3 Evaluation

The privacy check performed during Step 12 is at least used for synchronization of the privacy settings between the UE and the network.

NOTE: The serving network is trusted with the location service.

Solution #4 is proposed based on the assumption that the existing mechanisms for privacy control may be ineffective when trust domain between the entities vary, therefore the entities in serving network might not behave as expected. However, if the serving network is trusted with the location service as detailed in the note above, the assumption supporting solution #4 does not stand, therefore solution#4 is not required.

The existing mechanisms of privacy control in TS 23.273 [6] work well when the involved entities all behave as expected.

# 7 Conclusions

## 7.1 General conclusions

This study concludes that:

- The location data is suitably protected by the NAS security mechanism. It is confidentiality protected if NAS confidentiality protection is enabled.

- The confidentiality protection of broadcast assistance data in R-16 reuses the confidentiality protection mechanism in R-15.Therefore no new confidentiality mechanisms to protect broadcast assistance data are required.

## 7.2 Conclusions on Key Issue #1

For the key issue #1 (security and privacy in Bluetooth positioning) described in clause 5.1, it is concluded that the solution #1 (supervised Bluetooth measurements from UEs) described in clause 6.1 will be taken as a basis for normative work.

## 7.3 Conclusions on Key Issue #2

For the key issue #2 (security and privacy in TBS positioning) described in clause 5.2, it is concluded that no new security and privacy mechanism will be introduced for TBS positioning, as motivated by solution #2 (solution for TBS measurements from UEs) described in clause 6.2.

## 7.4 Conclusions on Key Issue #3

For the key issue #3 (security and privacy in WLAN positioning) described in clause 5.3, it is concluded that the solution #3 (supervised WLAN measurements from UEs) described in clause 6.3 will be taken as a basis for normative work.

## 7.5 Conclusions on Key Issue #4

For the key issue #4 (privacy control in LCS) described in clause 5.4, it is concluded that privacy control mechanisms defined in TS 23.273 [6] clause 6.1.2 are sufficient and effective, hence no new privacy control mechanism is required for normative work.

Annex A:  
Change history

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Change history** | | | | | | | |
| **Date** | **Meeting** | **TDoc** | **CR** | **Rev** | **Cat** | **Subject/Comment** | **New version** |
| 2019-09 | SA#85 | SP-190698 |  |  |  | Presented for information and approval | 1.0.0 |
| 2019-09 | SA#85 | SP-190895 |  |  |  | Revised to introduced the right version of the spec` | 1.0.1 |
| 2019-09 | SA#85 |  |  |  |  | Change control version | 16.0.0 |
| 2019-10 |  |  |  |  |  | EditHelp review | 16.0.1 |